12-15-2017

Emotionally and Socially Aware Approaches to Understanding and Changing Users' Cybersecurity Behavior

Michael Fagan
University of Connecticut - Storrs, michael.fagan@uconn.edu

Emotionally and Socially Aware Approaches to Understanding and Changing Users' Cybersecurity Behavior

Michael Fagan, PhD

University of Connecticut, 2017

Abstract: Security is a priority to most, but studies show that users commonly fail to adopt recommended cybersecurity behavior. Researchers have looked to user factors for explanations of this gap, finding security and convenience to be common considerations, along with perceptions of risks and past experiences. Some have tried to alter user behavior, but are targeted at specific advice and focused on rational motivations to persuade users.

In this thesis, three expertly recommended cybersecurity advice (i.e., updating software regularly, using two-factor authentication, using a secure password manager) are deeply explored. These results inform the design of videos in a systematic study of novel cybersecurity interventions aimed at altering users' behavior around these advices. First, users' rational motivations around each, including social motivations are studied, and then each advice is studied with more in-depth instruments, including those that gathered users' emotions in the varying contexts, which can influence decision-making.

These studies found that those who do not follow expert recommendations commonly see the risks in their decision as lower than those who do follow. Additionally, users rarely make social considerations in these contexts. Finally, negative emotions are found to be prevalent across many specific cases. These emotions may influence and trigger perceptions of negative past experiences, which in-turn hinders adoption. With these leads, novel video-based interventions are developed that incorporate appeals which address social motivations and emotions around cybersecurity advice. Awareness, perceptions, emotions, and behavior were measured before, immediately, two weeks, and one month after an intervention was delivered aimed at altering their behavior around one of the three test advices. This study finds that the emotion-based techniques may have merit since the groups which saw videos that used this approach had the largest and most sustained increases on variables that measured awareness and perceptions of benefits, costs, and risks. Also, the data demonstrates the role social motivations may have in cybersecurity behavior, showing the importance of both of these alternative approaches in this field.

Emotionally and Socially Aware Approaches to Understanding and Changing Users' Cybersecurity Behavior

Michael Fagan

B.A., Vanderbilt University, **2011**

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2017

APPROVAL PAGE

Doctor of Philosophy Dissertation

Emotionally and Socially Aware Approaches to
Understanding and Changing Users' Cybersecurity Behavior

Presented by

Michael Fagan, B.A.

Major-Advisor

____

Mohammad M. H. Khan

Associate-Advisor

____

Steven Demurjian

Associate-Advisor

____

Ross Buck

University of Connecticut
2017

Acknowledgments: There are many individuals that I must note for their help along the way. First, my adviser Dr. Mohammad Maifi Hasan Khan has been an invaluable help through my Ph.D. studies and research. I thank him for consistently pushing me to do my best work, while also fostering a free and open academic environment. It was only through his guidance that I came upon the usable security research track that led to this document, a change for which I owe Dr. Khan much gratitude. When my Ph.D. career first began, my research was focused on the system level, but in the Summer of 2012, Dr. Khan introduced me to the burgeoning field of usability security, and user-minded cybersecurity in general. We never looked back and have produced the work that has culminated into this thesis.

I would also like to thank my thesis committee of Dr. Khan, Dr. Ross Buck, and Dr. Steve Demurjian for their time, comments, and help through my career and on this thesis in particular. Special thanks goes out to the colleagues that I have collaborated with over the years, including Dr. Yusuf Albayram, Dr. Emil Coman, Dr. Bing Wang, Dr. Michael Zuba, and Nhan Nguyen. This thesis was made possible by funding from the National Science Foundation and the U.S. Department of Education.[1]

Thank you to Rebecca Randazzo and all of the CSE Department office staff for their consistent availability and aid as I have navigated the University's sometimes Byzantine procedures and processes. Finally, a special thanks to my parents, brother, grandmother, and all friends and family for their continued support through my career. In particular, I am grateful for my wife Stephanie, who has been along for the ride as I have worked towards my Ph.D. I could not have made it without her constant, loving support.

[1] This material is based upon work supported by the National Science Foundation under Grant Nos. CNS-1343766 and CNS-1251962. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation. I was also partially funded as a student by the Department of Education's GAANN Fellowship Nos. P200A130153 and P200A100141.

Credits: This thesis incorporates research results appearing in the following publications:

[31] This joint work with M. Khan appears in the Proceedings of *SOUPS '16*. This work is included in Sections 3.2 - 3.4.

[30] This joint work with Y. Albayram, M. Khan, and R. Buck appears in the journal *Human-centric Computing and Information Sciences*. This work is included in Sections 4.2 - 4.4.

[33] This joint work with M. Khan and R. Buck appears in the journal *Computers in Human Behavior*. This work is included in Sections 6.2 - 6.3.

[32] This joint work with M. Khan and N. Nguyen appears in the journal *Human-centric Computing and Information Sciences*. This work is included in Section 6.4.1.

[13] This joint work with R. Buck, M. Khan, and E. Coman appears in the *International Journal of Human–Computer Interaction*. This work is included in Section 6.4.2.

Table of Contents

Figures

Tables

1 Introduction

The Internet has only increased in pervasiveness over the years. Today, the Internet-of-Things has the potential to massively increase the utility of the tools and appliances we use every day, but the expansion of Internet connectivity to more devices presents a security challenge. In addition to the number of devices connected to the Internet, the size of the Internet using population is expected to grow in the coming years as multiple organizations work to expand the network's reach to currently underserved and "dark" parts of the globe [7,39,70]. As with devices, more users also means a new set of cybersecurity problems. These combined trends have the potential to increase the pervasiveness and scale of threats such as phishing attacks, hacking or take-over of accounts, and development of botnets, just to name a few.

Fortunately, many tools and techniques have been developed and deployed that can help users protect themselves, with new ones being developed to combat emerging threats. Unfortunately, studies have found wide divergence in what experts and non-experts do and think is safe online, following in the wake of earlier work that showed experts and non-experts harbored different mental models related to computer security [17,51]. Though it is easy to explain the divergence in behavior and perception as a result of knowledge gaps, researchers have increasingly begun to question this hypothesis, and instead look towards other reasons users could have to ignore good advice, including usability issues with particular behaviors/tools [25,40,56,59,63,66,67,96,99] and other rationally-based[2] concerns [20,46,47]. Expanding on this understanding of users' cybersecurity behavior, this thesis gathers data related to other influences on decisions that have not been as extensively studied in the field of computer science. In

[2] In this thesis, "rational" is used to describe concerns and motivations that are based around explicit and direct costs, benefits, and risks. More detail on this model of human decision-making is provided in 2.1.

particular, we use theory related to emotion's role in decision-making and an understanding of the power of social motivations to explore and alter users' cybersecurity perceptions and behaviors. First, the core research questions and the general approach used throughout the thesis are explained in Section 1.1. Section 1.2 outlines the specific work discussed in later Chapters.

1.1 Research Questions and General Approach

This thesis expands on prior work that has explored users' motivations and behavior around the plethora of cybersecurity advice available to them to secure their data and accounts. The existing literature has focused on individualized, rational frameworks to analyze how general users think about expertly recommended tools and techniques such as secure password managers, two-factor authentication, and regularly applying software updates, to name a few. Based on existing theories of human motivation in the areas of emotions [10,14,16,35,53,54,62,64,98] and social motivations [9,11,27,49,91,95,101,102,106], this thesis explores these aspects of motivation to more effectively understand and change users perceptions and behavior around cybersecurity decisions. To execute these approaches, though, the current state of users' emotions, perceptions, and experiences must be explored and considered. Overall, the work presented here approaches the following core research questions:

RQ1: How are the user factors that influence behavior around different cybersecurity decisions similar and different?

- What can we learn from these context specific concerns?

RQ2: What differences in opinions and perceptions are there between those who adopt and fail to adopt various cybersecurity advices?

RQ3: How does emotional context vary between different decisions?

- How do emotions relate to behavioral outcome?

RQ4: How are social considerations involved in personal security decisions?

RQ5: Would appeals that address emotions or social motivations be effective in changing perspectives and/or behavior?

These questions provide a framework to guide a series of investigations into users' motivation around cybersecurity advice that is recommended by experts chosen based on recent work surveying cybersecurity experts [51]. Three advices were selected as test cases to provide grounded contexts in which to investigate and experiment: applying software updates, activating two-factor authentication, and using a secure password manager. As suggested by RQs 1-4, a series of studies were performed to investigate the contours of Internet users' perceptions and behavior around the three test advice, including experiments that measure previously neglected components of motivation (i.e., emotions and social motivations). These informational studies build upon each other and paint a detailed picture of the perceptions and reasons that lead individuals to follow and not follow each advice. Towards RQ5, the final experiment not only tests the impact of videos incorporating content that is developed using the lessons about perceptions and motivations from prior work, but also explores the applicability of novel methods of altering cybersecurity motivations.

These results have value to the field in several notable ways. First, they can inform experts in how users think about specific security advice and cybersecurity in general. With this expanded knowledge, security experts may tailor their recommendations to take into account fuller models of user motivations. Next, researchers can use these results as they devise new security techniques, allowing them to incorporate better alignment with users' emotional and social motivations. Finally, software developers and others involved with end-product creation and distribution can use the results to these questions to better assess the quality of user-interface and security options included in their products by considering how users' may respond and interact with them on a deeper level than is currently used. This group may also find value in these results when thinking how to encourage adoption of more secure products and features.

1.2 Summary of Work Presented

To give the foundations of the work presented in the subsequent Chapters, Chapter 2 presents a survey of pertinent prior work that was used in the execution of the studies contained in this thesis. Notably, related studies in the field of usable security are discussed, along with the perspectives about cybersecurity decision-making that they put forward. A model for understanding how humans process messages aimed at altering their behavior is also explained. Another behavioral model is introduced that explains how emotions can impact decisions. Finally, the foundations of social motivations are discussed, along with the intersections of this topic with emotions and usable security. These starting points were used to design and execute a series of informational studies that gathered data about individuals' perceptions and motivations around select cybersecurity advice.

First, in Chapter 3, we present a study that looked to the rational side of users' considerations through a web-survey delivered to Mechanical Turk participants (N = 215) [31]. We start with rational motivations since this is a foundational part of decision-making, and has been the frame of numerous prior works in usable security. To expand on the literature, which all focus on specific advice in their designs, participants in this study were grouped by reported behavior on each of 3 advices: to update, to use a password manager, and to use 2-factor authentication. Participants in each group of followers and non-followers were asked to rate the individual and social costs, benefits, and risks of following and not following their group's target advice. Ratings mostly agreed with existing decisions. For example, those who reported updating generally rated the risks avoided and benefits of their decision as higher than those who reported not updating. Participants also provided open-ended responses explaining their decision, which revealed the common considerations of security and convenience, but also highlighted the differences in motivations between groups and advice. Overall, these comments lacked indications of social motivations, and ratings of social variables were all significantly lower than ratings for individual variables, suggesting social motivations currently play a small or no part in these decisions.

Though much was learned from the analysis of users' rational motivations, as work in psychology and communications has argued, emotions can play a role in decision-making [10,14,16,35,53,54,62,64,98]. Thus, several informative studies were also performed that explored users' behaviors, motivations, and novelly emotions in each of the three cybersecurity contexts targeted in the first study. Chapter 4 presents a work where samples of users (N = 136) and non-users (N = 111) of secure password managers were collected from Mechanical Turk [30]. Each group was sent the same survey asking about computer and cybersecurity experience, as well as experience with, perceptions of, and emotions when using a password manager[3]. In terms of computer and cybersecurity experience, both groups responded similarly. When it came to opinions and perceptions of password managers, the differences were much more significant. Comments explain why participants chose to use or not use a password manager and ratings of anticipated emotions when using the tool reveal more differences between the groups, including differences in opinion on how password managers affect the balance of security and convenience.

Though the results related to password managers provided valuable information about what users think of one kind of security advice, not all behaviors are the same, and some require repeated effort that is not as immediately beneficial as using a password manager. In Chapter 5,

[3] Note, non-users were asked to rate emotions they *predicted* they would feel if they used a password manager. In the case of both users and non-users, participants rate the same concept (*predicted* emotions when using a password manager), but do so with different previous experience with the tool.

two-factor authentication is used as a case study of such a behavior. Examination of a sample of 2FA users' opinions and emotions about the feature (N = 148) revealed differences in subgroups of users based on their perceptions of convenience of the feature, including stark differences in the emotion ratings from each subgroup. Analysis of the small number of participants who reported knowing 2FA, but not using it (N = 22) also highlights the importance of perceptions of convenience and past negative experiences on motivations to adopt the feature. Finally, differences between those who knew of 2FA, regardless of their behavior (N = 170) and those who did not know the feature (N = 125) revealed large gaps in users' self-assessment of cybersecurity knowledge, awareness, and access to good advice, possibly explaining why they had not heard of or did not recognize the fairly common feature.

For another perspective on emotions in cybersecurity, Chapter 6 contains an examination of users' history with, opinions of, and emotions related to software updates and update messages. Results for 2 surveys (N1 = 78, N2 = 172) showed that participants are commonly hesitant to apply updates [33]. Annoyance and confusion were cited by participants as common complaints about update messages they have encountered. Additionally, for some software, annoyance and confusion ratings correlated with participants' rated hesitation in applying updates. In the second sample (N = 172), after responding to the survey, participants viewed update and warning messages sampled from different systems and software [32]. The survey asked them to rate each of the messages on 4 emotional metrics: annoyance, confusion, importance, and noticeability. Ratings for annoyance and confusions were correlated, as were noticeability and importance, suggesting a link in the resonance of these pairs of emotions. Additionally, through analysis of the ratings in connection with design features of the messages, some "good" and "bad" aspects were identified. Open-ended responses from participants about what they liked and disliked about each message highlighted several trends in participants' opinions of the messages, including relationships between content of comments and emotion ratings. Finally, a third and more targeted study of emotions (N = 400) was performed on MTurk. The results show that users associate emotions with updates in ways that vary on four key emotional factors: positivity, anxiety, loneliness, and hostility related to update messages [13].

Chapter 7 presents the final study (N = 327) of this thesis, which involved the development of videos that aimed to change users' minds about a specific cybersecurity decision they have made using the lessons from the prior chapters, as well as clues from the literature. For each of the three advices targeted throughout this thesis, three videos were created (i.e., a total of 9 unique videos were tested). An initial video was created for each that presented the basic motivations to adopt the advice, as learned from the findings of prior studies. Using these "basic" videos as a starting point, two additional interventions were also developed for each advice. One highlighted the emotions users may feel around each advice, and explained why the possible negative ones are made up for by the positives when adhering. The other experimental video highlighted social motivations to adopt each advice by explaining how the decision to not follow puts people the user may know at risk. These videos were assessed using a survey that measured awareness, perceptions, emotions, and behavior, and the results show that the emotion-based motivational concepts may have merit in these contexts since the video which incorporated it seemed to show the most consistent increases in perceptions further away from the intervention. This shows possible lasting power of emotion-based appeals. Additionally, the results of this final study show possible power in social motivations, though in an unexpected way.

Chapter 8 concludes the thesis by summarizing the answers gathered related to the research questions, as well as outlining the specific contributions contained in this thesis. Finally, the final section discusses directions for future work on the topic of understand and changing users' motivations, perceptions, and behaviors around various cybersecurity advice.

2 Background on Human Motivation

This thesis draws on several existing tracks of research in the fields of computer science, psychology, and communications. First, Section 2.1 presents a survey of usable security studies that have centered on rational factors of users' behavior around cybersecurity, such as benefits, costs, and risk. Since the goal of this thesis is to design interventions, a model to understand human processing of messages is also presented. Next, in Section 2.2, the theorized connection between emotions and motivations is explained; with focus on how understanding emotions can help when trying to impact perceptions and influence positive behavior change. Finally, Section 2.3 discusses the theory of social motivations is, along with their application to cybersecurity, followed by a summary of this Chapter in Section 2.4.

2.1 Decision-making and Persuasive Communication

The role of the user in cybersecurity has been realized for some time, including the need to design with them in mind, informed by analysis of what motivates the diverse population that uses computing devices [3,29,41,77,85]. Though new technology can help increase security, as Forget, Chiasson, and Biddle remarked in a 2012 assessment of the learnability of a new authentication scheme, the ability for users to learn a new tool or technique is pivotal to their ability to adopt [37]. Beyond learnability, other users factors have been recognized as important towards security, including users' awareness and attitudes [22,34,36,38,43,44,61,71,86,92,103], their mental models [2,6,17,55,97], past experiences [28,66,96], and social influences [23,24]. Many of these and other works have incorporated key pillars of psychological theory in their application [50,58]. A common thread is the foundational view of users' decisions as rational, with them efficiently balancing known costs and benefits of action versus inaction.

2.1.1 Rational Components of Decision-Making around Cybersecurity

Human decision making is a complex mechanism encompassing a multitude of considerations. One broad way to view human decisions is as a balance of costs and benefits, where humans are rational actors who choose to minimize cost and/or maximize benefit. This view of computer security decision-making has been prominent. Herley in 2009 suggests that users' failure to adhere to good security behavior could be attributed to them finding the costs too high and/or benefits too low [46]. He supports this supposition by citing the low chance of an actual security breach for any given user and the high cost of daily security maintenance. Herley goes on to suggest that more data is needed to determine the actual costs and benefits of these decisions to better inform the advice experts give. By 2014, Herley had found the approach of researchers had not changed much [47], leading him to say in an article that year:

> It is easy to fall into the trap of thinking that if we can find the right words of slogan we can convince people to spend more time on security. … We argue that this view is profoundly in error. It presupposes that users are wrong about the cost-benefit tradeoff of security measures, when the bulk of the evidence suggests the opposite.

In short, what Herley argues is that rather than users being ill-informed about security, they could just be making a perfectly rational decision, at least in their eyes. This view is echoed by a 2012 work, "Death by a Thousand Facts." Here, Stewart and Lacey suggest that approaches to changing perceptions and behavior that utilize traditional, "security-awareness" content have and will continue to fail because, unlike it is assumed by some researchers, users are not ignorant about good security behavior [20]. More recent work also furthers this argument. In 2016, Forget et al., using a mixed methodological design, found that simple user engagement (i.e., how aware the user was of cybersecurity and how much they reported caring about it) was not a strong predictor of good security outcomes for users [36]. This indicates that merely encouraging users to get engaged and pay attention to their security may not be enough to alter their behavior in meaningful ways. For instance, this study found that knowledge gaps may play a role in lack of good security behavior, with the example of users having browser extensions installed that they did not fully understand, and some not knowing basic terminology such as "web browser" [36]. With these knowledge gaps, it could be that users' cost-benefit analyses are off due to fundamental misunderstandings around cybersecurity.

More evidence for this is found in the case for applying software updates. Wash et al. found that a significant portion of sampled Windows 7 users did not understand what updates were changing in their system and could not execute their intentions for computer management [99]. In 2016, these results were supported by Mathur et al.'s work that found users commonly lacked sufficient information to decide whether or not to apply software updates [67]. In 2017, this time in a work by Vitale et al., results of user experiences around operating system updates identified confusion and unclear mental models of changes being made by an update, calling back to the results of Wash et al. [97]. In addition to this deficiency in understanding how updates impact their system, Vaniea et al.'s study of updating behavior also suggests prior negative past experience could play a large role in users deciding not to apply updates [96]. A 2017 study by Mathur and Chetty repeated these results, finding that users who do not activate auto-updating on software likely have past negative experiences with software updating [66]. In all, these results suggest that users may be underestimating the risks of not applying updates due to lack of knowledge about how updates help them, and may be inflating the risks of applying an update due to one-time negative past experiences.

The balance of costs and benefits has also been seen in studies of user behavior around other cybersecurity tools and techniques. Two-factor authentication can increase the security of accounts where the feature is activated, but as Krol et al. found in 2015, costs of the technique in terms of added mental and physical effort presents barriers to adoption [59]. An earlier study by Gunson et al. in 2010 around 2FA in automated telephone banking also found that users consider the added security of the technique, but also the decreased usability [40]. A broader study of 2FA published in 2013 by De Cristofaro et al. used both interviews and a survey distributed through MTurk to assess 3 types of 2FA (i.e., one-time passwords generated by a security token, one-time passwords received via SMS, and one-time passwords generated by a dedicated smartphone app) [25]. In addition to finding ease of use and the amount of required effort being a core concern around 2FA, trustworthiness of the method also came up, showing that users are considering many kinds of costs around cybersecurity behavior.

Though costs and benefits are rational decision-making components that we all intuitively assess when faced with an option, humans have bounded rationality and must assess these components *to the best of their ability*, given limited information and cognitive capacity [88]. The results of prior work in usable security showing significant knowledge gaps between groups of users around cybersecurity [36,67,99] suggests that knowledge may alter perceptions of the costs and benefits of these decisions. Thus, it is possible experts and those who adhere to expert advice see the costs and/or benefits of adhering to good security behavior *differently* than those who do not follow such advice. Supportively, prior work has found divergence in mental models [17] and behavior of experts relative to non-experts. Notably, Ion et al.'s 2015 survey of experts and non-experts found that the suggestions experts had to stay safe online (e.g., update frequently, use 2FA) were vastly different than what average users thought was important to do (e.g., use anti-virus, only visit websites you know) [51]. Though these results may imply that knowledge is key in cybersecurity motivations since it seems average users might not know how to stay safe, other factors are also involved in these perceptions that may run deeper than simply how much a user knows. Recent work has shown stark differences in perceptions and behaviors of users from different countries [41,85], indicating that users may vary in behavior for demographic reasons, such as local custom and culture. Part of these differences could be attributed not only to how different individuals see costs and benefits, but also other pertinent aspects of these decisions.

Falling well in line with this conceptualization of security behavior, the literature also shows us that risk perception can be quite impactful. Howe's 2012 review of work towards understanding human psychology in the context of security identified security risks and risk perceptions as a key consideration for researchers [50]. Numerous studies into various aspects of usable security since have also looked to risk, including those that have investigated mental models [2,6,17,55,97], perceptions [38,44], and awareness of users [43,61,71]. Recent work, such as Kraus et al.'s 2016 work has demonstrated that the desire for security, which is related to risk, has power towards cybersecurity motivations [58].

Specific studies of adoption of particular secure behaviors have also found risk to be involved. A 2010 study of password manager usability published by Karole, Saxena, and Christin showed that when comparing three forms of password manager (i.e., online, phone-based, and USB-based), users opted for the phone manager, partly due to their discomfort in giving password control to an online entity [56]. This highlights how users sometimes worry about the risks in adopting actions that are recommended by experts. These worries may not be unfounded, though, since researchers have noted the possible risks in some password managers [63]. Thus, since good security behavior is always changing, users have to be informed by experts in novel ways to keep them up to date on how to stay safe.

Multiple methods have been attempted to inform users and encourage good behavior. In 2010, Albrechtsen and Hovden explored the use of small-group, activity based sessions towards impacting cybersecurity perceptions and behavior [5]. In these sessions, among other tasks, participants discussed various security scenarios involving risks to information and data. These interventions were found to significantly improve reported adoption of some secure behaviors, such as locking computers when they step away, as well as many aspects of awareness, such as responsibility and perceived skill [5]. More recently, in 2015, Larson assessed the impact a cybersecurity fair has on security perceptions [61]. Here, booths were set up that were aimed at teaching users about the risks to various systems and software, as well as ways to stay safe. Cybersecurity awareness scores before and after the fair were not significantly different, but the researcher identified that confusion due to the format of the fair and some of the content presented may have contributed to this lack of change in scores [61]. Using a more direct and issue-tailored intervention method, more success has been found by other studies, such as Harbach's 2014 work that leveraged personal information to highlight the effect of Android permissions on user's data [42]. This was meant to alter their perception of the risks associated with each permission, hopefully making them better realize what is at stake. The study found that users made more privacy-conscious decisions when presented with such information at app installation. Finally, in 2017, Albayram, Khan, and Fagan's study of video-based interventions towards encouraging the adoption of two-factor authentication (2FA) had a strong risk component in its analysis, finding that a thematic focus on risk made videos more interesting, informative, and useful, while those who saw the risk theme were also more willing to try 2FA [4]. Following all these prior works, the studies in this thesis prominently incorporate analysis of users' risk perceptions around cybersecurity behavior.

As the background work presented has shown, the task of altering behavior is one that depends on many factors to be successful. Organized models are needed to best understand how cybersecurity related messages (i.e., software update and warning messages, cybersecurity interventions) are received by users. We will use one particular model of communication that had been shown useful in decoding why a message may fail if the desired behavior change is not achieved.

2.1.2 Communication-Human Information Processing (C-HIP) Model

When humans are delivered a message, there are several conditions that must be met if the message or warning is to be successful at changing perceptions and/or altering behavior. Multiple studies in this thesis are grounded using a communication human-information processing model that lays out how information is processed by individuals and demonstrates the places where there may be an issue with the message or delivery that results in non-compliance [21]. Figure 2-1(a) shows a visual representation of the C-HIP model.

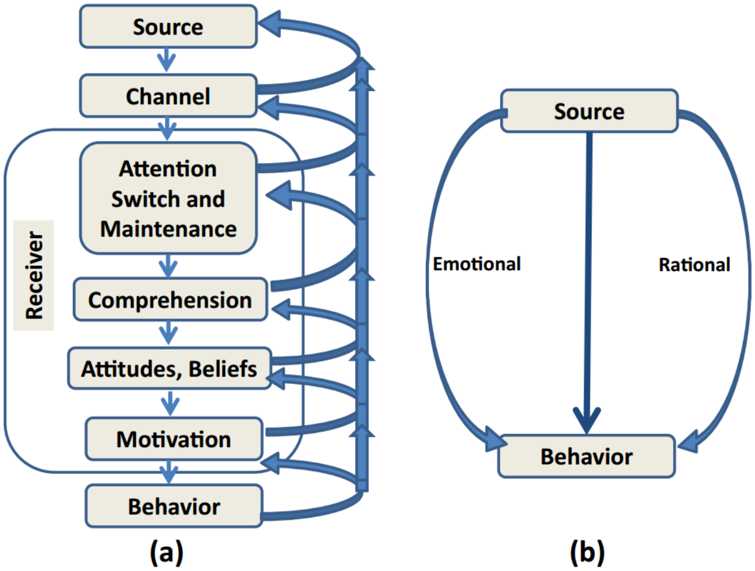


Figure 2-1: Visual representations of the (a) Communication-Human Information Processing model and (b) Affect-Reason Involvement model.

In the model, sources use channels in an attempt to elicit behaviors from receivers. When a message is sent through a channel, it is processed, according to the model, in several stages by the receiver, all of which can feed back to prior stages. First, the receiver must be paying attention to the channel to properly receive the message. For example, in the context of an update, this means the user has to see the update message if they are to be motivated to apply it. Next, the receiver must understand the message and comprehend what they are being told. If understood, the message's content and delivery must align with the receiver's attitudes and beliefs. This is a somewhat broad, but important stage. It is here that social motivations, emotions, values, and other deep-seated considerations can play a part in decision-making based on a delivered message. Finally, the message must properly inform a user how to utilize the provided information and motivate them to act.

This model is aimed at understanding how humans process a message and where the processing can go awry [107,110]. It has been used in the foundational design of all of the studies presented, even those which did not directly involve messaging. In particular, attitudes and beliefs are believed to play a key role in the efficacy of messages aimed at altering behavior, suggesting that the influences of this stage may impact decision-making generally, not just in response to direct messaging. Thus, understanding attitudes and beliefs about cybersecurity advice can help illuminate the complexities of users' motivations. Additionally, since a core goal of this thesis is study how to alter users' perceptions and behaviors through direct intervention, the experiments in Chapters 3-6 examine users' attitudes and beliefs about cybersecurity advice to understand how messages can be designed that are informed by the status quo, but also aim to alter perceptions in the minds of users.

The C-HIP model provides a grounding to guide this thesis' investigations into users' motivations and design of interventions to alter them, but expansion of "attitudes and beliefs" to identify specific components beyond the traditional rational perspective is needed to best approach the research questions. In particular, this thesis builds on two prior tracks that have not been studied previously in the context of usable security extensively.

2.2 Emotions and Motivations

The prior section presented the predominant method of understanding cybersecurity motivations, and is the grounding for numerous studies in the field of usable security, but emotion has gained increasing prominence in the understanding of how messages can be best communicated to individuals. The source and nature of emotions have been examined by researchers [15,16,45,73,74,100]. Emotions have also been studied for their theorized interaction with other constructs, such as societal behavior [10] and decision-making [53,62,64,14]. Simply, emotions are understood to manifest in individuals due to signals sent from the brain. Emotions can be labeled and categorized in many ways, but the most basic is by valance, which refers to whether the emotion makes the individual feel good or bad. An emotion that is "good" is said to have positive valence, while a "bad" emotion has negative valence.

Studies have found that the communication of good behavior also needs to consider emotions as they can impact decisions individuals make, particularly in charged and stressed situations [35,53,64]. Therefore, a pillar of this thesis' design and approach is the emotions users may feel in the context of cybersecurity decisions. Though the scope of research into emotions is very broad, this thesis draws on two theories in particular. First, the impact of emotions on behavior is formalized using the Affect-Reason-Involvement (ARI) model. Second, prosocial emotions are considered, as they may possess particular power towards influencing behavior.

2.2.1 Affect-Reason Involvement (ARI) Model

The Affect-Reason-Involvement (ARI) model argues that behaviors are motivations by one of three routes: rational, affective (emotional), or some combination [14]. A visual representation of the model can be seen in Figure 2-1(b).

Rational appeals are those that address the logical and logistical reasons an individual should change behavior. For example, common arguments individuals hear regarding the need to eat healthy and exercise is that doing so will improve one's overall health and longevity. This reasoning relies on informing individuals of the impact of their behavior and how changing can benefit them. Rational appeals are a dominant form of persuasion in our society from a public policy standpoint. Campaigns in various public policy fields, such as around the consumption of tobacco and alcohol, [8,106,108,109] have relied on rational and fear-based appeals to impact change among the population. Though the success of these campaigns, in some cases, cannot be denied, it can be argued that relying solely on rational perspectives puts public policy at a disadvantage relative to other sources of motivation individuals may have.

Emotional appeals differ from these rational appeals in a key way. Rather than concerning what an individual has to gain from a behavior change, these involve how the individual may feel, in terms of emotions around the behavior. This includes emotions that they may feel when considering a change in their behavior. For example, though speaking up in a meeting may help one in one's career, the not so uncommon fear of public speaking may overpower this rational reasoning. Of course, the emotions we feel are not this limited, and so emotional appeals may also address the feelings one may have at other stages of the decision or behavior. For example, some who do not quit smoking, despite decades of informational campaigns regarding the dangers and costs of the habit, may cite emotions of anxiety and frustration felt after quitting as their reasons for not trying to quit smoking (or failing to quit) [18]. In this case, the anticipated emotions the individual expects to feel, either from direct experience or from feedback from others who've made the same decision hinders their adoption of a rationally better-for-them behavior.

The power of emotions has been known for some time and harnessed before, notably by advertisers. The cliché "sex sells" relates to this knowledge, but the power of emotion in advertising is not limited to those of sexual desire. For quite some time, savvy businesses have harnessed the emotions we feel to influence our decisions to buy products and services. On the surface, this can be an appeal to how one would feel when consuming the product or service. For example, the slogan, "I'm lovin' it," from McDonalds, tries to convince the consumer that the food from the restaurant is flavorful and satisfying through the emotions evoked by the thought of love. Since emotions are involuntary and not fully understood in their manifestations, emotional appeals can also take more subtle forms. For example, a large number of corporations utilize blue in their logos (e.g., IBM, Chase Bank, Boeing, Ford Motors, AT&T, Amtrak several airlines), which has been shown to be associated with confidence, success, and reliability when used in this context [82]. Thus, intentionally or not, these corporations use colors that positively impact consumers' opinions of their brand through the emotional responses to the colors they see.

As indicated in the Figure 2-1, both of these vectors to motivate a behavior, according to the ARI model can be at work at the same time. This combined vector is most influential towards behavior since both the logical and subconscious reasons an individual may have are at play, and may work in a complimentary way. When thinking of how to use these vectors in an intervention, it is important to consider how context may frame the decision. Not only can the rational considerations of various behaviors be different, but the emotions involved may also vary

2.2.2 Prosocial Emotions

Emotions can impact us to act in ways that are more or less socially preferred. Essentially, when an emotion elicits socially preferred actions, they are categorized as prosocial [52]. For example, when two friends are bickering, one may scold the other for starting the fight in the first place, which causes feelings of guilt in the other. These feelings of guilt are considered prosocial since the subject is being motivated away from a behavior (i.e., whatever started the fight) by their friend instilling the emotion in them. Example negative prosocial emotions are embarrassment, shame, and as we saw, guilt. Please note that negative, in the context of prosocial emotions, refers to the valence of the emotions (i.e., whether the emotions makes one feel good/positive or bad/negative) and not the direction of the motivation. In all cases for prosocial emotions, the subject is being motivated *towards* socially positive behavior.

A positive prosocial emotion could be respect or trust. The literature on prosocial emotions shows that they develop in childhood and are impactful on behavior from several societal levels [76]. Cybersecurity behavior can also be interpreted through this lens. For example, some studies have shown that users cite bad past experiences with software updates as a reason for them to avoid future patches [96]. It could be that the past negative experiences eroded users' trust in the updates, thus reducing the prosocial emotions they felt to apply subsequent updates.

Though prosocial emotions are important to behavior, they have not been studied much in the context of cybersecurity in prior work. Thus, this thesis takes on prosocial emotions, along with emotions in general, as a core component to the studies presented in the proceeding

Chapters. Motivations that involve other people are not limited to feelings of prosocial emotions, and they may manifest in more direct and rational ways than through feelings. Social motivations have been studied and discussed broadly in the literature.

2.3 Social Motivations

It has been argued that when a social value is involved in the decision being made, social dynamics are much stronger than any external manipulations in effect through incentives or disincentives [95]. For example, if a decision involves one's moral convictions or social identity, then that can greatly impact the outcome of the decision. Volunteering and donating to charity are some actions which have more apparent social motivations to them since they involve directly helping others for little or no direct benefit to the actor, but decisions that do directly benefit the individual may also have social motivations behind them.

Actions to protect one's safety, for example, commonly involve the safety of others, and can therefore be partly socially motivated as well. This adds a new dynamic to the decision and behavior models we have discussed to this point. Social motivations fit inside the structure of rational decision-making; doing good onto others helps convince them to do good onto us. In fact, some argue that social motivations are merely a *kind* of individual motivation. That is, they argue, people engage in socially positive behavior because they want to get something from other people. This idea is debated in the literature [95], but for the purposes of this thesis, the difference is moot. Social motivations, whether they are truly distinct or not, are a discrete motivation that is an influence on the behavior of humans [9,11,27,49,91,95,101,105], and so have value in helping our understanding of users' motivations around cybersecurity.

In the frame of social motivations, some cybersecurity experts could be prone to secure behavior because for them a breach of security means an embarrassment of their social identity as an expert, while an average user would suffer no such status loss if they experienced a comparable attack, leading them to less secure behavior. It could also be that experts are more cognizant of social impacts of decisions. Thus, like with many decisions, it is possible to see social sides to what users do or do not do to protect their data and security. It may also be possible to better convince users to adopt expert advice through more targeted interventions that incorporate social cues. The use of social motivations has been studied [49], and was found to be impactful when used in interventions targeted at employees dealing with interpersonal office conflicts [91] and at-risk students in the school environment [104]. Researchers in usable security have also looked to social motivations to help understand and alter users' behavior.

2.3.1 Social Motivations in Cybersecurity Behavior

The use and study of social motivations around behaviors that involve cybersecurity is not new, but prior work in this field is limited. Das et al.'s 2014 work hinted to possible power in social motivations, finding that social persuasion was reported as a source of security behavior and advice [23]. A recent related work by Redmiles, Malone, and Mazurek further found that these sources of advice are commonly judged based on not only the sources' trustworthiness, but also base their assessment of the content of the advice itself, such as if the advice seems biased by marketing or may pose a risk to privacy [81].

Though social sources may be a place users go to for advice, how this advice is received depends on many factors, and, as a follow-up study by Das et al. found, leveraging social motivation to impact behavior change may be difficult [24]. Here, announcements on Facebook that did and did not incorporated social cues were used to encourage secure behavior, but found no significant difference in effectiveness of messages between those that has these social cues and those that did not [24]. These mixed results in the literature come in the wake of strong arguments made by some scientists as to the power and importance of social motivations in decision-making [9,11,27,49,91,95,101,105]. Notably, this prior attempt to harness social motivations relied on observability of users' decision by others. Though this observability argument has been shown to influence behavior in other game-based studies [87], it's possible that it may not be appropriate for the context of cybersecurity behavior. Therefore, social motivations constitute the final pillar of this thesis as it sets out to better understand the impact and influence of these vital components to behavior.

2.4 Summary

To expand on the current literature on applying emotional and social approaches towards increasing adoption of good cybersecurity behavior, this thesis presents several reports of original research that are influenced by and follow on the prior work discussed in this Chapter. In subsequent Chapters, a rational framework is used to understand motivations, as is the case in numerous prior studies of usable security and user behavior, but new lenses are also used to view users' motivations and behavior.

In particular, the studies expand on prior work through investigation of the emotions users report feeling around sample cases of good security behavior, like updating, using two-factor authentication, and using a secure password manager. Other studies incorporate an indirect or direct social component that offers additional clues towards how social motivations may interplay with motivations around these decisions. Exploring these aspects allows us to support prior work, while also generating new insights as to why users do what they do.

3 Understanding Users' Motivations from a Rational Perspective

A majority of research into cybersecurity, usable security, and users' decision-making has focused on a rational perspective of their decisions. In most cases, it is assumed that users make their decisions based on a balance of costs, benefits, and many times, risks. Prior work has taken this frame and used it to study actions around updating [66,67,96,99], password management [89,92], use of password managers [56,63], as well as adoption of these behaviors more generally [46,47,86], but in all these cases, the investigations were limited in scope to individual behaviors or concepts of cybersecurity very broadly.

Thus, in this Chapter a study is presented which takes the lead from the literature and specifically investigates the rational components of users' motivations around several cybersecurity behaviors. This is a novel investigation for the field that also helps inform the interventions that will be studied in a later Chapter. This Chapter begins with Section 3.1, which describes the design of the study, including how these rational components and clues from prior work are incorporated into this design. The results of this study support arguments in the literature [20,36,46,47] that motivating users to take up good cybersecurity behavior requires more than informational-based campaigns and/or improved engagement, and provide the initial foundation towards the paramount goal of designing interventions that aim to increase adoption of cybersecurity advice. Specifically, in Section 3.2, we see how specific perception gaps around risks and costs may play a role in users' motivation to follow the tested advice. Section 3.3 presents users' motivations, in their own words, using qualitative data collected for this study. Here, the balance of security and convenience is prominent, as is the importance of past experience towards current behavior. Section 3.4 discusses how social motivation, though applicable in the contexts tested, are not very prominent in our data. The results of this study are discussed related to prior work in Section 3.5. Finally, the Chapter is summarized in Section 3.6.

3.1 Experimental Approach

A rational decision framework (i.e., benefit/cost/risk) was used to design the quantitative instruments for this study, but social motivations were also added to the structure. This was inspired by the prominent track of literature arguing for and demonstrating the potential of attention to social considerations [9,11,23,27,49,91,95,101,106]. Additionally, these perceptions of individual and social costs, benefits, and risks all tie into users' attitudes and beliefs about the advice tested. As we know from the C-HIP model [21], any messaging aimed to increase adoption of these advices, such as those tested in a later Chapter, must conform with and/or manage users' attitudes and beliefs about each to be successful.

To execute this study, an initial screening sample was collected from Amazon's Mechanical Turk (MTurk) that asked basic demographic questions and if participants followed the 3 target pieces of advice:

- Keeping your software up to date
- Using a password manager
- Using two-factor authentication

This survey was advertised on the MTurk service to users who resided in the United States and were 18 years of age or older. An information sheet explained the study and participants who agreed to move forward where then delivered the screening survey. Upon completion of the survey, these participants were compensated $0.25.

Two groups were formed for each advice where all participants in one group reported following the advice, while the other group reported not following. All groups, across all advices contained 50 unique participants whom were contacted with the follow-up survey. One group (those who did not update) only had 48 eligible participants in the entire screening sample, so only this number of participants was contacted for follow-up. These groups were contacted with another web-survey through MTurk that first asked in an open-ended format why the participant chose to make the decision they did as per the group they were assigned. Next, participants were asked to rate on a 4-point Likert scale how much benefit, cost, and risk they feel they get from their decision to follow or not follow their groups' target advice and how much they think they would be benefited, cost, and put at risk if they changed their behavior and made the opposite decision. In addition to these individual phrasings (i.e., how much the decisions benefit/cost/out at risk the participant), we also asked how much the participants felt users of other computers are benefited, cost, or put at risk by their decision or would be by the opposite, thus incorporating the social aspects of the considerations the participants are making. Each respondent was compensated $4 for their complete response to this survey. Not all fifty participants contacted for each group responded, but final sample sizes were in the range of 30-41 participants for each group.[4] The format of all survey instruments from this study, and the basic demographics of all samples can be found in Appendix A.

The data collected from these follow-up participants was analyzed for clues into why some follow and others do not follow the advice tested in this study. Quantitative data was tested using Mann-Whitney U-Tests [65] to compare the differences in ratings for each variable

[4] Update: Follow = 39; Not Follow = 30
2FA: Follow = 36; Not Follow = 31
Pass. Manager: Follow = 41; Not Follow = 38

collected from those who reported following and those who reported not following, within each advice. The qualitative data was coded using a Grounded Theory approach [90]. The codebook was developed by the author, initially populated with deductive codes selected based on the study design and pertinent literature prior to data collection. These codes focused on broad concepts like "avoid risk" or "increase security" since context specific codes would be best developed inductively, while working with the data. A total of seven deductive codes were developed.

After data was collected, a random sample of one third of all comments from each group was gathered. These samples were then used to develop inductive codes that focused on more specific concerns extracted from user comments. Some examples of codes developed though inductive coding are "I don't want to" and "increase financial security," showing the range of reasons given by participants. Since the kinds of reasons varied from group to group and advice to advice, many codes did not apply across all comments, but some did. For example, "Low/no risk/Don't care if hacked" was applied to comments across multiple advices. A total of 32 inductive codes were created for all groups and included in the updated codebook.

These codes (deductive + inductive) were used as the codebook by a researcher other than the developer of the codebook, who was less involved in the study and its design. Through coding, additional codes were developed *in-vivo* by this other researcher and included in the final codebook used to interpret all qualitative data. In all, an additional twenty-four *in-vivo* codes were created.

The motivations of the sampled users around the tested advice can be best interpreted from the data collected from them through the mixed methods procedures employed in the study. First we will look to the quantitative data to see the most significant differences between those who follow each advice and those who do not (please note, the complete results of statistical testing, on all instruments in this Chapter, can be found in Appendix A). Next, the qualitative data will be used to give more depth to the motivations revealed by the quantitative analysis. Finally, a particular feature of both the quantitative and qualitative data is highlighted: the lack of social motivation.

3.2 Perception Gaps between Followers and Non-Followers

The most apparent result in the quantitative data overall was the propensity for participants to rate the costs, benefits, and risks of each decision as favoring their reported behavior. For example, for all advice, participants in the group that followed the advice rated the benefits to them of doing so as significantly higher than the groups who did not follow they thought they would experience if they changed ($p < 0.001$). The reverse was the case as well; those who did not follow each advice rated the benefits they got from this decision as higher than the groups who followed each projected they would get if they did not ($p \leq 0.002$). It is natural that individuals would see benefits in their decision, regardless of what it is, since individuals are prone to stick with their current behavior when faced with a decision to change that involves uncertainty. Known as status quo bias, studies have shown that individuals are prone to these rationalizations generally [84], as well as in the context of IT systems [57]. Instead, we must look beyond benefits to learn more about what motivates some and not others to adopt secure actions.

3.2.1 Risks Related to Following and Not Following

Analysis of participants' risk ratings showed similar results as seen for benefits. For all advice, those who followed rated the risks of not following as significantly higher than those who reported not following each (*p* ≤ *0.003*). For the risks to others of not following, moderately significant (*p* ≤ *0.044*) differences were found for 2FA and strongly significant (*p* ≤ *0.002*) differences were found between followers and non-followers for the other two advice (i.e., updating and using a password manager). This shows that users who end up following these advices may see risk in their prior behavior that other users do not. Since the risks of not following each of these advices are demonstrable, this finding is a strong lead on how to communicate with users in the hopes of having them take up these behaviors. It's possible that an intervention which incorporates a carefully toned discussion of the risks of not adopting good security behavior may be effective at changing users' perceptions and actions around such decisions.

Interestingly, only one advice had a significant difference on the risk of following between those who follow and did not follow: using a password manager. For the risk to the user of following, as Figure 3-1 shows, those who report not using a password manager see significantly more risk than those who report using the tool (*p* < *0.001*).

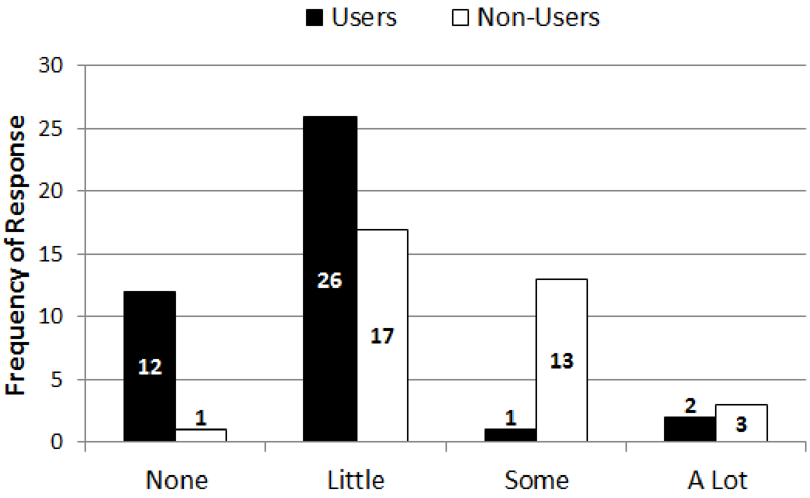


Figure 3-1: Response distribution of ratings from users and non-users of password managers for the risks of using the tool. Pass. Man. Yes = Participants who use a password manager, Pass. Man. No = Participants who do not use a password manager.

The pattern seen in Figure 3-1 highlights the importance of properly communicating all the benefits of a cybersecurity tool, especially those which bear a reputation for insecurity like password managers. Since many non-users rate the risk in adopting the tool as much higher than users, and since it is known that experts recommend the use of a secure password manager, increasing knowledge around this particular aspect for this tool may help encourage more to adopt. Naturally, this approach is context specific to password managers, and it may not carry for other advice. Nonetheless, this demonstrates the importance of considering cybersecurity behavior as a whole as well as around individual advices. As was the case for risks, other costs may vary in the eyes of average users between different behaviors they can adopt.

3.2.2 Costs of Not Following

The final component of the rational decision framework used to structure this study was cost of following and not following each of the advices tested. The most informative result here is on the costs of not following each advice. For the individual costs of not following, all groups that followed provided significantly higher ratings than those who reported not following ($p \leq 0.003$), except for using 2FA, where the differences were not significant.[5] Thus, for all advice except 2FA, it could be that those who follow feel they would lose something if they did not adhere.

For updating and using a password manager, the costs to users of other computers by the participants not following were also significantly higher when rated by those who followed compared to those who do not ($p \leq 0.001$). This shows possible social motivations related to

[5] It should be noted here that the followers and non-followers for 2FA did test significantly different in their ratings of the risks of not using 2FA, so this lack of significance in cost of not following does not represent a similarity in thinking between followers and non-followers about the dangers of not activating 2FA.

these advices, though subsequent analysis presented in this Chapter will call into question the strength of these social motivations.

3.3 Users' Motivations, in their Own Words

Despite the data showing an undeniable gap between those who follow each advice and those who do not when it comes to how they rate the benefits, costs, and risks of their decisions, to best understand specific motivations, which can further inform our approach to interventions, we turn to the qualitative data collected. Through coding of the comment given by each participant where they explain the reasons for their decision in their own words, several patterns were found. First, as we have seen in the analysis of prior studies presented in Chapter 2, there are several context specific concerns in the comments when looking from advice to advice. Despite these context differences, strong common trends did emerge as well, providing more valuable insight into user motivations.

3.3.1 Security and Convenience

Security, convenience, and the balancing of the two were apparent in numerous responses. Almost all those who reported using a password manager (37 of 41) mentioned the added convenience as a reason for them doing so, while just over half of comments from the same group mention security benefits as part of the motivation (22 of 41). For other advice, security was the top reason for users to adopt, such as comments gathered from those who use 2FA (31 of 36). A smaller portion of those who reported updating said security was a reason why than for these other two advice (19 of 39).

Looking to those who do not follow each advice, security and convenience continued to play large roles in participants' rated motivations around their decisions. Seventeen of the 38 of those who do not use a password manager report security as their reason for not using the tool. Convenience was more important to non-followers across other groups, being cited in comments from 15 of the 31 2FA non-users and 7 of the 30 of those who do not update regularly.

In all, these results demonstrate the important balance users are striking between security and convenience when considering following these and similar advice. Interventions would be wise to consider this in the specific context being targeted since the subject's perceptions, attitudes, and beliefs around the advice may have to be addressed before any change can be expected. In this case, that may mean, for example, interventions that encourage users to use 2FA by acknowledging the inconvenience of using the tool that some users see and countering with the importance of the added security of this setting. Other appeals should be adapted as appropriate for each context to maximize impact.

Though security vs. convenience proved a strong trend in the qualitative data, comments were not limited to this dynamic. The number of codes added *in-vivo* demonstrates the diversity in responses from participants, but one in particular is notable in its relation to prior work.

3.3.2 Power of Past Experiences

For some of the advices tested, users mention their past experiences as a reason for their decision one way or the other. For example, 7 of the 31 of those who do not use 2FA mentioned not doing so because they did not see any risk in that action. Even more, 8 from this group said their decision was driven by a confidence in current approach. Half of the 38 who do not use a password manager mention this same reason. These comments may reflect a lack of negative experience related to these participants' current, insecure behavior. If and when these negative experiences are had, these participants' minds may be changed, as could be reflected by comments from security-minded participants in groups that follow each advice. Additionally, 3 of 30 participants in the group that reported not updating said their decision was driven by a past negative experience with a software update. Prior work has found this a common reason users avoid updates [96].

Though security was a top reason given by those who adhered to the advices tested, past experience was not directly cited in any comments as reasons for the decision *to* update. On the flip side, *negative* past experiences were mentioned by some non-updaters, as predicted by prior work [28,96]. In addition some comments reflected a lack of negative past experiences by expressing confidence in techniques known to be insecure. It can also be argued that those who adhere to some advices and cite convenience as their reason for doing so are acting out of positive past experiences of convenience. Together, these trends show the overall power of past experiences in shaping current decisions and motivations around cybersecurity. Harnessing these experiences can be a way to promote adoption of these behaviors, either by addressing the negative experiences some may have had, or more effectively warning users of risks due to current actions. For example, those who do not update can be reminded that in doing so, even though they are avoiding a possible inconvenience, they are also introducing a security risk that may result in much more inconvenience if compromised. Included in this inconvenience is a possible risk to other computer users since a compromised machine could be used in an attack on others (e.g., as a member of a network of compromised machines executing a distributed denial of service attack [94]). As the final trend in the data will show, participants across advice did not pay much mind to this risk, or any social considerations.

3.4 Social Motivations to (Not) Follow Cybersecurity Advice

Despite the existence of risks to others by not updating, a small number overall mentioned any kind of social motivation in their reasoning. Of all comments, less than 10% of the 215 received were coded as social. It should be noted, though, that all were from those who adhered to their group's advice, falling in line with work demonstrating the power of social motivations towards moderating behavior, as presented in Chapter 2.

To better see this possible deficit in social motivations overall, for each variable (e.g., *Benefits of Following*, *Risk of Not Following*), the ratings for that variable across all advice were averaged and plotted in Figure 3-2, which shows that individual phrasings, garnered a higher average rating than social phrasings. This suggests that individual considerations are stronger than social in the tested cases.

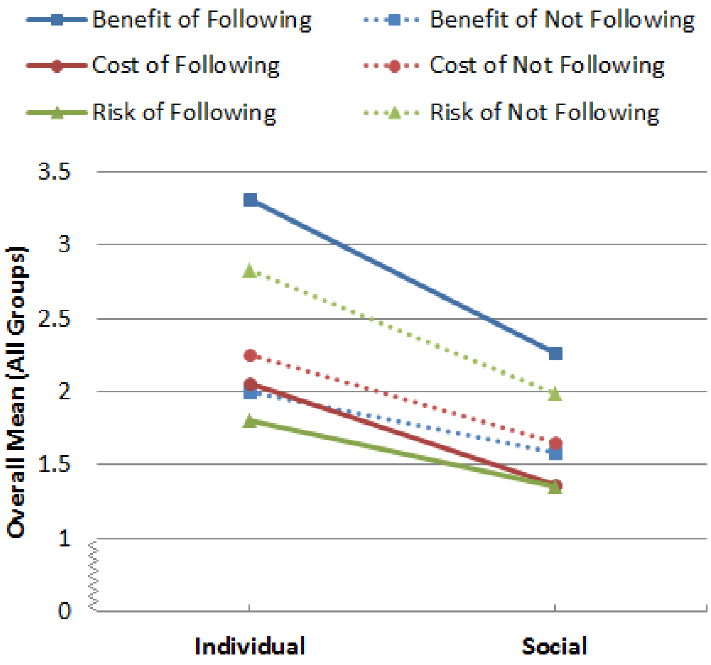


Figure 3-2: Plot of average ratings for each rational component showing the difference between Individual and Social ratings for benefits, costs, and risks.

Further testing of the data confirmed this interpretation. For all variables, the results of a Sign Test [26], which compared individual and social ratings to determine which is more likely to be rated higher yielded a p-value < 0.001, showing individual ratings were consistently rated higher than social. Thinking to the literature [9,11,23,27,49,91,95,101,106], this deficit in social motivation may help explain users' lack of adoption of cybersecurity tools and techniques. The desire to protect and help others can be a powerful regulator of action, but for the cybersecurity advice tested here, no such consideration of others exists. If the deficit can be reduced through intervention (e.g., by highlighting how cybersecurity actions can affect other computer users), more users may take up better behavior as suggested by experts.

3.5 Discussion

Rational concerns among users are common in the literature, and many of our results echo prior findings. For each advice, the reasons given by users in our study were similar to those reasons explored in other studies. Password managers, for example, were found to suffer from some fear among non-users of the tool that adopting could pose a security risk. This similar sentiment was seen in the results of Karole et al.'s analysis of password manager usability, where participants steered aware from online password managers like those asked about in our study due to concerns about the tool's security [56]. Negative past experiences, which have been found in multiple prior studies to be hindrances to individuals applying software updates [66,96], were also found in the data for this Chapter around updating. Additionally, a confidence in current approach, which could reflect a lack of negative past experiences related to their current behavior, was a reason given by some non-users of 2FA and password managers. Two-factor authentication was also noted as being inconvenient by non-users, but secure by users, which is similar to finds from Gunson's 2011 study of 2FA [40].

In many cases, these responses seemed to follow the rational framework of balancing costs and benefits that Herley has called for in exploring users' motivations [46,47]. Chief benefits and costs, in the case of cybersecurity advice, are convenience and security. The results in this Chapter show how users balance these two aspects in sometimes counter-intuitive ways, such as the security concerns mentioned around using a password manager. These results follow the many studies that have shown and theorized such a balancing among users [46,86,92,103]. Understanding the power of this dynamic is important towards learning how to change perceptions and behaviors, especially in light of the quantitative data presented in this Chapter. As the C-HIP model explains, messages aimed at changing behavior must conform to the receiver's attitudes and beliefs, which currently differ between users and non-users of all the advice tested according to these results. Since experts are likely to be adherents to an advice when recommending it [51], they must consider that those they are trying to convince probably see the costs and benefits involved differently.

One finding from prior work, the power of social motivations [23,95], was not found in this data. According to the ratings of costs, benefits, and risks, individual concerns seem to dwarf social considerations made by most users. The qualitative comments also generally lacked mentions of social considerations. It's possible that increasing the instances of these social considerations in the minds of users can make them more apt to adopt good behavior since psychologists have shown the power of social motivations [49,91,104]. Care must be taken, though, to avoid the traps of relying solely on informational and awareness based approaches in these interventions, as some have questioned the efficacy of this in the context of cybersecurity decisions [20,36,46,47]. Addressing components of motivation not studied here, such as emotions, will provide greater insight into how users think about these decisions.

3.6 Summary

In this initial study into users' motivation, we learn much about why some decide to follow and not follow a range of cybersecurity advice. As expected, perception gaps exist between adopters and non-adopters, but these gaps varied between advices. Qualitative data identified two trends that will come up in future Chapters. First, security and convenience are commonly balanced by users in their decisions. Second, past experiences can play a role in how users behave. These issues are all possibly addressed through directed interventions that take the existence of these concerns into account.

This study's data also offered another possible clue towards users' non-compliance with these and similar advices: social motivations are seemingly lower for these contexts. These motivations apply in all these cybersecurity contexts since the compromise of one machine or account on the network puts others at risk in many ways. Since the power of social motivations has been argued in other contexts [23,95], increasing how socially users thinking about these decisions may help encourage more of them to take up good behavior.

4 Emotions and Cybersecurity Behavior: Case Study in Password Manager Adoption

The results of the study discussed in the prior Chapter revealed multiple reasons users may have for the decisions they make, but as some argue [10,14,16,35,53,54,62,64,98], non-rational factors like emotions can also impact motivations. Thus, understanding the emotions users feel in the contexts of the advices explored in Chapter 3 will best inform researchers about how and why they make the decisions they do and help design videos that use emotionally informed approaches in a later Chapter. Emotions around these advices will be investigated through in-depth case studies since the prior work on this subject is limited.

The details of the present study into password managers are described in Section 4.1. In the next section, 4.2, we will see how users and non-users of the tool differ in their knowledge, opinions, and conceptions of password managers. In Section 4.3, we will see how feelings of convenience can play a large role in this particular context, offering a lesson as to how these benefits may be used in conjunction with security-focused appeals to more effectively influence individuals towards adopting good behavior. In-depth data collected about emotions around password managers is presented in Section 4.4, and reveals the concerns about security some individuals feel around the tool, despite expert recommendation. This clue points to the importance of proper communication to effectively explain to users the functions and security of these kinds of tools towards cybersecurity. The results of this study are discussed in relation to prior work in the usable security field in Section 4.5, followed by Section 4.6, which closes this Chapter.

4.1 Experimental Approach

In this study, two groups of participants were collected from Mechanical Turk (MTurk) using a single survey that automatically grouped participants based on their response to a screening question. One group was comprised of password manager users (N = 137) and the other of those who reported not using a password manager (N = 111). A survey was developed that asked about the participants' opinions of and experiences with password managers, based on prior work [89]. These instruments were presented as statements which the participant could agree with on a 5-point Likert scale. Statements were arranged in grids to allow participants to answer them quickly and efficiently.

In addition to the grid-based statements, participants were also asked to rate on a 5-point Likert scale how much they would feel each of 45 emotions when using a password manager. These instruments were developed using prior studies of emotional hierarchies [15,74] and scales [45,100]:

- One might feel CONFIDENT (e.g., because one is protected from possible danger).
- One might feel CONFUSED (e.g., because one does not expect how hard or easy the password manager is to use).
- One might feel AFRAID (e.g., because one's time is being used by the password manager).
- One might feel RESPECTFUL (e.g. because the system has given one tools to respond).
- One might feel SCORNFUL (e.g., because the danger is easily countered).
- One might feel POWERFUL (e.g., because one knows of danger and is taking precautions).

Finally, participants were asked in an open-ended format “Why do you choose (not) to use a password manager,” phrased appropriately for their reported use of password managers. All survey instruments used can be found in Appendix B.

This survey was distributed on MTurk and was available to users 18 years or older living in the United States. Participants viewed the study information sheet and, if they agreed to take part in the study, were then shown the grid of general cybersecurity perception statements, and finally asked to report whether they used a password manager or not. Each group was then asked the qualitative instrument and shown the password manager specific grid statements, followed by the in-depth emotions instruments. All participants were compensated $1 for their complete response to the survey. Basic demographics were also gathered from respondents and are presented in Appendix B.

By looking at the differences on the grid-based questions and qualitative reasons for behavior, more detail will be gathered related to users’ attitudes and beliefs about using a password manager. According to the C-HIP model [21], understanding these attitudes and beliefs is imperative towards design of messaging aimed at turning non-users into users. Relatedly, this study also gathers in-depth data about users’ emotions around using password managers. Though we know much about rational reasons users may have around using a password manager from the investigation in the last Chapter and in prior work, the ARI model and theory of emotion more generally predict that emotions may also play a role [10,14,16,35,53,54,62,64,98].

4.2 Users vs. Non-Users

The first goal of this study's analysis is to compare differences between users and non-users of password managers to help understand why they made the decisions they did. The value of comparing these two sub-populations lies in their juxtaposition in behavior, despite similarities in several other ways. In the previous Chapter, by examining the broad differences in perceptions of benefits, costs, and risks between followers and non-followers of sampled advice, many insights were gained, but as the qualitative data showed, considerations varied between different advices. Thus, we must look closely at differences between users and non-users of password managers on aspects to their decision that were not targeted specifically in the last Chapter's study.

4.2.1 Differences in Knowledge and Opinions

The first set of grid-based instruments can be seen in Table 4-1, which focused on participants' knowledge/opinions of and experience with security generally. Differences between each sample's response distributions are compared using a Mann-Whitney U-Test [65].

	Users	**Non-Users**	**U-Test**	
Statement	Mean (Med.)	Mean (Med.)	*U*	Sig.
I am doing a good job of protecting my computer security.	4.05 (4)	3.77 (4)	6241	0.005
I could do more to protect my accounts.	3.56 (4)	3.68 (4)	7352.5	0.628
I do not have time to pay attention to security.	1.96 (2)	2.09 (2)	7030.5	0.266
I do not feel my accounts are likely to be hacked.	3.23 (3)	3.15 (3)	7100	0.472
I do not know where to get computer security advice.	1.83 (2)	2.08 (2)	6603	0.084
I am knowledgeable about computer security.	3.91 (4)	3.64 (4)	6469	0.031
I care about computer security.	4.16 (4)	4.19 (4)	7297	0.625
I trust my computer.	3.66 (4)	3.72 (4)	7315.5	0.58

Table 4-1: Average and median rating of agreement with each general statement about computers and cybersecurity on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree" from users and non-users of password managers, along with the results of Mann-Whitney U-Tests comparing the distributions for each group.

Other than how good a job they say they are doing at protecting their computer security and their knowledge of computer security, ratings for these statements were not significantly different between groups, suggesting the sets of users are mostly similar other than their behavior around password managers. It is particularly interesting that there was no difference found on the statement “I could do more to protect my accounts,” since using a password manager is meant to further protect accounts. It could be that non-users take other steps that they feel brings them an equal amount of protection as users feel they get from password managers, but it could also be that non-users do not see a need for the added security given by password managers.

The significantly higher rating users aggregately gave in their assessment of how good of a job they think they were doing in protecting their computer security relative to non-users is notable, especially considering the strength of the significance ($p = 0.005$). This difference could possibly be an impact of users of the tool experiencing the security benefits first hand, thus being more likely to give a higher rating here than non-users. Since users also gave moderately higher ($p = 0.031$) ratings of their knowledge of computer security relative to non-users, it could be that the users sampled simply better understand computer security, and thus know they are doing a better job than non-users at protecting it.

It’s also somewhat notable that the differences in rating distribution for both groups were marginally significant ($p = 0.084$) for responses to the statement “I do not know where to get computer security advice.” Normally, significance this low would not be considered in the analysis, but given the other statements of significance, this result may give more insight. By the means seen in Table 4-1, non-users had a slightly higher mean for this rating, representing a higher magnitude agreement with the statement. If some non-users do not know where to get cybersecurity advice, this may explain their lower ratings of their overall computer security knowledge and confidence in security, as observed. Thus, for these users, interventions could be effective at altering their perceptions and behavior around using a password manager since such interventions can help increase their knowledge of security and provide them a good source for computer security advice.

4.2.2 Different Conceptions of the Tool

To understand further the differences between users and non-users, the second set of grid-based instruments asked about the tool in particular. The statements and statistics for responses from both groups can be seen in Table 4-2.

	Users	**Non-Users**	**U-Test**	
Statement	Mean (Med.)	Mean (Med.)	*U*	Sig.
I trust password managers.	3.77 (4)	3.05 (3)	4422.5	<0.001
Password managers are more secure.	3.58 (4)	2.98 (3)	5125	<0.001
Password managers help people.	4.28 (4)	3.85 (4)	5231.5	<0.001
Password managers are easy to use.	4.19 (4)	3.87 (4)	5742	<0.001
Password managers are more convenient.	4.16 (4)	3.84 (4)	5966	0.002
I understand the theory behind password managers.	4.14 (4)	3.89 (4)	6606.5	0.053
I understand why password managers are secure.	3.78 (4)	3.05 (3)	4580	<0.001
I worry that accessing my accounts may be more difficult with a password manager.	2.31 (2)	2.69 (2)	6063.5	0.004

Table 4-2: Average and median rating of agreement with each statement about password managers on a scale of 1 = “Strongly disagree” to 5 = “Strongly agree” from users and non-users of password managers, along with the results of Mann-Whitney U-Tests comparing the distributions for each group.

These statements produced more significant differences between users and non-users. Users agreed more with trusting password managers, finding them secure, helpful, easy to use, and convenient ($p \leq 0.002$). In addition, users agreed more with the statement “I understand why password managers are secure,” ($p < 0.001$) a possible clue as to why non-users have not adopted; they may not see the same benefits. Overall, these differences show that users have a much better view of the tool than non-users, particularly in areas such as trust, which are related to emotions and are important towards adoption.

Interestingly, non-users rated their agreement with the statement "I worry that accessing my accounts may be more difficult with a password manager," significantly higher than users (*p = 0.004*). This provides another clue as to why some choose to use the tool while others do not. It could be that some portion of non-users worries that the tool will be a detriment to their device use. This highlights the importance of usability towards security. If computer scientists desire adoption of security improving tools and techniques, it is unquestionably imperative for these solutions to be usable to individuals of average knowledge of computer science, as these results demonstrate. As seen in prior work and the last Chapter, negative past experiences are commonly cited by those who do not follow cybersecurity advice, so even small flaws in usability can have far reaching consequence due to the primacy that users seem to give their convenience. In addition, this highlights the avoidance of even perceived inconvenience that is not necessarily related to direct past experiences as a motivator of user's cybersecurity behavior.

4.3 Power of Convenience

Further exploration of the differences between users and non-users focused on the responses they provided explaining why each group of participants made the decision they did around using a password manager. Inductive coding was used to extract information from responses. The codebook was developed through sampling comments and having multiple researchers develop codes for their sample. These individual codebooks were then merged and the unified codebook, which contained a total of 19 codes, was used to code all comments. After coding, codes were conceptually merged to discover trends in the reasons given for using or not using a password manager. Table 4-3 below shows the summary of these trends and sample comments from the data.

	Reason	Count	Sample Response
Users	Convenience	49 (80.0%)	"It's convenient and easy to use."
	Security	15 (24.59%)	"It makes my password use more secure."
	Other	1 (1.6%)	"Work related purposes."
Non-Users	Security Concerns	51 (49.94%)	"I feel they aren't secure."
	Lack of Need	47 (42.34%)	"I can remember my passwords without the use of one."
	Lack of Time/Motivation	12 (10.81%)	"It's sometimes a hassle and I'm in a hurry."
	Inconvenience and Usability Concerns	10 (9.0%)	"It seems inconvenient."

Table 4-3: Counts of comments from users and non-users of password managers explaining their behavior that was assigned each code indicated.

For users, their reasons for using a password manager revolved mostly around the added convenience of the tool. Some also mentioned the security they felt they got from using a password manager, but this number was dwarfed by convenience. Most user participants mentioned convenience in their comments, showing the power this can have in motivating the adoption of a new technology. For non-users, security concerns about the safety of password managers and a lack of need for the tool were the chief reasons given for not using it. This highlights the constant balance of security and convenience, and how some are occasionally skeptical of convenience due to the possible security risks inherent in it. Also, some participants cited a lack of time or motivation to use the tool, which is interesting considering the added convenience many users report. It's possible that some of these non-users may be turned into users if these benefits were effectively communicated.

Repeating some of the findings from the prior Chapter, the data for this study showed participants' motivations generally revolved around the convenience they get from using the tool and, as is the case for non-users, concerns about security. As seen in Table 4-3, a relatively small portion of sampled users citied security in their comment compared to the number who mentioned convenience. These shows how benefits other than security can be very powerful at encouraging users to adopt secure tools and techniques. Developers should take note of this in the design of future security products to help encourage the adoption of this software, as recommended by experts. Additionally, in the design of interventions aiming to persuade subjects to adopt good security behavior, it would be pertinent to leverage and highlight any of these non-security benefits secure behavior may have as they may be powerful in leading more to be convinced by the appeal. Finally, there may be additional emotions users associate with password managers beyond security (or lack thereof) and convenience.

4.4 How Users *Feel* About Secure Password Managers

In addition to the previous quantitative and qualitative data, participants were also asked to rate the degree to which they anticipate they would feel each of 45 emotions when using a password manager. Mann-Whitney U-Tests were used to compare the distributions of ratings for each emotion given by users and non-users. When looking to the emotion ratings given by participants, there are some significant differences in the ratings given by users and non-users, as seen in Table 4-4.

	Users	**Non-Users**	**U-Test**	
Emotion	Mean (Med.)	Mean (Med.)	*U*	Sig.
Secure	3.80 (4)	3.50 (4)	6148	0.01
Energetic	2.58 (3)	2.21 (2)	6111	0.01
Admiring	2.66 (3)	2.32 (2)	6305	0.017
Suspicious	2.39 (2)	2.80 (3)	5788	0.01

Table 4-4: Average and median rating of the strength participants say they would feel each emotion when using a password managers on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree" from users and non-users of password managers, along with the results of Mann-Whitney U-Tests comparing the distributions for each group.

Though users rated feeling more secure, energetic, and admiring than non-users rated they would feel when using a password manager, non-users rated they would feel significantly more suspicious. As with the comments and trust ratings seen in prior sections, there seems to be a difference in opinion between the samples over the security of password managers. Also, these results suggest that users of password managers may be externally motivated to adopt the tool, as shown by their higher ratings for energetic and admiring, but these feelings could also be a result of them having experience with the tool and liking it.

	Users		**Non-Users**	
Rank	*Emotion*	Mean	*Emotion*	Mean
1	Secure	3.80	Secure	3.50
2	Confident	3.54	Confident	3.35
3	Trusting	3.49	Trusting	3.29
4	Happy	3.46	Happy	3.26
5	Grateful	3.42	Grateful	3.23
6	Cared-For	3.03	Powerful	2.83
7	Proud	3.00	Suspicious	2.80
8	Welcomed	2.97	Cared-For	2.77
9	Powerful	2.91	Proud	2.76
10	Triumphant	2.90	Welcomed	2.71

Table 4-5: The ten emotions that received the highest mean rating from password manager users and non-users.

Looking at the means of all emotions for both groups, a trend appears. As seen in Table 4-5, for both users and non-users, the emotions that received the first, second, third, fourth, and fifth highest mean ratings were the same. Secure was the only one of these that was significantly different between groups (as seen in Table 4-4). The other emotions, despite their high magnitude, were rated similarly between users and non-users, according to inference testing. Interestingly, secure was the highest rated emotion for both groups, showing that many non-users may acknowledge at least some of the security benefits of the tool, even if they do not feel motivated enough to adopt. Additionally, the rest of the top 10 emotions from each group by mean contained several of the same emotions, albeit in differing orders, with one notable addition for non-users: suspicious, which was the seventh highest rated emotion for this group. These combined results could reflect similar emotions associated with password managers between the groups, with key differences around security and suspicion that may be the hinge of behavior change. Addressing these limited emotional gaps between users and non-users may help turn more non-users around on their decision.

4.5 Discussion

These findings related to specific emotions around the use of password managers are novel for the field of usable security. Some prior studies have looked into the security of password managers [63], finding that there are some legitimate security concerns with some implementations of the tool. Our results possibly reflect this, with non-users rating suspicion much more highly than users of password managers did. Relatedly, a usability assessment of three types of password managers found that users opted for phone-based applications relative to online versions of password managers [56]. Again, this may be reflected in the higher suspicion rating from non-users in the current study.

Despite this focus on security for non-users, qualitative results for this study found that convenience, rather than security was a key reason users cite for adopting a password manager. Considering other advice people can adopt, such as updating software, these results contrast with the *inconvenience* non-updaters report as a reason to not want to update [66,67,96,97,99]. Inconvenience in using 2FA has also been noted in prior work [25,40,59]. Convenience continues to be a theme in users' considerations, even annoying those who are security conscious and knowledgeable. Since some security protocols, tools, and techniques require inconvenience to be traded for security, security researchers would be wise to take note of these results. They show, as prior work has argued [46,47], that users' decisions not to adopt cybersecurity advice, in some cases, boil down to avoiding *extra effort*.

4.6 Summary

The results of this Chapter further our understanding of users' perceptions and motivation around the adoption of password managers. Users of the tool like the convenience they get from it, sometimes without even thinking of the security. It's possible this added convenience may also put some users off since a good number of those who do not use the tool report worry about security. This thinking is bolstered by emotion analysis that shows that suspicion and security are among the emotions rated most differently between users and non-users. These security concerns are important to address in interventions to encourage password manager use, but the results of this Chapter can also inform motivations around cybersecurity advice more generally.

The balance of security and convenience, as seen in many studies [46,47,86,92,103], may also reflected in the emotion ratings seen in this study. In addition to suspicion and security, other positive emotions were also rated significantly differently between users and non-users, with users feeling more admiring and energetic than non-users. This divergence could be related to the commonly cited convenience enjoyed by users of the tool. Interventions that highlight this aspect of password managers to non-users may be effective for that context, but not all advice is the same. Exploring emotions around additional cybersecurity behavior will further inform our understanding of how they may interact with security decision-making more broadly.

5 Emotions and Cybersecurity Behavior: Case Study in 2-Factor Authentication

Though the added security is obvious to many experts, the results in Chapter 3 showed two-factor authentication (2FA) is also perceived as a high-cost way to preserve security that non-users worry is inconvenient. Unlike password managers, despite both protecting account security, 2FA requires semi-regular effort when logging in from new devices or when accessing accounts that require the regular use of feature. To best understand how these differences in context impact motivation around 2FA compared with other advice, this Chapter presents a study that investigated emotions individuals associate with 2FA.

Section 5.1 will present the design and execution of the study used to collect the data analyzed in this Chapter. These procedures resulted in a sample which was divided and analyzed as three sub-groups: users (N = 148), non-users who are aware of 2FA (N = 22), and those who had not heard of 2FA at all (N = 125). Though the prior Chapter focused on analyzing differences between users and non-users of password managers, the sample collected for this Chapter related to 2FA was more complex, with many reporting not having heard of the feature. For this reason, the analysis in this Chapter will divide the data differently to extract findings related to individuals' emotions around 2FA and how they may impact decisions to use the tool or not. In this vein, Section 5.2 discusses how even those with the same behavior around 2FA differed in their perceptions of the tool. Next, Section 5.3 explores the reasons non-users report for avoiding 2FA, along with a description of the emotions this group associates with the feature. Finally, a third group of general users, those who do not know 2FA, are investigated in Section 5.4. All of these results are discussed next to prior, related studies in Section 5.5. The Chapter is finally summarized in Section 5.6.

5.1 Experimental Approach

One survey was used on Mechanical Turk (MTurk) to collect 3 samples totaling 295 participants. The survey was advertised to users of the service who are 18 years or older and reside in the United States. First, the study's information sheet was shown to participants. If they agreed to continue and take part in the study, participants then responded to a grid that presented a series of statements about computers and cybersecurity that they were asked to agree with on a 5-point Likert scale (i.e., the same statements as used in the initial grid in the last Chapter's study). Then they were asked if they knew what two-factor authentication is, as well as if they currently use the feature. These instruments served as branching questions where those who said they knew 2FA were shown another grid of statements, this time about 2FA in particular, as well as instruments designed to gather participants' ratings of 45 emotions they may feel while using 2FA. These instruments asked about 45 distinct emotions and prompted participants to imagine they were using. Finally, those who know what 2FA was were also asked to report, in open-ended format, why they decided to follow or not follow the advice, as indicated by their responses to the earlier instruments. Those who reported not knowing 2FA were not shown additional instruments. All participants were compensated $1 each. All survey instruments as well as statistical summaries of basic demographic instruments are included in Appendix C.

Like with the last Chapter, the grid-based quantitative instruments, emotion instruments, and qualitative reasons for using or not using 2FA will help inform users' attitudes and beliefs around this particular advice, as defined in the C-HIP model [21]. Unlike the study presented in Chapter 3, more specific perceptions than basic cost, benefits, and risk can be assessed. In particular, we focus on emotions, which we have seen can be very informative to understand motivations overall. The findings from this study can help build informed interventions that aim to alter users' perceptions and behavior around 2FA by looking at how different users see the feature and how that may influence decisional outcome.

5.2 Same Behavior, Different Perceptions

In the previous Chapter, the differences between users and non-users of password managers were examined. In the case of using 2FA, though, relatively few of those who had heard of 2FA report having never used the feature compared to those who had never used a password manager. Statistical testing yielded no significant differences between the responses of users and non-users of 2FA on any of the study's survey instruments. This could show similar thinking among both groups, but the lack of results could also be related to the stark imbalance in sample size between users (N = 148) and non-users (N = 22).

To best understand users' considerations around the use 2FA, another breakpoint for the sample was selected. Non-users of the tool were removed so that only those who reported using 2FA were analyzed from this point. Next, the distribution of responses for each instrument was examined to find instruments that received divided responses from participants. In this process, most were found to be heavily skewed towards one end of the scale or the other, showing general agreement among all participants in their ratings on these instruments. Ratings for one statement, though, were found to be more evenly distributed across the possible responses. The response distribution for this statement is shown in Figure 5-1.

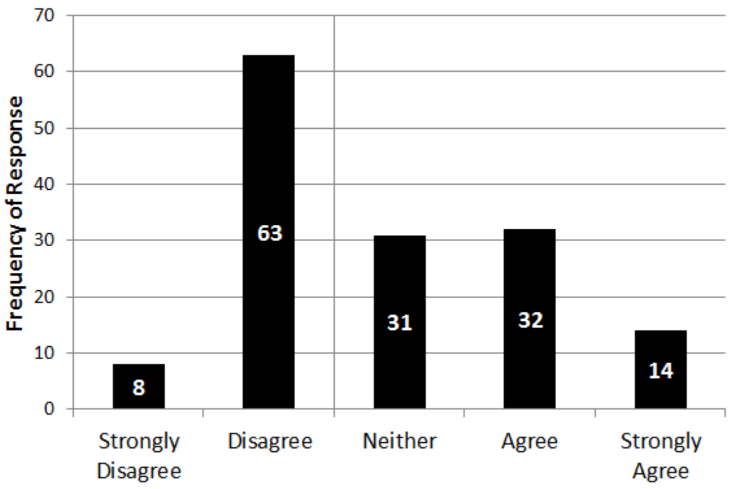


Figure 5-1: Distribution of agreement with the statement "two-factor authentication is more convenient," for those who reported using 2FA.

As seen in the figure, based on agreement ratings with the statement "two-factor authentication is more convenient," two, roughly even groups of users can be created. One of these groups all disagree or strongly disagree with the statement that 2FA is more convenient (N = 71), while the other are indifferent or agree with that statement (N = 77). This breakpoint also has contextual significance in that convenience is a core trade-off with security, and inconvenience, as seen in Chapters 3 and 4, and in prior work [46,47,86,92,103], is a common reason non-users of the feature have to not adopt. Thus, it is important to compare users that also think 2FA is inconvenient with users who do not hold this opinion. In doing so, we can best understand how users view 2FA more broadly to inform intervention approaches for this advice.

On statements about their history with computers and cybersecurity generally, there was no differences between these two groups, indicating similarities in their self-perceptions. On the set of statements about 2FA specifically, responses between the two groups were only different for one: "two-factor authentication is easy to use" ($U = 1608.5, p < 0.001$). This result is not surprising since perceptions of how easy the tool is to use are closely related to overall views on convenience. In fact, agreement with the statements "two-factor authentication is easy to use" and “two-factor authentication is more convenient,” were strongly correlated (*$r = 0.477, p < 0.001$*). Comparisons of the 45 emotion ratings yielded further significant results.

A total of 17 emotions had distributions test significantly different between those who rated disagreement with the statement “two-factor authentication is more convenient” and those who were indifferent or agreed with the statement, showing a large divergence in the emotions different groups of users feel about 2FA. As seen in Table 5-1, there was a mix of emotions that had different distributions, but across all, those who were indifferent or found 2FA to be more convenient rated the emotion higher than those who did not find 2FA more convenient. This is particularly interesting since differences spanned both positive and negative emotions, as well as those that are individualistic and prosocial, suggesting that the group who is indifferent or finds 2FA more convenient have generally stronger emotional reactions to using the tool.

	Not More Convenient	**Indifferent/More Convenient**	**U-Test**	
Emotion	Mean (Med.)	Mean (Med.)	*U*	Sig.
Friendly	2.28 (2)	3.06 (3)	1682.5	< 0.001
Energetic	2.14 (2)	2.92 (3)	1726.5	< 0.001
Respectful	2.63 (3)	3.26 (3)	1792.5	< 0.001
Admiring	2.21 (2)	2.83 (3)	1860	0.001
Welcomed	2.56 (3)	3.25 (3)	1864.5	0.001
Contemptuous	1.52 (1)	2.04 (2)	1927.5	0.001
Cared-For	2.77 (3)	3.30 (3)	2002	0.003
Dishonored	1.28 (1)	1.70 (1)	2095.5	0.004
Humiliated	1.27 (1)	1.66 (1)	2117.5	0.005
Isolated	1.51 (1)	1.90 (2)	2088.5	0.006
Proud	2.70 (3)	3.26 (3)	2053	0.007
Lonely	1.35 (1)	1.78 (1)	2129.5	0.008
Afraid	1.51 (1)	1.94 (2)	2132	0.011
Triumphant	2.69 (3)	3.19 (3)	2100.5	0.012
Happy	3.01 (3)	3.44 (3)	2085	0.013
Grateful	3.19 (3)	3.56 (4)	2095	0.014
Ashamed	1.46 (1)	1.84 (2)	2175	0.018

Table 5-1: Average and median rating of the strength participants say they would feel each emotion when using 2FA on a scale of 1 = “Strongly disagree” to 5 = “Strongly agree” from those who do not find 2FA more convenient and those indifferent or who do find it more convenient, along with the results of Mann-Whitney U-Tests comparing the distributions for each group.

Also, as seen in Table 5-2, the list of top ranked emotions from both groups share many of the same emotions, but overall, the mean magnitude of emotion ratings for the indifferent/more convenient group were higher. Notably, several of the emotions whose distributions were found to be significantly different, such as cared-for, happy, and respectful are also in both groups' list of top rated emotions. If, as these results suggest, those who do not find 2FA convenient are also generally less emotionally impacted by the tool, this adds color to the picture of 2FA motivations by implying a strong focus on convenience that predicts other aspects of perceptions around the feature. On the surface and at a minimum, this shows the balance of security and convenience that users make, but also that this balance is not always seen the same, even among those who share the same behavior. Looking to the results in the prior Chapter, users of both 2FA and password managers seem to rate emotions similarly around each respective advice.[6] Notably, emotions of security, confidence, and trust are all prominent among users of both advices, possibly reflecting the added security these users experience as a result of their decision to follow. This similarity across two different advices further confirms the centrality of security in these decisions, and how emotions related to security seem to be associated with following. Despite these similarities, each advice does present a different context for users, and digging deeper can better inform about how these contextual differences may impact emotions around 2FA in ways not seen for password managers.

[6] Looking to the emotions listed in Table 5-2 and Table 4-5, many of the same entries appear, such as secure, trusting, confident, grateful, and cared-for, among others. Also, the mean ratings for these emotions were similar between the two advices.

	Not More Convenient		**Indifferent/More Convenient**	
Rank	*Emotion*	Mean	*Emotion*	Mean
1	Secure	3.90	Secure	3.86
2	Trusting	3.55	Confident	3.68
3	Confident	3.48	Grateful	3.56
4	Grateful	3.19	Trusting	3.49
5	Happy	3.01	Happy	3.44
6	Powerful	2.93	Cared-For	3.30
7	Cared-For	2.77	Respectful	3.26
8	Proud	2.70	Proud	3.26
9	Triumphant	2.69	Welcomed	3.25
10	Respectful	2.63	Triumphant	3.19

Table 5-2: The ten emotions that received the highest mean rating from those who do not find 2FA more convenient and those indifferent or who do find it more convenient.

Low emotional arousal, especially on positive emotions such as happy and grateful means that the 2FA users sampled who say they do not think 2FA is more convenient may be on the edge of becoming non-users of the feature. By the ratings in Table 5-2, the top emotion for both groups was secure, and this emotion was rated similarly by each. Therefore, though all users see the security in using 2FA, those who find it convenient, or at the least, not *inconvenient* are likely to more strongly associate positive emotions with use of the feature, which can then better regulate their motivation to continue using the tool despite the continued effort. The differences among users show how complex these decisions can be, with even those who follow the same advice having drastically different views on it. This complexity is only increased when looking to the motivations of non-users of 2FA, including both those who are aware of the feature, and those who are not.

5.3 Non-Users: “Haven't needed it, nor has it been offered”

Unlike with password managers, where all participants analyzed had heard of the tool, the balance of users and non-users who were also aware of 2FA was not even. Despite 295 total responses to our survey, only 22 reported knowing about 2FA while not using it. Likely because the sample size of those who use 2FA was much greater than the sample of non-users, statistical testing yielded no significant differences on responses to the various quantitative instruments used. Qualitative data from non-users in response to the question asking them to explain why they choose not to use the feature is quite telling about this group. These responses were reviewed for themes by the head researcher due to the small number of comments gathered, and the small length of each response which would make full inductive coding relatively unhelpful.

Many participants were blunt in their responses. For example “sounds inconvenient,” “not wanting to spend the time,” and “just too much,” were all short comments from non-users that expressed similar sentiments about the time and effort needed to use 2FA. These comments support the findings on similar data presented in Chapter 3, and show continued contrast with the reasons given for non-followers of other advice. For example, as seen in the prior Chapter, fears about security risks were a common reason for non-users to avoid password managers, but a desire for convenience was cited as a benefit by many users. Here, for 2FA, inconvenience is a prime motivator for non-users, showing how ostensibly similar concerns can be anchored in varying ways depending on the context of the decision.

Beyond inconvenience, participants citied other reasons to explain their non-adoption of 2FA. Some report that they have not been compelled to use the feature, either due to their own lack of motivation, a lack of external suggestion to activate it, or both. For example, one participant summed their reasoning as “because I don't use a lot of things that have it,” while another said, “haven't needed [2FA], nor has it been offered.” In both of these cases, proliferation as well as better communication of 2FA and its availability may encourage these individuals to activate the feature, as experts recommend.

Better communication may also clear up some points of confusion users reported that motivated them not to use 2FA. For example, one stated “two-factor authentication is no replacement for a strong password.” In this case, though the user shows understanding of the importance of a strong password, they seem to miss that 2FA can be *combined* with a strong password and the added security should be considered independent of the password strength. Other participants were upfront with their lack of awareness as a reason to not use 2FA: “[I do not use 2FA] because I'm not sure exactly how it works or what to do.” Increasing awareness may help in some of these participants’ cases towards motivating them to use 2FA, but not every non-user can be turned by these means.

Some comments revealed very legitimate reasons for avoiding the tool. One participant shared a story showing the possible risks of using 2FA if things go drastically wrong:

> My son had 2 factor authentication on his Gmail account and lost access to his cell phone. Consequently, it took him 6 months to regain access to his Gmail account. This was an unusual situation, but made me nervous.

Other participants stated they could not easily use 2FA because they did not have ready access to a cell phone. These cases highlight how accessibility and usability may limit users’ motivations to adopt some advice. Though the population without a cell phone may be small, as shown in these comments, users may still worry about *if* they lose access to their cell phone and how that may impact their ability to use other services. As with other advice such as updating, these personal negative experiences as depicted in the longer participant quote above can have drastic impacts of users’ attitudes and beliefs about particular advice, lowering motivation for them to adopt. Management of these negative experiences, either through communications or improved usability is an important step towards improving overall cybersecurity behavior.

	Users		**Non-Users**	
Rank	*Emotion*	Mean	*Emotion*	Mean
1	Secure	3.88	Secure	3.73
2	Confident	3.59	Confident	3.64
3	Trusting	3.52	Grateful	3.50
4	Grateful	3.38	Trusting	3.45
5	Happy	3.24	Happy	3.27
6	Powerful	3.06	Cared-For	3.09
7	Cared-For	3.05	Proud	2.91
8	Proud	2.99	Powerful	2.86
9	Respectful	2.96	Triumphant	2.77
10	Triumphant	2.95	Respectful	2.71

Table 5-3: The ten emotions that received the highest mean rating from 2FA users and non-users.

Despite compelling negative reasons to avoid using the feature given by some non-users, their response to the emotion instruments told a slightly different story. Though no statistically significance was found in the differences in distributions of individual emotions for users of 2FA versus non-users, non-users had notably lower ratings for emotions, as seen in Table 5-3. This was true despite a similar ordering of emotions by mean for each group. In all, this indicates that though users and non-users associate the same emotions with using 2FA, non-users rate the magnitude of those emotions lower. This contrasts with the case of password managers as seen in the prior Chapter, where users and non-users differed on core emotions associated with using the tool. Here, the difference seems to be mainly around how *strongly* the emotions are felt rather than which. Like with those who thought 2FA was not more convenient, low arousal of emotions may be part of non-users' lack of adoption of the feature and interventions that address this arousal gap may be successful in changing perceptions of 2FA as well as encourage more to adopt it. Though these results show the complexities of users' considerations around this advice, for some participants, their decision to not use 2FA was driven by other, more direct forces, specifically, a lack of awareness of the feature.

5.4 What's Two-Factor Authentication?

In addition to users and non-users of 2FA, this study also collected a third, group of general users: those who do not know what 2FA is at all. This group was (N = 125) comparable in size to the group of participants who had heard of the feature, regardless of their behavior (N = 170). Considering this, responses to the initial grid statements, which were the only instruments those who did not know what 2FA was were presented besides the branching question asking them about their knowledge of the feature. Table 5-4 shows the mean and median ratings of agreement for the statements found to be significantly different between the two groups.

	"Know"	**"Don't Know"**	**U-Test**	
Statement	Mean (Med.)	Mean (Med.)	*U*	Sig.
I am doing a good job of protecting my computer security.	3.92 (4)	3.62 (4)	8508	0.001
I do not have time to pay attention to security.	1.98 (2)	2.24 (2)	8797	0.007
I do not know where to get computer security advice.	1.94 (2)	2.33 (2)	8269	< 0.001
I am knowledgeable about computer security.	3.91 (4)	3.35 (4)	7190.5	< 0.001

Table 5-4: Average and median rating of agreement with each general statement about computers and cybersecurity on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree" from those who know of 2FA and those who do not know what 2FA is, along with the results of Mann-Whitney U-Tests comparing the distributions for each group. Note: only significant results are shown.

Overall, those who did not know what 2FA was also reported doing worse of a job protecting their computer security, having less time to pay attention to security, know less about where to get advice, and are less knowledge about computer security compared to those who at least heard of 2FA, including non-users. This suggests that there could be a correlation between how "plugged into" cybersecurity a user is (i.e., how much awareness and engagement they have) and users' knowledge of and ability to recognize basic security advice such as 2FA. Though increased engagement has not been shown to increase security outcomes [36], and some have questions the efficacy of increasing users' awareness as a way to increase cybersecurity adoption [20,46,47], it does seem that for some advice, lack of awareness plays at least part of the role for non-adoption.

5.5 Discussion

Prior work [46,47,86,92,103], including the study in Chapter 3 has found a centrality of security and convenience when it comes to cybersecurity, but in those cases, the division was centered around followers and non-followers of good advice. Here, for 2FA, differences around convenience were found even among those who exhibit the *same* behavior. When thinking to the prominence of convenience in the rationale of the small number of non-users of 2FA examined in this study, it could be that these users who do not think there is convenience in using 2FA are on the verge of becoming non-users. These results also follow those of prior studies that have identified usability and convenience as core concerns around 2FA [25,40,59]. Since using 2FA requires at least some regular effort and many users at least perceive added effort due to the feature, managing these attitudes and beliefs about cost may help encourage adoption and continued use. This challenge is distinct from the lessons learned for password managers, where security concerns among non-users were most apparent. These differences in advice context also seem to impact the emotions users associate with each, though patterns between advice are becoming apparent, namely the prominence of security and trust across multiple behaviors.

Emotional perceptions can only be formed, though, if users are aware and informed about the decision and/or behavior. As seen in this sample, many users are not aware of 2FA, and so have no chance to use the tool until some form of messaging or intervention changes that. This is not to suggest that the task of encouraging users to adopt 2FA is as simple as informing them of its existence. Prior work has argued against this approach [20,36,46,47], and as seen in the qualitative data from non-users of the feature, use of 2FA may be impeded by users' circumstances, such as access to an independent device on which to receive the second factor. Additionally, negative past experiences, as well as general perceptions of inconvenience may also hinder the motivation of some to activate 2FA. These issues require more sophisticated intervention approaches than simply informing users of 2FA since users' attitudes and beliefs and emotions are also different between groups that are informed about and use the tool.

5.6 Summary

Two-factor authentication proved different than password managers in many respects related to perceptions and emotions. Password managers are, based on the sample analyzed in Chapter 4, fairly known by users on MTurk, but stark divisions exist between users and non-users. For 2FA, many participants did not know of the advice, though most that knew 2FA reported using it. Also, in this sample, differences were much more apparent between different groups of users than between users and non-users of the feature. In particular, those who rated that they disagreed with the statement "two-factor authentication is more convenient," had significant differences on ratings of many emotions compared with those that were indifferent or agreed with the statement. This could reflect an important divergence based on convenience for even many that follow the advice. In all, though, these results continue to support the importance of convenience in both use of 2FA and password managers, tools/features that aim to increase account security, but in different ways.

Not all good behavior is directly related to accounts and security. For example, software updates, which are needed across many devices and software, do not always contain security patches, though vital fixes are delivered from time to time. Updates are also different than password managers and 2FA in that they are usually prompted by messages (if not just automatic entirely), which presents a unique vector for motivations.

6 Emotions and Cybersecurity Behavior: Case Study in Software Updates

As the results presented in the prior two Chapters demonstrate for password managers and 2FA, the emotional perceptions of users can vary between different cybersecurity advices, just like rational considerations. Studying emotional responses to various cybersecurity advices will not only help us understand individuals' motivations around these decisions, but will also inform the design of emotionally aware videos targeted at changing individuals' behavior. Behavior change will be the goal of the next Chapter, but first, in this Chapter, people's emotional perceptions of the last of the three core advice focused on within this thesis will be studied.

Section 6.1 explains the experimental design of each of the two separate studies discussed in this Chapter, including the two-phased survey of University students discussed in the first subsection, and the larger study using Mechanical Turk presented in the second subsection. Section 6.2 highlights users' reported hesitation to apply updates, Section 6.3 talks about the importance of emotions such as annoyance and confusions to updating behavior, and Section 6.4 presents analysis of in-depth ratings from participants, were we find strong trends in the variance of users' ratings of positive emotions and negative emotions. These results are discussed with relation to prior work in Section 6.5, followed by a closing summary in Section 6.6.

6.1 Experimental Approach

Two survey-based studies were performed to better understand why users choose to update software or not when prompted. Each study targeted different aspects of participants' decision and experiences around software updates, including messages used to deliver them.

Therefore, they all give insight into disparate components of motivation around this key cybersecurity behavior, while also building upon the findings of each towards a broader understanding of what motivates users.

Since software updates are contextually different than adoption of other tools and techniques, such as using a password manager and activating 2FA, our investigation into users' background with this advice had to be different from the approaches used in the prior Chapters. Notably, since update messages are a key aspect of apply software updates and are seen by many, they are studied specifically, along with users' general history and opinions around updating. We investigate the attitudes and beliefs of users around updating and update messages. In addition to this, the comprehensibility and noticeability of particular messages, both key aspects of the C-HIP model [21], was also examined through the data. Finally, by gathering users' emotions in response to actual messages, and emotions users predict they would feel when faced with an update, we can better understand the emotional vectors to users' decisions around updating, as predicted by theory on emotions and motivation [10,14,16,35,53,54,62,64,98].

6.1.1 Two-Phased Survey of Experience

The first study performed around updating encompassed two stages that gathered separate samples. First, a short survey was developed and sent to a sample of users at a University campus (N=78). These participants were not compensated The survey was hosted on a University web-server and was advertised using regularly distributed University email digests that contained information about the procedures, as well as a link to the hosted survey. Table 6-1 below shows the complete content of this initial, short survey, other than the basic demographic questions asked.

Question	Notes
For each of the following, rate on a scale of 1 to 7 how knowledgeable you are in using each software or device.	Microsoft Windows, Apple Laptops or Desktops, Linux, iPhone, Android
How much do you worry about your computer's security?	> Rate from 1 to 7
How much do you care about keeping your software up to date?	
How much do you worry about your computer's privacy?	
Have you ever been hesitant to apply an update?	> Yes, No, I don't know
Have you ever been annoyed by an update message?	
Have you ever been confused by an update message?	

Table 6-1: Content of short survey distributed to the initial sample of participants. These instruments were also used as the base of the extended, follow-up survey distributed to a larger, additional sample.

After the initial pilot sample was collected, the survey was extended to include more instruments and a new sample from the same University campus was gathered (N=172). In addition to the initial survey instruments, participants were asked to report from a list the software which they used, and they were then delivered surveys similar to the initial survey, but phrased for each of the software the participant reported using. The same methods were used to collect this sample as with the last survey (i.e., an advertisement posted in University email digests with a link to the survey hosted on a University web-server). Through this, we were able to identify trends in behavior and experiences around updates between different types of software. Table 6-2 below shows the software asked about on the extended survey.

Software	Category
Microsoft Windows	Operating Systems
Apple laptops or desktops	
Linux	
iPhone	Mobile OS
Android	
Mozilla Firefox	Web Browser
Google Chrome	
Internet Explorer	
Safari	
Microsoft Office	Productivity Software
OpenOffice	
Adobe Acrobat	
Libre Office	
iTunes	Media Software
QuickTime	
Windows Media Player	
VLC	
Skype	Communication Software
Norton products	Security Software
MacAfee products	
Malwarebytes	

Table 6-2: List of software packages asked about on the extended follow-up survey. For each software, participants were asked to report their frequency of use of the software, how often they saw updates from the software, as well as to report their hesitation in applying updates for each. Finally, they were asked to rate how annoying, confusing, important, and noticeable they generally found the software's update messages to be.

In addition to the specific software on the list in the table above, participants were asked if they reported playing video games and about their updating behavior around video games. For each of the listed software a participant reported using, they were also asked how annoying, confusing, important, and noticeable they found that software's update messages.

Finally, after the software-based instruments, all participants were shown sample update and warning messages taken from disparate types of software across many systems and asked to rate how annoying, confusing, important, and noticeable they found each message to be. A 5-point Likert scale was used on this survey, similar to those used for in-depth emotion instruments in Chapters 4 & 5, but only for four emotions to reduce the overall length of the survey since these instruments were asked for a dozen sample messages. Participants were also offered the opportunity to provide positive and negative open-ended feedback about each message. The sample messages used, as well as all survey instruments, and the basic demographics of samples collected can be found in Appendix D.

6.1.2 Surveying Reported Emotions When Faced with an Update Message

The second update related study was executed using Mechanical Turk (MTurk) and was targeted at gathering participants' emotions around updating with increased granularity. Four hundred participants were gathered through the service. Any member of the MTurk population was eligible to participate as long as they were at least 18 years of age and resided in the United States. Interested eligible participants were shown the information sheet for the study. If they wanted to participate after reading the sheet, participants would then begin the survey. After completing the survey, each respondent was compensated $1.00 for their participation.

Similarly to the in-depth emotion instruments used in the previous chapters, each participant was asked to rate on a 5-point Likert scale, anchored from "never," to "all the time," the degree to which they think they would feel each of 45 emotions when encountering an unexpected software update message while using the computer. Participants were asked to rate the emotions in both of two cases: one where the update message interrupted casual web-browsing (representing the *relaxed* state), and another where the message interrupted them as they worked on an important deadline (representing the *pressured* state). Specifically, participants were asked to "imagine a situation where the warning to update software appears while you are (surfing the web with no specific purpose/hard at work on an important project with a looming deadline)." In these contexts, participants were then presented with the instruments asking them to rate how much they anticipate they would feel each of the emotions.

With this data, we can dig deep into what emotions users associate with updating, and use these findings to understand not only how and why they may make the decisions they do, but also help improve how we measure emotional response in these contexts. By looking at the data collected in both of the studies discussed in this Chapter, a detailed and broad picture of motivations around updating becomes apparent.

6.2 Prevalence of Hesitation

As expected, numerous participants in both rounds of the first study indicated that they have hesitated to update in the past. Figure 6-1 shows the number who say they have ever delayed an update.

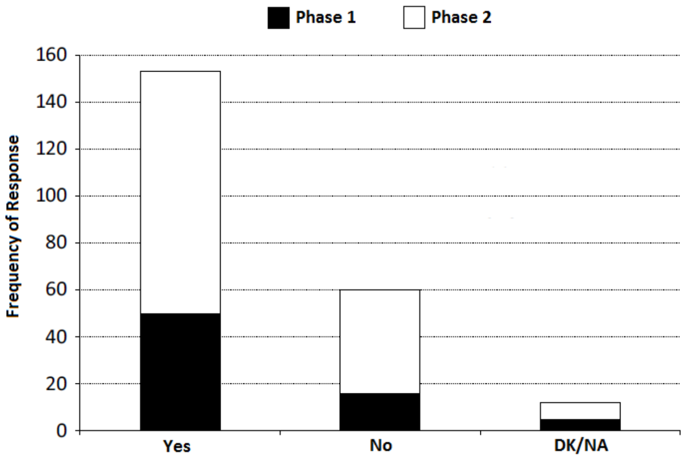


Figure 6-1: Frequency of responses to the question "Have you ever been hesitant to apply an update?" DK/NA is the category used for missing responses or responses of "I don't know."

Most participants had some history of hesitating to apply an update, but the longer second survey dug deeper by asking participants to report their hesitation to apply updates for the particular software they use. Table 6-3 below shows the reported delay to respond to each software's update messages generally, as reported by users of each software.

Software	**Immediately**	***Within…***				**Never**
		1 day	3 days	A week	A month	
Windows (%)	11	24	13	23	16	13
Apple PC (%)	5	16	7	30	39	4
iPhone (%)	21	21	22	11	18	6
Android (%)	21	18	18	12	18	15
Firefox (%)	26	17	7	9	17	24
Chrome (%)	14	20	11	8	4	43
IE (%)	9	0	19	9	25	38
Safari (%)	4	8	6	12	8	62
MS Office (%)	17	16	10	12	15	30
Acrobat (%)	13	15	10	13	18	31
iTunes (%)	13	10	7	13	32	24
WMP (%)	14	16	10	8	6	47
QuickTime (%)	12	0	8	16	16	48
VLC (%)	14	6	9	9	14	49
Skype (%)	20	10	7	14	14	34
Video Games (%)	38	12	12	4	10	24
Norton (%)	19	19	13	23	3	23
MacAfee (%)	11	14	17	14	11	31
Malwarebytes (%)	50	19	6	6	6	13

Table 6-3: Response rates for each software representing the reported average delay in applying an update after seeing an update message. Note: Distributions are shown as a percentage of all those who reported using each software, and samples with size < 15 are not shown.

The table shows hesitation, though common, varied between software. In some cases, such as Malwarebytes, many participants reported applying updates quickly. In others, such as Safari, most participants reported never applying these updates. There are several explanations for the tendency of users to hesitate. As seen in prior work [46,47,86,92,103] and the results in previous Chapters, security and convenience are common considerations for users. In Chapter 3, many users of 2FA, for example, mentioned the added security in their reasons why they used the feature. In a similar vein, users may be more attentive to Malwarebytes' updates since this is an anti-virus software that has direct relations to security overall. There are many other reasons that may explain this hesitation, though.

6.3 Prominence of Annoyance and Confusion

Prior work has pointed to negative past experiences as a reason for neglecting to update [66,96]. We hypothesize that annoyance and confusion could be an emotional result of these negative experiences with updates. Our survey asked participants if they have ever been annoyed by an update message. As can be seen in Figure 6-2, a large majority of our participants said they had. Similarly, Figure 6-3 shows that a large number of participants also report being confused by an update message, though in not nearly the unanimity as with annoyance.

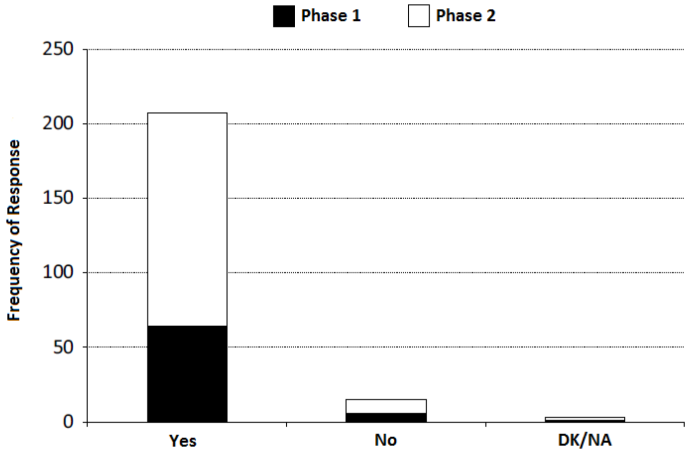


Figure 6-2: Frequency of responses to the question "Have you ever been annoyed by an update message?" DK/NA is the category used for missing responses or responses of "I don't know."

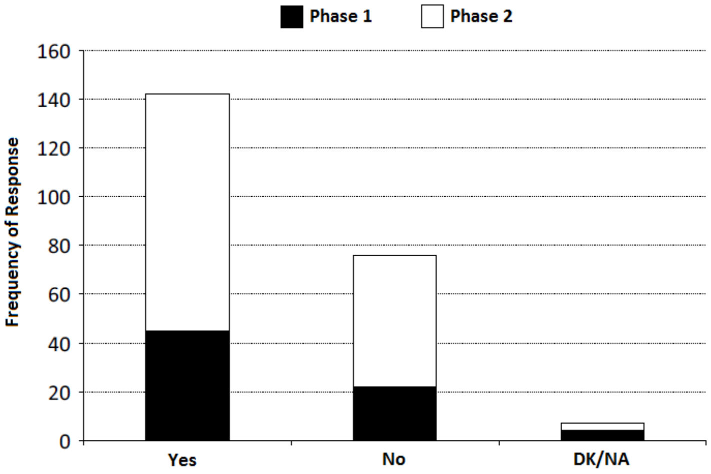


Figure 6-3: Frequency of responses to the question "Have you ever been confused by an update message?" DK/NA is the category used for missing responses or responses of "I don't know."

Again, the extended second survey expanded on these concepts by phrasing them for specific software. Table 6-4 below shows the average annoyance and confusion rating (on a 7-point scale) for each software package, as rated by the participants who reported using each. In addition, the table shows the correlation between participants' annoyance and confusion rating for each software with their reported length of hesitation in applying the software's update, using Pearson's R-value [75].

Software	**Average Rating**		**Correlation w/ Hesitation**	
	Annoyance	Confusion	Annoyance	Confusion
Windows	4.5	3.1	**0.40**	**0.31**
Apple PC	4.0	2.8	**0.38**	**0.26**
iPhone	3.6	2.5	**0.35**	**0.23**
Android	3.3	2.6	**0.22**	**0.24**
Firefox	3.4	2.5	0.09	0.06
Chrome	2.4	2.0	0.07	**0.11**
IE	3.5	3.1	**0.16**	0.03
Safari	2.5	2.3	0.08	**0.12**
MS Office	3.1	2.6	0.07	0.07
Acrobat	3.7	2.5	-0.02	-0.01
iTunes	4.3	2.8	**0.44**	**0.25**
WMP	2.9	2.6	-0.04	-0.02
QuickTime	3.5	2.6	**-0.10**	0.07
VLC	2.6	1.9	**-0.36**	**-0.39**
Norton	4.0	3.3	**0.15**	0.06
MacAfee	3.2	2.3	**0.19**	**0.60**
Malwarebytes	2.7	2.0	**0.36**	**0.33**

Table 6-4: Average ratings of annoyance and confusion resulting from each software's update messages, as reported by users. Correlation between annoyance and hesitation, as well as confusion and hesitation is shown using Pearson's R-value. R-values ≥ 0.1 in magnitude are marked.

For some software, annoyance and confusion were rated prominently (i.e., an average rating of 4 or above). In some of these cases, ratings to these emotions were found to be correlated with how long participants reported delaying applying that software's update when presented with a message. This suggests some connection in hesitation and these emotions, which can help inform why users hesitate. If they are confused, they may not understand why the update is important. Annoyance and other negative emotions will also dissuade users from updating since people try to avoid these negative feelings instinctually. To gain more insight into emotions around updating, we next look to a core component of update delivery: update/warning messages.

6.4 Emotions Elicited By Software Update and Warning Messages

To see how users react to messages in a more direct and immediate way, participants in the second phase of the first study rated sample real-world update and warning messages on 4 emotions: annoyance, confusion, importance, and noticeability. Through analysis of the gathered rankings, overall, confusion and annoyance were found to be correlated with Pearson's r = 0.50. Importance and noticeability were also correlated with an r = 0.42. Thus, to rank the emotional impact of each image, we summed the average negative valence ratings (i.e., annoyance and confusion) and subtracted this from the sum of average positive valence ratings (i.e., importance and noticeability). Equation 4-1 below details how these ratings are calculated.

$$\text{Rank} = \frac{(\text{Rating}_{noticeable} + \text{Rating}_{important}) - (\text{Rating}_{annoy} + \text{Rating}_{conf})}{7}$$

Equation 6-1: Definition used to calculate a comparative rank of each image that considers the four ratings gathered from users.

In the equation, the combined magnitude of the ratings is divided by 7 to normalize on a scale of 0 to 1 since all ratings were given on a 7-point Likert scale. Table 6-5 shows the average rating for each emotion, for each image, along with the resulting rank.

Image #	Important	Annoying	Confusing	Noticeable	Rank
04	3.6	4.5	4.2	4.1	-0.15
06	4.3	4.4	4.0	4.5	0.06
14	3.0	3.8	2.2	3.4	0.06
10	3.9	4.2	4.1	4.9	0.07
13	3.5	4.0	3.6	4.6	0.07
07	3.6	4.3	3.0	4.8	0.13
01	3.7	3.5	3.4	4.6	0.18
08	4.6	3.9	3.5	4.8	0.28
03	3.6	3.8	2.5	4.9	0.29
09	3.6	3.4	2.3	4.8	0.33
12	3.8	3.3	2.3	5.0	0.39
02	5.4	4.3	3.1	6.0	0.51
05	5.9	4.1	3.6	6.3	0.58
11	4.8	2.8	2.2	4.8	0.61
Average	4.1	3.9	3.1	4.8	0.24

Table 6-5: Average ratings of each emotion for each image along with the resulting rank as calculated using Equation 5-1.

As the table shows, there was a large spread in the ranking each message received. Some came out high (> 0.5), such as Images 11, 5, and 2, while others, such as 4, 6, 14, and 10 came in very low (< 0.1). When looking to these images, it is apparent that certain features are shared by each group of images. Based on the open-ended comments, the “good” messages (i.e., those ranked highly) provided the user with the necessary information they needed to understand the content. In addition, most of the “good” messages contained bright and noticeable features, though these came at a trade-off, causing some participants to question the messages’ legitimacy. For “bad” messages that ranked low using the rating-based metric, comments showed common complaints of uninformative or confusing messages, flat and boring designs that go unnoticed, and in some cases, confusing options being offered.

6.4.1 Extended Qualitative Analysis

Inspired by the usefulness of the participants' comments towards helping understand which message features were possibly responsible for the ratings seen in the data, the qualitative data was further analyzed. In all, the participants provided 809 positive comments and 866 negative comments. Bottom-up inductive coding was used to categorize them, with no deductive codes developed *a priori*. Initial coding was performed by a team member who had not been involved with the execution or design of the study. Fifty-two codes were assigned to positive comments, while negative comments were assigned 38 unique codes. The lead researcher then reviewed this schema and performed further analysis using the emotion ratings for each image.

Correlation analysis was used to gain further insight into the features mentioned in comments and their relationship to participants' reported emotions. Table 6-6 shows Pearson's correlation coefficients [75] between the frequency of a code being applied to an image and that magnitude of each emotion's average rating for that image. For each image, counts of all positive design/layout codes were summed and used to determine the correlation between the application of codes in this category with the average rating for each emotion. This process was repeated for positive content codes, as well as negative design/layout and content codes with the results for all being highlighted in Table 6-6.

	Code/Comment Type	Confusion	Annoyance	Noticeability	Importance
Codes for Positive Comments	Tells the importance/benefits	-0.45	-0.56	-	-
	Easy to understand	-0.58	-0.54	-	-
	Concise	-0.69	-0.74	-	-
	Looks trustworthy/legitimate	-0.45	-0.65	-	-
	Cleaner looking	-	-0.51	-	-
	Button/link for more information	-	-0.54	-	-
	Brand effect	-	-0.72	-	-
	Simple language	-	-	0.51	0.41
	Alerting design	-	-	0.57	0.63
	Choice of color	-	-	0.54	-
	Makes the user want to take action	-	-	-	0.72
	All positive design/layout	-0.14	-0.24	0.55	0.57
	All positive content	-0.31	-0.36	0.41	0.41
Codes for Negative Comments	Too technical	0.82	0.64	-	-
	Too much content	0.70	0.60	-	-
	Ambiguous language	0.67	0.55	-	-
	Unpleasant color		0.49	-	-
	Boring	0.65	0.48	-0.37	-
	Confusing	0.53	0.47	-	-
	Annoying		0.42	-	-
	Fell of authenticity	0.44	0.36	-	-
	Charging money for the update	0.34	0.31	-	-
	Makes users worried regarding adverse consequences of applying update	0.48	-	-	-
	Use of scare tactics/threat	-	0.27	-	-
	Use of hard-to-read font size	-	0.53	-0.45	-0.38
	Does not explain the benefit of the update	-	-	-	-0.40
	Not noticeable	-	-	-0.71	-0.46
	Pops up/interruption	-	-	-0.43	-0.48
	Negative attitudes towards the software brand	-	-	-0.59	-
	All negative design/layout	0.53	0.61	-0.10	0.23
	All negative content	0.61	0.45	-0.35	-0.43

Table 6-6: Correlation using Pearson's R-value is shown between the frequency of application for each code, along with the ratings of confusion, annoyance, noticeability, and importance across the 14 images tested. Overall correlation between the frequency of application of all positive and negative comments with each emotion is also shown. Note: Only correlations of magnitude > 0.10 are included in this table.

As seen in the table, negative codes were strongly correlated with annoyance and confusion overall. This trend continued for many of the individual codes used to categorize the negative comments. Positive codes, on the other hand, were correlated strongly overall with ratings of importance and noticeability. Though some of the codes applied to positive comments also correlated with importance and noticeability when counted individually, several codes correlated strongly with confusion and annoyance, showing the complexity of participants' emotional response to the tested update messages.

These results all show the interplay of emotions when individuals are presented with an update or warning message. These emotions can impact their eventual decisions to apply the update, as possibly indicated by the correlations between annoyance/confusion and hesitation across software. Emotions span much more than just annoyance, confusion, importance, and noticeability, as seen in the in-depth studies of 2FA and password managers in prior Chapters. Looking to more detailed data will unlock new findings about how individuals react to notifications for software updates.

6.4.2 A Broader View of Emotions Related to Software Updates

To gather more in-depth ratings from a sample of Internet users, after the data presented in prior sections was collected, another study was executed that refocused away from specific software and towards updates in general. As described in Section 3.1.2, this study collects two sets of 5-point Likert scale ratings for 45 emotions from a total of 400 participants. To understand the structure of participants' set of ratings for each task (i.e., relaxed and pressured), two methods of analysis were used.

Exploratory Structural Equation Modeling (ESEM) is a method of analyzing data which combines the techniques of Exploratory and Confirmatory Factor Analysis [68]. It is a useful technique when there is limited knowledge and prior measurement of a component, as is the case for emotions in the context of updating. ESEM Factors were calculated on the data for both tasks separately. The loadings of the ESEM were analyzed to discover each factor's structure. A summary of the resulting ESEM factors for both tasks are presented in Table 6-7 (please note: the full ESEM results can be found in Appendix D).

	1. Positive			***2. Anxiety***	
	Relaxed	*Pressure*		Relaxed	*Pressure*
Confident	0.822	*0.853*	**Nervous**	0.692	*0.749*
Secure	0.813	*0.858*	**Anxious**	0.680	*0.723*
Grateful	0.811	*0.816*	**Confused**	0.610	*0.535*[B]
Happy	0.781	*0.803*	**Afraid**	0.573	*0.727*
Respectful	0.771	*0.788*[A]	**Freaked out**	0.534	*0.654*
	3. Loneliness			***4. Hostility***	
Ashamed	0.825	*0.823*	**Disdainful**	0.821	*0.717*
Abandoned	0.824	*0.761*[C]	**Scornful**	0.747	*0.751*
Lonely	0.821	*0.833*	**Contemptuous**	0.676	*0.659*
Humiliated	0.802	*0.767*	**Hostile**	0.634	*0.573*
Isolated	0.787	*0.774*	**Resentful**	0.574	*0.600*

Table 6-7: Factor loadings for the best five items of the four identified factors resulting from the ESEM analysis on data collected for both the relaxed and pressured task. The full factor loadings are included in Appendix D. Notes: A: Cared-for loaded higher, .799; B: Dismayed loaded higher, .644; C: Embarrassed loaded higher .795

A picture begins to appear that describes the nature of users' emotion around updating. The Positive emotions factor was the first in the ESEM and encompassed the positive emotions included in the total list of 45 in strong and significant loadings. This is interesting as it could indicate that some users see updates in a positive light, while others do not, which would produce the strong variance on this initial factor. This is also reminiscent of the results in the prior two Chapters related to password managers and 2FA. For password managers, users and non-users differed on specific positive emotions (i.e., admiring and energetic), while for 2FA, the magnitude of ratings on several positive emotions was much lower from participants who also rated 2FA not convenient. In all three case studies, it seems that differences between different groups of individuals around ratings of positive emotions may be related to their behavior around following each advice. That is, those who see each advice in a more positive light are found to be more likely to also be a follower of the advice. Though interventions may find success in highlighting these positive emotions, as seen in the prior Chapters, other kinds of emotions are also involved.

The other three factors from the ESEM analysis, which explained the rest of the variance, all point to different, but all negative themes. Anxiety is a logical second strongest factor since the surprise of an update, and repeated worry about possible negative consequences from the update may produce anxiety in some, but not others. This is reminiscent of the extra suspicion that non-users of password managers reported relative to users of the tool. The final two factors point to two other kinds of negative emotions, one based around sadness and isolation, with emotions like lonely, abandoned, and ashamed, the other based around anger, with emotions like scornful and contemptuous. This shows the complexity in how users feel about unexpected updates. In some cases, users rate that they feel lonelier and more abandoned due to the appearance of such a message, while other users seem to feel hostility in response to those messages.

Thinking to the other results in this Chapter, there are clues that help understand these trends. The anxiety users feel may be related to the issues they report having in the past with updates. Previous negative experience may also explain the abandonment some report feeling in response to updates. These past bad updates may have caused the user to feel abandoned in the moment, and they are remembering this experience now. Chapter 3, for example, found that negative past experiences were a reason from non-updaters in particular, as has prior work [66,96]. Addressing these issues through better, less intrusive updates as well as better communication to assuage these concerns for users, is vital to increasing the number of users who regularly apply software updates. Also, as seen in the data for 2FA in Chapter 5, one participant reported a similar negative past experience that led them to avoid 2FA, so negative past experiences are not limited in effect to updating, but span to other cybersecurity advice.

Another particular aspect of updates may also help explain these emotion results. This Chapter and prior studies [96,99] have found that interruption plays a factor in users' decisions to update in response to messages. This may explain the hostility some users feel. Hostility may be a natural extension of the common annoyance and confusion participants in the prior study reported. Here, again, the design of update messages and mechanisms, as well as the approaches of persuasion to update must be precisely tuned to repair these negative impressions some users have to maximize the overall likelihood of update application.

6.5 Discussion

Updating is an important behavior for users to adopt as it helps keep all software free of known security vulnerabilities, which protects individuals and the network from attack. Thus, it is imperative that we understand if users update, why they do and do not, if they don't. Their responses to the messages used to convince them to apply an update (i.e., software update messages). Hesitation was common in our results, as was annoyance and confusion with updates, which follows on the heels of prior work that has shown users commonly do not know what updates are changing in their systems [99] nor have necessary information to properly decide to apply an update or not [67]. It's possible that these issues with updates manifest in our data as confusion, annoyance, and hesitation to apply. Analysis of in-depth emotion ratings found that much of the variance in ratings was based around ratings to positive emotions, showing that some participants rate these high, while others rate these low. Further variance was explained through ratings of negative emotions, again with some participants rating these higher than others. High instances of negative emotions and low instances of positive emotions around a decision may lead an individual away from adopting that behavior [16]. Thus, interventions that address these divergent emotions, particularly instances of negative emotions, may be effective at encouraging users to more frequently apply software updates in response to messages.

The source of the negative emotions, though, is likely disparate, as indicated in the qualitative analysis and findings of prior work [66,67,96,97,99]. Past negative experiences certainly play a role [66,96]. Experiences with updates are not all related to negative outcomes of an update. In fact, users have an *experience* with updates every time they see an update message. Our results show that update messages commonly contain poor wordings and bad designs that instill negative emotions in users. If users see many of these "bad" messages, it will degrade their expectations about updates generally, which may be reflected in the instances of negative emotions observed in our data. This aspect is somewhat specific to updating since the other advices tested in this thesis (i.e., use of 2FA and password manager) generally do not have regular, associated messaging like software updating does with update messages, but our results also finds commonality in the considerations users make around all three of these decisions.

The time and effort needed to update, such as a system restart, is enough to put some off from updating. This kind of inconvenience also stands in the way of systems that encourage the activation of automatic updating, as Mathur et al. found recently [66]. As seen in prior Chapters and prior work [46,47,86,92,103], convenience/inconvenience plays an important role for other decisions as well. Therefore, any intervention aiming to alter perceptions and behavior around any cybersecurity advice would be wise to consider how convenience/inconvenience is involved in the advice.

6.6 Summary

The three studies described in this Chapter all explore users' emotions around updating, as well as software update and warning messages. Negative emotions are common around updates. Namely, annoyance and confusion were reported by large swaths of users. These emotions were correlated with design features mentioned in user comments, and the emotions of users as reported in a more directed study varied primarily on how much users felt positive emotions (indicating a strong variance on how different users felt these emotions and possibly indicating that users feel negative emotions around updating). The other three factors that described the variance in this data also all focused on negative emotion sets, showing the strong interplay of these towards updating. These results illuminate the emotions individuals feel around the final of the three advices used as case studies in this thesis. The next Chapter will use these results, as well as the results from Chapters 3-6 to design informed video-based interventions targeted at the same three advices.

7 Cybersecurity Interventions Using Novel Emotional and Social Content

The previous chapters have demonstrated several key leads towards new methods of encouraging more user adoption of good cybersecurity behavior. First, clear perception gaps and motivation gaps were found across multiple samples of cybersecurity advice followers and non-followers. Next, additional data showed that social motivations around many of these decisions, at least in the eyes of participants, are low. This is true despite the demonstrable impacts one's cybersecurity behavior has on others due to the interconnectivity of the Internet and computer networks more generally. Finally, it is clear that emotions play a role in motivations around all the advices sampled in our studies. The prevalence of certain emotions over others allows a deeper understanding of these users' motivations, but exploring current emotions and perceptions can only go so far.

As prior work has shown and argued [35,53,54,60,98], interventions which address these gaps in perceptions and negative emotions can increase the likelihood of users adopting these kinds of behaviors, possibly through novel approaches such as emotional inoculation and social motivation. To test this, a final study was performed that utilized video-based interventions to deliver similar, but varied content that incorporated appeals which highlighted the emotions the viewer may feel around the decision or social-based reasons that exist in support of them taking up good security behavior.

Prior studies used to inform the approach of intervention in this study, as well as a specific technique that harnesses emotions towards persuasion are discussed in Section 7.1. Using this prior work as a base, Section 7.2 describes the design of the videos and the study procedures in detail. Section 7.3 presents the hypotheses of how the videos may impact participants. Statistical analysis and visualization of the differences in measured variables, for each group, throughout the study, are presented in Section 7.4. These results are then discussed in Section 7.5, with focus on the performance of the experimental emotionally and socially aware videos, as well as comparisons to prior work. Finally, Section 7.6 closes the Chapter.

7.1 Literature for Intervention Design

The studies presented in prior chapters have been exploratory in focus, but the study in this Chapter looks to alter users' perceptions and behavior around following sample cybersecurity advice. Thus, some additional related work was drawn upon for this study that was not used extensively or at all in the design of the previous studies. First, an overview of literature supporting the use of video as the method of intervention communication is discussed. Next, a particular emotionally aware communication technique known as emotional inoculation is introduced along with background on its use in other contexts.

7.1.1 Interventions in Cybersecurity

Researchers have looked to the impact of various interventions styles on security behavior and perceptions, including small-group sessions [5], cybersecurity fairs [61], and alteration of existing interfaces with personal examples [42]. Though there are merits to these targeted and tuned approaches, they are also logistically intensive and, in the case of altering the delivery of messages in software, hard to duplicate across many current and future cybersecurity behaviors. A more modular and efficient method of intervention was called for to maximize the scope of the experiment and adoptability of materials developed therein.

Video-based interventions have been studied and identified as more effective than other means possible for our overall experimental design [48,69,78,79,93]. One recent prior work investigated three delivery methods for security awareness information and found that video out-performed text and game-based approaches [93]. This follows on the several studies in other domains that have shown that video is more effective than text [48]. For risk communication generally and the teaching of new authentication methods, video was also shown to be effective in recent work [78]. Newer studies have begun to explore the applicability of video in persuading users to take up expertly advised computer security behavior. One such effort designed video interventions to promote use of two-factor authentication, finding correlations in decisions to use two-factor authentication and how interesting/informative/useful the viewers found the videos [4].

The study in this Chapter also incorporates two persuasive approaches that have been used in the past to understand and frame users' cybersecurity behavior, but has not been extensively explored for interventions aimed at changing perceptions and behavior. One of these approaches, use of social motivation, is relatively straight-forward to incorporate into existing, informational-based video approaches since its possible power was inspired by the general lack of social consideration found in prior data. Thus, videos which used social motivations were developed by explaining possible social impacts of the users' behavior in each cybersecurity context which users are less likely to be aware of. The other approach, motivation through emotions, required more due diligence to properly execute since this is a more experimental method for cybersecurity.

7.1.2 Emotional Inoculation

The connection between cybersecurity decisions and emotions is a newer track in the broader literature of cybersecurity and usable security. Thus, to understand how to incorporate emotionally aware appeals in the interventions for this study, it is necessary to look to other fields to find comparable applications of such appeals that may be adapted for the contexts here. Emotional inoculation is one such practical application of emotionally aware persuasion that has been shown to be effective in other decisions that involve risk when used in interventions [53,54]. Prior studies found emotional inoculation important towards reducing stress in surgical patients [60], encouraging individuals to be physically active [98], understanding individuals perceptions of crisis [10], and encouraging condom use [35].

Emotional inoculation is the theory that people can be introduced to the emotions they may feel in certain situations, which will help them overcome these emotions when faced with the decisions in their life. Related to the theory that emotions can interfere with decision-making, emotional inoculation allows for individuals to see past these feelings and think more rationally about the situations they are presented with. Though emotional inoculation may happen as an indirect by-product of an unrelated intervention or event, the effects of emotional inoculation can be targeted for, based on understanding of the emotions that are likely to be felt. Using the theory this way calls for individuals to be introduced to the emotions they may feel in the heat of a decision so that they can overcome the motivations resulting from these emotions, when faced with the decision in their lives. This approach is anchored in the theory of emotions as important influences on behavior. In essence, the approach works to make users aware of strong emotions they may feel that could interfere with the rational side of their mind. For example, in a recent study Ferrer et al., emotional inoculation interventions were developed for condom use that explained the need for receivers to remember to stop for a moment and put on a prophylactic device, even while they will be experiencing intense sexual emotions [35]. By making the receiver aware of this in a prior intervention, reports of condom use in sexual encounters increased significantly more than for a control group which received traditionally tuned appeals.

It may be possible to similarly inoculate computer users to emotions they may feel while deciding to follow cybersecurity advice. In addition to reducing or at least making users aware of negative emotions they could feel, like fear or frustration, emotional inoculation approaches in this realm may also try to increase instances of positive emotions users can feel. Prior work has called for cybersecurity researchers to look to the healthcare sector to determine strategies for increasing overall security [83] and understanding cybersecurity behavior [72], as there have been noted similarities between issues of cybersecurity and some issues involved in healthcare. The prior success of emotional inoculation in the healthcare realm [35,60] may mean similar success in the context of cybersecurity advice.

7.2 Experimental Approach

To test the impact of videos that incorporate alternative approaches to persuasion on cybersecurity perceptions and behavior, the three advices that were explored in the previous Chapters were used again as case studies (i.e., updating software frequently, using two-factor authentication, and using a secure password manager). For each advice, three videos were developed and tested.

7.2.1 Video Design and Development Process

The first video, referred to in this Chapter as the Basic video, was different in content for each advice, but followed a similar style and broad outline. Each Basic video started by introducing the viewer to the basic science around each advice, but in a way that is understandable to average users who may not have much technical knowledge. For example, in the Basic video targeted at convincing viewers to begin updating software regularly, the first portion of the video talks about the software development cycle and how that can lead to flaws in software that must be patched with regular software updates. After the basics about the advice are established, each video then moves into an explanation of how not following the advice could lead to negative consequences. This is based on prior work's recommendation, where researchers call for targeted risk communications, among other things, "describe particular vulnerabilities that the user may be exposed to" [12]. For example, in the two-factor authentication Basic video, this section focused on how the viewer's accounts can be accessed by unauthorized users more easily when not activating two-factor authentication. These scripts were informed by the lessons learned in the studies discussed in Chapters 3-6. All three discussed security and convenience, but specific issues were varied for each advice to focus on the context specific issues identified in the prior Chapters.

Thus, all Basic videos followed a similar structure and were aimed at presenting basic information explaining the background as to why following the advice is important, as well as demonstrating how the viewer can be negatively affected by negligence. Importantly, this information was all presented in a clear and easy to follow way. The scripts were written to avoid technical jargon and extraneous content that may have confused or misled viewers. These scripts were then recorded, and those recordings were timed to a highly-animated PowerPoint presentation that provided visual demonstrations and summaries of the content being communicated in the recorded voice-overs. Through this process, three videos were created that could be used as a common starting point for alterations that highlight either the emotions viewers may feel or social motivations around each advice.

For each advice, two additional videos were developed. One incorporated emotional inoculation targeting a reduction in the various emotions users feel around each decision that can hinder their adoption of the advice, as well as bringing to viewer's minds the positive emotions they can feel if they take up the advice. The second video for each highlighted reasons for following the advice that are focused on other users, such as impacts decisions can have on individuals the viewers may know personally. For each new video, the Basic script for the applicable advice was used as a starting point. Changes and modifications were made, where possible, to tune the overall tone and message of the updated videos in a way that reflected the alternative persuasion methods. This process was done carefully to preserve the overall structure of the videos (i.e., general explanation followed by possible negative outcome of not following). Care was also taken to maintain the understandability of the videos.

In the context of the advice targeted in this study, the emotional inoculation content incorporated into each advice's Emotion video was based around concerns that have been well documented in prior work and the exploratory work presented in Chapters 3-6 of this thesis. For example, in the Emotion video for the group who reported not updating, discussion was added to the script that addressed possible inconvenience related to taking the time to apply updates and possible unintended negative consequences of applying an update, including the annoyance and frustration they may feel. Viewers were reminded of the benefits of updating that they should remember despite these negative feelings, as well as the positive emotions they may feel when utilizing the improved software that comes from software updates.

Social motivations were incorporated into the third video for each advice by highlighting places where the viewers' decisions could impact the people they know. For example, the 2FA and Password Manager Basic videos discussed how accounts can be accessed by hackers if not properly protected. The Social videos for these advices accentuated that a compromised email or social media account could then be used to launch attacks against the friends and family of the viewer.[7] Through this approach, these videos aim to increase the viewers' awareness and appreciation for the risk to others their cybersecurity decisions can have.

Using the updated scripts for each advice's Emotion and Social video, new audio was recorded for the additional videos. PowerPoint presentations were used for each video, with slight alterations in the timing being made as needed. Transcripts of the audio in each video can be found in Appendix E.   To test these videos, it is first necessary to establish the measure by which they will be assessed. A survey was designed to gather data on behavior change, as well as key aspects of participants' understanding and perceptions that are important towards impacting change.

7.2.2 Definition of Variables

Four variables were specifically targeted in this study: awareness, perceptions, emotions, and behavior. A survey was used to gather data on each of these variables that could then be analyzed to assess the possible impact of each video on participants, which will be referred to as

[7] Please note that care was taken to avoid injecting too much fear into the video appeals. Since risks are being discussed in these videos, it's possible that some participants may feel fear, but the scripts were written to merely mention these risks without exaggerating the possible outcomes or trying to scare the viewers into changing their behavior. Instead, they are informed how to adopt behaviors to protect against risks, and how adopting those behaviors can lead to positive outcomes.

the assessment survey. All groups, for each advice, were delivered similar assessment surveys, though the surveys did vary between advices. All instruments were developed from prior work and were designed and tested to be straight-forward for participants. In order to more intuitively analyze the data collected and reduce the number of statistical tests performed so as to reduce the likelihood of introducing false positive results (Type II error), intuitive scores were derived from the raw data collected from participants, which were then used in the analysis presented in subsequent sections of this Chapter.

Awareness instruments were true/false and multiple-choice in format, similar to what would appear on a basic cybersecurity quiz or test. They were designed based on instruments used in other studies that looked to assess cybersecurity awareness in various circumstances, such as before and after attending a cybersecurity fair [61] or around mobile-phone security [71]. For each advice, three true/false and four multiple-choice instruments were developed. Though the three true/false questions were the same for each advice (albeit slightly altered to ask about the target advice), the multiple-choice questions did differ more drastically in content, though similar concepts were targeted across the three advices. For analysis, two scores were calculated from these responses. One captured the number of True/False instruments responded to with "False," which is considered the *more aware* answer. The second awareness score was a tally of a score based on the four multiple-choice instruments contained in each awareness survey. Scores were calculated for these based on the key of *aware* answers that are marked on the survey instruments in Appendix E. In both cases, a higher score represented an increase in awareness, but each captured different components of this variable.

Perceptions of costs, benefits, and risks of following and not following the tested advices were measured using the same instruments used in Chapter 3. Instruments were different for each advice (i.e., they asked about the costs/benefits/risks around the specific advice), but were similar in format. Users' ratings to these instruments were used to calculate 4 scores, each capturing a different and unique aspect of motivation around following the groups' target advices. An Individual and Social phrasing of the *Motivations to Follow* and *Motivations to Not Follow* were calculated from each participant's provided set of perception ratings. Each of the 4 scores were calculated using the benefits, costs, and risk rating that matches the score, as noted in the following equation:

$$\text{Score} = \ Rating_{benefit} - \frac{(Rating_{cost} + Rating_{risk})}{2}$$

Equation 7-1: Definition used to calculate each perception score used in the analysis of this study. For example, the Individual Motivation to Follow for an Update participant was calculated by subtracting the mean of the participant's rating of the costs and risks to them if they were to update from the participant's rating of the benefits to them if they updated.

Emotions were gathered with a single, but dense instrument that asked participants to rank the top five emotions they anticipate they would feel when adhering to their group's target advice. Participants were given a list of 45 emotions to selection from in a drop-down list, the same list of emotions as used in the work presented in Chapters 4, 5, and 6. This method of data collection for emotions was chosen relative to the emotion instruments used in Chapters 4-6 to minimize the survey length with the goal of reducing survey fatigue in participants [80]. The instruments used in these prior Chapters, though detailed in their reach, were lengthy and required significant effort from participants. The same list of emotions was used in the reworked instrument, but since participants select their top emotions rather than rate all emotions, we can hone in on key changes in the minds of participants as opposed to ratings for each and every emotion. Using these rankings of emotions from participants, two scores were derived; one that measured the number and prominence of positive emotions selected, another measuring the number and prominence of prosocial emotions selected. Table 7-1 below shows those emotions from the full list of 45 available to participants designated as positive and/or prosocial for this calculation.

Positive		Prosocial	
Confident	Vigorous	Confident	Trusting
Secure	Proud	Secure	Ashamed
Surprised	Triumphant	Cared-For	Guilty
Cared-For	Grateful	Friendly	Embarrassed
Friendly	Respectful	Welcomed	Humiliated
Welcomed	Admiring	Grateful	Dishonored
Powerful	Trusting	Respectful	
Energetic	Happy	Admiring	

Table 7-1: Emotions designated "positive" and "prosocial" in our study for the purposes of calculating emotion scores.

For each emotion score, if participants chose an emotion that is included on the respective list in Table 7-1, that score would be increased by a reverse weight of the rank. For example, if a participant included a positive emotion as the strongest emotion they would feel, then 5 points would be added to their Valence score, but if they ranked the same emotion as the second strongest they would feel, only 4 is added to the Valence score. If they ranked a positive emotion as the third strongest, 3 would be added, and so on. The same procedure was used for Prosocial scores using the emotions in the list of Prosocial emotions above.

Finally, behavior was assessed through a single multiple-choice instrument that directly asked if the participant had changed their behavior around their groups target advice since the last time they reported their behavior (i.e., the last complete survey response they provided). If they reported a behavior change, participants were then asked to provide an open-ended explanation as to what motived the change. This method of behavior change collection was selected due to the diversity of advice chosen and to make it safest and easiest for participants to take part in the study. Though means could have been devised to gather hard data on whether participants started following each behavior, doing so would have been much more privacy endangering due to the access the researchers would need to their computer systems. Such methods may have also biased our sample since some privacy conscious individuals may be dissuaded from participating due to the invasive nature of the methods. Additionally, each advice would require a different method of data gathering, which may also have to be tailored for different operating systems and device profiles (e.g., smartphones, PCs), introducing numerous logistical issues. Instead, the more convenient, single instrument described was used, with participants also providing more detail about the change to make it harder for them to misreport due to bias or mistake.

These instruments were arranged in the order described for each advice's assessment survey. The instruments for each survey can be found in Appendix E. Surveys were delivered to participants a total of 4 times through the study, across two stages to gather multiple snapshots of participants' perceptions and behavior throughout the study.

7.2.3 Study Procedures

To allow for the most diverse population possible, the survey was administered remotely through the web-service Mechanical Turk (MTurk). We used a screening procedure to collect a large initial sample that was then used to randomly fill unique groups of participants. The screening survey was short, only asking basic demographic information and for the participant to report whether they follow each of the study's 3 target advice. This survey on MTurk was open to users 18 years of age or older who lived in the United States. For each video, groups of 30 were assembled based on their eligibility as ascertained through their screening data. An additional group of 30 was created for each advice and designated the Control group, who would view no video, but still respond to the assessment survey at each stage of the study. Participants were considered eligible for a group if they reported not following their group's target advice on their screening survey. Random eligible participants were assigned to the groups in the study such that the resulting groups were all unique. If a participant contacted did not respond to our survey in a timely manner, another eligible participant was selected and contacted from the screening sample. To avoid bias in the analysis, participants who reported changing their behavior from the screening survey before the intervention stage were not considered in the final samples. Final sample sizes for each group were all in the 24-30 range.[8] These samples of participants were then contacted across the two stages of the study.

In the first stage, participants were delivered the assessment survey, then, for all groups except one, the participants were asked to watch their group's video. For the Control groups, this stage ended after a complete response was received to the initial assessment survey. For the groups that received an intervention, after viewing the video, participants were allowed to proceed to the post-intervention survey, which had all the same instruments as the assessment survey minus the behavior question since behavior could not logically change in the short time of viewing the video. All participants were compensated $4 for their complete response at this stage.

The second stage took place over the month after participants were initially delivered their group's intervention (or in the case of Control participants, after they responded to the initial assessment survey). At two weeks and one month after the delivery of each intervention, each participant was contacted with their advice's assessment survey. For complete responses to each additional assessment survey, participants were compensated $2.

[8] Update: Control = 29; Basic = 24; Emotion = 26; Social = 24
2FA: Control = 26;Basic = 29; Emotion = 29; Social = 26
Pass. Manager: Control = 30; Basic = 30; Emotion = 30; Social = 28

7.3 Hypotheses of Video Impact

Using the data gathered as described above, we can assess the impact of the videos on each variable, with particular focus on how the videos that incorporates the alternative approaches to persuasion (i.e., emotional inoculation and social motivations) compared to the Basic videos and Control groups. To guide our analysis, hypotheses were developed based on the results of prior work and intuition. Hypotheses are based around how changes will be observed in each group across the steps and stages of the study on the scores described in the prior section. Changes in scores will be discussed relative to whether the change reflects higher propensity for the groups to adopt the target advice. This is intuitive in some cases, such as behavior, where we will look for higher rates of participants reporting following their target advice. For others, more specific definitions are needed to describe "changes towards following."

For example, for the awareness instruments, a change towards them following would be an increase in awareness scores since, according to prior work [51] those who better understand the contexts of cybersecurity advice are more likely to adopt. Similarly to behavior, in case of perceptions, a change towards following would be intuitively represented by an increase in the motivation to follow and/or a decrease in motivation to not follow. For emotions, an increase in either or both the valence and prosocial scores is considered a change towards following since, according to prior work on emotions and motivations [16,76], and the results in prior Chapters, individuals are more likely to take up a behavior if they view it in a positive light, and even more so if they feel a social motivation to adhere, as would be represented in a high prosocial score.

Hypothesis 1 (Hypo1): We expect the groups which see the videos that incorporate emotional inoculation concepts to have strong impacts on emotions scores relative to other video groups. Additionally, based on the results of prior work [35,53,54,60,98], we anticipate changes observed in the groups which see an Emotion video to be longest lasting relative to other video groups on all variables.

Hypothesis 2 (Hypo2): We expect the groups which see the videos that incorporate social appeals to have strong impacts on scores related to social aspects (i.e., social motivations to follow and not follow, prosocial score) relative to other video groups. Based on prior work [91,95,104], we also anticipate that the Social videos will outperform the Basic videos, but it is unknown how they will compare to the Emotion videos overall.

7.4 Evaluation of Score Changes

To see the differences over time in the scores calculated based on the data collected from participants, each variable score's mean value is plotted in the subsequent figures at each stage of the study, for each group. Referring back to the hypotheses, we will go through the results seen in those plots, and discuss the key statistical significance of differences using two non-parametric tests: Mann-Whitney U-Tests [65] and Sign Tests [26].[9] In both cases, since the sample sizes are not exceedingly large, exact calculations of these tests are used.

Mann-Whitney U-Tests will be used to assign significance to differences observed on a variable *at* a single stage, *between* the Control group and one of the video groups. As a reminder, Mann-Whitney U-Tests measure if one distribution is greater than the other through

[9] The full results for both forms of statistical testing used in this Chapter are presented in Appendix E.

the calculation of a rank-sum of random comparisons of cases from each group. More detail on the Mann-Whitney U-Test can be found in prior literature [65].

Sign Tests will be used to assign significance to differences seen between post-intervention scores (i.e., those calculated based on data collected immediately after the intervention, 2 weeks from the intervention, or 1 month from the intervention) and the scores calculated from participant's data right before they watched their group's intervention video. Sign Tests are similar to Mann-Whitney U-Tests, but rather than comparing the distribution of two samples, Sign Tests assess the degree to which values in one set are higher than values in another. Thus, the test can be used to compare repeated measures from the same participants, as is being done here. More details on Sign Tests can also be found in the literature [26].

7.4.1 Awareness

Figure 7-1 shows the plots for both awareness scores, for all groups that were gathered for this study.

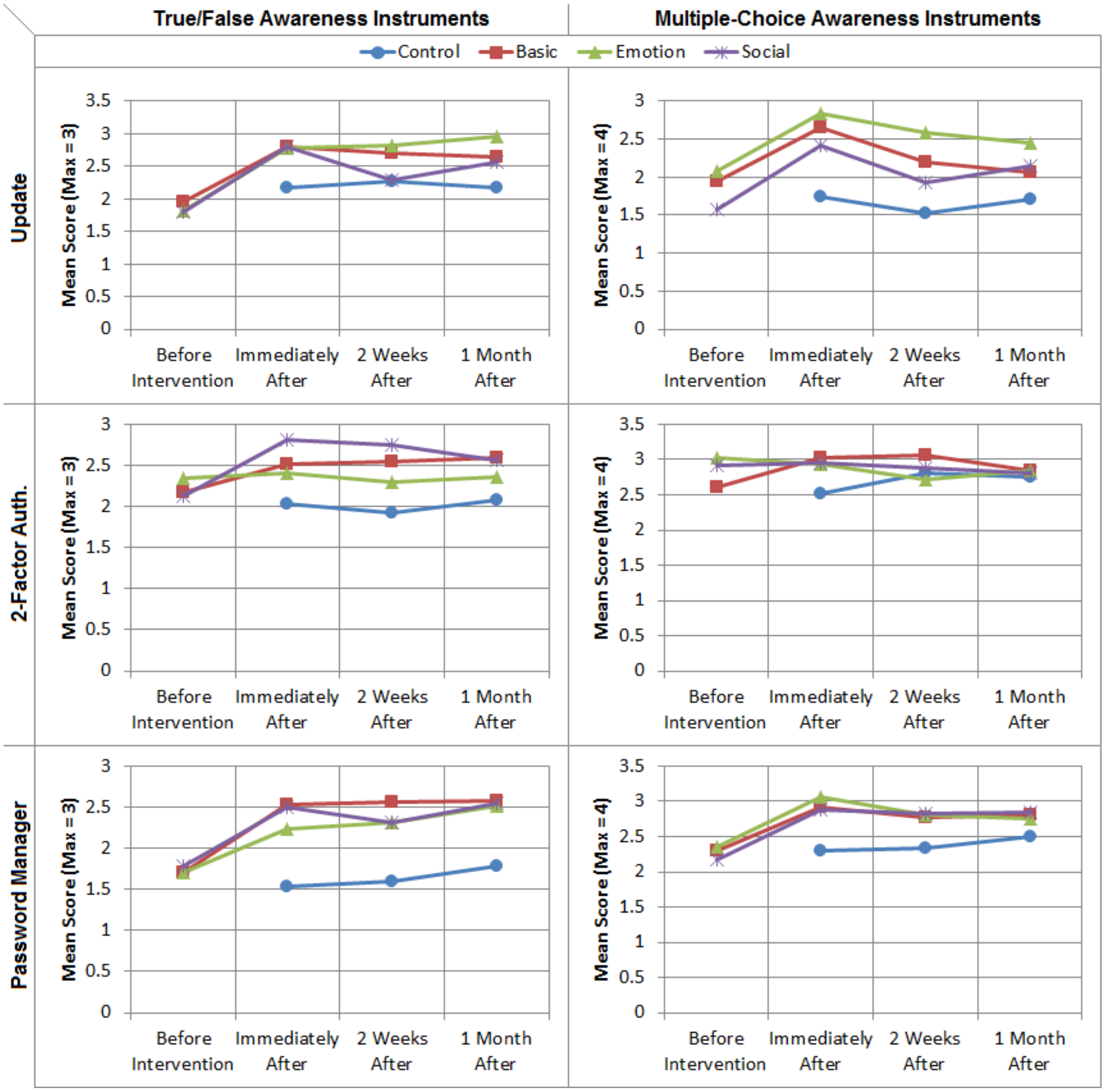


Figure 7-1: Mean values for both awareness scores for each group, plotted at each stage of the study.

The Update groups had the most pronounced awareness shift across both scores, according to testing. All video groups had significantly higher scores than the Control for both awareness measures immediately after the intervention ($\forall, p \leq 0.017$). Sign Testing confirms that these post-intervention scores are also significantly greater than the scores collected from

Update video group participants before viewing their respective video ($\forall, p \leq 0.007$). Despite these apparent immediate gains, only the Emotion group had the changes stay consistently significant over the follow-up period. Both scores were significantly different for this group compared to the Control at the first and second follow-ups ($\forall, p \leq 0.048$). Sign Tests showed that the true/false score differences were significantly different at each follow-up stage compared to pre-intervention scores ($\forall, p \leq 0.004$), but the multiple-choice scores did not test significant.

Groups targeted at use of a password manager also all had strong changes, but not as consistently at the follow-ups as the Update groups. According to Mann-Whitney U-Tests, the true/false awareness scores, at all stages were significantly higher than the Control ($\forall, p \leq 0.017$), which was supported by Sign tests comparing the true/false scores for each Password Manager group at each stage with participants' pre-intervention scores ($\forall, p \leq 0.041$). The Password Manager groups also had significant increases for the multiple-choice score immediately after the intervention, but these differences were generally not very strong (*For Basic and Social,* $0.03 \leq p \leq 0.08$), except for the Emotion group ($p = 0.003$). At the follow-up stages, for the multiple-choice scores, the Basic and Social group's scores were significantly greater at 2-weeks (*Basic* $p = 0.031$, *Social* $p = 0.019$), but not 1 month after the intervention. For using a password manager, the Emotion group had no significant differences compared to the Control at either follow-up stage. Sign testing of the Password Manager groups data agreed with these U-Test results.

Looking to 2FA, the true/false scores were greater than the Controls at each stage for Basic and Social groups ($\forall, p \leq 0.04$), but not the Emotion group. Sign Tests found that the changes for all 2FA groups were not significantly higher than the participants' pre-intervention responses, though, except for the Social group, which was significant at each stage ($p < 0.001$ *@*

immediately after, p < 0.001 @ 2 weeks, p = 0.021 @ 1 month). Tests found no significant changes in multiple-choice awareness scores for 2FA groups.

Thus, most video groups saw the true/false scores increase after intervention and continue to remain higher through the follow-ups. A notable exception was the Emotion group for 2FA. Changes were less consistent for the multiple-choice scores, whose instruments focused on deeper and more difficult aspects of the advice than the true/false instruments, possibly accounting for this discrepancy in performance. Awareness is only part of motivation overall, though, so the other variables must be explored to see other possible impacts of the videos.

7.4.2 Perceptions

Figure 7-2 shows a plot of all 4 motivation scores calculated from the perceptions data collected from participants. As a reminder, these scores are the *Individual Motivation to Follow* (INDF), the *Social Motivation to Follow* (SOCF), the *Individual Motivation to Not Follow* (INDN), and the *Social Motivation to Not Follow* (SOCN). How each of these scores is calculated can be found in Section 6.1.3 of this Chapter. Please note that, in the plots, the *Motivation to Follow* scores are plotted with solid lines, while the *Motivation to Not Follow* scores are plotted with dotted lines.

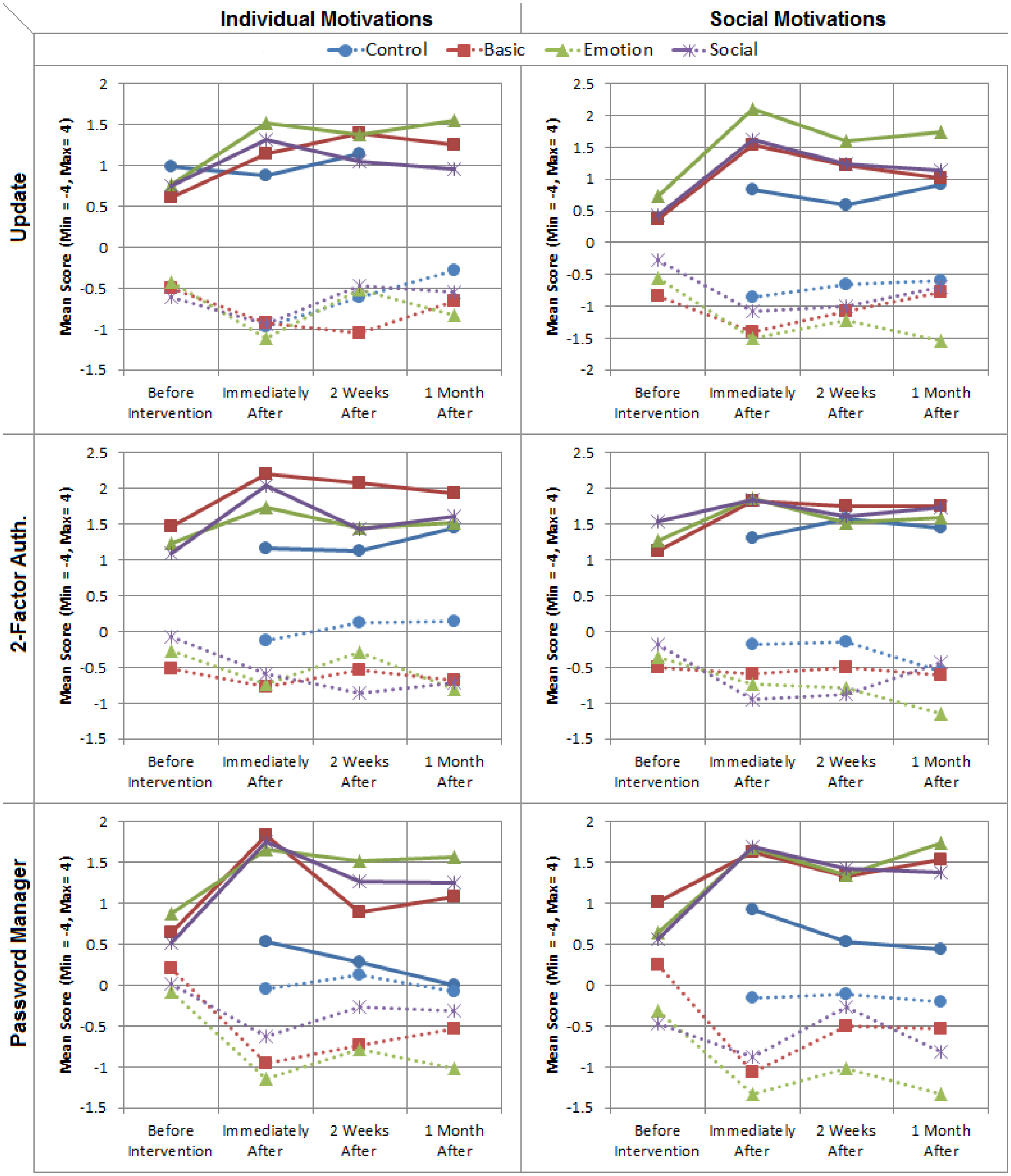


Figure 7-2: Mean values for all scores calculated from the perception data gathered from participants plotted for each stage of the study. Note: Each plot shows the Motivation to Follow (solid line) and Motivation to Not Follow (dotted line) for both the Individual and Social vector.

Statistical testing comparing the differences between each video group with the Control groups seen in Table 7-2 helps identify the strongest trends in the changes seen through the study. In the case of updating and using a password manager, the Emotion groups, according to Mann-Whitney U-Tests had the strongest and most consistent results compared to the Controls. For 2FA, though changes were not as significant as for the other two advices, results of the Emotion group proved interesting. For the Password Manager Emotion group, for all scores at the post-intervention and both follow-ups, except for SOCF at the first follow-up, differences between this group's scores and the Controls' were significantly greater (*∀ except SOCF @ 2 weeks,* $0.001 \leq p \leq 0.011$).

The results for the Update Emotion group are similar, but not as consistent as with the Password Manager group. Immediately after the intervention three scores tested significantly greater for the Emotion group (*INDF* $p = 0.024$, *SOCF* $p < 0.001$, *SOCN* $p = 0.015$). At follow-up points, the *Social Motivation to Follow* (SOCF) continued to be significant at both 2 weeks ($p = 0.005$) and 1 month ($p = 0.009$), and the *Social Motivation to Not Follow* (SOCN) tested significantly greater than the Control at the one month mark ($p = 0.004$), but not at 2 weeks. The 2FA Emotion group only had a slightly significant difference for one score at the intervention stage: SOCF ($p = 0.044$). Interestingly, though they were not different than the Control at other stages, both *Motivation to Not Follow* scores from the Emotion group did test significantly different at the follow-up one month from the intervention (*INDN* $p = 0.009$, *SOCN* $p = 0.043$). In all, according to comparisons of the video groups with the Control groups, it would seem that those who saw emotionally aware videos had interesting changes in perceptions, particularly by the second follow-up, where these were generally the only groups to still see any differences.

For other video groups, though the Basic and Social groups did commonly have significant changes immediately after the intervention. For the Password Manager Basic and Social groups, the initial changes immediately after the intervention were significant ($\forall, 0.001 \leq p \leq 0.043$), while two scores tested significantly greater for the Update Basic group (*SOCF* $p = 0.028$, *SOCN* $p = 0.039$), and one score for the Update Social group (*SOCF* $p = 0.007$) at the same stage. Unlike the Emotion groups, at follow-ups, these changes were inconsistent for Password Manager and Update Basic and Social groups.[10] A notable aspect of these perception scores results for these two advices is the Social groups' lack of consistent and strong change on social motivation scores, which is somewhat counterintuitive.

Unlike these two advices, though, the 2FA Social group did garner interesting results. Immediately after the intervention, the 2FA Social group had significantly different scores from the Control for both the *Social Motivation to Follow* and *Not Follow* (*SOCF* $p = 0.017$, *SOCN* $p = 0.039$), but differences in the Individual Motivation scores did not test significant. Only one of these held in significance at the first follow-up (*SOCN* $p = 0.028$), but the *Individual Motivation to Not Follow* score was also different for the 2FA Social group at this stage ($p = 0.043$). For 2FA, at least right after the intervention, it seems the Social video may have had the intended impact on social scores. More notable than the 2FA Social group changes are the 2FA Basic group changes. This group had significant differences for these Individual Motivation scores (*INDF* $p = 0.028$, *INDN* $p = 0.034$), but no significance for the differences in the Social Motivation scores. At the first follow-up, these scores continued to be significantly different, as

[10] According to statistical testing of the follow-up data, only one score for the Password Manager Basic group had changes that tested consistently significant at both follow-ups (INDF @ 2 weeks $p = 0.035$, INDF @ 1 month $p = 0.008$). Otherwise, only one score for each the Password Manager Social (SOCF $p = 0.03$) and Basic (INDN $p = 0.048$) group tested significantly different at the first follow-up, and only one other score for the Password Manager Social group tested significantly different at the second follow-up (SOCN $p = 0.022$). Update Basic and Social groups had no significant differences at either follow-up.

well as one of the social score (*INDF* $p = 0.002$, *INDN* $p = 0.035$, *SOCN* $p = 0.041$). By the second follow-up, only INDN for the 2FA Basic group still tested significantly different compared to the Control ($p = 0.019$). Thus, unlike Emotion groups for other advice, the 2FA Basic group changes were not consistently significant across follow-ups, which was also the case for the 2FA Social group, despite strong initial change for social perception scores. To help sift through these mixed results, another test will look at the data from another perspective.

The results of Sign testing mirrored these findings from Mann-Whitney U-Testing. For two advices, updating and using a password manager, the Emotion groups had significant differences between results received before the intervention to immediately after for all scores calculated (*Update,* $\forall, p \leq 0.001$, *Pass. Man.,* $\forall, p \leq 0.013$). By 2 weeks after the intervention, both significant differences on 3 of the 4 scores compared to scores from before the intervention. For updating, all scores but the *Individual Motivation to Not Follow* score were still significantly greater ($\forall, p \leq 0.013$). For using a password manager, all but the *Social Motivation to Follow* score were still significantly higher ($\forall, p \leq 0.035$). At one month, 3 scores for the Update Emotion group were still significantly greater than before the intervention ($\forall$ *but INDN,* $p \leq 0.019$), while all 4 scores for the Password Manager Emotion group were now significantly greater than before the intervention ($\forall, p \leq 0.012$).

As before, the 2FA Emotion groups' scores were not as consistently changed as the two groups just discussed. Neither were differences in scores for other videos for all advice. Though several videos had strong differences in scores from before intervention to immediately after, such as the Password Manager ($\forall$ *scores,* $p \leq 0.009$) and Update ($\forall$ *but INDN,* $p \leq 0.031$) Basic groups, as well as the 2FA ($\forall$ *but SOCF,* $p \leq 0.027$) and Password Manager ($\forall$ *but SOCN,* $p \leq 0.035$) Social groups, none of these groups had more than one or two scores still test significantly different at each follow-up checkpoint. Thus, the Emotion groups for updating and using a password manager were the only in the study to see extended change in the perception scores calculated. Also like before, the Social groups saw scores return to pre-intervention levels more quickly, and social scores were still not significantly raised, even at stages when individual scores were.

The main take-away from these perception results is the strong changes seen for Emotion groups across the study for 2 advices, which contrasts with other video groups for all advice that may have had strong changes immediately after the interventions, but limited changes by the follow-up data collections. Rational perceptions, as seen in prior Chapters, are only part of the picture around motivations, and so other variables measured must be examined to understand how the videos may have impacted emotions.

7.4.3 Emotions

Two scores were extracted from the ranking of the top 5 emotions participants report they would feel adhering to their group's target advice. One measures how many positive emotions the participant selects, as well as how prominently those positive emotions are placed in the ranking. The second score does the same, but for prosocial emotions rather than positive emotions. Figure 7-3 shows the plots of the means for these scores, calculated for the data at each stage of the study, for each group.

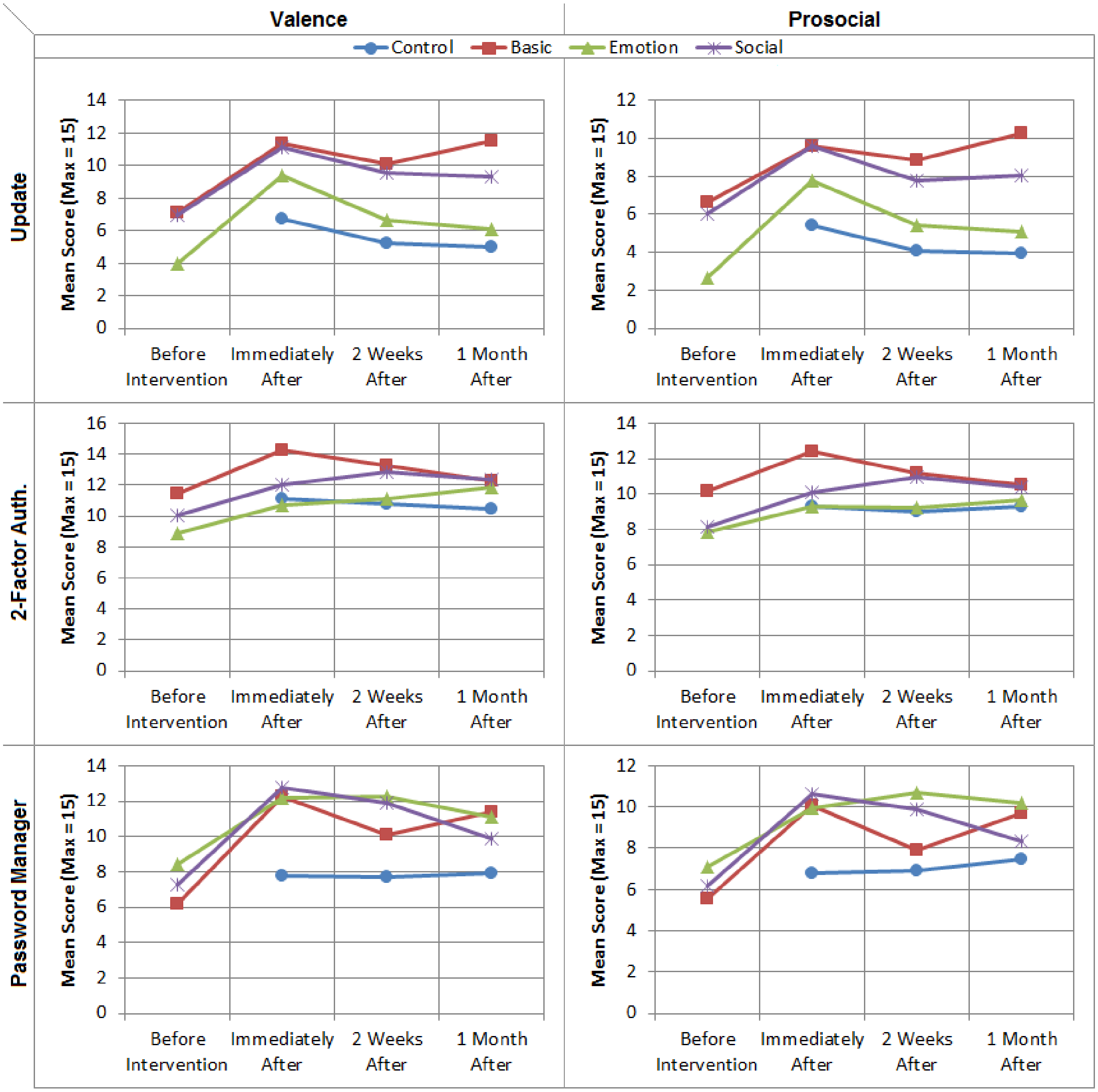


Figure 7-3: Mean Valence (i.e., positive/negative) and Prosocial scores plotted for each group, at each stage of the study calculated based on participants' ranking of emotions they anticipate feeling while following their group's target advice.

As can be seen in the figure, changes in scores were different across all three advices. Notably, the Password Manager Emotion group had the largest and most consistent changes on both scores for all videos, while the Update video groups all did well except the Emotion. The 2FA video groups exhibited little change on these scores.

Statistical testing confirms these conclusions. For the Password Manager Emotion group, the differences of both scores with the Control group were strongly significant at all stages except the Prosocial score at the second follow-up ($\forall$ *except Prosocial @ 1 month*, $0.001 \leq p \leq 0.036$). The scores from this group immediately after and 2 weeks after the intervention were also found to be significantly greater than the scores garnered by the same participants before the video ($\forall$, $0.001 \leq p \leq 0.043$). The other Password Manager groups had strong differences compared to the Control immediately after the intervention ($\forall$, $0.001 \leq p \leq 0.011$), but only the Valence score for the Social group's first follow-up ($p = 0.004$) and the Basic group's second follow-up ($p = 0.013$) were still significant in that stage of the study. Sign Test results for these two video groups was similar, with both scores testing significantly different immediate after the interventions for both groups ($\forall$, $p \leq 0.009$). The Basic group had Valence scores that were significantly greater at both follow-ups ($p = 0.001$ *@ both*), but only the first follow-up was significant for this score ($p = 0.001$). Both scores were also significantly greater at the first follow-up compared to before the intervention for the Password Manager Emotion group (*Valence* $p = 0.027$, *Prosocial* $p = 0.015$).

Similarly, the Update Basic and Social groups both had significantly higher scores compared with the Control at each stage after the intervention ($\forall$, $p \leq 0.034$), but none of the differences were significant for the Emotion group. The results of Sign Tests found that only the differences in these scores immediately after the intervention were consistently significantly greater than the scores the same participants gave before, but this was the case for all three video groups ($\forall$, $p \leq 0.035$).

For the 2FA groups, only one group at one stage had scores that were significantly different from the Control groups'. This was the Basic group immediately after the intervention

(*Valence p = 0.006*, *Prosocial p = 0.015*). These results are reminiscent of the 2FA perception score changes for video groups, which was also the lowest of all three advices. Interestingly, the groups targeting updating and using a password manager had significant changes on emotion scores at several stages through the study, much like groups for these advices did on perception scores. Unlike the perception scores, though, the significant changes were most consistent for Basic and Social groups, whereas the Emotion groups had the most consistent changes on perceptions. The results, for the respective videos, may reflect changes impacted in participants that could lead them to a behavior change towards following their groups target advice sometime in the future. Our study also measured changes in behavior *during* the execution of the study to see rates of behavior change, at least for the first month after intervention.

7.4.4 Behavior

Behavior was measured in our study using two survey instruments, one which asked the participant to report if they had changed behavior. This includes changes towards or away following their groups' target advice. Figure 7-4 shows the frequency of those who reported a change in each group of the study.

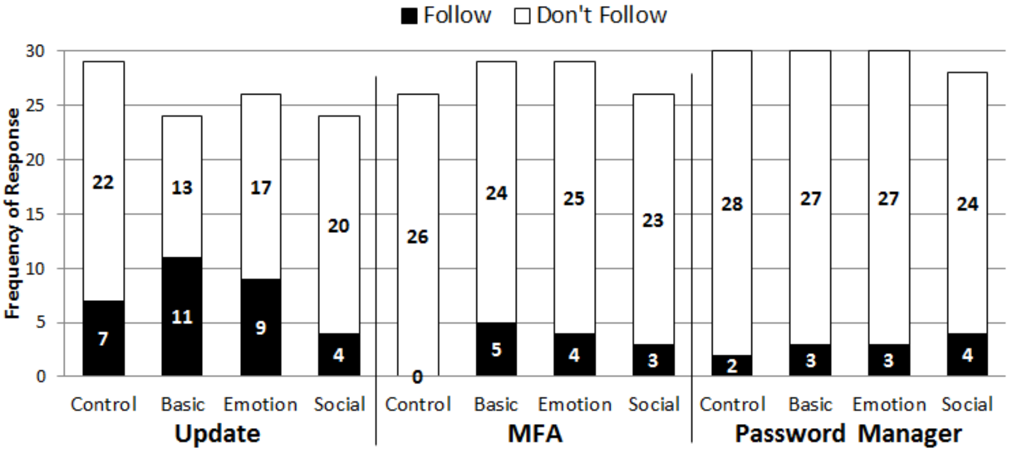


Figure 7-4: Frequency of participants who reported beginning to follow their group's target advice sometime during the study and continued to follow by the end.

As seen in the figure, the advice which saw the most participants begin to follow by the end of the study was updating regularly, where 31 of 103 participants across all groups, including the Control[11] reported a change towards updating without reporting in a subsequent survey that they had stopped. The other advice saw lower rates of adoption across all groups.

Interestingly, for two of the three advices, the Basic video has the largest number of participants report a change after viewing, though these rates are closely followed by the Emotion groups in each case. For the Password Manager, all videos performed similarly in terms of behavior change, but not significantly differently than change seen in that advice' Control. Using Chi-Squared tests to assess differences in the number of participant who report a change by the end of the study across groups within each advice yielded no significant results. This suggests that though some video groups had nominally higher reports of positive behavior change by the end of the study, these results are statistically significant.

7.5 Discussion of Results

Though prior work has expressed and shown the power of emotionally and socially aware appeals towards human behavior in other fields [35,53,54,60,91,95,98,104], work leveraging these concepts for cybersecurity behavior is limited [24]. To address this literature gap, this thesis explored the motivations users have around multiple security advices in order to design informed interventions that utilize these novel-for-the-field concepts and aim to encourage user adoption of secure behavior.

The results discussed in the previous section provide insight into the viability of these concepts towards this goal. First, we look to the behavior results with additional context

[11] Among groups that saw a video, overall, 24 of 74 (32%) participants reported a change that was sustained until the end of the study.

provided by the qualitative data collected. Then, the results of each experimental intervention approach will be discussed, with comparisons to prior work included where applicable.

7.5.1 Digging into Behavior Change

To better understand these trends in behavior reported by participants, the qualitative data collected from those who reported a change was analyzed. If a participant reported an alteration in behavior on a survey, they were asked to explain why they decided to, using an open-ended qualitative instrument. These responses were coded by one researcher, with the codes being reviewed and approved by another. An initial codebook that contained the codes of “security” and “convenience” was used to begin the coding process for data for each advice. In each case, specific codes were developed inductively to better capture the comments than the two initial codes code. These codes differed between advices, but similarities in final codebooks were shared. A total of 17 codes were developed for Update group comments, 11 for 2FA, and 7 for Password Manager comments. Table 7-2 shows the top codes for each advice, as well as the number of comments from each group that was assigned each code.

Advice	**Code**	**Code Assignment Counts**			
		Control	*Basic*	*Emotion*	*Social*
Update	***Security***	3	11	6	2
	It’s important	-	3	2	-
	Inspired by our survey	-	2	3	-
	Prompted to update/Noticed an update was needed	2	1	2	-
2FA	***Security***	1	4	5	2
	Have more knowledge	-	2	1	-
Pass. Man.	***Security***	1	3	2	1
	Convenience	1	1	1	2
	Have more knowledge	-	1	1	1

Table 7-2: Top codes assigned to comments from participants in each group along with the frequency of each codes’ assignment.

Security, one of the initial codes used in the codebook for each advice, was also the top code assigned to comments for all of them. Even many Control participants, who saw no video, but nonetheless ended up changing through the study, cited this as their motivation, showing the importance of security to users. This follows from other studies, particularly those which aimed to alter individuals' behavior around cybersecurity advice. For example, in the case of app permissions on Android, the researchers found that personalizing risk was effective in making users take more care in their decisions [42]. Arguably, this change was driven by users' innate desire for security that is also reflected in the fact that even many Control participants reported altering behavior in this Chapter's study due to a desire for security. Relatedly, convenience was a common code for one advice, using a password manager, which is expected considering the findings of Chapters 3 and 4. In all, the centrality of security and convenience in the qualitative data is not surprising based on the findings of all the prior Chapters and these concepts' prominent track in the literature [46,47,86,92,103].

Patterns on other codes prove more telling. Several Update participants were inspired to change behavior, in their own words, due to our survey/video. One participant from each the 2FA and Password Manager groups also citied our survey/video as their motivation, but even more participants from these two groups cited having more knowledge or information as the reason of their decision change. These findings follow from prior work that found correlation between behavior change around 2FA after an informational video and participants' ratings of how interesting and useful they found the video [4]. The C-HIP model puts emphasis on the necessity of messages to conform with or address gaps in receivers' attitudes and beliefs. It's possible that the connection between *informativeness* and usefulness seen in this Chapters' data and the prior work may be the participants having the messages connect with and/or change their attitudes and beliefs, which they communicate as the videos being “informative” or “useful.”

Looking to the Update groups, some here mention an update prompt or noticing an update being available in their reason for changing their behavior. Though not shown in the table, two 2FA participants who changed their behavior said they did so, at least in part, due to a new account prompting them to activate the feature. These results show the possible power the messaging contained in the videos tested, particularly if utilized in a larger and more robust intervention campaign. A necessary stage of the C-HIP model is gathering the receivers’ attention. Though this study did as much as possible to make sure participants’ viewed their video, it’s possible that some paid limited attention while viewing or had their mind wander during some parts of the video. It is on this front that more regular delivery and maintenance of the message contained in these videos may reap gains. If users are presented these messages on multiple occasions, or reminded of the core content in the future, more may adopt the advice being targeted since the likelihood of getting their attention with well-designed and tuned messages is higher.

One final observation of the results in Table 7-2, the Basic and Emotion groups were more likely to mention security in their comments than the Control and Social groups. This was the case for all three advices, even the Password Manager groups, where the Social group reported the most behavior change of any of this advice’s groups. The Social groups’ overall lack of thinking around security in their comments could be a clue as to why the Social groups had the lowest rates of reported behavior change. Those who did not report a change may also not be thinking about security, which is a key motivator to adopt the advice tested. This finding is not the only notable changes for groups that saw the experimental videos. Both the emotional inoculation and social motivation approaches had results that show the importance of each in the motivations of users around cybersecurity advice.

7.5.2 Using Emotional Inoculation

As explained in Chapter 2, emotions have been long theorized to have important influence on human decision-making. Knowing this, some researchers have attempted to harness this fact in approaches to communication and persuasion. One such attempt is emotional inoculation. As described earlier in this Chapter, the goal of emotional inoculation is to reduce the propensity of individuals to feel emotions that hinder their adoption of a behavior, while increasing instances of emotions that encourage adoption.

In prior work, emotional inoculation has been shown to have stronger and longer lasting impacts on individuals than traditional forms of communication [35], which is what inspired the proposition in Hypothesis 1. Looking to the data, our results support these prior findings and this Hypothesis. For the Update and Password Manager groups, the participants who saw the videos which incorporated emotional inoculation had increases on many scores that continued to remain significantly higher during the follow-up stages. This was particularly the case at the extended follow-up (i.e., 1 month from intervention), where the Emotion groups had significant differences while groups that saw other videos did not, even for 2FA, which was the advice with the least amount of score change overall.

Looking to the emotion score results in particular, part of Hypothesis 1 is not supported in the data. On emotion scores, the Emotion groups sometimes had *lower* changes in Valence and/or Prosocial scores than the other video groups relative to the Controls. It should be noted that most of these same groups did exhibit significant results on Sign Test comparing *within* group increases in the scores. Thus, though changes relative to the Controls were not significant according to U-Tests, scores were significantly higher when compared with responses from the same group before and after the intervention. Improvement of emotion scores in anyway can help encourage adoption, so these results show mixed performance on change in emotion scores due to the videos.

Though emotion scores did not move as expected, looking at this data in another way helps us understand how emotions are involved in cybersecurity decision making, as suggested by prior work on motivations broadly [14,16]. Based on the existing theory, it is expected that those who feel more positive and prosocial emotions when considering the advice would be more likely to adopt that advice. To see trends in the changes in scores for participants that did not change their behavior by the end of the study with those that did, exact Sign Tests were performed to compare the differences in Emotion scores participants garnered before their intervention with each collection point after. Rather than separating the data by video group, as in the prior Sign Tests, here, participants were placed in one of two groups for each advice: those who reported following by the end, and those who reported not following. One advice had interesting results with this line of analysis: updating.

For both the Valence and Prosocial scores, participants in both of these new groups had significantly higher ($p \leq 0.001$) score immediately after the intervention compared to just before. Interestingly, only the sample of participants who changed their behavior towards updating by the end of the study reported significantly higher Prosocial scores at both follow-ups (*$p = 0.002$ @ 2 weeks, $p = 0.004$ @ 1 month*), and moderately higher Valence scores, but only at the one month check-in ($p = 0.035$). It could be that these increased positive and prosocial emotions individuals are reporting to still feel at follow-ups around updating are contributing to their collective decisions to begin updating. Conversely, the lack of sustained changed in emotional outlook of participants around updating could indicate that the appeals were not as powerful as would first appear when only looking immediately after then intervention. This offers a possible partial explanation for why more participants did not change their behavior. One final note on these emotion findings is the increase in Prosocial scores among those who started updating, which follows on prior work demonstrating the power of such emotions [76], and social motivations more generally [95].

7.5.3 Highlighting Social Motivations

Though emotional inoculation has been demonstrated as an effective communication method in other fields, this thesis presents the first investigation of harnessing this technique towards motivating cybersecurity advice adoption. Social motivation, on the other hand, has been attempted by some studies when it comes to cybersecurity. One notable work here found that Facebook notification with social cues were *not* more likely to promote good security behavior than prompts that lacked such cues [24], suggesting difficulty in harnessing these motivations in the computer domain. Our results tell a similar story.

Though deep analysis of those who began updating by the end of the study showed possible power in prosocial emotions, participants who saw Social videos generally did not have prominent nor sustained changes on scores through the study. Neither proposition in Hypothesis 2 was supported by the results, with the Social videos not outperforming the Basic videos, as predicted.

These results should not discount the importance of social motivations around computer security advice in the mind of the reader. Similar to the sustained increase in Prosocial scores seen for those who began updating by the end of the study, these same Sign Tests (i.e., for those who follow each advice, and those who do not) were run for the other scores. For those who reported updating by the end of the study, scores of the *Social Motivation to Follow* were both significantly higher ($p = 0.001$) at both follow-up check-points, while other perception variables did not see similar significant differences for this group at these stages. Like with the Prosocial score result, these findings could reflect a strong and unique connection between social motivations to adhere to these advices and the likelihood that an individual will choose to change their behavior since this one social score was the only of all perception scores to be significantly higher at the follow-up stages.

7.6 Summary

Though behavior change was not as strong as would be hoped based on the expected and demonstrated power of emotional inoculation and social motivations towards increasing adoption of good, but otherwise neglected behavior, the sustained significant changes in other variables measured for the Emotion groups demonstrate the applicability of emotional inoculation towards cybersecurity advice. Since these scores represent key pillars of motivation, as argued by models of human motivation and communication [14,16,21,95], sustained and significant increases in them for those who view the videos tested here is the first step towards behavior change. Thus, future researchers would benefit from taking the lead from these findings and exploring how to adapt emotional inoculation to be more effective on behavior directly, possibly through the expansion to repeated messaging campaigns that remind users of the content presented just once in this study.

The results presented here also help demonstrate the importance of emotions and notably social motivations towards behavior change around cybersecurity. For participants who reported updating by the end of the study, at both follow-ups, Prosocial and *Social Motivation to Follow* scores were all found to be significantly higher than the scores given by participants before the intervention. These findings stand out since other perception scores did not exhibit this pattern for this group, and the Valence score did not exhibit the pattern nearly as strongly as the Prosocial score. It should be noted that these results were not repeated for the other two advice tested in this study, but it is possible this is a feature of the lower number of those who reported using 2FA (N = 12) or a password manager (N = 12) compared to updating (N = 31) by the end of the study. As such, more work into the interplay between emotions, social motivations, and behavior around cybersecurity is called for, with the findings here advancing our understanding of these relationships.

8 Conclusion

Cybersecurity is an increasingly important issue in our society. Though many value security and experts call for increases in it, significant portions of users have failed to adopt basic security advice given by these experts. Updating software, using two-factor authentication, and using a secure password manager are among the numerous behaviors or tools users can adopt to increase their cybersecurity. Understanding why some take these advices up while other do not is an important first steps towards impacting change in their behavior. Thus, the first several studies presented explored users' motivations around various security advices.

Recalling from Chapter 1, the first research question of this thesis sought to understand how different cybersecurity decisions compare and contrast in users' considerations. The studies presented that looked into users' motivations generated many findings, including that some advices, such as using a password manager come with added convenience that users appreciate, while others, such as using 2FA or updating are inconvenient for users, and they know it. Despite these differences, the dominance of security vs. convenience was apparent overall, showing the balances that users, who sometimes lack technical knowledge, must make. The importance of past experiences was also found for several advices, such as 2FA and updating.

The second research question asked how adopters and non-adopters of cybersecurity behavior differ in their perceptions, across all three advices. Perception gaps were found that may explain why users make the decisions they do. As some argue, non-followers could just see less benefit and more risk/cost in adopting, at least currently. The comparison of users and non-users of password managers was particularly telling, with non-users worrying about the security of password managers in general. On the other hand, users say they use the tool primarily for the additional convenience, showing the complexity in how people think about security issues. Related to 2FA, differences in perceptions of the technique were most apparent for different users of 2FA than between users and non-users of the feature. Additionally, many non-users reported having never heard of 2FA before taking our survey, showing a possible unique awareness gap for this advice.

Emotions related to these advices were the focus of the third research question, a topic broached in the studies presented in Chapter 4, 5, and 6. In the case of updating, annoyance and confusion were prominent in survey. Deep analysis of targeted data also revealed factors of variance that centered on emotional valence in response to update messages, suggesting some have positive reactions, while others have negative ones. For password managers, users and non-users differed mostly in their emotions around their ratings of suspicion and security of the tool, revealing the deep rift caused by perceptions of insecurity associated with password managers. Two-factor authentication offered another perspective, where the divide between users and non-users was more centered on having heard of the tool and thoughts on how convenient it is to use rather than perceptions about the security of the tool.

Social motivations, the focus of the fourth research question, were also studied. The studies that explored existing motivations found a lack of social considerations, but analysis of the data in the final study found potential power in social motivations towards behavior change. Specifically, when comparing those who followed their groups' target advice by the end of the study to those who did not, the only score that was consistently higher at both follow-ups for those who started following was the *Social Motivation to Follow*. Though interventions had mixed results for the application of social motivations towards encouraging good security behavior, this area remains ripe for future work.

The final research question of this thesis asked how the application of emotionally and socially aware persuasion concepts would perform in altering perceptions and/or behavior around cybersecurity. Chapter 7 discusses a study into just this, finding mixed results for social appeals, but evidence for the applicability of emotional inoculation in the realm of cybersecurity. For key perceptions related to motivation to adhere to some of the advice tested, the groups which saw an emotionally tuned video had the most sustained changes through the study. This final study also shows that different approaches may be warranted for different advice since behavior change varied between advices, as did changes in other variables. Like with social motivations, these findings present a foundation for future work to further explore how to best utilize emotional inoculation approaches towards encouraging cybersecurity.

In the next section, the specific contributions of this thesis will be identified in Chapters and sections. Then, Section 8.2 explains in more detail some anticipated tracks of future work.

8.1 Summary of Contribution

The contributions of this thesis are:

1. An analysis of the decision specific concerns across multiple cybersecurity behaviors, including the decision to apply updates, use a password manager, and use 2FA.
    a. As explained in Chapter 6, updating is partially reliant on update messages, which can be interpreted in several ways by users. These interpretations are impacted by the context, including what the user is doing when they receive the message (which can result in annoyance or impact importance/noticeability) and by anticipated impact of applying the update, which can be formed by negative past experiences.

   b. As Sections 4.3 highlighted for password managers, 5.2 showed for 2FA, and 3.3 demonstrated for all three target advice, all decisions succumb to the balancing of security and convenience. In some cases, such as the use of password managers, this works in the tool's advantage since it offers a distinct convenience (e.g., secure auto-fill) to users, while others such as 2FA and updating are hurt by the inherent inconvenience in using the technique.

2. Comparison of those who decide both ways when faced with a series of cybersecurity decisions.
   a. Section 3.2 described how these results were repeated in the data for other decisions such as updating, and using 2FA, with significant perception gaps being found for several advices on benefits, costs, and risks. As discussed in Section 4.2, password manager users looked much more kindly on the tool, finding it more secure than non-users, who were distrustful of it.
   b. Deeper exploration into 2FA suggested that non-adopters of that advice may be motivated by a lack of knowledge about the tool. In Section 5.3, some participants who were aware of 2FA, but did not use it cited reasons for not using that were based on incorrect assumptions. Additionally, as explored in Section 5.4, many sampled participants reported not having heard of 2FA before taking our survey, and these participants reported less overall cybersecurity knowledge and access than those who reported having heard of the feature.
3. Emotional responses to decisions and contexts depended on the decisions being made and had differing relationships with behavior.

   a. For 2FA, as seen in Section 5.2, groups that exhibited the same behavior, but vary in perceptions can have different emotional perspectives on the advice. In this case, those who did not find using 2FA as "more convenient" had significantly lower magnitudes for ratings of emotions, despite a similar overall structure in ratings given compared to other users of 2FA.
   b. For updating, as seen in Sections 6.2 and 6.3, annoyance and confusion were common and related with hesitation to apply updates across different software, which was also common. Section 6.4 showed that features of the sample messages, both positive and negative were correlated with ratings of annoyance and confusion. Importance and noticeability was also involved, but to less of a degree than annoyance and confusion.
   c. Deeper analysis presented in Section 6.4.2 showed that regardless of the stress of the task when delivered, users vary strongly in the valence of the emotions they feel in response to update messages, with ratings of positive emotions explaining much of the variance observed in the data, according to statistical analysis.
   d. When looking to password managers as presented in Section 4.4, key emotions such as security and suspicion were rated significantly differently by users and non-users. In addition, users were more admiring and energetic when using password managers based on reports, suggesting users may have more motivation around the tool than non-users.

4. Social considerations, through multiple studies and methods came out consistently lower than individual concerns.
   a. Qualitative data presented in Section 4.3 that was collected from participants as to their reasons for using a password manager focused mainly on individual reasons, as

did the reasons given by non-users of 2FA to explain their decisions discussed in Section 5.3. Qualitative data discussed in Section 3.3 for all decisions revealed a similar lack of social consideration in reasons given, as further explored in 3.4.

   b. Quantitative ratings of individual and social benefits, costs, and risks of following various cybersecurity advices discussed in Section 3.2 had significantly higher ratings for all individual variables than their social variables, as noted in 3.4. This again suggests the current supremacy of individual considerations in thinking about these decisions.

5. Interventions were developed that incorporate emotionally and socially-conscious appeals in an attempt to better motivate users to take up expert-advised cybersecurity practice than other appeals.

   a. As Section 7.4 lays out, the efficacy of several kinds of content was tested on multiple variables, including awareness, perceptions, and behavior, which allowed the identification of emotional inoculation as a potentially effective method of persuasion in the discussion of Section 7.5. Additionally, as further explained in the same section, some value was seen in the social motivations for some advice as several social variables were significantly different between those who ended up following the target advice by the end of the study relative to those who didn't.

8.2 Future Work

Though much is learned through the investigations presented in this thesis, research continues with the goal of further expanding our understanding of why users make the cybersecurity decisions they do. Fortunately, the work presented here can serve as a guide to several key areas that need further investigation.

First, further study of the application of emotional inoculation and social motivations towards encouraging adoption of cybersecurity advice is needed. Though the work here provides a foundation, repetition and expansion of the studies here will allow for more and deeper understanding of these approaches' applicability. These extensions can also include other advice to provide additional context to analysis of performance. Investigation of the use of these concepts and/or interventions in more elaborate campaigns or through other modes of communication would also be valuable since some data indicates that behavior change may come from the repeated intervention as opposed to a single intervention, as was tested here. Finally, repetition of the study investigating these interventions will serve to confirm the results.

These calls for expansion also include users' motivations. Exploration of the contours of user motivation around additional cybersecurity behaviors is needed. In particular, large-scale, systematic gathering of data related to users' perceptions and behavior around many decisions, as called for in prior work [46,47], would be welcomed and could be developed based upon the methods and instruments utilized in the studies here. The more exploratory data that is collected, the better interventions can be in how they address the concerns users have.

The expansion to other advice would also provide new contexts in which to learn about the broader patterns seen in data. The balance of security and convenience may be common throughout these security advices, but could also be irrelevant in unique cases. Only further and expanded investigations can determine this and other questions related to the patterns identified in the data collected this far. New investigations into motivations may also reveal new patters in users' thinking that are valuable towards designing effective interventions aimed at getting them to adopt good behavior.

References

[1] Abawajy, Jemal. “User Preference of Cyber Security Awareness Delivery Methods.” Behaviour & Information Technology 33.3 (2014): 237-248.

[2] Abu-Salma, Ruba, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. “Obstacles to the Adoption of Secure Communication Tools.” Proceedings of the Symposium on Security and Privacy. New York: IEEE, 2017.

[3] Adams, Anne, and Martina Angela Sasse. “Users are not the enemy.” Communications of the ACM 42.12 (1999): 40-46.

[4] Albayram, Yusuf, Mohammad Maifi Hasan Khan, and Michael Fagan. “A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA).” International Journal of Human–Computer Interaction (2017): 1-16.

[5] Albrechtsen, Eirik, and Jan Hovden. “Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An intervention study.” Computers & Security 29.4 (2010): 432-445.

[6] Asgharpour, Farzaneh, Debin Liu, and L. Jean Camp. “Mental Models of Security Risks.” Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2007.

[7] AT&T. “Deployment to Rural Areas and Underserved Populations.” Advertisement. Aug. 2017. 24 Aug. 2017 <http://about.att.com/content/csr/home/issue-brief-builder/people/deployment-to-rural-and-underserved-areas.html>.

[8] Babor, Thomas. Alcohol: No Ordinary Commodity: Research and Public Policy. Oxford: Oxford UP, 2010.

[9] Baumeister, Roy F., and Mark R. Leary. “The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation.” Psychological Bulletin 117.3 (1995): 497.

[10] Billings, Robert S., Thomas W. Milburn, and Mary Lou Schaalman. “A Model of Crisis Perception: A Theoretical and Empirical Analysis.” Administrative Science Quarterly (1980): 300-316.

[11] Blader, Steven L., and Tom R. Tyler. “Testing and Extending the Group Engagement Model: Linkages between Social Identity, Procedural Justice, Economic Outcomes, and Extrarole Behavior.” Journal of Applied Psychology 94.2 (2009): 445.

[12] Blythe, Jim, Jean Camp, and Vaibhav Garg. “Targeted Risk Communication for Computer Security.” Proceedings of the International Conference on Intelligent User Interfaces. New York: ACM, 2011. 295-298.

[13] Buck, Ross, Mohammad Khan, Michael Fagan, and Emil Coman. "The User Affective Experience Scale: A Measure of Emotions Anticipated in Response to Pop-Up Computer Warnings." International Journal of Human–Computer Interaction (2017): 1-10.

[14] Buck, Ross, Erika Anderson, Arjun Chaudhuri, and Ipshita Ray. "Emotion and in Persuasion: Applying the ARI Model and the CASC Scale." Journal of Business Research 57.6 (2004): 647-656.

[15] Buck, Ross. Emotion: A Biosocial Synthesis. Cambridge: Cambridge UP, 2014.

[16] -----. Human Motivation and Emotion. Hoboken, NJ: John Wiley & Sons, 1988.

[17] Camp, L. Jean. "Mental Models of Privacy and Security." IEEE Technology and Society Magazine 28.3 (2009).

[18] Centers for Disease Control and Prevention. "Quitting Smoking." Fast Facts and Fact Sheets. 1 Feb. 2017. 23 Aug. 2017 < https://www.cdc.gov/tobacco/data_statistics/fact_sheets/cessation/quitting>.

[19] Clark, James M., and Allan Paivio. "Dual Coding Theory and Education." Educational Psychology Review 3.3 (1991): 149-210.

[20] Clarke, Nathan, and David Lacey. "Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness." Information Management & Computer Security 20.1 (2012): 29-38.

[21] Conzola, Vincent C., and Michael S. Wogalter. "A Communication–Human Information Processing (C–HIP) Approach to Warning Effectiveness in the Workplace." Journal of Risk Research 4.4 (2001): 309-322.

[22] Cranor, Lorrie Faith, Joseph Reagle, and Mark S. Ackerman. "Beyond Concern: Understanding Net Users' Attitudes about Online Privacy." The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy. Eds. Ingo Vogelsang and Benjamin M. Compaine. Cambridge, MA: MIT UP, 2000. 47-70.

[23] Das, Sauvik, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. "The Effect of Social Influence on Security Sensitivity." Proceedings of the Symposium on Usable Privacy and Security. Berkeley: USENIX, 2014. 143-157.

[24] Das, Sauvik, Adam DI Kramer, Laura A. Dabbish, and Jason I. Hong. "Increasing Security Sensitivity with Social Proof: A Large-Scale Experimental Confirmation." Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014. 739-749.

[25] De Cristofaro, Emiliano, Honglu Du, Julien Freudiger, and Greg Norcie. "A comparative usability study of two-factor authentication." Proceedings of them NDSS Workshop on Usable Security. Reston, VA: Internet Society, 2014.

[26] Dixon, Wilfrid J., and Alexander M. Mood. “The Statistical Sign Test.” Journal of the American Statistical Association 41.236 (1946): 557-566.

[27] Dunning, David, ed. Social Motivation. Psychology Press, 2011.

[28] Dunphy, Paul, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. “Understanding the Experience-Centeredness of Privacy and Security Technologies.” Proceedings of the New Security Paradigms Workshop. New York: ACM, 2014.

[29] Egelman, Serge, and Eyal Peer. “The Myth of the Average User.” Proceedings of the New Security Paradigms Workshop. New York: ACM, 2015.

[30] Fagan, Michael, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. “An Investigation into Users’ Considerations towards Using Password Managers.” Human-centric Computing and Information Sciences 7.12 (2017): 1-20.

[31] Fagan, Michael, Mohammad Maifi Hasan Khan. “Why Do They Do What They Do: A Study of What Motivates Users to (Not) Follow Computer Security Advice.” Proceedings of Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2016. 59-75.

[32] Fagan, Michael, Mohammad Maifi Hasan Khan, and Nhan Nguyen. “How Does this Message Make You Feel?: A Study of User Perspectives on Software Update/Warning Message Design.” Human-centric Computing and Information Sciences 5.36 (2015): 1-26.

[33] Fagan, Michael, Mohammad Maifi Hasan Khan, and Ross Buck. “A Study of Users’ Experiences and Beliefs about Software Update Messages.” Computers in Human Behavior 51 (2015): 504-519.

[34] Felt, Adrienne Porter, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. “Android Permissions: User Attention, Comprehension, and Behavior.” Proceedings of the Symposium on Usable Privacy and Security. New York: ACM, 2012.

[35] Ferrer, Rebecca A., Jeffrey D. Fisher, Ross Buck, and K. Rivet Amico. “Pilot Test of an Emotional Education Intervention Component for Sexual Risk Reduction.” Health Psychology 30.5 (2011): 656.

[36] Forget, Alain, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. “Do or Do Not, There is No Try: User Engagement May Not Improve Security Outcomes.” Proceedings of the Twelfth Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2016. 97-111.

[37] Forget, Alain, Sonia Chiasson, and Robert Biddle. “Supporting Learning of an Unfamiliar Authentication Scheme.” Proceedings of the World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education. Chesapeake, VA: AACE, 2012. 1002-1011.

[38] Garg, Vaibhav, and Jean Camp. “End User Perception of Online Risk under Uncertainty.” Proceedings of the Hawaii International Conference on System Science. New York: IEEE, 2012. 3278-3287.

[39] Google Fiber. “Expansion Plans.” 24 Aug. 2017 < https://fiber.google.com/newcities/>.

[40] Gunson, Nancie, Diarmid Marshall, Hazel Morton, and Mervyn Jack. “User Perceptions of Security and Usability of Single-factor and Two-factor Authentication in Automated Telephone Banking.” Computers & Security 30.4 (2011): 208-220.

[41] Harbach, Marian, Alexander De Luca, Nathan Malkin, and Serge Egelman. “Keep on Lockin'in the Free World: A Multi-National Comparison of Smartphone Locking.” Proceedings of the Conference on Human Factors in Computing Systems. New York, ACM, 2016. 4823-4827.

[42] Harbach, Marian, Markus Hettig, Susanne Weber, and Matthew Smith. “Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions.” Proceedings of the Annual ACM Conference on Human Factors in Computing Systems. New York: ACM, 2014. 2647-2656.

[43] Harbach, Marian, Sascha Fahl, and Matthew Smith. “Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness.” Proceedings of the Computer Security Foundations Symposium. New York: IEEE, 2014.

[44] Harbach, Marian, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. “It’s a Hard Lock life: A Field Study of Smartphone (Un) Locking Behavior and Risk Perception.” Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2014. 213-230.

[45] Harmon-Jones, Cindy, Brock Bastian, and Eddie Harmon-Jones. “The Discrete Emotions Questionnaire: A New Tool for Measuring State Self-Reported Emotions.” PLOS One. 11.8 (2016): 1-25.

[46] Herley, Cormac. “So Long, and No Thanks for the Externalities: the Rational Rejection of Security Advice by Users.” Proceedings of the New Security Paradigms Workshop. New York: ACM, 2009.

[47] -----. “More is Not the Answer.” IEEE Security & Privacy 12.1 (2014): 14-19.

[48] Herron, Carol, Holly York, Cathleen Corrie, and Steven P. Cole. “A Comparison Study of the Effects of a Story-based Video Instructional Package Versus a Text-based Instructional Package in the Intermediate-level Foreign Language Classroom.” Calico Journal (2006): 281-307.

[49] Hogg, Michael A., and Dominic Abrams. “Towards a Single-process Uncertainty-reduction Model of Social Motivation in Groups.” Group Motivation: Social Psychological Perspectives. Eds. Michael Hogg and Dominic Abrams. Hertfordshire, UK: Harvester Wheatsheaf, 1993. 173-190.

[50] Howe, Adele E., Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. “The Psychology of Security for the Home Computer User.” Proceedings of the Symposium Security and Privacy. New York: IEEE, 2012. 209-223.

[51] Ion, Iulia, Rob Reeder, and Sunny Consolvo. “’... No One can Hack my Mind:’ Comparing Expert and Non-Expert Security Practices.” Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2015. 327-346.

[52] Jackson, Melanie, and Marie S. Tisak. “Is Prosocial Behaviour a Good Thing? Developmental Changes in Children's Evaluations of Helping, Sharing, Cooperating, and Comforting.” British Journal of Developmental Psychology 19.3 (2001): 349-367.

[53] Janis, Irving L., and Leon Mann. “Coping with Decisional Conflict: An Analysis of How Stress Affects Decision-Making Suggests Interventions to Improve the Process.” American Scientist 64.6 (1976): 657-667.

[54] Janis, Irving L. “Emotional Inoculation: Theory and Research on Effects of Preparatory Communications.” Psychoanalysis and the Social Sciences 5 (1958): 119-154.

[55] Kang, Ruogu, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. “’My Data just Goes Everywhere:’ User Mental Models of the Internet and Implications for Privacy and Security.” Proceedings of the Symposium on Usable Privacy and Security. Berkeley: USENIX, 2015. 39-52.

[56] Karole, Ambarish, Nitesh Saxena, and Nicolas Christin. “A Comparative Usability Evaluation of Traditional Password Managers.” Proceedings of the International Conference on Information Security and Cryptology. New York: IEEE, 2010. 233-251

[57] Kim, Hee-Woong, and Atreyi Kankanhalli. “Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective.” Management Information Systems Quarterly 33.3 (2009): 567-582.

[58] Kraus, Lydia, Ina Wechsung, and Sebastian Möller. “Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones.” Proceedings of the European Workshop on Usable Security. Reston, VA: Internet Society, 2016.

[59] Krol, Kat, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. ““They brought in the horrible key ring thing!” Analysing the Usability of Two-Factor Authentication in UK Online Banking.” Proceedings of them NDSS Workshop on Usable Security. Reston, VA: Internet Society, 2015.

[60] Langer, Ellen J., Irving L. Janis, and John A. Wolfer. “Reduction of Psychological Stress in Surgical Patients.” Journal of Experimental Social Psychology 11.2 (1975): 155-165.

[61] Larson, Stephen. “The Cyber Security Fair: An Effective Method for Training Users to Improve their Cyber Security Behaviors.” Information Security Education Journal 2.1 (2015): 11-19.

[62] Lerner, Jennifer S., and Dacher Keltner. “Beyond Valence: Toward a Model of Emotion-Specific Influences on Judgment and Choice.” Cognition and Emotion 14.4 (2000): 473-493.

[63] Li, Zhiwei, Warren He, Devdatta Akhawe, and Dawn Song. “The Emperor's New Password Manager: Security Analysis of Web-based Password Managers.” Proceedings of the USENIX Security Symposium. Berkeley, CA: USENIX, 2014. 465-479.

[64] Loewenstein, George, and Jennifer S. Lerner. “The Role of Affect in Decision Making.” Handbook of Affective Science. Eds. Richard J. Davidson, Klaus R. Scherer, and H. Hill Goldsmith. Oxford: Oxford UP, 2003. 619- 642.

[65] Mann, Henry B., and Donald R. Whitney. “On a Test of Whether One of Two Random Variables is Stochastically Larger than the other.” The Annals of Mathematical Statistics (1947): 50-60.

[66] Mathur, Arunesh, and Marshini Chetty. “Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates.” Proceedings of Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2017. 175-193.

[67] Mathur, Arunesh, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. “They Keep Coming Back Like Zombies”: Improving Software Updating Interfaces.” Proceedings of Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2016. 43-58.

[68] Marsh, Herbert W., Gregory Arief D. Liem, Andrew J. Martin, Alexandre JS Morin, and Benjamin Nagengast. “Methodological Measurement Fruitfulness of Exploratory Structural Equation Modeling (ESEM): New Approaches to Key Substantive Issues in Motivation and Engagement.” Journal of Psychoeducational Assessment. 29 (2011): 322-346.

[69] Mayer, Richard E., and Valerie K. Sims. “For whom is a Picture Worth a Thousand Words? Extensions of a Dual-Coding Theory of Multimedia Learning.” Journal of Educational Psychology 86. 3 (1994): 389-401.

[70] Metz, Cade. “Facebook’s Giant Internet-Beaming Drone Finally Takes Flight.” Wired 21 July 2016. 24 Aug. 2017 <https://www.wired.com/2016/07/facebooks-giant-internet-beaming-drone-finally-takes-flight/>.

[71] Mylonas, Alexios, Anastasia Kastania, and Dimitris Gritzalis. “Delegate the Smartphone User? Security Awareness in Smartphone Platforms.” Computers & Security 34 (2013): 47-66.

[72] Ng, Boon-Yuen, Atreyi Kankanhalli, and Yunjie Calvin Xu. “Studying Users' Computer Security Behavior: A Health Belief Perspective.” Decision Support Systems 46.4 (2009): 815-825.

[73] Niedenthal, Paula M., Sylvia Kruth-Gruber, and Francois Ric. Psychology and Emotion: Interpersonal, Experiential, and Cognitive Approaches. New York: Psychology Press. 2006.

[74] Panksepp, Jaak. Affective Neuroscience: The Foundations of Human and Animal Emotions. Oxford: Oxford UP, 1998.

[75] Pearson, Karl. " On Lines and Planes of Closest Fit to Systems of Points in Space." The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science 2.11 (1901): 559-572.

[76] Penner, Louis A., et al. "Prosocial Behavior: Multilevel Perspectives." Annual Review of Psychology 56 (2005): 365-392.

[77] Petsas, Thanasis, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. "Two-factor Authentication: Is the World Ready?: Quantifying 2FA Adoption." Proceedings of the European Workshop on System Security. New York: ACM, 2015. 1-7.

[78] Pfleeger, Shari Lawrence, and Deanna D. Caputo. "Leveraging Behavioral Science to Mitigate Cyber Security Risk." Computers & Security 31.4 (2012): 597-611.

[79] Podszebka, Darcy, Candee Conklin, Mary Apple, and Amy Windus. Television's Effect on Vocabulary and Comprehension. Bloomington, IA: ERIC/RCS, 1998.

[80] Porter, Stephen R., Michael E. Whitcomb, and William H. Weitzer. "Multiple Surveys of Students and Survey Fatigue." New Directions for Institutional Research 121 (2004): 63-73.

[81] Redmiles, Elissa M., Amelia R. Malone, and Michelle L. Mazurek. "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security." Proceedings of the Symposium on Security and Privacy. New York: IEEE, 2016. 272-288.

[82] Ridgway, Jessica, and Beth Myers. "A Study on Brand Personality: Consumers' Perceptions of Colours Used in Fashion Brand Logos." International Journal of Fashion Design, Technology and Education 7.1 (2014): 50-57.

[83] Rowe, Brent, Michael Halpern, and Tony Lentz. "Is a Public Health Framework the Cure for Cyber Security?" CrossTalk 25. 6 (2012): 30-38.

[84] Samuelson, William, and Richard Zeckhauser. "Status Quo Bias in Decision Making." Journal of Risk and Uncertainty 1.1 (1988): 7-59.

[85] Sawaya, Yukiko, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior." Proceedings of the Conference on Human Factors in Computing Systems. New York: ACM, 2017. 2202-2214.

[86] Shay, Richard, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "Encountering Stronger Password Requirements: User Attitudes and Behaviors." Proceedings of the Symposium on Usable Privacy and Security. New York: ACM, 2010.

[87] Shariff, Azim F., and Ara Norenzayan. "God is Watching You: Priming God Concepts Increases Prosocial Behavior in an Anonymous Economic Game." Psychological Science 18.9 (2007): 803-809.

[88] Simon, Herbert A. "Rational Choice and the Structure of the Environment." Psychological Review 63. 2 (1956): 129.

[89] Stobert, Elizabeth, and Robert Biddle. "The Password Life Cycle: User Behaviour in Managing Passwords." Proceedings of the Symposium on Usable Privacy and Security. Berkeley, CA: USENIX, 2014. 243-255.

[90] Strauss, Anselm, and Juliet M. Corbin. Grounded Theory in Practice. Los Angeles: SAGE Publications, 1997.

[91] Struthers, C. Ward, Réjeanne Dupuis, and Judy Eaton. "Promoting Forgiveness Among Co-workers Following a Workplace Transgression: The Effects of Social Motivation Training." Canadian Journal of Behavioural Science 37.4 (2005): 299-308.

[92] Tam, Leona, Myron Glassman, and Mark Vandenwauver. "The Psychology of Password Management: A Tradeoff between Security and Convenience." Behaviour & Information Technology 29.3 (2010): 233-244.

[93] Tempelman-Kluit, Nadaleen. "Multimedia Learning Theories and Online Instruction." College & Research Libraries 67.4 (2006): 364-369.

[94] Tracy, Miles, Wayne Jansen, Karen Scarfone, and Theodore Winograd. "Guidelines on Securing Public Web Servers: Recommendations of the National Institute of Standards and Technology." Special Publication. Washington, DC: US Dept. of Commerce, 2002.

[95] Tyler, Tom R. Why People Cooperate: The Role of Social Motivations. Princeton, NJ: Princeton UP, 2010.

[96] Vaniea, Kami E., Emilee Rader, and Rick Wash. "Betrayed by Updates: How Negative Experiences Affect Future Security." Proceedings Conference on Human Factors in Computing Systems. New York: ACM, 2014.

[97] Vitale, Francesco, Joanna Mcgrenere, Aurélien Tabard, Michel Beaudouin-Lafon, and Wendy E. Mackay. "High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades." Proceedings of the Conference on Human Factors in Computing Systems. New York: ACM, 2017. 4242-4253.

[98] Wankel, Leonard M., and Carol Thompson. "Motivating People to be Physically Active: Self-Persuasion vs. Balanced Decision Making." Journal of Applied Social Psychology 7.4 (1977): 332-340.

[99] Wash, Rick, Emilee Rader, Kami Vaniea, and Michelle Rizor. "Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences." Proceedings of the New Security Paradigms Workshop. New York: ACM, 2014.

[100] Watson, David, Lee A. Clark, and Auke Tellegen. “Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales.” Journal of Personality and Social Psychology 54.6 (1988): 1063-1070.

[101] Weiner, Bernard. Social Motivation, Justice, and the Moral Emotions: An Attributional Approach. New York: Psychology Press, 2006.

[102] -----. “On Sin Versus Sickness: A Theory of Perceived Responsibility and Social Motivation.” American Psychologist 48.9 (1993): 957-965.

[103] Weir, Catherine S., Gary Douglas, Martin Carruthers, and Mervyn Jack. “User Perceptions of Security, Convenience and Usability for eBanking Authentication Tokens.” Computers & Security 28.1 (2009): 47-62.

[104] Wigfield, Allan, and Kathryn R. Wentzel. “Introduction to Motivation at School: Interventions that Work.” Educational Psychologist 42.4 (2007): 191-196.

[105] Winter, Søren C., and Peter J. May. “Motivation for Compliance with Environmental Regulations.” Journal of Policy Analysis and Management 20.4 (2001): 675-698.

[106] Witte, Kim, and Mike Allen. “A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns.” Health Education & Behavior 27. 5 (2000): 591-615.

[107] Wogalter, Michael S., David M. DeJoy, and Kenneth R. Laughery. “Organizing Theoretical Framework: A Consolidated Communication-Human Information Processing (C-HIP) Model.” Warnings and Risk Communication (1999): 13-21.

[108] Wogalter, Michael S., and David A. Dietrich. “Enhancing Label Readability for Over-the-Counter Pharmaceuticals by Elderly Consumers.” Proceedings of the Human Factors and Ergonomics Society Annual Meeting 39.2 Los Angeles: SAGE Publications, 1995. 143-147.

[109] Wogalter, Michael S., and John W. Brelsford. “Incidental Exposure to Rotating Warnings on Alcoholic Beverage Labels.” Proceedings of the Human Factors and Ergonomics Society Annual Meeting 38.5 Los Angeles: SAGE Publications, 1994. 374-378.

[110] Wogalter, Michael S., Gail A. Fontenelle, and Kenneth R. Laughery. “Behavioral Effectiveness of Warnings.” Proceedings of the Human Factors and Ergonomics Society Annual Meeting 29.7 Los Angeles: SAGE Publications, 1985. 679–683.

Appendix A

Survey instruments, sample descriptions, and complete statistical results for the study presented in Chapter 3 can be found in this Appendix.

Survey Instruments

The study in Chapter 3 was executed using an initial screening survey, as well as follow-up instruments sent to participants after they were groups by behavior to gather their ratings of rational components to their decisions.

Screening Survey

The following instruments were used to gather basic demographics and behavior data from participants. Participants were then contacted based on their responses to this survey.

1. What is your age? _____
2. What is your gender?
   - ○ Male
   - ○ Female
   - ○ Other
3. Do you use a laptop of desktop computer that you or your family owns?
   - ○ Yes
   - ○ No
4. How would you rate your general computer expertise?
   - ○ Very poor
   - ○ Poor
   - ○ Fair
   - ○ Good
   - ○ Very good
5. How would you rate your computer security expertise?
   - ○ Very poor
   - ○ Poor
   - ○ Fair
   - ○ Good
   - ○ Very good
6. How often would you say you use the computer?
   - ○ Never
   - ○ Rarely

    - Sometimes
    - Often
    - All the time
7. Do you keep your computer’s software up to date?
    - Yes
    - No
    - I don’t know
8. Do you use two-factor authentication (e.g., 2-Step Verification) for at least one of your online accounts?
    - Yes
    - No
    - I don’t know
9. Do you use a password manager (e.g., LastPass, OnePass, KeePass) to manage your online account passwords?
    - Yes
    - No
    - I don’t know
10. Do you change your passwords frequently?
    - Yes
    - No
    - I don’t know

Follow-Up Survey

Groups of participants who reported following each target advice in this study were sent the following survey, with the bracketed blocks being replaced as appropriate for each advice, using the following language:

Update: “keep(ing) your computer’s software up to date”

Password Manager: “us(e/ing) a password manager”

2FA: “us(e/ing) two-factor authentication”

Template for Follow Groups:

1. Please explain in a few sentences why you choose to [follow the advice].

   ____
   ____
   ____

2. How much would you say you are benefited by you [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
3. How much would you say users of other computers are benefited by you [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
4. How much would you say you are cost or inconvenienced by you [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure

5. How much would you say users of other computers are cost or inconvenienced by you [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
6. How much would you say you are put at risk by you [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
7. How much would you say users of other computers are put at risk by you [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
8. How much would you say you would be benefited if you did not [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
9. How much would you say users of other computers would be benefited if you did not [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
10. How much would you say you would be cost or inconvenienced if you did not [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure

11. How much would you say users of other computers would be cost or inconvenienced if you did not [follow the advice]?
    - ○ None
    - ○ Little
    - ○ Some
    - ○ A lot
    - ○ Not sure
12. How much would you say you would be put at risk if you did not [follow the advice]?
    - ○ None
    - ○ Little
    - ○ Some
    - ○ A lot
    - ○ Not sure
13. How much would you say users of other computers would be put at risk if you did not [follow the advice]?
    - ○ None
    - ○ Little
    - ○ Some
    - ○ A lot
    - ○ Not sure

Template for Not Follow Groups:

1. Please explain in a few sentences why you choose not to [follow the advice].
2. How much would you say you are benefited by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
3. How much would you say users of other computers are benefited by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
4. How much would you say you are cost or inconvenienced by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
5. How much would you say users of other computers are cost or inconvenienced by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
6. How much would you say you are put at risk by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
7. How much would you say users of other computers are put at risk by you not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure

8. How much would you say you would be benefited if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
9. How much would you say users of other computers would be benefited if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
10. How much would you say you would be cost or inconvenienced if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
11. How much would you say users of other computers would be cost or inconvenienced if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
12. How much would you say you would be put at risk if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
13. How much would you say users of other computers would be put at risk if you did [follow the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure

Sample Descriptive Statistics

			Gender		**Age**		**Computer Expertise**		**Security Expertise**	
	Group	**N**	*Male*	*Female*	*Avg.*	*St.D.*	*Avg.*	*St.D.*	*Avg.*	*St.D.*
Update	*Follow*	39	20	19	38.4	14	4.15	0.7	3.56	0.8
	Not Follow	30	12	18	35.8	11	3.77	0.8	2.93	0.6
Password Manager	*Follow*	41	19	22	33.2	8.7	4.24	0.6	3.63	0.9
	Not Follow	38	16	22	34.0	9.7	4.30	0.7	3.50	0.7
2FA	*Follow*	36	20	16	36.6	13	4.31	0.7	3.86	0.9
	Not Follow	31	19	12	32.9	9.0	4.26	0.7	3.77	0.7

Statistical Inference Testing Results

Follower vs. Non-Follower Mann-Whitney U-Tests

			…of Following				**… of Not Following**			
			Follow	*Not Follow*	*M-W U-Test*		*Follow*	*Not Follow*	*M-W U-Test*	
			Avg.(Med.)	*Avg.(Med.)*	*U*	*Sig.*	*Avg.(Med.)*	*Avg.(Med.)*	*U*	*Sig.*
Benefit…	*Ind.*	Upd.	3.77(4)	2.97(3)	274.5	<0.001	1.51(1)	2.13(2)	347.5	0.002
		P.M.	3.78(4)	2.50(2.5)	154.5	<0.001	1.68(1)	2.70(3)	302.0	<0.001
		2FA	3.71(4)	2.90(3)	243.5	<0.001	1.59(1.5)	2.62(3)	161.5	<0.001
	Social	Upd.	2.71(3)	2.39(3)	338.0	0.286	1.40(1)	1.58(1)	371.0	0.371
		P.M.	2.08(2)	1.70(1)	498.5	0.155	1.39(1)	1.68(1)	511.0	0.142
		2FA	2.48(2)	2.29(2)	390.0	0.489	1.59(1)	1.92(1.5)	313.5	0.237
Risk…	*Ind.*	Upd.	1.56(2)	1.72(2)	496.5	0.335	3.42(4)	2.77(3)	336.5	0.002
		P.M.	1.83(2)	2.53(2)	342.5	<0.001	2.88(3)	1.80(2)	302.5	<0.001
		2FA	1.56(1)	1.62(1)	498.5	0.729	3.42(3)	2.61(3)	243.5	<0.001
	Social	Upd.	1.13(1)	1.38(1)	369.5	0.047	2.67(3)	1.76(1)	262.5	<0.001
		P.M.	1.41(1)	1.53(1)	628.0	0.707	1.92(2)	1.29(1)	409.0	0.002
		2FA	1.31(1)	1.48(1)	433.5	0.47	2.48(3)	1.79(2)	289.0	0.013
Cost…	*Ind.*	Upd.	2.03(2)	2.1(2)	527.5	0.444	2.95(3)	2.00(2)	247.5	<0.001
		P.M.	1.73(2)	2.18(2)	533.0	0.011	3.15(3)	1.75(1)	244.5	<0.001
		2FA	2.00(2)	2.39(2)	405.5	0.036	1.76(1)	1.57(1)	446.5	0.451
	Social	Upd.	1.22(1)	1.29(1)	431.0	0.781	2.32(2)	1.59(1)	248.0	0.001
		P.M.	1.28(1)	1.52(1)	565.5	0.213	1.84(1)	1.03(1)	354.0	<0.001
		2FA	1.52(1)	1.44(1)	403.5	0.786	1.69(1)	1.41(1)	343.0	0.356

Individual vs. Social Rating Sign Tests

	… of Following					**… of Not Following**				
	Ind.>	*Soc.>*	*Tie*	*Z*	*Sig.*	*Ind.>*	*Soc.>*	*Tie*	*Z*	*Sig.*
Benefit	176	10	62	-12.1	<0.001	108	38	99	-5.71	<0.001
Cost	112	8	148	-9.4	<0.001	174	6	85	-12.45	<0.001
Risk	165	21	75	-10.49	<0.001	102	11	140	-8.47	<0.001

Appendix B

Survey instruments, sample descriptions, and complete statistical results for the study presented in Chapter 4 can be found in this Appendix.

Survey Instruments

1. What is your gender?
    - ○ Male
    - ○ Female
    - ○ Other
2. What is your age?
    - ○ 18-25
    - ○ 26-34
    - ○ 35-54
    - ○ 55-64
    - ○ 65+
3. What is the highest level of education you have received?
    - ○ Less than High School
    - ○ High School / GED
    - ○ Some College
    - ○ 2-year College Degree
    - ○ 4-year College Degree
    - ○ Master's Degree
    - ○ Doctoral Degree
    - ○ Professional/Medical Degree (JD, MD)
4. How would you rate your general computer expertise?
    - ○ Very low
    - ○ Low
    - ○ Below average
    - ○ Average
    - ○ Above average
    - ○ High
    - ○ Very high
5. Do you know what a password manager is?
    - ○ Yes
    - ○ No
6. Have you ever used a password manager?
    - ○ Yes
    - ○ No

General Statements

Please rate how much you agree or disagree with each statement. (1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree or Disagree, 4 = Agree, 5 = Strongly Agree)

_ I am doing a good job of protecting my computer security.
_ I could do more to protect my accounts.
_ I do not have time to pay attention to security.
_ I do not feel that my accounts are likely to be attacked.
_ I do not know where to get computer security advice.
_ I am knowledgeable about computer security.
_ I care about computer security.
_ I trust my computer.
_ I am worried about the security of some of my account/devices more than others.

Password Manager Statements

Please rate how much you agree or disagree with each statement. (1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree or Disagree, 4 = Agree, 5 = Strongly Agree)

_ I trust password managers.
_ Password managers are more secure.
_ Password managers help people.
_ Password managers are easy to use.
_ Password managers are more convenient.
_ I understand the theory behind password managers.
_ I understand why password managers are secure.
_ I worry that accessing my accounts may be more difficult with a password manager.

Qualitative Instruments

Users: Why do you choose to use a password manager? ________________________________

Non-Users: Why do you choose not to use a password manager? _________________________

Emotion Instruments

Users: Imagine you are using your password manager to log into a website.

Non-Users: Imagine you start using a password manager to log into a website.

1. One might feel CONFIDENT (e.g., because one is protected from possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
2. One might feel SECURE (e.g., because one is protected from possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
3. One might feel SAD (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
4. One might feel DEPRESSED (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
5. One might feel DOWN (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
6. One might feel AFRAID (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
7. One might feel NERVOUS (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
8. One might feel ANXIOUS (e.g., because one's time is being used by the password manager).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
9. One might feel ANGRY (e.g., because using the password manager is inconvenient).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
10. One might feel INSULTED (e.g., because using the password manager is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
11. One might feel HOSTILE (e.g., because using the password manager is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
12. One might feel SURPRISED (e.g., because one does not expect how hard or easy the password manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
13. One might feel DAZED (e.g., because one does not expect how hard or easy the password manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
14. One might feel CONFUSED (e.g., because one does not expect how hard or easy the password manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
15. One might feel FREAKED OUT (e.g., because one does not expect how hard or easy the password manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
16. One might feel DISGUSTED (e.g., because using the password manager is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

17. One might feel DISMAYED (e.g., because using the password manager is inconvenient).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
18. One might feel DISTRAUGHT (e.g., because using the password manager is inconvenient).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
19. One might feel CARED-FOR (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
20. One might feel FRIENDLY (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
21. One might feel WELCOMED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
22. One might feel POWERFUL (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
23. One might feel ENERGETIC (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
24. One might feel VIGOROUS (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
25. One might feel ISOLATED (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
26. One might feel LONELY (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
27. One might feel ABANDONED (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
28. One might feel PROUD (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
29. One might feel TRIUMPHANT (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
30. One might feel ARROGANT (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
31. One might feel ASHAMED (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
32. One might feel GUILTY (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
33. One might feel EMBARRASSED (e.g., because one’s precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
34. One might feel SCORNFUL (e.g., because the danger is easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
35. One might feel CONTEMPTUOUS (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
36. One might feel DISDAINFUL (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
37. One might feel One might feel HUMILIATED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

38. One might feel DISHONORED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
39. One might feel RESENTFUL (e.g., because the danger is not easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
40. One might feel GRATEFUL (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
41. One might feel RESPECTFUL (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
42. One might feel ADMIRING (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
43. One might feel TRUSTING (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
44. One might feel SUSPICIOUS (e.g. because the tool may be unreliable).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
45. One might feel HAPPY (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

Sample Descriptive Statistics

		Gender			**Age**			
Group	N	*Male*	*Female*	*Not Given*	*18-25*	*26-34*	*35-54*	*55-64*
Users	137	90	46	1	31	59	41	6
Non-Users	111	56	55	-	31	41	30	9

Statistical Inference Testing Results

Users vs. Non-Users Mann-Whitney U-Tests for Emotion Ratings

	Average (Median)		**U-Test Results**	
	Users	*Non-Users*	*U*	*Sig.*
Confident	3.54 (4)	3.35 (3)	6588	*0.069*
Secure	3.8 (4)	3.50 (4)	6148.5	*0.005*
Sad	1.50 (1)	1.55 (1)	7180	*0.388*
Depressed	1.49 (1)	1.55 (1)	7089.5	*0.295*
Down	1.54 (1)	1.64 (1)	7030.5	*0.253*
Afraid	1.77 (2)	1.85 (2)	7425.5	*0.734*
Nervous	2.00 (2)	2.12 (2)	7032.5	*0.282*
Anxious	1.97 (2)	2.12 (2)	6827.5	*0.224*
Angry	1.69 (2)	1.82 (2)	6742	*0.122*
Insulted	1.47 (1)	1.60 (1)	6840.5	*0.155*
Hostile	1.60 (1)	1.68 (2)	7123.5	*0.344*
Surprised	2.31 (2)	2.45 (2)	6955	*0.279*
Dazed	1.76 (1)	1.85 (2)	7249	*0.496*
Confused	2.08 (2)	2.28 (2)	6522	*0.057*
Freaked-Out	1.74 (2)	1.89 (2)	6891.5	*0.174*
Disgusted	1.52 (1)	1.59 (1)	7039.5	*0.256*
Dismayed	1.80 (2)	1.83 (2)	7315	*0.581*
Distraught	1.64 (2)	1.81 (2)	6801.5	*0.119*
Cared-For	3.03 (3)	2.77 (3)	6497	*0.06*
Friendly	2.77 (3)	2.54 (3)	6656.5	*0.102*
Welcomed	2.97 (3)	2.71 (3)	6573.5	*0.055*
Powerful	2.91 (3)	2.83 (3)	7242.5	*0.497*
Energetic	2.58 (3)	2.21 (2)	6111.5	*0.006*
Vigorous	2.42 (3)	2.28 (2)	7028.5	*0.347*
Isolated	1.66 (1)	1.65 (1)	7386.5	*0.67*
Lonely	1.45 (1)	1.52 (1)	7386.5	*0.755*
Abandoned	1.55 (1)	1.63 (1)	7281.5	*0.518*
Proud	3.00 (3)	2.76 (3)	6561	*0.07*
Triumphant	2.90 (3)	2.67 (3)	6687.5	*0.09*
Arrogant	1.89 (2)	1.88 (2)	7525.5	*0.882*
Ashamed	1.66 (1)	1.71 (1.5)	7207.5	*0.589*
Guilty	1.74 (2)	1.85 (2)	7064.5	*0.363*
Embarrassed	1.77 (2)	1.80 (2)	7288	*0.633*
Scornful	1.69 (1)	1.60 (1)	7156.5	*0.376*
Contemptuous	1.79 (1)	1.76 (2)	7438	*0.85*
Disdainful	1.65 (1)	1.63 (1)	7334.5	*0.671*
Humiliated	1.42 (1)	1.42 (1)	7517.5	*0.947*
Dishonored	1.52 (1)	1.51 (1)	7585.5	*0.97*
Resentful	1.70 (2)	1.90 (2)	6712.5	*0.13*
Grateful	3.42 (4)	3.23 (3)	6628.5	*0.068*
Respectful	2.85 (3)	2.58 (3)	6613	*0.084*
Admiring	2.66 (3)	2.32 (2)	6305.5	*0.017*
Trusting	3.49 (4)	3.29 (3)	6489	*0.056*
Suspicious	2.39 (2)	2.80 (3)	5788	*0.001*
Happy	3.46 (4)	3.26 (3)	6684.5	*0.085*

Appendix C

Survey instruments, sample descriptions, and complete statistical results for the study presented in Chapter 5 can be found in this Appendix.

Survey Instruments

7. What is your gender?
   - ○ Male
   - ○ Female
   - ○ Other
8. What is your age?
   - ○ 18-25
   - ○ 26-34
   - ○ 35-54
   - ○ 55-64
   - ○ 65+
9. What is the highest level of education you have received?
   - ○ Less than High School
   - ○ High School / GED
   - ○ Some College
   - ○ 2-year College Degree
   - ○ 4-year College Degree
   - ○ Master’s Degree
   - ○ Doctoral Degree
   - ○ Professional/Medical Degree (JD, MD)
10. How would you rate your general computer expertise?
    - ○ Very low
    - ○ Low
    - ○ Below average
    - ○ Average
    - ○ Above average
    - ○ High
    - ○ Very high
11. Do you know what two-factor authentication is?
    - ○ Yes
    - ○ No
12. Have you ever used two-factor authentication?
    - ○ Yes
    - ○ No

General Statements

Please rate how much you agree or disagree with each statement. (1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree or Disagree, 4 = Agree, 5 = Strongly Agree)

_ I am doing a good job of protecting my computer security.

_ I could do more to protect my accounts.

_ I do not have time to pay attention to security.

_ I do not feel that my accounts are likely to be attacked.

_ I do not know where to get computer security advice.

_ I am knowledgeable about computer security.

_ I care about computer security.

_ I trust my computer.

_ I am worried about the security of some of my account/devices more than others.

Two-Factor Authentication Statements

Please rate how much you agree or disagree with each statement. (1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree or Disagree, 4 = Agree, 5 = Strongly Agree)

_ I trust two-factor authentication.

_ Two-factor authentication is secure.

_ Two-factor authentication helps people.

_ Two-factor authentication is easy to use.

_ Two-factor authentication is more convenient.

_ I understand the theory behind two-factor authentication.

_ I understand why two-factor authentication is secure.

Qualitative Instruments

Users: Why do you choose to use two-factor authentication? ______________________________

Non-Users: Why do you choose not to use two-factor authentication? ______________________

Emotion Instruments

Users: Imagine you are using two-factor authentication to access an account.

Non-Users: Imagine you start using two-factor authentication to access an account.

1. One might feel CONFIDENT (e.g., because one is protected from possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
2. One might feel SECURE (e.g., because one is protected from possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
3. One might feel SAD (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
4. One might feel DEPRESSED (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
5. One might feel DOWN (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
6. One might feel AFRAID (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
7. One might feel NERVOUS (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
8. One might feel ANXIOUS (e.g., because one's time is being used by two-factor authentication).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
9. One might feel ANGRY (e.g., because using two-factor authentication is inconvenient).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
10. One might feel INSULTED (e.g., because using two-factor authentication is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
11. One might feel HOSTILE (e.g., because using two-factor authentication is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
12. One might feel SURPRISED (e.g., because one does not expect how hard or easy two-factor authentication is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
13. One might feel DAZED (e.g., because one does not expect how hard or easy two-factor authentication manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
14. One might feel CONFUSED (e.g., because one does not expect how hard or easy two-factor authentication is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
15. One might feel FREAKED OUT (e.g., because one does not expect how hard or easy two-factor authentication manager is to use).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
16. One might feel DISGUSTED (e.g., because using two-factor authentication is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
17. One might feel DISMAYED (e.g., because using two-factor authentication is inconvenient).
    ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

18. One might feel DISTRAUGHT (e.g., because using two-factor authentication is inconvenient).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

19. One might feel CARED-FOR (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

20. One might feel FRIENDLY (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

21. One might feel WELCOMED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

22. One might feel POWERFUL (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

23. One might feel ENERGETIC (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

24. One might feel VIGOROUS (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

25. One might feel ISOLATED (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

26. One might feel LONELY (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

27. One might feel ABANDONED (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

28. One might feel PROUD (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

29. One might feel TRIUMPHANT (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

30. One might feel ARROGANT (e.g., because one knows of danger and is taking precautions).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

31. One might feel ASHAMED (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

32. One might feel GUILTY (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

33. One might feel EMBARRASSED (e.g., because one's precautions may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

34. One might feel SCORNFUL (e.g., because the danger is easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

35. One might feel CONTEMPTUOUS (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

36. One might feel DISDAINFUL (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

37. One might feel One might feel HUMILIATED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

38. One might feel DISHONORED (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

39. One might feel RESENTFUL (e.g., because the danger is not easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
40. One might feel GRATEFUL (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
41. One might feel RESPECTFUL (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
42. One might feel ADMIRING (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
43. One might feel TRUSTING (e.g. because the system has given one tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
44. One might feel SUSPICIOUS (e.g. because the tool may be unreliable).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
45. One might feel HAPPY (e.g., because one is protected from possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

Sample Descriptive Statistics

			Gender			**Age**					
Group		**N**	*M*	*F*	*N. G.*	*18-25*	*26-34*	*35-54*	*55-64*	*65+*	*N.G.*
Users	*Not more convenient*	71	54	17	-	11	30	26	3	1	-
	Indifferent/More convenient	77	50	27	-	20	36	19	2	-	-
Non-Users		22	12	10	-	7	6	6	3	-	-
Don’t Know		125	55	68	2	20	54	39	10	1	1

Statistical Inference Testing Results

Not Convenient vs. Other Users Mann-Whitney U-Tests for Emotion Ratings

	Average (Median)		**U-Test Results**	
	Not more convenient	*Indifferent/More convenient*	*U*	*Sig.*
Confident	3.48 (3)	3.68 (4)	2388	*0.206*
Secure	3.90 (4)	3.86 (4)	2706.5	*0.909*
Sad	1.59 (1)	1.74 (1)	2650.5	*0.725*
Depressed	1.54 (1)	1.70 (1)	2591.5	*0.542*
Down	1.73 (2)	1.90 (2)	2629.5	*0.667*
Afraid	1.51 (1)	1.94 (2)	2123	*0.011*
Nervous	1.75 (2)	1.84 (2)	2676	*0.812*
Anxious	2.10 (2)	2.09 (2)	2716	*0.944*
Angry	2.15 (2)	1.96 (2)	2276.5	*0.065*
Insulted	1.61 (1)	1.92 (2)	2329.5	*0.154*
Hostile	1.96 (2)	1.87 (2)	2495.5	*0.332*
Surprised	2.20 (2)	2.38 (2)	2484.5	*0.319*
Dazed	1.70 (1)	1.87 (2)	2414	*0.24*
Confused	2.27 (2)	2.08 (2)	2420	*0.208*
Freaked-Out	1.65 (1)	1.88 (2)	2470	*0.272*
Disgusted	1.54 (1)	1.66 (1)	2587	*0.637*
Dismayed	2.14 (2)	1.95 (2)	2405.5	*0.186*
Distraught	1.94 (2)	2.05 (2)	2653	*0.744*
Cared-For	2.77 (3)	3.30 (3)	2002	*0.003*
Friendly	2.28 (2)	3.06 (3)	1682.5	*< 0.001*
Welcomed	2.56 (3)	3.25 (3)	1864.5	*0.001*
Powerful	2.93 (3)	3.18 (3)	2414	*0.204*
Energetic	2.14 (2)	2.92 (3)	1726.5	*< 0.001*
Vigorous	2.32 (2)	2.65 (3)	2215	*0.074*
Isolated	1.51 (1)	1.90 (2)	2088.5	*0.006*
Lonely	1.35 (1)	1.78 (1)	2129.5	*0.008*
Abandoned	1.42 (1)	1.71 (1)	2384	*0.121*
Proud	2.70 (3)	3.26 (3)	2053	*0.007*
Triumphant	2.69 (3)	3.19 (3)	2100.5	*0.012*
Arrogant	1.87 (2)	2.06 (2)	2513.5	*0.37*
Ashamed	1.46 (1)	1.84 (2)	2175	*0.018*
Guilty	1.58 (1)	1.82 (2)	2344.5	*0.103*
Embarrassed	1.65 (1)	1.84 (2)	2453.5	*0.241*
Scornful	1.55 (1)	1.79 (2)	2313	*0.074*
Contemptuous	1.52 (1)	2.04 (2)	1927.5	*0.001*
Disdainful	1.61 (1)	1.81 (1)	2439	*0.211*
Humiliated	1.27 (1)	1.66 (1)	2117.5	*0.005*
Dishonored	1.28 (1)	1.70 (1)	2095.5	*0.004*
Resentful	1.90 (2)	2.03 (2)	2651	*0.737*
Grateful	3.19 (3)	3.56 (4)	2095	*0.014*
Respectful	2.63 (3)	3.26 (3)	1792.5	*<0.001*
Admiring	2.21 (2)	2.83 (3)	1860	*0.001*
Trusting	3.55 (4)	3.49 (4)	2696.5	*0.88*
Suspicious	2.24 (2)	2.30 (2)	2671.5	*0.802*
Happy	3.01 (3)	3.44 (3)	2085	*0.013*

Users vs. Non-Users Mann-Whitney U-Tests for Emotion Ratings

	Average (Median)		U-Test Results	
	Users	*Non-Users*	*U*	*Sig.*
Confident	3.59 (4)	3.64 (4)	1530.5	*0.67*
Secure	3.88 (4)	3.73 (4)	1530.5	*0.618*
Sad	1.67 (1)	1.55 (1)	1500	*0.509*
Depressed	1.62 (1)	1.55 (1.5)	1619	*0.963*
Down	1.82 (2)	1.52 (1)	1305	*0.198*
Afraid	1.73 (2)	1.59 (1.5)	1548.5	*0.686*
Nervous	1.8 (2)	1.95 (2)	1416.5	*0.291*
Anxious	2.09 (2)	2.00 (2)	1560	*0.74*
Angry	2.05 (2)	2.14 (2)	1525.5	*0.617*
Insulted	1.77 (1)	1.59 (1)	1437	*0.382*
Hostile	1.91 (2)	1.77 (2)	1516	*0.579*
Surprised	2.29 (2)	2.18 (2)	1511.5	*0.573*
Dazed	1.79 (2)	1.68 (1)	1513	*0.6*
Confused	2.17 (2)	2.18 (2)	1596.5	*0.878*
Freaked-Out	1.77 (2)	1.82 (2)	1513.5	*0.565*
Disgusted	1.61 (1)	1.5 (1)	1464.5	*0.419*
Dismayed	2.04 (2)	1.95 (2)	1601.5	*0.897*
Distraught	2.00 (2)	1.68 (1.5)	1335.5	*0.149*
Cared-For	3.05 (3)	3.09 (3)	1577.5	*0.807*
Friendly	2.69 (3)	2.41 (2.5)	1395.5	*0.264*
Welcomed	2.92 (3)	2.59 (2.5)	1355	*0.19*
Powerful	3.06 (3)	2.86 (3)	1466.5	*0.437*
Energetic	2.55 (3)	2.38 (2)	1399.5	*0.448*
Vigorous	2.49 (3)	2.59 (2)	1568.5	*0.856*
Isolated	1.71 (1)	1.68 (1.5)	1604.5	*0.905*
Lonely	1.57 (1)	1.50 (1)	1559.5	*0.715*
Abandoned	1.57 (1)	1.41 (1)	1464.5	*0.376*
Proud	2.99 (3)	2.91 (3)	1543.5	*0.685*
Triumphant	2.95 (3)	2.77 (3)	1464.5	*0.434*
Arrogant	1.97 (2)	1.77 (1.5)	1502.5	*0.535*
Ashamed	1.66 (1)	1.59 (1)	1502.5	*0.518*
Guilty	1.70 (2)	1.59 (1)	1441.5	*0.342*
Embarrassed	1.75 (2)	1.64 (1)	1544	*0.67*
Scornful	1.68 (1)	1.55 (1.5)	1588.5	*0.839*
Contemptuous	1.79 (2)	1.82 (1)	1562.5	*0.741*
Disdainful	1.71 (1)	1.32 (1)	1311	*0.1*
Humiliated	1.47 (1)	1.18 (1)	1293	*0.057*
Dishonored	1.50 (1)	1.36 (1)	1407.5	*0.226*
Resentful	1.97 (2)	1.95 (2)	1620	*0.969*
Grateful	3.38 (3)	3.50 (3.5)	1504	*0.578*
Respectful	2.96 (3)	2.71 (3)	1345.5	*0.325*
Admiring	2.54 (2)	2.68 (3)	1521	*0.643*
Trusting	3.52 (4)	3.45 (3.5)	1578.5	*0.807*
Suspicious	2.27 (2)	2.27 (2)	1614.5	*0.947*
Happy	3.24 (3)	3.27 (3)	1598	*0.926*

Appendix D

Survey instruments, sample descriptions, and complete statistical results for the studies presented in Chapter 6 can be found in this Appendix.

Survey Instruments

University Study

Basic Instruments

1. What is your age? _____
2. What is your gender? _____
3. Have you ever been hesitant to apply an update?
   - ○ Yes
   - ○ No
   - ○ I Don't Know
4. Have you ever been annoyed by an update message?
   - ○ Yes
   - ○ No
   - ○ I Don't Know
5. Have you ever been confused by an update message?
   - ○ Yes
   - ○ No
   - ○ I Don't Know

In-Depth Software Instruments

For the software listed in the chart below, participants in the second phase of the University study were asked to report whether they used each. If they reported using, the following survey instruments were then presented to them, with [software] being replaced with the specific software from the list, as appropriate.

Category	**[Software]**
Operating Systems	Microsoft Windows
	Apple laptops or desktops
	Linux
	iPhone
	Android
Web Browser	Mozilla Firefox
	Google Chrome
	Internet Explorer
	Safari
Productivity Software	Microsoft Office
	Open Office
	Adobe Acrobat
	Libre Office
Media Software	iTunes
	QuickTime
	Windows Media Player
Security Software	Norton products
	McAfee products
	Malwarebytes
Other	Skype
	Video Games

1. Approximately how long after you see a [software] update message do you wait to apply the update?
    - Immediately
    - 1 day
    - 3 days
    - A week
    - A month
    - Never
2. On a scale of 1–7, rate how much you agree with each statement.

    1 = do not agree at all, 7 = agree completely

    _ [Software] update messages are annoying.

    _ [Software] update messages are confusing.

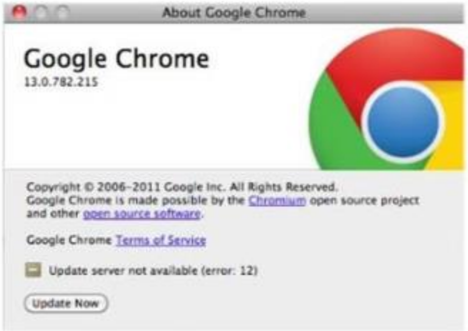
In-Depth Sample Message Instruments

Participants in the second phase of the University study were also shown a series of sample, real-world update and warning messages. With each image, the following survey instruments were displayed to all participants.

1. Rate from 1 = not at all, to 7 = very
   _ How important is the message?
   _ How annoying is the message?
   _ How confusing is the message?
   _ How noticeable is the message?
2. What did you like about the message? ____

   ____
3. What did you dislike about the message? ____

   ____

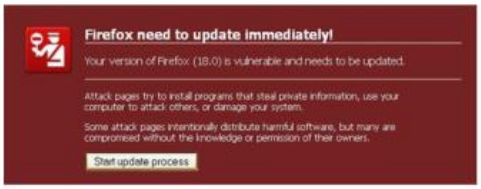


Copyright © 2006-2011 Google Inc. All Rights Reserved.
Google Chrome is made possible by the Chromium open source project and other open source software.

Google Chrome Terms of Service

Update server not available (error: 12)

Image 1



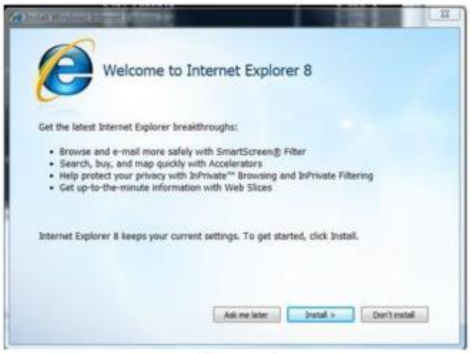
Firefox need to update immediately!

Your version of Firefox (18.0) is vulnerable and needs to be updated.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Image 2

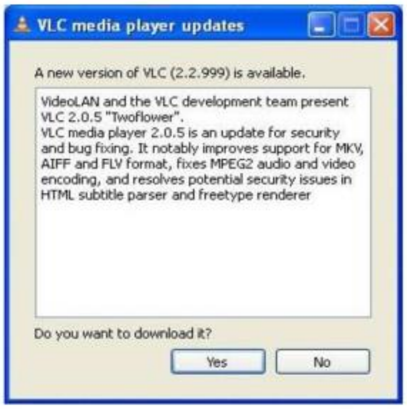


Get the latest Internet Explorer breakthroughs:

- Browse and e-mail more safely with SmartScreen® Filter
- Search, buy, and map quickly with Accelerators
- Help protect your privacy with InPrivate™ Browsing and InPrivate Filtering
- Get up-to-the-minute information with Web Slices

Internet Explorer 8 keeps your current settings. To get started, click Install.

Image 3

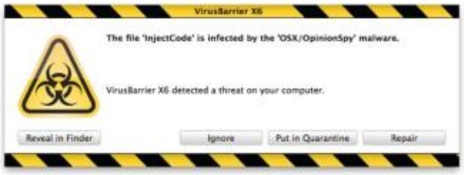


A new version of VLC (2.2.999) is available.

VideoLAN and the VLC development team present VLC 2.0.5 "Twoflower".
VLC media player 2.0.5 is an update for security and bug fixing. It notably improves support for MKV, AIFF and FLV format, fixes MPEG2 audio and video encoding, and resolves potential security issues in HTML subtitle parser and freetype renderer

Do you want to download it?

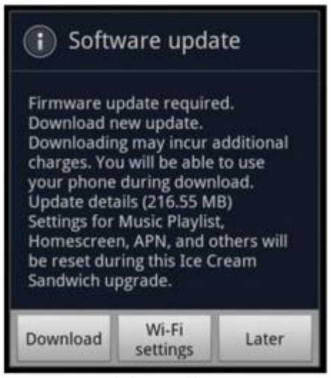
Image 4



The file 'InjectCode' is infected by the 'OSX/OpinionSpy' malware.

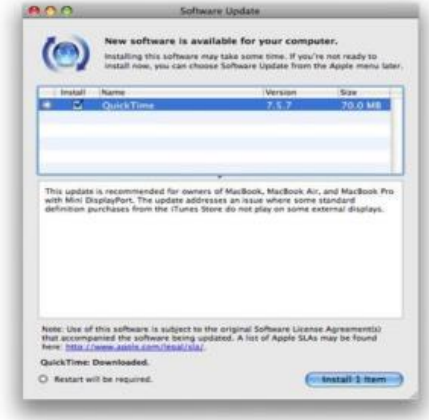
VirusBarrier X6 detected a threat on your computer.

Image 5



Firmware update required. Download new update. Downloading may incur additional charges. You will be able to use your phone during download. Update details (216.55 MB) Settings for Music Playlist, Homescreen, APN, and others will be reset during this Ice Cream Sandwich upgrade.

Image 6



Software Update

New software is available for your computer.

Installing this software may take some time. If you're not ready to install now, you can choose Software Update from the Apple menu later.

Install	Name	Version	Size
☑	QuickTime	7.5.7	70.0 MB

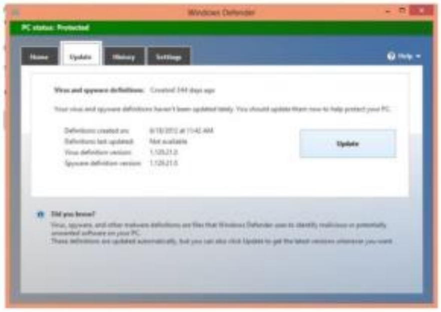
This update is recommended for owners of MacBook, MacBook Air, and MacBook Pro with Mini DisplayPort. The update addresses an issue where some standard definition purchases from the iTunes Store do not play on some external displays.

Note: Use of this software is subject to the original Software License Agreement(s) that accompanied the software being updated. A list of Apple SLAs may be found here: http://www.apple.com/legal/sla/.

QuickTime: Downloaded.

○ Restart will be required.

Image 7



Windows Defender

PC status: Protected

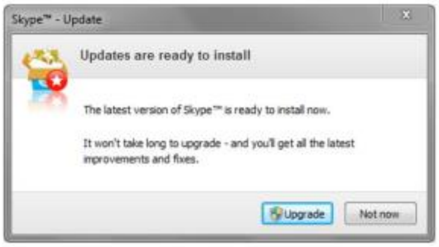
Virus and spyware definitions: Created 344 days ago

Your virus and spyware definitions haven't been updated lately. You should update them now to help protect your PC.

Definitions created on: 6/18/2012 at 11:42 AM
Definitions last updated: Not available
Virus definition version: 1.129.21.0
Spyware definition version: 1.129.21.0

Did you know?
Virus, spyware, and other malware definitions are files that Windows Defender uses to identify malicious or potentially unwanted software on your PC.
These definitions are updated automatically, but you can also click Update to get the latest versions whenever you want.

Image 8



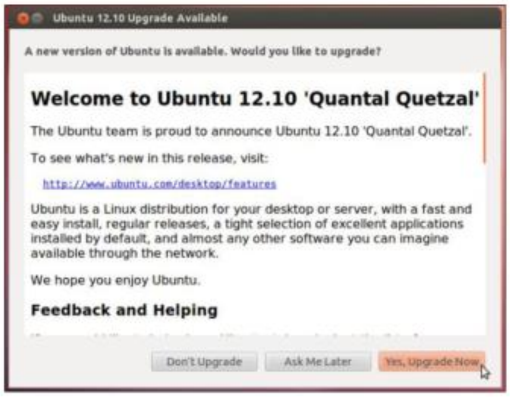
Skype™ - Update

Updates are ready to install

The latest version of Skype™ is ready to install now.

It won't take long to upgrade - and you'll get all the latest improvements and fixes.

Image 9



Ubuntu 12.10 Upgrade Available

A new version of Ubuntu is available. Would you like to upgrade?

Welcome to Ubuntu 12.10 'Quantal Quetzal'

The Ubuntu team is proud to announce Ubuntu 12.10 'Quantal Quetzal'.

To see what's new in this release, visit:

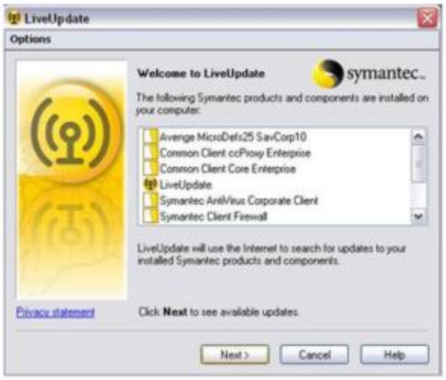
http://www.ubuntu.com/desktop/features

Ubuntu is a Linux distribution for your desktop or server, with a fast and easy install, regular releases, a tight selection of excellent applications installed by default, and almost any other software you can imagine available through the network.

We hope you enjoy Ubuntu.

Feedback and Helping

Image 13



LiveUpdate

Options

Welcome to LiveUpdate

The following Symantec products and components are installed on your computer:

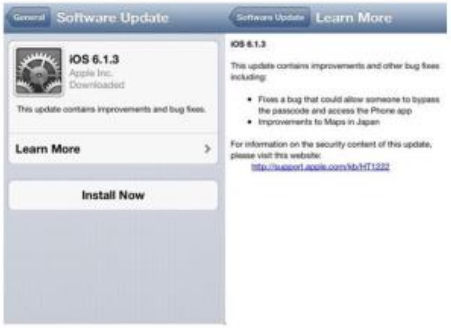
- Avenge MicroDefs25 SavCorp10
- Common Client ccProxy Enterprise
- Common Client Core Enterprise
- LiveUpdate
- Symantec AntiVirus Corporate Client
- Symantec Client Firewall

LiveUpdate will use the Internet to search for updates to your installed Symantec products and components.

Privacy statement

Click **Next** to see available updates.

Image 10



iOS 6.1.3
Apple Inc.
Downloaded

This update contains improvements and bug fixes.

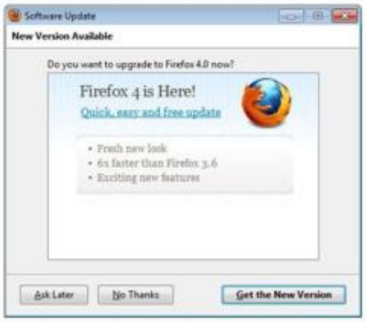
iOS 6.1.3

This update contains improvements and other bug fixes including:

- Fixes a bug that could allow someone to bypass the passcode and access the Phone app
- Improvements to Maps in Japan

For information on the security content of this update, please visit this website:
http://support.apple.com/kb/HT1222

Image 11



Software Update

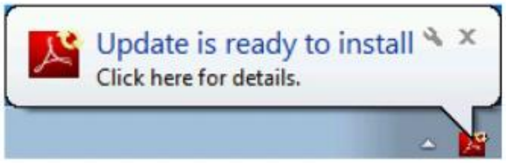
New Version Available

Do you want to upgrade to Firefox 4.0 now?

Firefox 4 is Here!
Quick, easy and free update

- Fresh new look
- 6x faster than Firefox 3.6
- Exciting new features

Image 12



Update is ready to install
Click here for details.

Image 14

Mechanical Turk Study

The following instruments were used through Mechanical Turk to gather in-depth emotion ratings from users related to software updates. The emotions instruments (questions 3-47) were shown twice, once with the *Relaxed* prompt preceding the instruments, then again after the *Pressured* prompt.

1. What is your age?
   - 18-25
   - 26-34
   - 35-54
   - 55-64
   - 65+
2. What is your gender?
   - Male
   - Female

Relaxed: Imagine a situation where the warning to update software appears while you are surfing the web with no specific purpose.

Pressured: Imagine a situation where the warning to update software appears while you are hard at work on an important project with a looming deadline.

3. One might feel CONFIDENT (e.g., because one is warned of possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
4. One might feel SECURE (e.g., because one is warned of possible danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
5. One might feel SAD (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
6. One might feel DEPRESSED (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
7. One might feel DOWN (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
8. One might feel AFRAID (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
9. One might feel NERVOUS (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
10. One might feel ANXIOUS (e.g., because one's work is attacked and in danger).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
11. One might feel ANGRY (e.g., because one's work is being attacked).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
12. One might feel INSULTED (e.g., because one's work is being attacked).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
13. One might feel HOSTILE (e.g., because one's work is being attacked).
   ○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

14. One might feel SURPRISED (e.g., because one does not expect the interruption).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
15. One might feel DAZED (e.g., because one does not expect the interruption).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
16. One might feel CONFUSED (e.g., because one does not expect the interruption).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
17. One might feel FREAKED OUT (e.g., because one does not expect the interruption).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
18. One might feel DISGUSTED (e.g., because one's work is being attacked).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
19. One might feel DISMAYED (e.g., because one's work is being attacked).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
20. One might feel DISTRAUGHT (e.g., because one's work is being attacked).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
21. One might feel CARED-FOR (e.g., because one is warned of possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
22. One might feel FRIENDLY (e.g., because one is warned of possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
23. One might feel WELCOMED (e.g., because one is warned of possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
24. One might feel POWERFUL (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
25. One might feel ENERGETIC (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
26. One might feel VIGOROUS (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
27. One might feel ISOLATED (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
28. One might feel LONELY (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
29. One might feel ABANDONED (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
30. One might feel PROUD (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
31. One might feel TRIUMPHANT (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
32. One might feel ARROGANT (e.g., because one is warned and can respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
33. One might feel ASHAMED (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
34. One might feel GUILTY (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
35. One might feel EMBARRASSED (e.g., because one’s response may be inadequate).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time
36. One might feel SCORNFUL (e.g., because the attack is easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

37. One might feel CONTEMPTUOUS (e.g., because the attack is easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

38. One might feel DISDAINFUL (e.g., because the attack is easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

39. One might feel HUMILIATED (e.g., because the attack is not easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

40. One might feel DISHONORED (e.g., because the attack is not easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

41. One might feel RESENTFUL (e.g., because the attack is not easily countered).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

42. One might feel GRATEFUL (e.g., because the system has given one the tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

43. One might feel RESPECTFUL (e.g., because the system has given one the tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

44. One might feel ADMIRING (e.g., because the system has given one the tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

45. One might feel TRUSTING (e.g., because the system has given one the tools to respond).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

46. One might feel SUSPICIOUS (e.g., because the warning may be unreliable).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

47. One might feel HAPPY (e.g., because one is warned of possible danger).
○ Never ○ Rarely ○ Sometimes ○ Often ○ All of the Time

Sample Descriptive Statistics

		Gender			**Age**			
	N	***Male***	***Female***	***N. G.***	***18-25***	***26-34***	***35-54***	***55+***
MTurk	**400**	**190**	**209**	**1**	**65**	**155**	**136**	**44**

		Gender		**Age**	
	N	*Male*	*Female*	*Avg.*	*St.D.*
University Phase 1	71	41	30	33	14
University Phase 2	155	62	93	22	5.4

Factor Loadings for ESEM Analysis

	1. Positive		**2. Anxious**		**3. Lonely**		**4. Hostile**	
Emotion	*R*	*P*	*R*	*P*	*R*	*P*	*R*	*P*
Happy	**0.781***	**0.803***	-0.014	-0.047	0.042	0.022	-0.008	-0.048
Confident	**0.822***	**0.853***	0.077	0.071	-0.170*	-0.167*	0.042	-0.007
Secure	**0.813***	**0.858***	0.177*	0.097*	-0.220*	-0.310*	-0.099	-0.013
Respectful	**0.771***	**0.788***	-0.013	0.018	0.077	0.081	0.026	-0.03
Grateful	**0.811***	**0.816***	0.228*	0.165*	-0.103	-0.152*	-0.119*	-0.103*
Friendly	**0.705***	**0.694***	-0.125*	-0.214*	0.214*	0.162*	-0.037	0.008
Cared-for	**0.753***	**0.799***	0.100*	0.003	0.028	-0.04	0.001	0.003
Welcomed	**0.705***	**0.743***	-0.085*	-0.166*	0.148*	0.141*	-0.037	0.022
Trusting	**0.755***	**0.785***	0.128*	0.08	-0.071	-0.145*	-0.140*	-0.042
Admiring	**0.692***	**0.753***	-0.018	-0.081*	0.129*	0.139*	0.112*	0.016
Triumphant	**0.670***	**0.698***	0.004	0.003	0.109	0.073	0.098	0.058
Proud	**0.652***	**0.726***	-0.072	-0.131*	0.120*	0.138*	0.175*	0.018
Powerful	**0.714***	**0.757***	-0.082	-0.05	-0.015	-0.003	0.206*	0.163*
Energetic	**0.620***	**0.641***	-0.152*	-0.045	0.217*	0.214*	0.076	-0.029
Vigorous	**0.630***	**0.614***	0.021	0.03	0.216*	0.108	0.068	0.096
Confused	0.016	0.032	**0.610***	**0.535***	0.189*	0.213*	-0.006	0.059
Anxious	0.013	0.005	**0.680***	**0.723***	0.237*	0.049	0.039	0.097
Nervous	0.023	0.062	**0.692***	**0.749***	0.252*	0.085	-0.054	0.069
Freaked out	-0.041	0.024	**0.534***	**0.654***	0.257*	0.115*	0.112*	0.121*
Afraid	0.04	0.008	**0.573***	**0.727***	0.425*	0.237*	-0.023	-0.071
Surprised	0.235*	0.252*	**0.469***	**0.538***	-0.029	-0.135*	0.117	0.155*
Dismayed	0.037	0.006	**0.451***	**0.644***	0.150*	0.034	0.324*	0.242*
Distraught	0.01	-0.051	**0.434***	**0.551***	**0.444***	0.124*	0.106*	0.267*
Suspicious	-0.105*	-0.021	**0.477***	0.381*	-0.026	-0.088	0.168*	0.244*
Dazed	0.105*	0.162*	0.324*	**0.484***	0.327*	0.222*	0.062	0.089
Sad	0.026	0.029	0.195*	**0.484***	**0.601***	**0.498***	0.104*	-0.029
Depressed	-0.048	-0.064	0.225*	**0.503***	**0.678***	**0.542***	0.016	-0.061
Down	-0.06	-0.008	0.363*	**0.597***	**0.512***	**0.422***	0.137*	-0.05
Lonely	0.041	-0.001	-0.069	-0.038	**0.821***	**0.833***	-0.002	0.027
Abandoned	0.005	-0.016	0.028	0.143*	**0.824***	**0.761***	-0.037	0.006
Ashamed	0.061	0.028	-0.022	0.012	**0.825***	**0.823***	-0.022	0.028
Isolated	0.016	0.015	0.087*	0.121*	**0.787***	**0.774***	-0.056	0.012
Humiliated	-0.018	0.034	0.032	0.100*	**0.802***	**0.767***	0.023	0.066
Embarrassed	0.044	0.051	0.073	0.007	**0.777***	**0.795***	-0.029	0.073*
Guilty	0.012	0.096*	0.017	0.06	**0.749***	**0.687***	0.059	0.024
Dishonored	0.038	0.084*	-0.003	0.053	**0.721***	**0.570***	0.139*	0.253*
Disdainful	0.124*	0.116*	0.014	0.021	-0.048	0.047	**0.821***	**0.717***
Scornful	0.120*	0.017	0.009	-0.025	0.037	0.110*	**0.747***	**0.751***
Contemptuous	0.113*	0.183*	0.062	0.017	0.027	0.057	**0.676***	**0.659***
Hostile	-0.068	-0.042	0.225*	0.372*	0.025	-0.037	**0.634***	**0.573***
Resentful	-0.025	-0.076	0.351*	0.289*	0.005	-0.075	**0.574***	**0.600***
Disgusted	-0.011	-0.062	0.204*	0.294*	0.110*	0.177*	**0.573***	**0.434***
Angry	-0.066	-0.088*	0.381*	**0.466***	-0.024	-0.055	**0.565***	**0.481***
Insulted	-0.022	0.067	0.075	0.141*	0.385*	0.306*	**0.436***	**0.454***
Arrogant	0.298*	0.350*	-0.106*	-0.173*	0.251*	0.263*	**0.405***	0.365*

Notes: * is p<.05 significant; loadings > .4 and significant in bold. *R* = Relaxed, *P* = Pressured

Appendix E

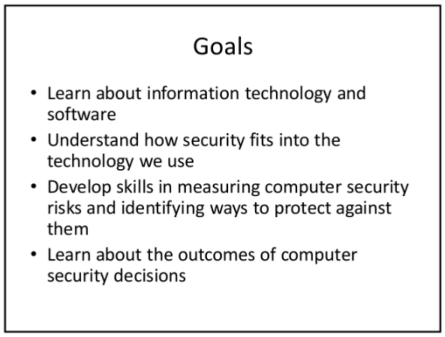
Intervention scripts and slides, sample descriptions, and complete statistical results for the study presented in Chapter 7 can be found in this Appendix.

Intervention Video Slides and Scripts

Update Slides

The Impacts of Your Cybersecurity Decisions

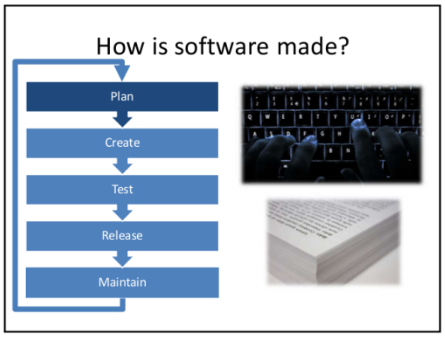
1



Goals

- Learn about information technology and software
- Understand how security fits into the technology we use
- Develop skills in measuring computer security risks and identifying ways to protect against them
- Learn about the outcomes of computer security decisions

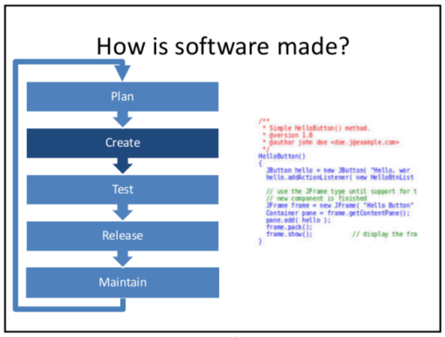
2



How is software made?

Plan → Create → Test → Release → Maintain

3



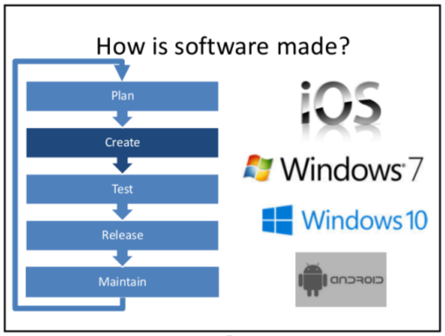
How is software made?

Plan → Create → Test → Release → Maintain

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // new component is finished
  JFrame frame = new JFrame( "Hello Button"
  Container pane = frame.getContentPane();
  pane.add( hello );
  frame.pack();
  frame.show();          // display the fra
}
```

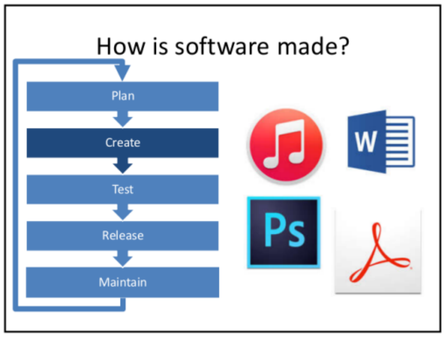
4



How is software made?

Plan → Create → Test → Release → Maintain

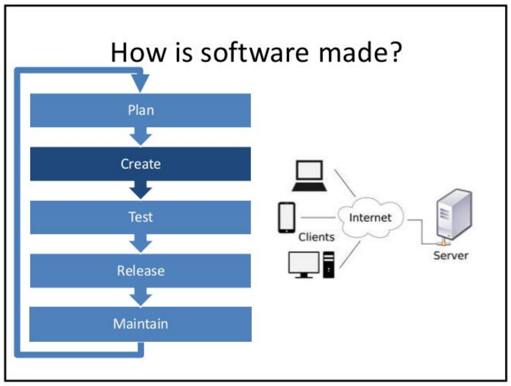
5



How is software made?

Plan → Create → Test → Release → Maintain

6



How is software made?

Plan

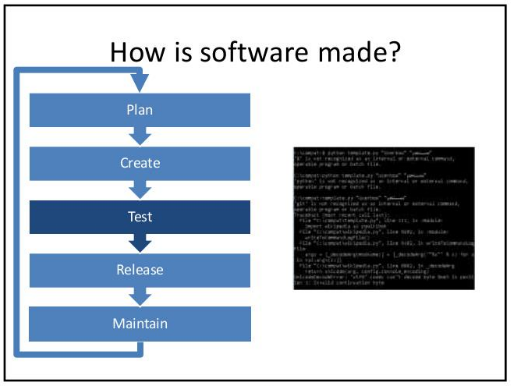
Create

Test

Release

Maintain

7



How is software made?

Plan

Create

Test

Release

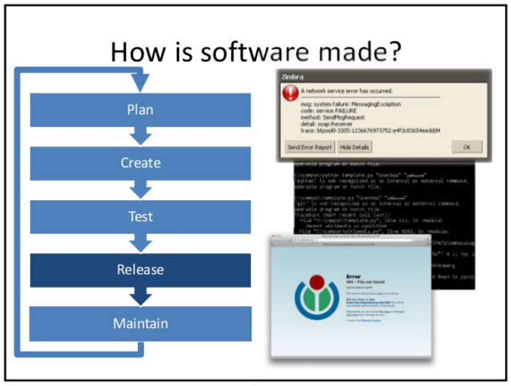
Maintain

```
C:\compat>$ python template.py "UserBox" "[illegible]"
'$' is not recognized as an internal or external command,
operable program or batch file.

C:\compat>python template.py "UserBox" "[illegible]"
'python' is not recognized as an internal or external command,
operable program or batch file.

C:\compat>template.py "UserBox" "[illegible]"
'git' is not recognized as an internal or external command,
operable program or batch file.
Traceback (most recent call last):
  File "C:\compat\template.py", line [illegible], in <module>
    import wikipedia as pywikibot
  File "C:\compat\wikipedia.py", line [illegible], in <module>
    [illegible]
  File "C:\compat\wikipedia.py", line [illegible], in [illegible]
[illegible]
    [illegible]
  File "C:\compat\wikipedia.py", line [illegible], in _decodeArg
    return unicode(arg, config.console_encoding)
UnicodeDecodeError: 'utf8' codec can't decode byte [illegible] in posit
ion [illegible]: invalid continuation byte
```

8



How is software made?

Plan

Create

Test

Release

Maintain

Zimbra

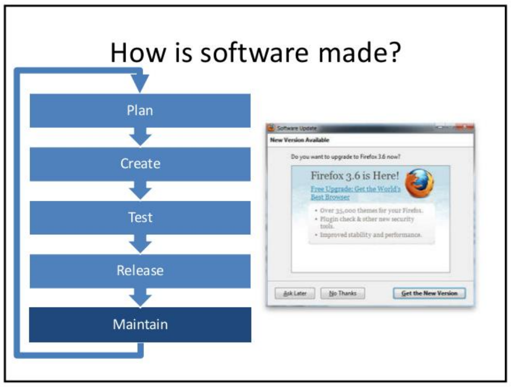
A network service error has occurred.

```
msg: system failure: MessagingException
code: service.FAILURE
method: SendMsgRequest
detail: soap:Receiver
trace: btpool0-3305:1236676973752:e4f3c63654eeddd4
```

Error

404 – File not found

9



How is software made?

Plan

Create

Test

Release

Maintain

Software Update

New Version Available

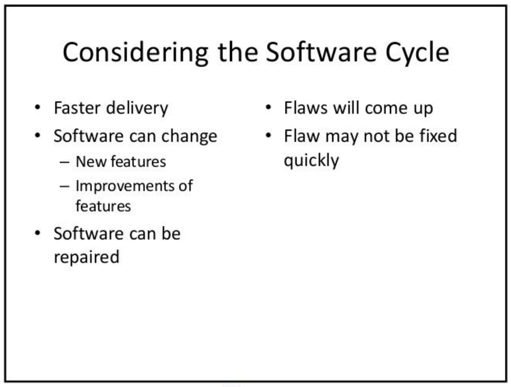
Do you want to upgrade to Firefox 3.6 now?

Firefox 3.6 is Here!

Free Upgrade: Get the World's Best Browser

- Over 35,000 themes for your Firefox.
- Plugin check & other new security tools.
- Improved stability and performance.

10

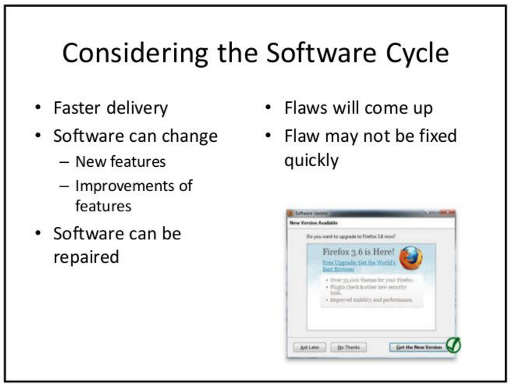


Considering the Software Cycle

- Faster delivery
- Software can change
  - New features
  - Improvements of features
- Software can be repaired

- Flaws will come up
- Flaw may not be fixed quickly

11



Considering the Software Cycle

- Faster delivery
- Software can change
  - New features
  - Improvements of features
- Software can be repaired

- Flaws will come up
- Flaw may not be fixed quickly

Software Update

New Version Available

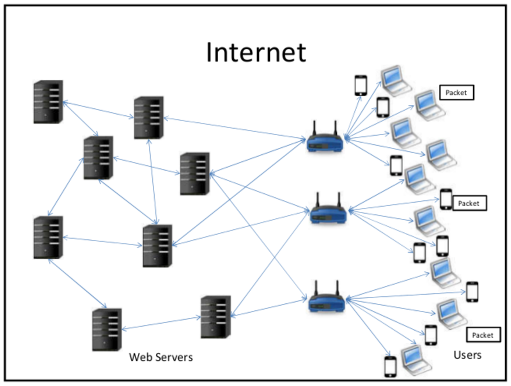
Do you want to upgrade to Firefox 3.6 now?

Firefox 3.6 is Here!

Free Upgrade: Get the World's Best Browser

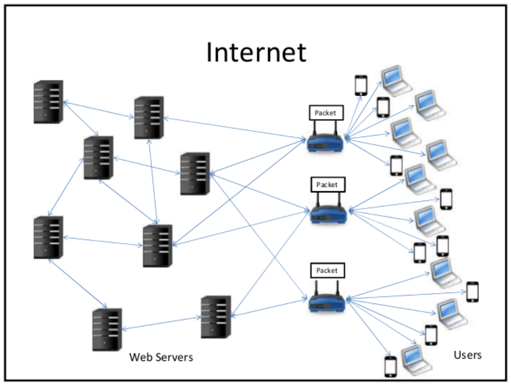
- Over 35,000 themes for your Firefox.
- Plugin check & other new security tools.
- Improved stability and performance.

12



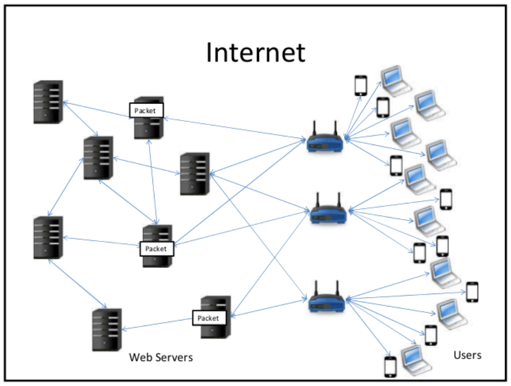
Internet

13



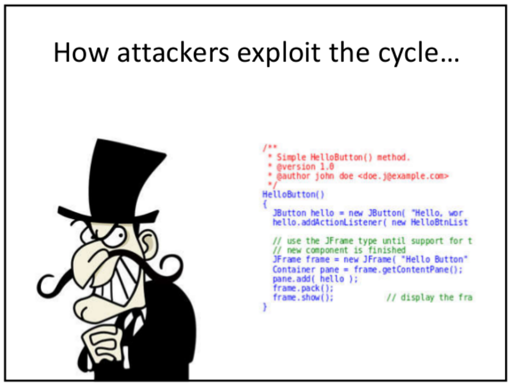
Internet

14



Internet

15

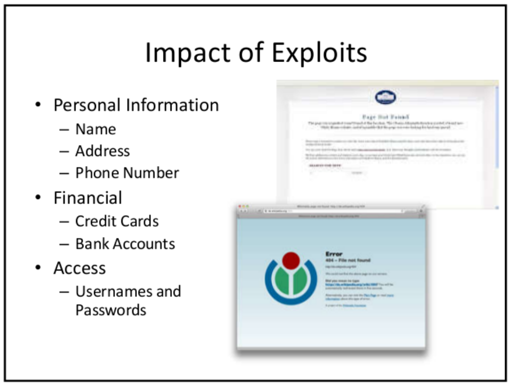


How attackers exploit the cycle…

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // new component is finished
  JFrame frame = new JFrame( "Hello Button"
  Container pane = frame.getContentPane();
  pane.add( hello );
  frame.pack();
  frame.show();            // display the fra
}
```

16



Impact of Exploits

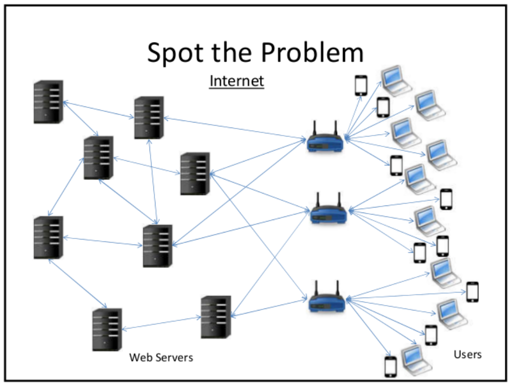
- Personal Information
  - Name
  - Address
  - Phone Number
- Financial
  - Credit Cards
  - Bank Accounts
- Access
  - Usernames and Passwords

Page Not Found

Error

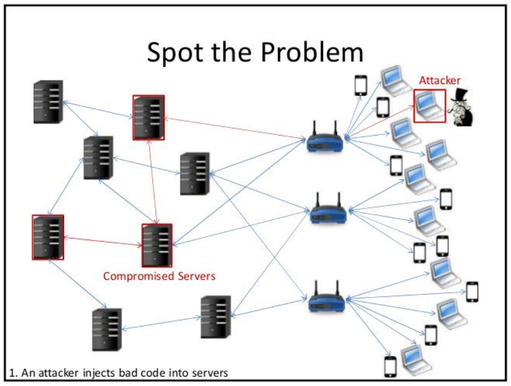
404 – File not found

17



Spot the Problem

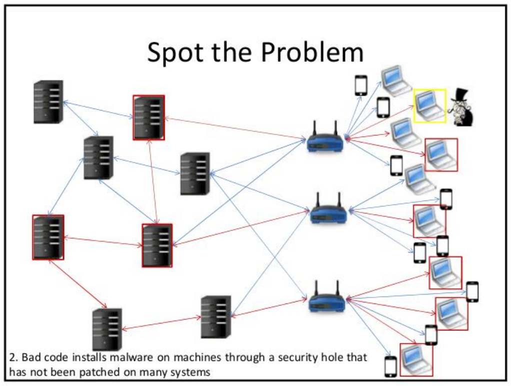
18



Spot the Problem

1. An attacker injects bad code into servers

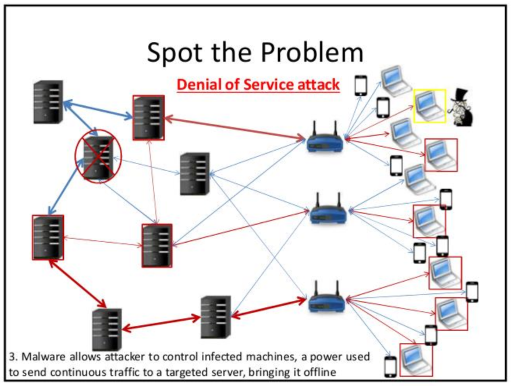
19



Spot the Problem

2. Bad code installs malware on machines through a security hole that has not been patched on many systems

20

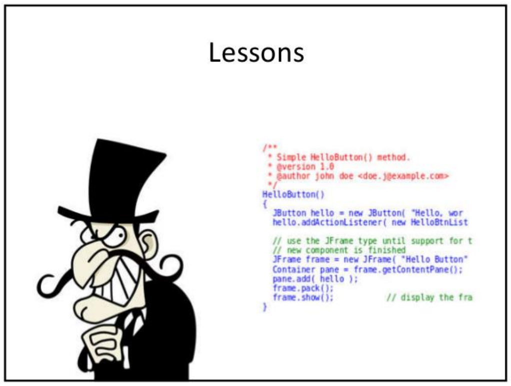


Spot the Problem

Denial of Service attack

3. Malware allows attacker to control infected machines, a power used to send continuous traffic to a targeted server, bringing it offline

21

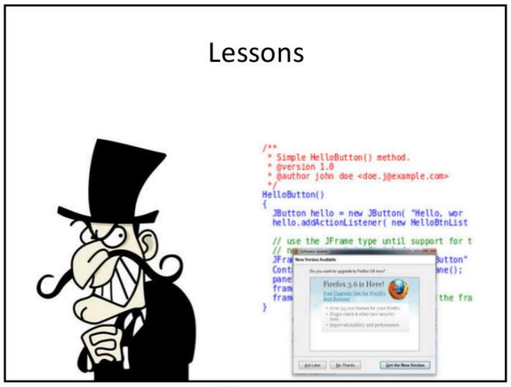


Lessons

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // new component is finished
  JFrame frame = new JFrame( "Hello Button"
  Container pane = frame.getContentPane();
  pane.add( hello );
  frame.pack();
  frame.show();             // display the fra
}
```

22

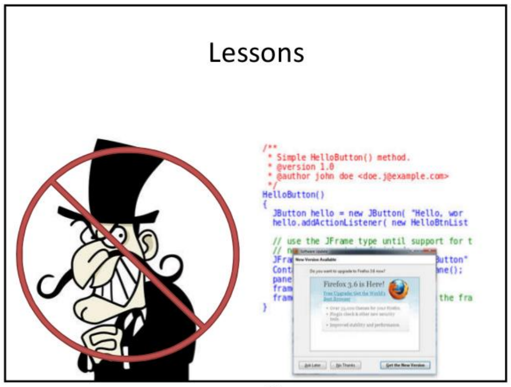


Lessons

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // n
  JFra                                   Button"
  Cont                                   ne();
  pane
  fram
  fram                                   the fra
}
```

23



Lessons

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // n
  JFra                                   Button"
  Cont                                   ne();
  pane
  fram
  fram                                   the fra
}
```

24

Update Basic

Software development is a large task that has many accepted methods, but there are basics that most developers follow. We will explain these basics to help you understand how security vulnerabilities arise. Most software is developed in a cycle, meaning development never quite stops. Instead, once a product is created, it is continuously tuned and improved as time goes on. Sometimes this is done to add new features that weren't needed or considered before. Other times, flaws and bugs in the original program need to be fixed.

When creating a new program, the first step is to plan what the interface and outputs of the software will be. This step also involves creating some kind of documentation that will serve as a guide in later stages.

When the software is planned and the outlines and blueprints of the program are ready, it is time to actually make it. This step can be very time-consuming, especially for software like operating systems or highly specific, heavyweight programs like productivity software such as Microsoft Word or Adobe PDF Acrobat or even entertainment and creative software, like Adobe Photoshop or Apple iTunes. Software that uses the Internet or other networks that allow it to communicate with other machines can be even harder to create due to the larger number of interactions to consider.

As development completes and a seemingly working program remains, testing usually follows to find issues that aren't so apparent. This process may utilize outside organizations or individuals, commonly known as beta testers who purposely try to break a program to find its flaws.

Once problems in the software have been identified and repaired, the software is released to the public, but the development cycle continues into maintenance. Though testing will find many issues, problems can be hidden, only appearing under specific circumstances when installed and used on personal devices. Therefore, as these issues are reported, regular software updates or patches are released that address the problems.

Creating software in this cycle presents benefits and negatives. On one hand, software can be created fast and changed easily. Additionally, products can be delivered much sooner than would otherwise be possible. On the other hand, flaws on delivery are almost unavoidable and there is always the possibility that the cycle will end before all issues are resolved, like when a product is no longer supported due to it being too old.

Thus, applying software updates in a timely manner is important to making sure security is the best it can be. Since flaws are unavoidable, providers utilize software updates to improve their products and the services they deliver.

Though the negative aspects of the cycle can be reduced by prompt and regular updating, the introduction of networked components to software has made the likelihood of flaws both appearing and being found much higher. When software uses networks like the Internet, it sends information between computers, which allows easy communication between devices and people, while also making computing power shareable via web-based applications.

With easier communication comes a trade off from security. Since machines other than your own are involved when the Internet is utilized, you are open to attack by remote actors. Such actors work hard to find flaws in software they can exploit called "back-doors." Like all flaws, back-doors are commonly patched in software updates, but even known exploits can be viable for attackers since so much software remains out of date.

Backdoor exploits can be used in many ways. Depending on the particular software and flaw being utilized, attackers could access data, such as personal information, credit card numbers, or credentials to bank accounts. Some flaws may also allow attackers to access other programs or features outside of the software that contains the flaw. In this case, a resourceful attacker can do many things, such as a distributed denial of service attack, commonly known as a DDoS attack, or “Dee-Dos.” Though there are other ways to execute a DDoS attack, we will see how flaws in software can be used as the starting point for this kind of exploit.

Here is a representation of the internet. On one end, you have the various web servers that host the content we view and services we use. On the other end, we have the end-users and their devices, including PCs and smart-phones.

Information travels easily from end to end, as well as between servers, and some end users.

In the mass of information flowing in all directions, a malicious actor can arise. The attacker uploads a virus to a compromised server to be downloaded by anyone who visits the website hosted on the server.

Before anyone notices, the virus infects many people’s devices. Using existing back-doors in out-of-date software on the infected machines, the attacker might have a lot of access and power. In this case, maybe they want to take out a web-service they don’t like.

The attacker can generate tons of junk messages targeting a particular website or service. His virus can send short requests over the Internet from the various infected machines. Though each message or request is small, if a large number of machines partake in the attack, the cumulative traffic can shut down the website or service, especially if the victim is caught off guard.

Backdoor exploits can be used for many attacks and so closing these flaws is imperative towards securing the entire Internet. Apply software updates is a key step to closing any security flaws in the software you use, and is among the most expert recommended actions an individual can take to increase their security. Though not all updates contain security patches, keeping programs up to date helps stop frustration with software before it begins.

Update Emotion

Software development is a large task that has many accepted methods, but there are basics that most developers follow. We will explain these basics to help you understand how security vulnerabilities arise. Most software is developed in a cycle, meaning development never quite stops. Instead, once a product is created, it is continuously tuned and improved as time goes on. Sometimes this is done to add new features that weren't needed or considered before. Other times, flaws and bugs in the original program need to be fixed.

When creating a new program, the first step is to plan what the interface and outputs of the software will be. This step also involves creating some kind of documentation that will serve as a guide in later stages.

When the software is planned and the outlines and blueprints of the program are ready, it is time to actually make it. This step can be very time-consuming, especially for software like operating systems or highly specific, heavyweight programs like productivity software such as Microsoft Word or Adobe PDF Acrobat or even entertainment and creative software, like Adobe Photoshop or Apple iTunes. Software that uses the Internet or other networks that allow it to communicate with other machines can be even harder to create due to the larger number of interactions to consider.

As development completes and a seemingly working program remains, testing usually follows to find issues that aren't so apparent. Since companies know how annoying, frustrating, and confusing problems with software can be, they may utilize outside organizations or individuals, commonly known as beta testers who purposely try to break a program to find flaws so that they can be fixed.

Once problems in the software have been identified and repaired, the software is released to the public, but the development cycle continues into maintenance. Though testing will find many issues, hidden annoying problems can still remain. Software updates are therefore used to repair and maintain software after it is released.

Creating software in this cycle presents benefits and negatives. On one hand, software can be created fast and changed easily. Additionally, products can be delivered much sooner than would otherwise be possible. On the other hand, flaws on delivery are almost unavoidable and there is always the possibility that the cycle will end before all issues are resolved, like when a product is no longer supported due to it being too old. Therefore, you may run into frustrating issues while using the software, which providers work to remedy with regular updates.

Thus, applying software updates in a timely manner is important. Even though an unexpected update message may surprise you and be annoying if it interrupts a task or you may fear the changes the update will make, taking notice and applying the update will help avoid further frustration from faulty or insecure software and also increase your satisfaction with software.

Though the negative aspects of the cycle can be reduced by prompt and regular updating, the introduction of networked components to software has made the likelihood of flaws both appearing and being found much higher. When software uses networks like the Internet, it sends information between computers, which allows easy communication between devices and people, while also making computing power shareable via web-based applications.

With easier communication comes a trade off from security. Since machines other than your own are involved when the Internet is utilized, you are open to attack by remote actors. Such actors work hard to find flaws in software they can exploit called "back-doors." Like all flaws, back-doors are commonly patched in software updates, but even known exploits can be viable for attackers since so much software remains out of date.

Backdoors can be used in many ways, sometimes without the victim even realizing it. Depending on the particular software and flaw, attackers could access personally and financially sensitive data, and even try to steal assets or identity. In either case, the victim is sure to have significantly negative experiences and have to work hard to recover from the damages.   Some flaws may also allow attackers to access other programs or features outside of the software that contains the flaw. In this case, a resourceful attacker can do many things, such as a distributed denial of service attack, commonly known as a DDoS or "Dee-Dos" attack. Though there are other ways to execute a DDoS attack, we will see how flaws in software can be used as the starting point for this particularly annoying exploit.

Here is a representation of the internet. On one end, you have the various web servers that host the content we view and services we use. On the other end, we have the end-users and their devices, including PCs and smart-phones.

Information travels easily from end to end, as well as between servers, and some users, this is something everyone involved is happy about. This includes email, video, music, as well as other data.

In the mass of information flowing in all directions, a malicious actor can arise. The attacker uploads a virus to a compromised server to be downloaded by anyone who visits the website hosted on the server.

Before anyone notices, the virus infects many people's devices. Using existing back-doors in out-of-date software on the infected machines, the attacker might have a lot of access and power. In this case, maybe they want to take out a web-service they don't like.

The attacker can generate tons of junk messages targeting a particular website or service. His virus can send short requests over the Internet from the various infected machines. Though each message or request is small, if a large number of machines partake in the attack, the cumulative traffic can shut down the website or service, especially if the victim is caught off guard. With the website being overwhelmed, legitimate users cannot access the content, causing widespread annoyance, frustration, and confusion, while also hurting user's opinion of the website.

Backdoors can be used for many attacks and so closing these flaws is imperative towards securing the entire Internet, while also avoiding frustration and confusion. Recommended by security experts, applying software updates can increase security while also making you happier through improved performance. Though taking the time can be annoying or you may worry about the changes that will come, keeping programs up to date helps stop frustration with software before it begins.

Update Social

Software development is a large task that has many accepted methods, but there are basics that most developers follow. We will explain these basics to help you understand how security vulnerabilities arise. Most software is developed in a cycle, meaning development never quite stops. Instead, once a product is created, it is continuously tuned and improved as time goes on. Sometimes this is done to add new features that weren't needed or considered before. Other times, flaws and bugs in the original program need to be fixed.

When creating a new program, the first step is to plan what the interface and outputs of the software will be. This step also involves creating some kind of documentation that will serve as a guide to the many diligent programmers that could be involved in later stages.

When the software is planned and the outlines and blueprints of the program are ready, it is time to actually make it. This step can involve a lot of work from many people connected to a project, especially for software like operating systems or highly specific, heavyweight programs like productivity software such as Microsoft Word or Adobe PDF Acrobat or entertainment and creative software, like Adobe Photoshop or Apple iTunes. Software that uses the Internet or other networks can be even harder to create since many people's devices can be involved in the software.

As development completes and a seemingly working program remains, testing usually follows to find issues that aren't so apparent. This process may utilize outside organizations or individuals, commonly known as beta testers who purposely try to break a program to find its flaws.

Once problems in the software have been identified and repaired, the software is released to the public, but the development cycle continues into maintenance. Though testing will find many issues, problems can be hidden, only appearing under specific circumstances when installed and used on personal devices. Therefore, as these issues are reported, regular software updates or patches are released that address the problems.

Creating software in this cycle presents benefits and negatives. On one hand, software can be created fast and changed easily to help as many people as possible by providing them useful programs. On the other hand, flaws on delivery are almost unavoidable and can impact many users, depending on how widely used the software is.

Thus, applying software updates in a timely manner is important to making sure your security, as well as the security of other people's devices is as good as it can be. Since flaws are unavoidable, providers utilize software updates to improve their products and the services for all their users.

Though the negative aspects of the cycle can be reduced by prompt and regular updating, the introduction of networked components to software has made the likelihood of flaws both appearing and being found much higher. When software uses networks like the Internet, it sends information between computers, which allows easy communication between devices and people, while also making computing power shareable via web-based applications.

With easier communication comes a trade off from security. Since machines other than your own are involved when the Internet is utilized, you are open to attack via other devices, and your device can be used to attack others. This can be done using software exploits called "back-doors." Like all flaws, back-doors are commonly patched in software updates, but even known exploits can be viable for attackers since so much software remains out of date.

Backdoor exploits can be used in many ways. Depending on the particular software and flaw being utilized, attackers could access data, such as personal information, credit card numbers, or credentials to bank accounts. Some flaws may also allow attackers to access other programs or features outside of the software that contains the flaw. In this case, a resourceful attacker can impact many users in many ways, such as a distributed denial of service attack, commonly known as a DDoS or "Dee-Dos" attack. Though there are other ways to execute a DDoS attack, we will see how flaws in software can be used as the starting point for this kind of exploit and how users can be impacted by the security behavior of others.

Here is a representation of the internet. On one end, you have the various web servers that host the content we view and services we use. On the other, we have many different end users and their devices, including PCs and smart-phones.

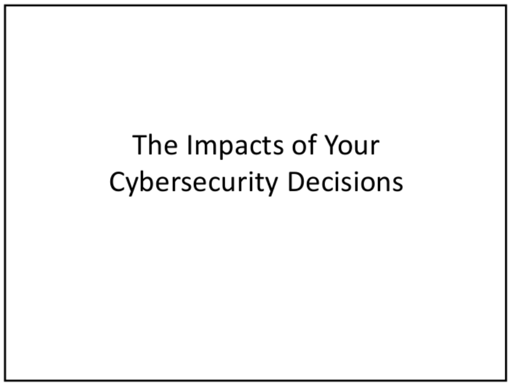
In the mass of information flowing in all directions, a malicious actor can arise. The attacker uploads a virus to a compromised server to be downloaded by anyone who visits the website hosted on the server.

Before anyone notices, the virus infects many people's devices. Using existing back-doors in out-of-date software, the attacker can use the infected machines as a group to do many things. In this case, maybe they want to take out a web-service they don't like.

The attacker can generate tons of junk messages targeting a particular website or service. His virus can send short requests over the Internet from the various infected machines. Though each message or request is small, if a large number of machines partake in the attack, the cumulative traffic can shut down the website or service, especially if the victim is caught off guard. In this case, because some people didn’t apply appropriate security patches, no one will be able to access the targeted website or service during the attack and even for some time in the aftermath.

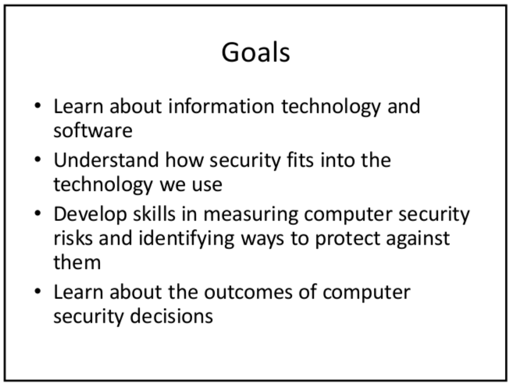
Backdoors can be used for many attacks and so closing these flaws is imperative towards securing the entire Internet. Applying software updates is a key step in closing any security flaws that may exist is in the software you use and is among the most expert recommended actions a user can take to increase security. Though not all updates contain security patches, keeping your programs up to date is important to everyone’s protection.

Password Manager Slides



The Impacts of Your Cybersecurity Decisions

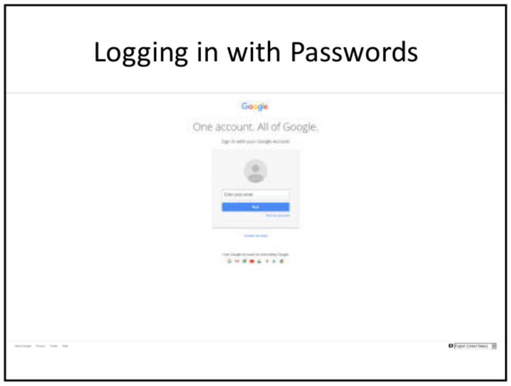
1



Goals

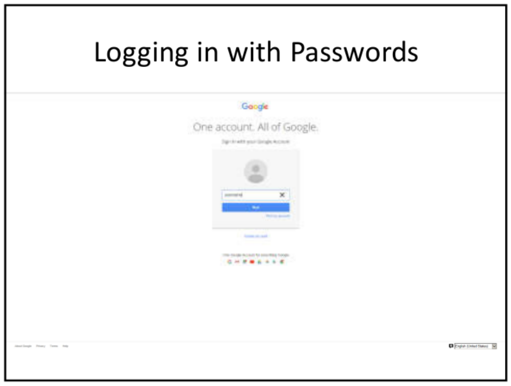
- Learn about information technology and software
- Understand how security fits into the technology we use
- Develop skills in measuring computer security risks and identifying ways to protect against them
- Learn about the outcomes of computer security decisions

2



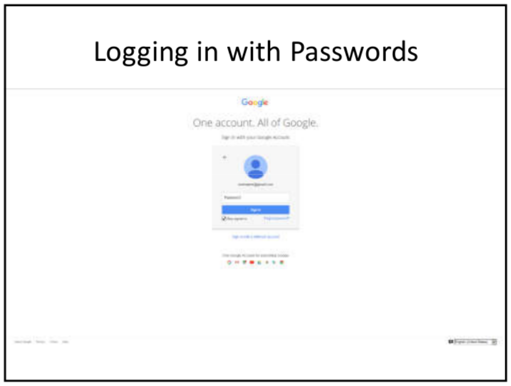
Logging in with Passwords

3



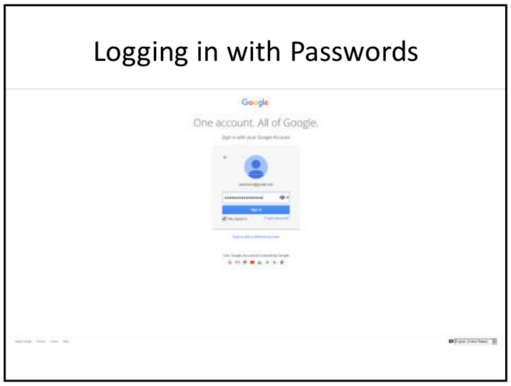
Logging in with Passwords

4



Logging in with Passwords

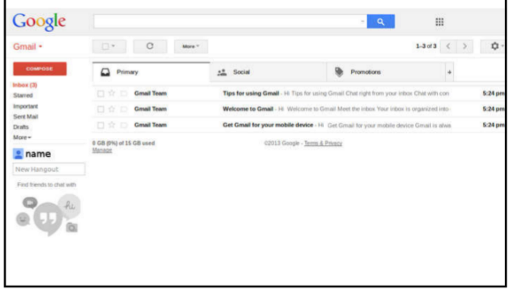
5



Logging in with Passwords

6

Logging in with Passwords



Gmail Team — Tips for using Gmail - Hi Tips for using Gmail Chat right from your inbox Chat with con — 5:24 pm

Gmail Team — Welcome to Gmail - Hi Welcome to Gmail Meet the inbox Your inbox is organized into — 5:24 pm

Gmail Team — Get Gmail for your mobile device - Hi Get Gmail for your mobile device Gmail is alwa — 5:24 pm

0 GB (0%) of 15 GB used
Manage

©2013 Google - Terms & Privacy

7

Simple passwords…

Password
123456
12345678
Qwerty
abc123
dragon

trustno1
football
Iloveyou
Ashley
passw0rd
987654321
qazwsx

welcome
photoshop
batman
letmein
12121212

8

Simple passwords…

Password
123456
12345678
Qwerty
abc123
dragon

trustno1
football
Iloveyou
Ashley
passw0rd
987654321
qazwsx

welcome
photoshop
batman
letmein
12121212

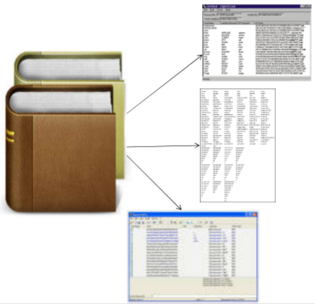
Easy to remember, but easy to guess!

9

Dictionary Attacks

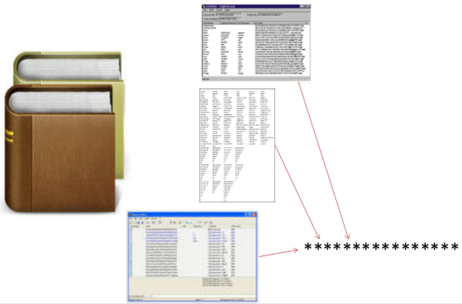
10

Dictionary Attacks

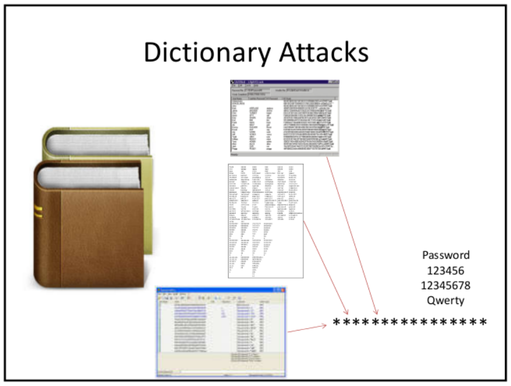


11

Dictionary Attacks



12

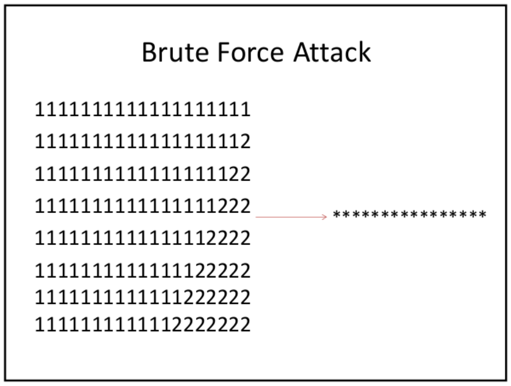


Dictionary Attacks

Password
123456
12345678
Qwerty

****

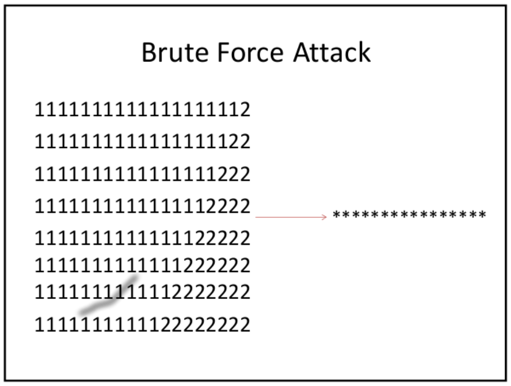
13



Brute Force Attack

1111111111111111111
1111111111111111112
1111111111111111122
1111111111111111222 → ****************
1111111111111112222
1111111111111122222
1111111111111222222
1111111111112222222

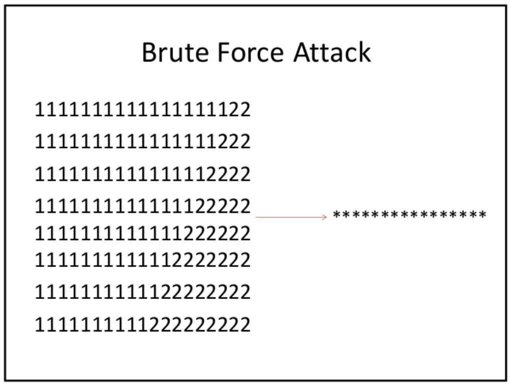
14



Brute Force Attack

1111111111111111112
1111111111111111122
1111111111111111222
1111111111111112222 → ****************
1111111111111122222
1111111111111222222
1111111111112222222
1111111111122222222

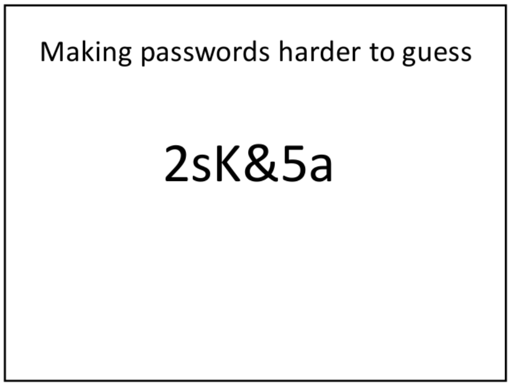
15



Brute Force Attack

1111111111111111122
1111111111111111222
1111111111111112222
1111111111111122222 → ****************
1111111111111222222
1111111111112222222
1111111111122222222
1111111111222222222

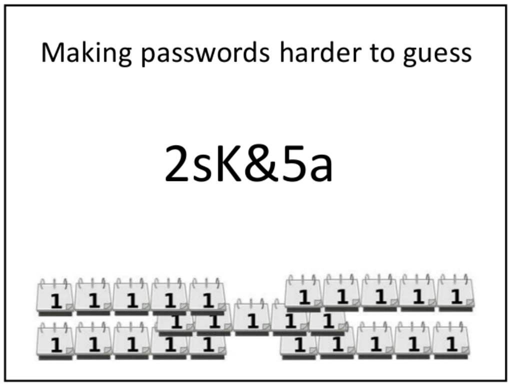
16



Making passwords harder to guess

2sK&5a

17

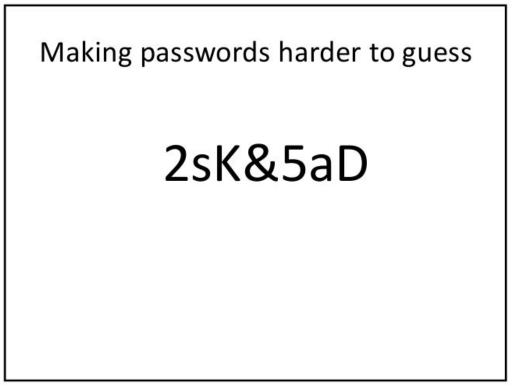


Making passwords harder to guess

2sK&5a

1 1 1 1 1 1 1 1 1 1
1 1 1 1 1
1 1 1 1 1 1 1 1 1 1

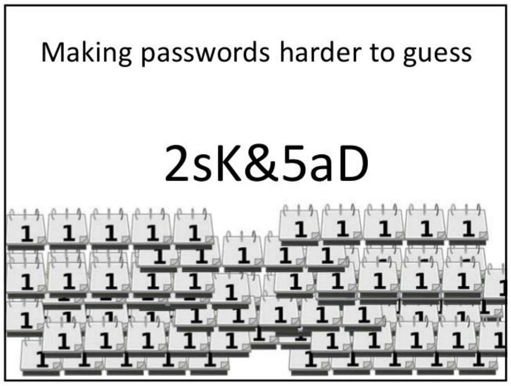
18



Making passwords harder to guess

2sK&5aD

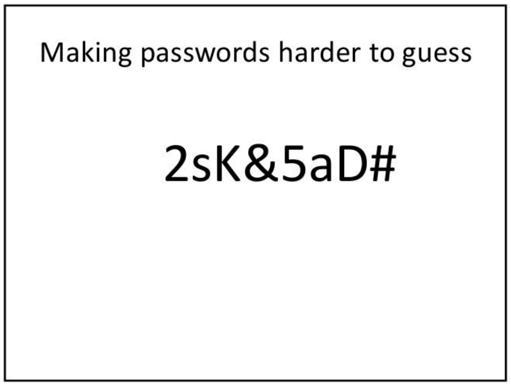
19



Making passwords harder to guess

2sK&5aD

20



Making passwords harder to guess

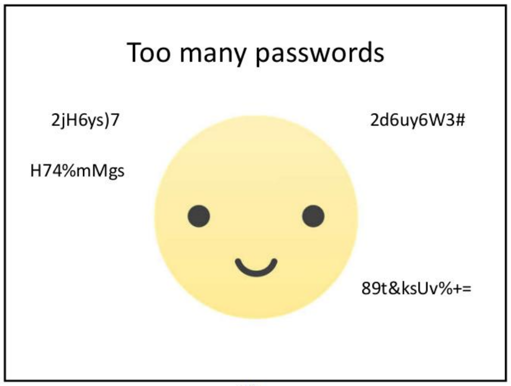
2sK&5aD#

21

Making passwords harder to guess

2sK&5aD#

22



Too many passwords

2jH6ys)7

H74%mMgs

2d6uy6W3#

89t&ksUv%+=

23

Too many passwords

2jH6ys)7

H74%mMgs

Fj7&-*672

GuARZy#KT4xtN^

2d6uy6W3#

sL7dHYk6TXuj

Pt+P2am3P%

89t&ksUv%+=

3mx@SpPv&S29DZ

24

Too many passwords

teTK74Ga3XPw D6U6N2XJhxgT zAatNd4YWR29

2jH6ys)7 2d6uy6W3#

H74%mMgs sL7dHYk6TXuj

Fj7&-*672 Pt+P2am3P%

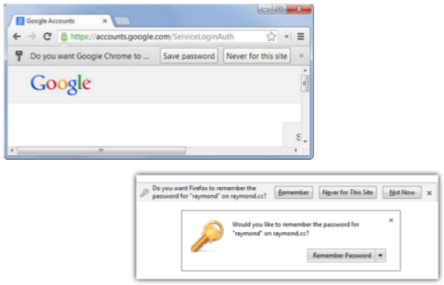
89t&ksUv%+=

GuARZy#KT4xtN^ 3mx@SpPv&S29DZ

EnSYG/TwRrqFS LgCm*!yz89fzE!J

25

Browser Password Management



Google Accounts

https://accounts.google.com/ServiceLoginAuth

Do you want Google Chrome to ... Save password Never for this site

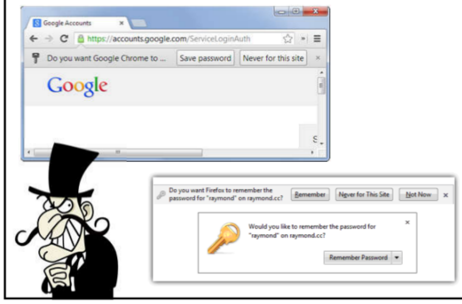
Do you want Firefox to remember the password for "raymond" on raymond.cc? Remember Never for This Site Not Now

Would you like to remember the password for "raymond" on raymond.cc?

Remember Password

26

Browser Password Management



Google Accounts

https://accounts.google.com/ServiceLoginAuth

Do you want Google Chrome to ... Save password Never for this site

Do you want Firefox to remember the password for "raymond" on raymond.cc? Remember Never for This Site Not Now

Would you like to remember the password for "raymond" on raymond.cc?

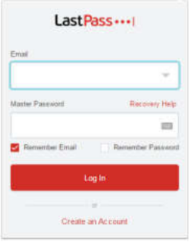
Remember Password

27

Secure Password Managers

28

Using a Secure Password Manager



Email

Master Password Recovery Help

☑ Remember Email ☐ Remember Password

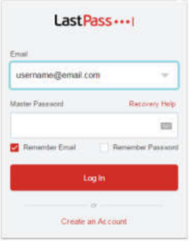
Log In

or

Create an Account

29

Using a Secure Password Manager



Email

username@email.com

Master Password Recovery Help

☑ Remember Email ☐ Remember Password

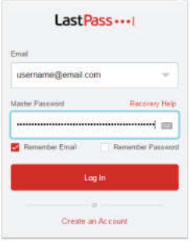
Log In

or

Create an Account

30

Using a Secure Password Manager



LastPass•••|

Email

username@email.com

Master Password — Recovery Help

••

☑ Remember Email ☐ Remember Password

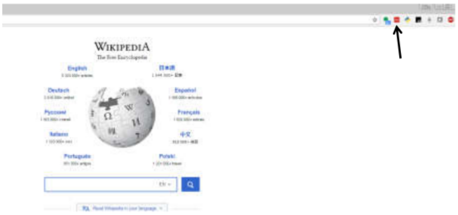
Log In

or

Create an Account

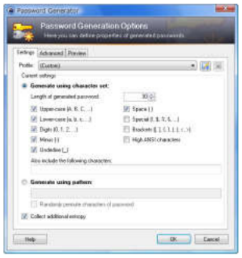
31

Using a Secure Password Manager



32

Generating new passwords



Password Generator

Password Generation Options

Here you can define properties of generated passwords.

Settings | Advanced | Preview

Profile: (Custom)

Current settings

● Generate using character set:

Length of generated password: 30

☑ Upper-case (A, B, C, ...)

☑ Lower-case (a, b, c, ...)

☑ Digits (0, 1, 2, ...)

☑ Minus (-)

☑ Underline (_)

☑ Space ( )

☐ Special (!, $, %, &, ...)

☐ Brackets ([,], {, }, (,), <, >)

☐ High ANSI characters

Also include the following characters:

○ Generate using pattern:

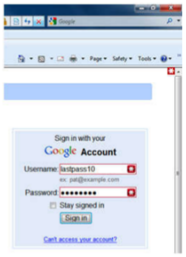
☐ Randomly permute characters of password

☑ Collect additional entropy

Help OK Cancel

33

Auto-fill when logging in



Sign in with your Google Account

Username: lastpass10

ex: pat@example.com

Password: ••••••••

☐ Stay signed in

Sign in

Can't access your account?

34

Encryption is key!

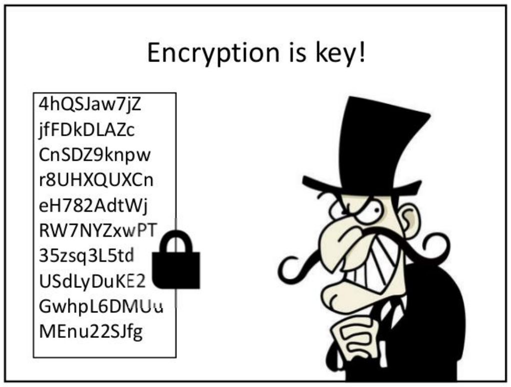
4hQSJaw7jZ
jfFDkDLAZc
CnSDZ9knpw
r8UHXQUXCn
eH782AdtWj
RW7NYZxwPT
35zsq3L5td
USdLyDuKE2
GwhpL6DMUu
MEnu22SJfg

35

Encryption is key!

4hQSJaw7jZ
jfFDkDLAZc
CnSDZ9knpw
r8UHXQUXCn
eH782AdtWj
RW7NYZxwPT
35zsq3L5td
USdLyDuKE2
GwhpL6DMUu
MEnu22SJfg

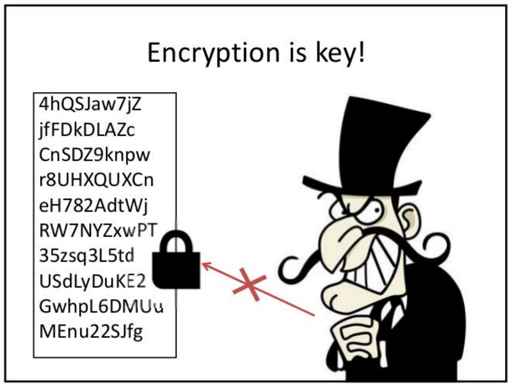
36



Encryption is key!

4hQSJaw7jZ
jfFDkDLAZc
CnSDZ9knpw
r8UHXQUXCn
eH782AdtWj
RW7NYZxwPT
35zsq3L5td
USdLyDuKE2
GwhpL6DMUu
MEnu22SJfg

37



Encryption is key!

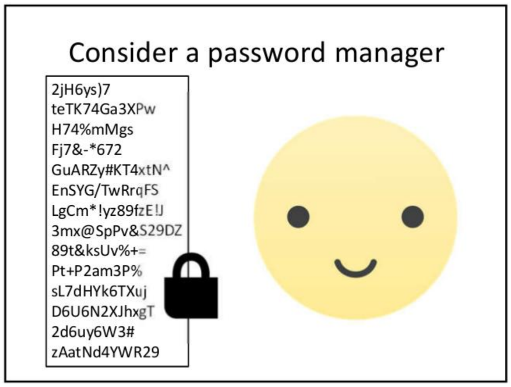
4hQSJaw7jZ
jfFDkDLAZc
CnSDZ9knpw
r8UHXQUXCn
eH782AdtWj
RW7NYZxwPT
35zsq3L5td
USdLyDuKE2
GwhpL6DMUu
MEnu22SJfg

38

Consider a password manager

teTK74Ga3XPw
D6U6N2XJhxgT
zAatNd4YWR29
2jH6ys)7
2d6uy6W3#
sL7dHYk6TXuj
H74%mMgs
Fj7&-*672
Pt+P2am3P%
89t&ksUv%+=
GuARZy#KT4xtN^
3mx@SpPv&S29DZ
EnSYG/TwRrqFS
LgCm*!yz89fzE!J

39



Consider a password manager

2jH6ys)7
teTK74Ga3XPw
H74%mMgs
Fj7&-*672
GuARZy#KT4xtN^
EnSYG/TwRrqFS
LgCm*!yz89fzE!J
3mx@SpPv&S29DZ
89t&ksUv%+=
Pt+P2am3P%
sL7dHYk6TXuj
D6U6N2XJhxgT
2d6uy6W3#
zAatNd4YWR29

40

Password Manager Basic

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the software, attackers can also use stolen usernames and passwords to hack into an account. Making the keys harder to guess is important to securing your information.

Passwords are everywhere. Most, if not all the accounts we use on the Internet require us to select a password. Studies have found that creating and remembering passwords for so many accounts can be hard, leading many people to use simple passwords and to reuse them across accounts.

Simple and common passwords are just waiting to be cracked. Take these for example. They are all short and easy to remember. That makes them good for recalling when it's time to log in, but an attacker can also very easily guess these passwords without much computing effort. In most cases, attackers utilize two methods to guess passwords.

First, they try passwords selected from a dictionary. Dictionaries are files that contain common, simple, and expected passwords, such as common words, quotes, or numerical combinations. Sometimes dictionaries even include passwords stolen in other ways, so if someone reuses passwords across accounts and one of those accounts leaks their information, attackers can more easily access the person's other accounts.

If a dictionary attack fails, attackers usually try a brute force method to guess the password. This is where a computer or network of computers guesses all possible combinations of characters until one works. Here, increasing complexity of passwords is the best defense. The longer and more random a password is, the harder it will be to guess. Keep in mind, what looks random to a human may not be so random to a computer. The best way to create truly random passwords is to use a random password generator.

Length is also important towards making a password harder to guess. Each character adds exponentially more time to how long it would take to guess a password. For example, the following six character, random password would take about 25 years to guess, assuming a thousand guesses per second.

Adding just one random character, as for this updated password, would increase the guess time to twenty-two centuries! That’s two thousand, two hundred years. Go to eight characters, and the time is at two thousand centuries. Clearly, adding only a few characters can make a password much harder to guess.

But, if every password, for every account was a long, complex, random string of digits, letters, and symbols, how are people supposed to remember them all? It is true, the burden of security can easily become too much when utilizing many accounts across many providers, but taking steps to preserve security is still important.

Password managers are important tools that you can use to help manage your passwords in a way that increases security, while also making life easier. Not all password managers are equal, though. Many web browsers include a built in password remember and auto-fill feature. Be wary of this form of password manager. In some cases, your passwords will be saved in a way that can be easily stolen and seen by attackers. This is not always the case, so we recommend you do your research before using a web-browser’s built in password manager.

If you do not use a browser that can securely store passwords, or you would like a password manager that can deliver your passwords on multiple devices, you can also consider a web-based, encrypted password manager, such as OnePassword or LastPass.

In general, these managers work by storing all saved passwords on a web-server. To make the passwords secure, all the passwords are encrypted using the “master password.” The master password is set by the owner and used to unlock the manager and authenticate the legitimate owner of the account. Secure password managers do not store this master password and so, by encrypting the other passwords with it, an attacker who accesses the password manager database will also need master passwords to make use of that data.

Most online, secure password managers offer two main features to help with security. First, they commonly include a password generator that allows users to choose many aspects of the password they want to produce. These can be toggled with security in mind or to meet some password requirements for the account being created. When a new password is generated, the password manager can automatically save the password with the entered username.

The second core password manager feature adds the most convenience. To ease the burden of remembering so many long, random passwords, password managers will auto-fill when they detect a browser loads a log-in screen. In doing so, the password manager does the remembering and typing for the user. This allows them to choose security over memorability when creating new passwords, thus making their accounts harder to access through password cracking.

Though handing all your passwords off to a single password manager may seem like a security risk in that an attacker could get all your passwords in a single attack, if a password manager is secure and used with a long, complex, random master password, the benefits to security across all accounts is worth the very small risk in putting all passwords in this one place.

Password managers can help you create and manage secure passwords for the many accounts you use. If used right, a good password manager can vastly improve the security of your information online, and so using one is commonly recommended by many security experts. According to recent surveys, for added security and convenience, it might be worth looking into a password manager to manage your own accounts.

Password Manager Emotion

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the software, attackers can also use stolen usernames and passwords to hack into an account. Making the keys harder to guess is important to securing your information.

Passwords are everywhere. Most, if not all the accounts we use on the Internet require us to select a password. Studies have found that creating and remembering passwords for so many accounts can be frustrating and confusing, especially when log ins fail because users can’t recall the specific password they have to remember. Unfortunately, this leads many users to use and reuse simple passwords.

Simple and common passwords are just waiting to be cracked, leading to even more annoyance and anxiety later. For example, these passwords are all short and easy to remember, which makes them easier to use. Unfortunately, an attacker can also guess these passwords, utilizing two methods, among others.

First, they try passwords selected from a dictionary, which contain common, simple, and expected passwords. Passwords of common words, quotes, or numerical combinations, or passwords used by many users are also easy to guess using a dictionary and so using these passwords will put one at risk of the negative experiences of having an account accessed by an attacker.

If a dictionary attack fails, attackers usually try a brute force method to guess the password. This is where a computer or network of computers guesses all possible combinations of characters until one works. Here, complexity is the best defense. The longer and more random a password is, the harder it will be to guess. Though long passwords are harder to remember, making the log in process more annoying, the adding security can help avoid even more annoying events later that could come from using a weak password.

Length is also important towards making a password harder to guess. Each character adds exponentially more time to how long it would take to guess a password. For example, the following six character, random password would take about 25 years to guess, assuming a thousand guesses per second.

Adding just one random character, as for this updated password, would increase the guess time to twenty-two centuries! That’s two thousand, two hundred years. Go to eight characters, and the time is at two thousand centuries. Clearly, adding only a letter or two, which should not add a lot of confusion or frustration, can make a password much harder to guess, increasing your security.

But, if every password, for every account was a long, complex, random string of digits, letters, and symbols, how are people supposed to remember them all? Too many passwords can easily be confusing when having to recall the right one. Long passwords are more annoying to type in. Fortunately, there are tools available to you that can help stay secure while avoid many of these negatives.

Password managers can help manage your passwords automatically in a way that increases security. Not all password managers are equal, though, and using some easy to access forms of the tool could do more harm than good. Some managers do not store passwords in a secure way. This is not always the case, so doing research when deciding to choose a password manager and avoiding the easiest option without checking it out first is the best way to make a decision that increase how secure you feel in your choice.

If you do not use a browser that can securely store passwords, or you would like a password manager that can deliver your passwords on multiple devices, you can also consider a web-based, encrypted password manager, such as OnePassword or LastPass.

In general, these managers work by storing all saved passwords on a web-server. To make the passwords secure, all the passwords are encrypted using the "master password." The master password is set by the owner and used to unlock the manager and authenticate the legitimate owner of the account. Secure password managers do not store this master password and so, by encrypting the other passwords with it, an attacker who accesses the password manager database will also need master passwords to make use of that data. Making sure you choose a secure master password will maximize your security, even though having a long, complex, random master password might be annoying.

Most online, secure password managers offer two main features to help with security. First, they commonly include a password generator that allows users to choose many aspects of the password they want to produce. These can be toggled to create stronger passwords that help one feel secure, or to meet password requirements for the account being created to make the account creation processes more pleasant. When a new password is generated, the password manager can automatically save it.

Password managers will also auto-fill when they detect the user is at a log-in screen, and so, the password manager does the remembering and typing for the user. This allows one to choose security over memorability when creating new passwords, since there will no longer be annoyance and confusion because of having to remember secure passwords.

Handing all your passwords off to a single password manager may make you nervous in that an attacker could get all your passwords in one attack. But, when using a password manager, since secure passwords for all your accounts can be automatically generated and typed, along with a long and random master password to securely store them, even though typing in this one password may be annoying, the cumulative security across all accounts will be worth it.

Password managers can help you create and manage passwords for the many accounts you use in a way that makes you happier and more secure. Though you may have some worries about the tool, using a password manager is one of the most commonly recommended secure actions users can take, according to recent surveys of advice from security experts. To feel more secure, it might be worth looking into a password manager to manage your accounts.

Password Manager Social

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the software, attackers can also use stolen usernames and passwords to hack into an account. Making the keys harder to guess is important to securing your information.

Passwords are everywhere. Most, if not all the accounts we use on the Internet require us to select a password. Studies have found that creating and remembering passwords for so many accounts can be hard, leading many people to use simple passwords and to reuse them across accounts.

Simple and common passwords are just waiting to be cracked. Take these for example. They are all short and easy to remember. If these passwords were used for a social media or email account, they could easily be cracked and the accounts used to launch attacks against people the victim is connected with through the accounts. For example, an attacker with access to an email account could send malicious emails to those in the contact list, including the victim's friends and family, and these emails could ask for money or to try and compromise the accounts of these people as well.

Fortunately, there are ways to protect against your passwords being cracked, but first let's understand the ways an attacker can crack a password. First, they try passwords selected from a dictionary. Dictionaries are files that contain common, simple, and expected passwords that are used by many users. Sometimes dictionaries even include passwords stolen in other ways, so if you use a common password that is stolen and added to a dictionary, other users can be attacked more easily. Passwords of common words, quotes, or numerical combinations are also easy to guess using a dictionary since these passwords are used and known by many individuals.

If a dictionary attack fails, attackers usually try a brute force method to guess the password. This is where a computer or network of computers guesses all possible combinations of characters until one works. Here, increasing complexity of passwords is the best defense. The longer and more random a password is, the harder it will be to guess. Keep in mind, what looks random to a human may not be so random to a computer. The best way to create truly random passwords is to use a random password generator. Length is also important towards making a password harder to guess. Each character adds exponentially more time to how long it would take to guess a password. For example, the following six character, random password would take about 25 years to guess, assuming a thousand guesses per second. Adding just one random character, as for this updated password, would increase the guess time to twenty-two centuries! That's two thousand, two hundred years. Go to eight characters, and the time is at two thousand centuries.

Clearly, adding only a few characters can make a password much harder to guess, and thus protect you and others from attack. But, if every password, for every account was a long, complex, random string of digits, letters, and symbols, how are people supposed to remember them all? It is true, the burden of security can easily become too much when utilizing many accounts across many providers, but taking steps to preserve security is important to all Internet users.

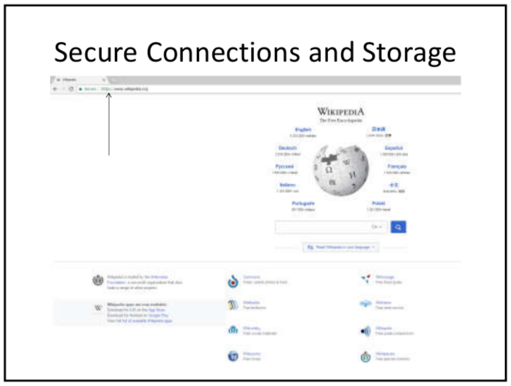
Password managers are important tools any user can use to help manage passwords in a way that increases the entire Internet's security, while also making life easier for the users. Not all password managers are equal, though, and using the wrong kind may put yours and others security at risk. Many web browsers include a built in password remember and auto-fill feature, but these may save passwords in a way that can be easily stolen and seen by attackers. This is not always the case, so we recommend researching before using a web-browser's built in password manager.

If you do not use a browser that can securely store passwords, or you would like a password manager that can deliver your passwords on multiple devices, you can also consider a web-based, encrypted password manager, such as OnePassword or LastPass. In general, these managers work by storing all saved passwords on a web-server. To make the passwords secure, all the passwords are encrypted using the "master password." The master password is set by the owner and used to unlock the manager and authenticate the legitimate owner of the account. Secure password managers do not store this master password and so, by encrypting the other passwords with it, an attacker who accesses the password manager database will also need master passwords to make use of that data.

Most online, secure password managers offer two main features to help with security. First, they commonly include a password generator that allows users to choose many aspects of the password they want to produce. These can be toggled with security in mind or to meet some password requirements for the account being created. Keep in mind that using better passwords means your accounts are much harder for an attacker to access and use for additional malicious acts against others. The second core password manager feature adds the most convenience. To ease the burden of remembering so many long, random passwords, password managers will auto-fill when they detect a browser loads a log-in screen. In doing so, the password manager does the remembering and typing for us. This allows anyone who uses a password manager to more easily choose security over memorability when choosing a new password, further protecting security for all.

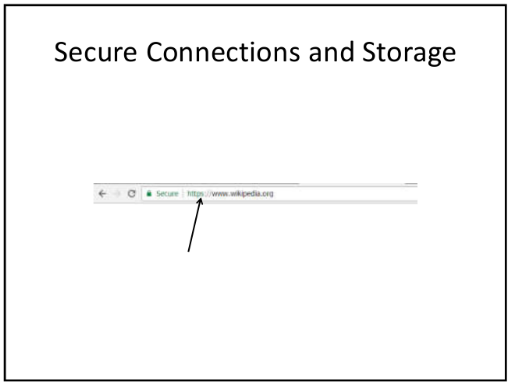
Though password managers may make you susceptible to having all passwords stolen in one attack, if a secure password manager is used with a properly long, complex, and random master password, the benefit to security across all accounts and to other users is worth it. If used right, a good password manager can vastly improve your and other’s security, and so using one is commonly recommended by security experts and used by many individuals, according to recent surveys. According to recent surveys, for added security and convenience, it might be worth looking into a password manager to manage your own accounts.

2FA Slides



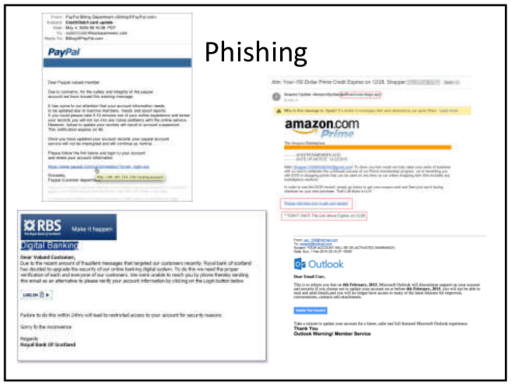
Secure Connections and Storage

7



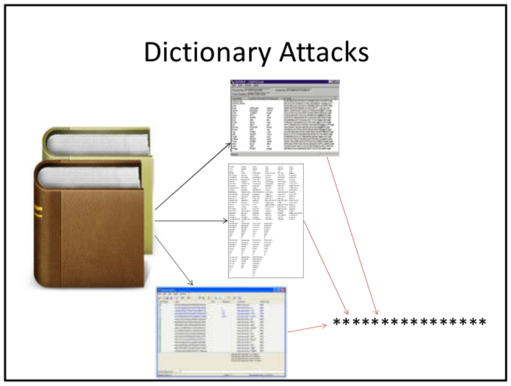
Secure Connections and Storage

8



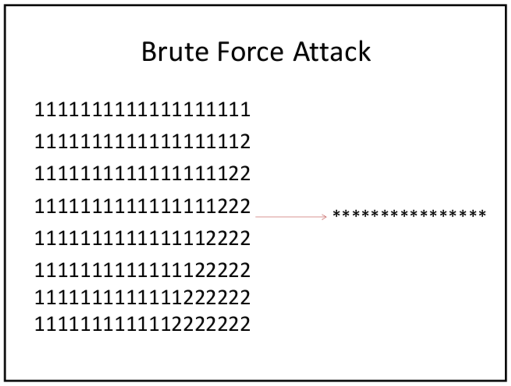
Phishing

9



Dictionary Attacks

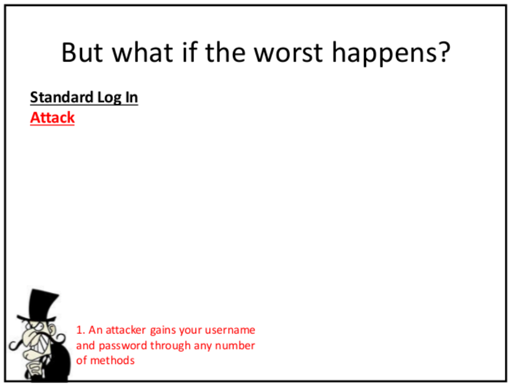
10



Brute Force Attack

1111111111111111111
1111111111111111112
1111111111111111122
1111111111111111222 → ****************
1111111111111112222
1111111111111122222
1111111111111222222
1111111111112222222

11

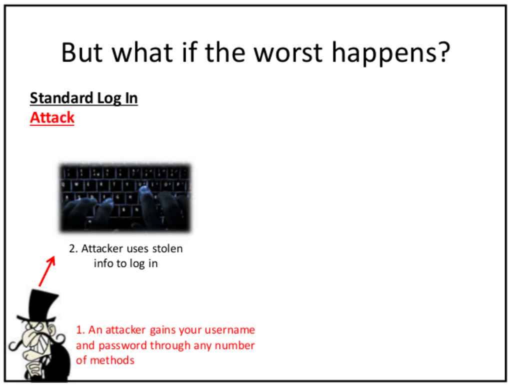


But what if the worst happens?

Standard Log In
Attack

1. An attacker gains your username and password through any number of methods

12



But what if the worst happens?

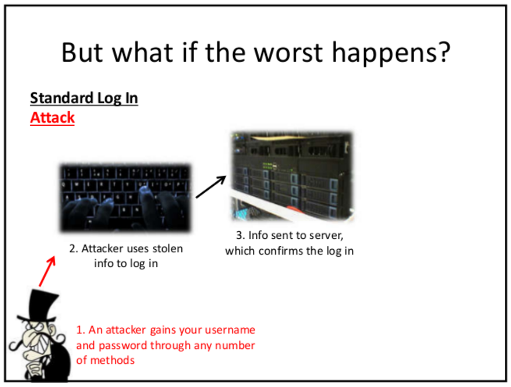
Standard Log In

Attack

2. Attacker uses stolen info to log in

1. An attacker gains your username and password through any number of methods

13



But what if the worst happens?

Standard Log In

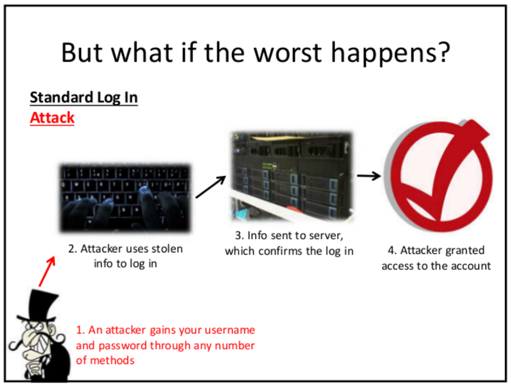
Attack

2. Attacker uses stolen info to log in

3. Info sent to server, which confirms the log in

1. An attacker gains your username and password through any number of methods

14



But what if the worst happens?

Standard Log In

Attack

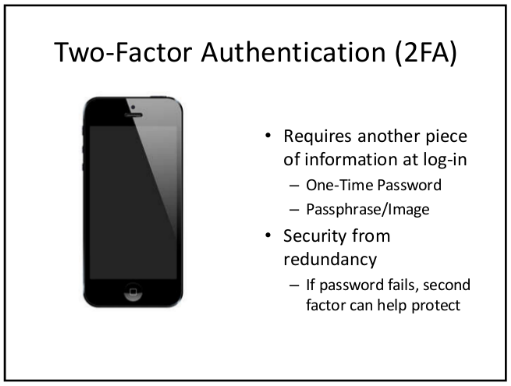
2. Attacker uses stolen info to log in

3. Info sent to server, which confirms the log in

4. Attacker granted access to the account

1. An attacker gains your username and password through any number of methods

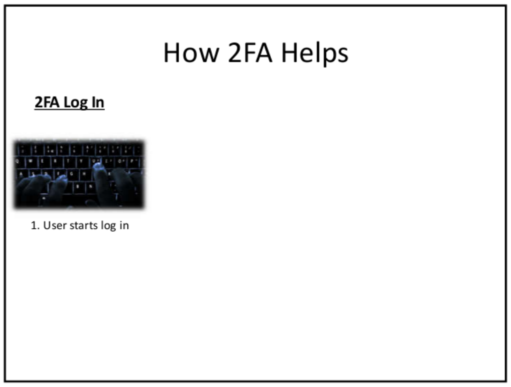
15



Two-Factor Authentication (2FA)

- Requires another piece of information at log-in
  - One-Time Password
  - Passphrase/Image
- Security from redundancy
  - If password fails, second factor can help protect

16

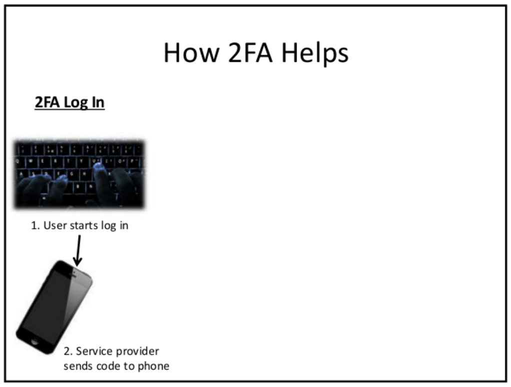


How 2FA Helps

2FA Log In

1. User starts log in

17



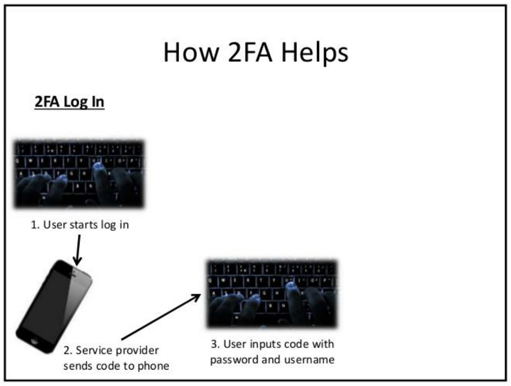
How 2FA Helps

2FA Log In

1. User starts log in

2. Service provider sends code to phone

18



How 2FA Helps

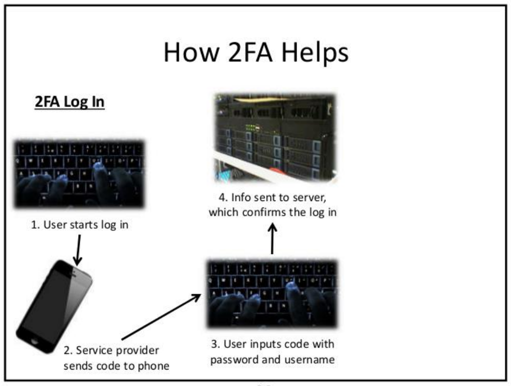
2FA Log In

1. User starts log in

2. Service provider sends code to phone

3. User inputs code with password and username

19



How 2FA Helps

2FA Log In

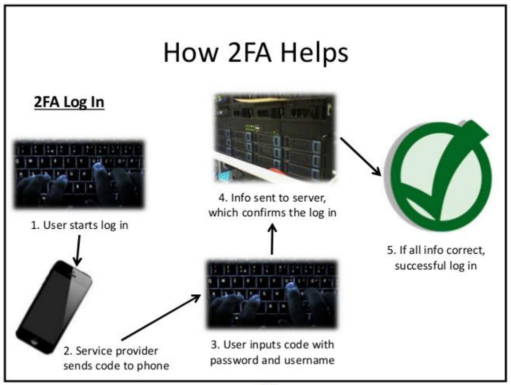
1. User starts log in

2. Service provider sends code to phone

3. User inputs code with password and username

4. Info sent to server, which confirms the log in

20



How 2FA Helps

2FA Log In

1. User starts log in

2. Service provider sends code to phone

3. User inputs code with password and username

4. Info sent to server, which confirms the log in

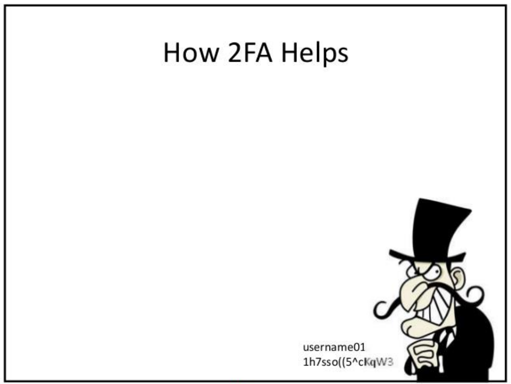
5. If all info correct, successful log in

21

How 2FA Helps

username01
****

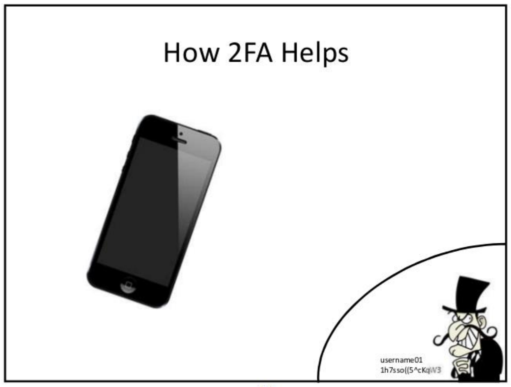
22



How 2FA Helps

username01
1h7sso((5^cKqW3

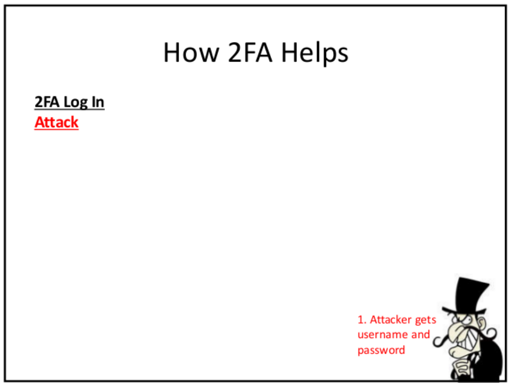
23



How 2FA Helps

username01
1h7sso((5^cKqW3

24



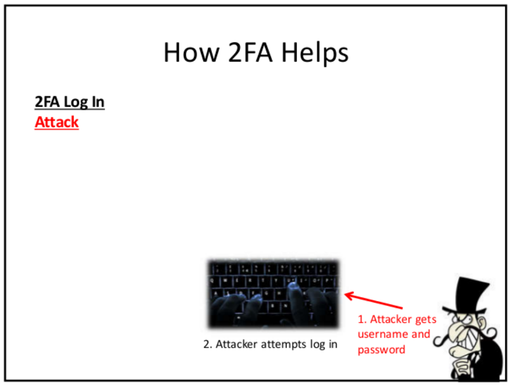
How 2FA Helps

2FA Log In

Attack

1. Attacker gets username and password

25



How 2FA Helps

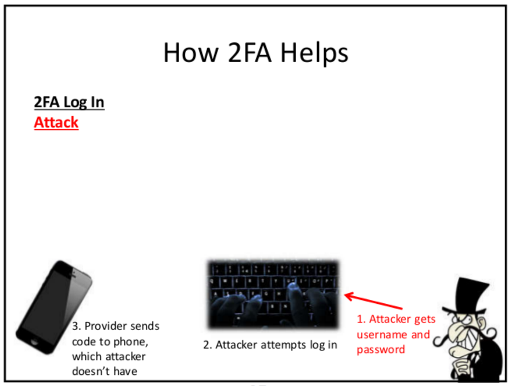
2FA Log In

Attack

2. Attacker attempts log in

1. Attacker gets username and password

26



How 2FA Helps

2FA Log In

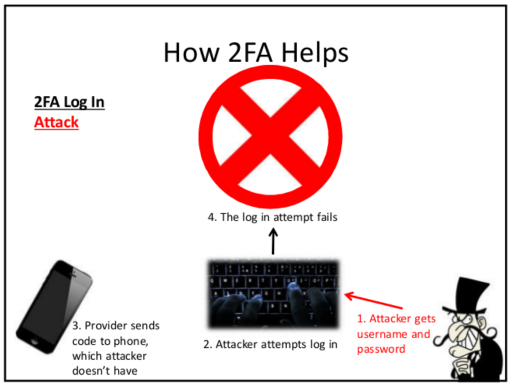
Attack

3. Provider sends code to phone, which attacker doesn't have

2. Attacker attempts log in

1. Attacker gets username and password

27



How 2FA Helps

2FA Log In

Attack

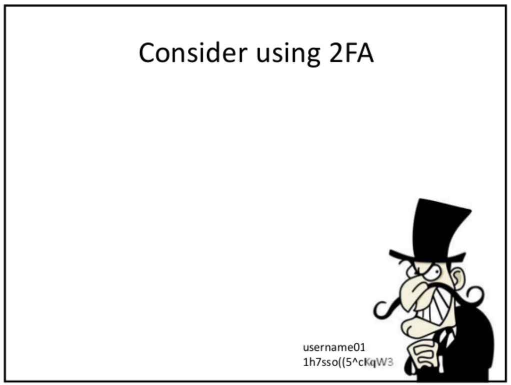
4. The log in attempt fails

3. Provider sends code to phone, which attacker doesn't have

2. Attacker attempts log in

1. Attacker gets username and password

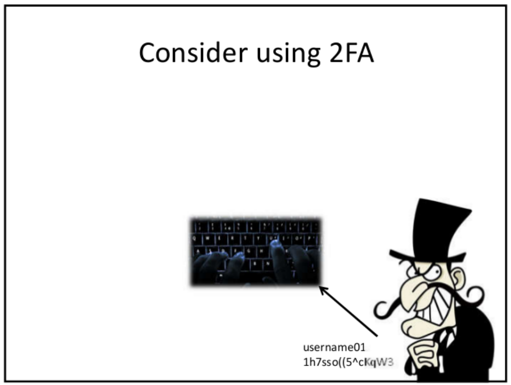
28



Consider using 2FA

username01
1h7sso((5^cKqW3

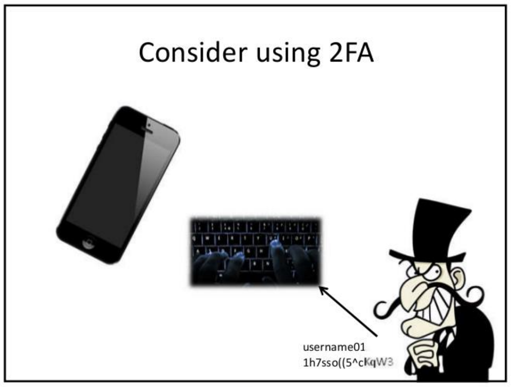
29



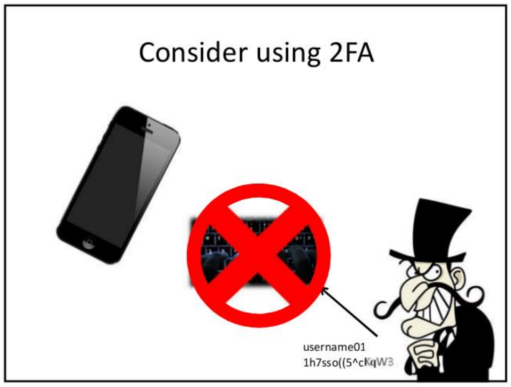
Consider using 2FA

username01
1h7sso((5^cKqW3

30


Consider using 2FA

31


Consider using 2FA

32

2FA Basic

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the program, attacks do not need to be that sophisticated. If they can steal or guess a password and username, an attacker doesn't need a "hack" to get in. They can just use the log-in screen.

Imagine the standard log-in procedure for many websites and Internet services you use. Most times, you must navigate to a log-in page. There, you type in your username and password. That information is sent to the server, which checks that, what you typed in matches what the server has on record. If everything checks out, you're in!

This process relies on a few things to be secure. First, the information sent between your device and the servers should be encrypted in some way. Many times, this is done using the more secure HTTPS as opposed to the standard HTTP. You can see if your connection is secured this way by looking for the HTTPS at the beginning of the URL in your address bar.

You must also trust that the server is not handling or storing information in a way that is easily accessible. You cannot control this, of course, but most major providers do handle and store data properly. Finally, there is your part of securing the credentials you use to log in. If an attacker can get a hold of log-in credentials, any encryption or safe storage is useless to stop an attack. After all, they'd have the keys!

Attackers can get your credentials in any number of ways. Sometimes, they can trick people into giving up the data voluntarily through a phishing attack, where the attacker sends a bogus email to the victim, telling them they must log-in for some reason, but the link provided is to the attacker's website rather than the real service. So, when the person types in their information, it is saved, by the attacker to be used later. Many times, attackers are not so sophisticated and instead resort to guessing a password using what's called a brute-force attack. With a username usually known by some other means, high-powered computers and password dictionaries are used to guess a password. Depending on the uniqueness and complexity of the password being guessed, this can be a very effective way to gain access to an account.

With the username and password, the attack on a standard account is very easy. The attacker goes to the same log-in screen everyone else uses. They then type in the stolen information. If the information is still current and passes the checks on the server's side, the attacker is allowed access, the server thinking that it is the legitimate account owner logging in.

Thus, making sure your accounts are secure is important to thwart easy attacks. There are many ways to achieve this. Though more complexity in passwords makes them harder to guess, as we saw, attackers have other ways to learn passwords than just guessing. You can get more security through redundancy by enabling two-factor authentication, sometimes called two-step log-in, and multi-factor log-in, among other names.

When using two-factor authentication, people are asked for an extra piece of information with their username and password. Many times, this additional information is a one-time password, which is a random string of letters and numbers generated by the server and sent to the person logging in. Though it looks like a regular password, a one-time password is only good for a short period of time, and a new one is created every time the additional piece of information is needed to verify a log-in. The one-time password can be sent to people in many ways, but email, phone-call, or SMS text message are the most popular.

Here's how a two-factor authentication usually works. First, the username and password are entered at the log-in screen, as usual. If the device being used is not recognized, the service will ask for the individual trying to log in to enter a one-time password that will be automatically sent to the account owner's other device or email account. In this case, the one-time password is sent as a text message to their phone. The message arrives within a few seconds and the account owner, who is the one attempting the log-in enters the additional information. The server confirms that all the information is correct, and access is granted.

The added security comes from the fact that, by entering the one-time password with a username and regular password, the server has additional assurance that it is really the account owner trying to log in, since the attacker would need to have not only the username and regular password, but also access to the one-time password, which means the owner's email account or phone. Though remotely accessing or guessing a regular password and username can be easy for some attackers, accessing the account owner's email, and even more so their phone can be very difficult.

Let's see how using two-factor authentication can stop an attack. The attacker has a paired username and password, so they try to log into the account through the standard log-in screen for the service. Since the attacker is using an unrecognized device, if the account owner had two-factor authentication activated, the service will request that a one-time password be entered as well. That one-time password will be sent to the account owner's device or account, which the attacker probably can't access. Thus, they enter the wrong one-time password and are not granted access to the account.

By using two-factor authentication, even if an attacker has your username and password, they cannot access your account very easily. It's no surprise that using two-factor authentication is among the most common advice given by security experts as a way for individuals to secure their accounts and information. Though more time may be needed to log-in from new devices, when a new device is registered, the additional factor is no longer needed. Thus, the added one-time effort will be worth it in terms of the protection given to your account.

2FA Emotion

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the program, attacks do not need to be that sophisticated. If they can steal or guess a password and username, an attacker doesn't need a "hack" to get in. They can just use the log-in screen.

Imagine the standard log-in procedure for many websites and Internet services you use. Most times, you must navigate to a log-in page. There, you type in your username and password. That information is sent to the server, which checks that, what you typed in matches what the server has on record. Without too much effort, if everything checks out, you're in, happily enjoying the service!

This process relies on a few things to be secure. First, the information sent between your device and the servers should be encrypted in some way. Many times, this is done using the more secure HTTPS as opposed to the standard HTTP. You can see if your connection is secured this way by looking for the HTTPS at the beginning of the URL in your address bar. You must also trust that the server is not handling or storing information in a way that is easily accessible by unauthorized users. Though data can be stolen from a server if it is not safeguarded properly, there are other ways to steal log-in credentials. Therefore, you must also make sure your do your part to secure your information, even though doing so may be annoying.

Let's see some of the ways an attacker can try to steal a log-in. Sometimes, they can confuse users by sending a bogus email telling them that they must log-in for some reason, but the link provided is to the attacker's website rather than the real service, and so the attacker can save the data when it is typed in. Making sure to read emails carefully and check where they are from, even though it may be annoying and confusing is important to avoiding phishing attacks. Attackers do not need to be so sophisticated and can also try to access your account by guessing your password in what is called a brute-force attack.

With the username and password, the attack on a standard account is very easy. The attacker goes to the same log-in screen everyone else uses. They then type in the stolen information. If the information is still current and passes the checks on the server's side, the attacker is allowed access, the server thinking that it is the legitimate account owner logging in. From here, an attacker can cause many negative situations for users that may be frustrating, confusing, and tiring to deal with.

Thus, making sure your accounts are secure is important to thwart easy attacks. There are many ways to achieve this. Though more complexity in passwords makes them harder to guess, as we saw, attackers have other ways to learn passwords than just guessing. You can feel more secure through redundancy by enabling two-factor authentication, sometimes called two-step log-in.

When using two-factor authentication, people are asked for an extra piece of information with their username and password. Many times, this additional information is a one-time password, which is a random string of letters and numbers generated by the server and sent to the person logging in. Though it looks like a regular password, a one-time password is only good for a short period of time, and a new one is created every time the additional piece of information is needed to verify a log-in. The one-time password can be sent to people in many ways, but email, phone-call, or SMS text message are the most popular.

Here’s how a two-factor authentication usually works. First, the username and password are entered at the log-in screen, as usual. If the device being used is not recognized, the service will ask for the individual trying to log in to enter a one-time password that will be automatically sent to the account owner’s other device or email account. In this case, the one-time password is sent as a text message to their phone. The message arrives within a few seconds and the account owner, who is the one attempting the log-in enters the additional information. The server confirms that all the information is correct, and, if so, access is granted, with the user happily enjoying the service, secure in the knowledge that two-factor authentication is helping keep their account safe.

The added security comes from the fact that, by entering the one-time password with username and regular password, the server has additional assurance that it is really the legitimate user trying to log in, since the attacker would need to have not only the user's username and regular password, but also access to the one-time password, meaning the user's email or phone, which is much harder than guessing a password. Thus, though having to type in the additional piece of information can be annoying, using two-factor authentication can help a user feel more secure, even if secure passwords are already used.

Let's see how using two-factor authentication can stop an attack. The attacker has a paired username and password, so they try to log into the account through the standard log-in screen for the service. Since the attacker is using an unrecognized device, if the account owner had two-factor authentication activated, the service will request that a one-time password be entered as well. That one-time password will be sent to the account owner's device or account, which the attacker probably can't access. Thus, they enter the wrong one-time password and are not granted access to the account.

By using two-factor authentication, even if an attacker has your username and password, they cannot access your account very easily. It's no surprise that using two-factor authentication is among the most common advice given by security experts as a way for individuals to secure their accounts and information. Though using two-factor authentication may be more work and annoying, this added one-time effort will make you and your account more secure.

2FA Social

Understanding your role in computer security, especially around web accounts is important towards taking the right steps to secure your information. Though many attacks on software use some kind of backdoor that allows an attacker to gain unauthorized access through a glitch or flaw in the program, attacks do not need to be that sophisticated. If they can steal or guess a password and username, an attacker doesn't need a "hack" to get in. They can just use the log-in screen.

Imagine the standard log-in procedure for many websites and Internet services you use. Many times, a user must navigate to a log-in page. There, they type in their username and password. That information is sent to the server, which checks that it matches what it has on record. If everything checks out, they're in!

This process relies on a few things to be secure. First, the information sent between the device and the servers should be encrypted in some way, such as using HTTPS. You can see if your connection is secured this way by looking for the HTTPS at the beginning of the URL in your address bar. Users must secure their credentials because, if these are stolen, an attacker can access an account very easily. Depending on the account, this can impact many people. For example, an attacker with access to an email account could send malicious emails to those in the contact list, including the victim's friends and family that may ask for money or to try and compromise their accounts as well.

Attackers can get credentials in any number of ways. Sometimes, they can trick users into giving up the data voluntarily through a phishing attack, where the attacker sends a bogus email telling the user they must log-in for some reason, but when the user types their information in to the bogus webpage, it is saved, by the attacker to be used later. These kinds of attacks can be launched against those in the contact list of a user whose account has been broken into, so securing your account is important to stopping threats to others too. Many times, attackers are not so sophisticated and instead resort to guessing a password using what's called a brute-force attack. With a username usually known by some other means, high-powered computers and password dictionaries are used to guess a password. Depending on the uniqueness and complexity of the password being guessed, this can be a very effective way to gain access to an account.

With the username and password, the attack on a standard account is very easy. The attacker goes to the same log-in screen everyone else uses. They then type in the stolen information. If the information is still current and passes the checks on the server's side, the attacker is allowed access, the server thinking that it is the legitimate account owner logging in. Once in, the attacker may be able to use the account to gain information or further attack not only the user, but those who are linked to the attacked account.

Thus, making sure our accounts are secure is important to thwart easy attacks that can impact many other people. There are many ways to achieve this. Though more complexity in passwords makes them harder to guess, as we saw, attackers have other ways to learn passwords than just guessing. More security can be gained through redundancy in the form of two-factor authentication.

When using two-factor authentication, people are asked for an extra piece of information with their username and password. Many times, this additional information is a one-time password, which is a random string of letters and numbers generated by the server and sent to the person logging in. Though it looks like a regular password, a one-time password is only good for a short period of time, and a new one is created every time the additional piece of information is needed to verify a log-in. The one-time password can be sent to people in many ways, but email, phone-call, or SMS text message are the most popular.

Here’s how a two-factor authentication usually works. First, the username and password are entered at the log-in screen, as usual. If the device being used is not recognized, the service will ask for the individual trying to log in to enter a one-time password that will be automatically sent to the account owner’s other device or email account. In this case, the one-time password is sent as a text message to their phone. The message arrives within a few seconds and the account owner, who is the one attempting the log-in enters the additional information. The server confirms that all the information is correct, and access is granted.

The added security comes from the fact that, by entering the one-time password with a username and regular password, the server has additional assurance that it is really the account owner trying to log in, since the attacker would need to have not only the username and regular password, but also access to the one-time password, which means the owner’s email account or phone. Though remotely accessing or guessing a regular password and username can be easy for some attackers, accessing the account owner’s email, and even more so their phone can be very difficult. By securing accounts with two-factor authentication, it makes it harder for attackers to use your account to threaten others.

Let’s see how using two-factor authentication can stop an attack. The attacker has a paired username and password, so they try to log into the account through the standard log-in screen for the service. Since the attacker is using an unrecognized device, if the account owner had two-factor authentication activated, the service will request that a one-time password be entered as well. That one-time password will be sent to the account owner’s device or account, which the attacker probably can’t access. Thus, they enter the wrong one-time password and are not granted access to the account.

By using two-factor authentication, even if an attacker has a username and password, they cannot access an account very easily, this protects not only the account owner’s data, but the data of others as well. It’s no surprise that using two-factor authentication is among the most common advice given by security experts as a way for users to secure accounts and information online, and has been adopted by many users already. Though more time may be needed to log-in from new devices, this added one-time effort will be worth the extra security for everyone.

Screening Survey

The following instruments were used to gather basic demographics and behavior data from participants. Participants were then contacted based on their responses to this survey.

1. What is your age? _____
2. What is your gender?
    - ○ Male
    - ○ Female
    - ○ Other
3. Do you use a laptop of desktop computer that you or your family owns?
    - ○ Yes
    - ○ No
4. How would you rate your general computer expertise?
    - ○ Very poor
    - ○ Poor
    - ○ Fair
    - ○ Good
    - ○ Very good
5. How would you rate your computer security expertise?
    - ○ Very poor
    - ○ Poor
    - ○ Fair
    - ○ Good
    - ○ Very good
6. How often would you say you use the computer?
    - ○ Never
    - ○ Rarely
    - ○ Sometimes
    - ○ Often
    - ○ All the time
7. Do you keep your computer's software up to date?
    - ○ Yes
    - ○ No
    - ○ I don't know
8. Do you use two-factor authentication (e.g., 2-Step Verification) for at least one of your online accounts?
    - ○ Yes
    - ○ No
    - ○ I don't know

9. Do you use a password manager (e.g., LastPass, OnePass, KeePass) to manage your online account passwords?
   - ○ Yes
   - ○ No
   - ○ I don’t know

Follow-Up Survey

Behavior Instruments

Note: [following advice] was replace as appropriate for each advice, with the following phrasings:

> *Update:* “keeping your computer’s software up to date”
>
> *Password Manager:* “using a password manager (e.g., LastPass, OnePass, KeePass) to manage your online account passwords”
>
> *2FA:* “using two-factor authentication (e.g., 2-step verification, 2-step log-in) for at least one of your online accounts”

1. Since the last survey, have you started or stopped [following advice]?
   - ○ Yes, I’ve started
   - ○ Yes. I’ve stopped
   - ○ No, I have not changed my behavior
   - ○ I Don’t Know
   - ○ No Answer/I prefer not to answer
2. Why did you start or stop [following advice]? ____
   ____

Awareness Instruments

Unique surveys were developed for each advice to assess awareness around core concepts related to that advice. The awareness instruments for each advice are given below, with the *correct* response(s) marked.

Update Instruments

1. Applying updates doesn't usually help your system's security.
   - ○ True
   - ○ **False**
   - ○ No Answer/I prefer not to answer

2. My decision to update my device's software only affects me.
   - True
   - **False**
   - No Answer/I prefer not to answer

3. Since software updates mainly focus on superficial changes, many are worth skipping.
   - True
   - **False**
   - No Answer/I prefer not to answer

4. Which of the following are the usual benefits of updating your computer's software? (select all that apply)
   - □ **Get the newest features**
   - □ **Increase software security**
   - □ Delete private information
   - □ Remove malware such as viruses
   - □ No Answer/I prefer not to answer

5. In general, which software is the most important to update?
   - **Operating system (i.e., Windows, Android, iOS, OSX)**
   - Browser (e.g., Firefox, Chrome)
   - Anti-virus software
   - Updating software isn't important
   - No Answer/I prefer not to answer

6. Which of the following are stages of the software development cycle? (select all that apply)
   - □ **Create**
   - □ **Plan**
   - □ Network
   - □ Profit
   - □ No Answer/I prefer not to answer

7. Which of the following attacks can utilize out-of-date software to shut-down a website?
   - Brute-Force password cracking
   - **DDoS attack**
   - Use of stolen credentials
   - Phishing attack
   - No Answer/I prefer not to answer

Password Manager Instruments

1. Using a password manager doesn't usually help your account security.
   - True
   - **False**
   - No Answer/I prefer not to answer

2. My decision to use a password manager only affects me.
    - True
    - **False**
    - No Answer/I prefer not to answer

3. Since password managers centralize passwords, any password manager is automatically insecure.
    - True
    - **False**
    - No Answer/I prefer not to answer

4. Which strategy is best to produce and store secure passwords?
    - Use different sentences from your favorite books as passwords and only store them by writing them on a piece of paper
    - **Use a secure password manager with a secure master password to create long, random, unique passwords for all accounts**
    - Use names of friends and meaningful numbers (i.e., birthday, apartment number, etc.) to create complex, unique passwords and store them in a note file on your smartphone
    - All methods are equally secure
    - No Answer/I prefer not to answer

5. Which are the most important qualities of a good password? (select all that apply)
    - □ Easy to remember
    - □ Short
    - □ **Unique**
    - □ **Random/complex**
    - □ No Answer/I prefer not to answer

6. Which of the following features of secure password managers are most helpful for security? (select all that apply)
    - □ **Random password generation**
    - □ **Account management and auto-fill features**
    - □ Access to account credentials from anywhere
    - □ Centralization of credentials
    - □ No Answer/I prefer not to answer

7. Which of the following attacks is easiest when short, simple passwords are used?
    - **Brute-Force password cracking**
    - DDoS attack
    - Use of stolen credentials
    - Phishing attack
    - No Answer/I prefer not to answer

2FA Instruments

1. Using two-factor authentication doesn't usually help your account security.
   - ○ True
   - ○ **False**
   - ○ No Answer/I prefer not to answer

2. My decision to use two-factor authentication only affects me.
   - ○ True
   - ○ **False**
   - ○ No Answer/I prefer not to answer
3. Since using two-factor authentication takes extra time, it's not worth it.
   - ○ True
   - ○ **False**
   - ○ No Answer/I prefer not to answer

4. In general, which accounts are most important to secure?
   - ○ **Financials and other accounts that touch money**
   - ○ Email
   - ○ Social Media
   - ○ Account security isn't important
   - ○ No Answer/I prefer not to answer

5. Which of the following can best secure your online accounts?
   - ○ Scan your computer for viruses weekly
   - ○ Delete cookies regularly
   - ○ **Activate two-factor log-in on as many account as possible**
   - ○ None of the above
   - ○ No Answer/I prefer not to answer

6. Which of the following are forms of two-factor log-in? (select all that apply)
   - □ **Entering a one-time password sent to your smart-phone with username and password**
   - □ **Entering the response to a security question in addition to username and password**
   - □ Checking "remember me" when logging in with a username and password
   - □ Using a password manager to save and manage usernames and passwords
   - □ No Answer/I prefer not to answer

7. Which of the following attacks is thwarted by using two-factor log-in?
   - ○ **Brute-Force password cracking**
   - ○ DDoS attack
   - ○ Use of stolen credentials
   - ○ Man-in-the-Middle attack
   - ○ No Answer/I prefer not to answer

Perceptions Instruments

Note: [following the advice] was replace as appropriate for each advice, with the following phrasings:

Update: “keeping your computer’s software up to date”

Password Manager: “using a password manager”

2FA: “using two-factor authentication”

Prompt: For each question below, respond as if you use a password manager, even if you do not.

1. How much would you say you are benefited by [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
   - ○ No Answer/I prefer not to answer

2. How much would you say users of other computers are benefited by [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
   - ○ No Answer/I prefer not to answer

3. How much would you say you are cost or inconvenienced by [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
   - ○ No Answer/I prefer not to answer

4. How much would you say users of other computers are cost or inconvenienced by [following the advice]?
   - ○ None
   - ○ Little
   - ○ Some
   - ○ A lot
   - ○ Not sure
   - ○ No Answer/I prefer not to answer

5. How much would you say you are put at risk by [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

6. How much would you say users of other computers are put at risk by [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

Prompt: For each question below, respond as if you did not use a password manager, even if you do.

7. How much would you say you are benefited by not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

8. How much would you say users of other computers would be benefited by not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

9. How much would you say you are cost or inconvenienced by [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

10. How much would you say users of other computers are cost or inconvenienced by not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

11. How much would you say you are put at risk by not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

12. How much would you say users of other computers are put at risk by not [following the advice]?
    - None
    - Little
    - Some
    - A lot
    - Not sure
    - No Answer/I prefer not to answer

Emotion Instrument

Note: [follow the advice] was replace as appropriate for each advice, with the following phrasings:

Update: “keep your computer’s software up to date”

Password Manager: “use a password manager”

2FA: “use two-factor authentication”

List of emotions to select from:

(1) Confident
(2) Secure
(3) Sad
(4) Depressed
(5) Down
(6) Afraid
(7) Nervous
(8) Freaked-Out
(9) Anxious
(10) Angry
(11) Insulted
(12) Hostile
(13) Surprised
(14) Dazed
(15) Confused
(16) Disgusted
(17) Dismayed
(18) Distraught
(19) Cared-For
(20) Friendly
(21) Welcomed
(22) Powerful
(23) Energetic
(24) Vigorous
(25) Isolated
(26) Lonely
(27) Abandoned
(28) Proud
(29) Triumphant
(30) Arrogant
(31) Ashamed
(32) Guilty
(33) Embarrassed
(34) Scornful
(35) Contemptuous
(36) Disdainful
(37) Humiliated
(38) Dishonored
(39) Resentful
(40) Grateful
(41) Respectful
(42) Admiring
(43) Trusting
(44) Suspicious
(45) Happy

1. Image you are faced with the decision to [follow the advice], please rate the top 5 emotions you predict you would feel:
    a. The emotion I would feel most strongly is __________
    b. The emotion I would feel second most strongly is __________
    c. The emotion I would feel third most strongly is __________
    d. The emotion I would feel fourth most strongly is __________
    e. The emotion I would feel fifth most strongly is __________

Sample Descriptive Statistics

			Gender			Age	
	Group	**N**	*Male*	*Female*	*Other*	*Avg.*	*St.D.*
Update	*Control*	27	12	15	-	33.2	9.6
	Basic	24	9	15	-	35.7	13.3
	Emotion	26	12	14	-	34.3	10.6
	Social	24	11	13	-	34.6	9.7
Password Manager	*Control*	30	18	11	1	34.7	10.6
	Basic	30	20	10	-	35.0	9.7
	Emotion	30	12	18	-	35.8	11.2
	Social	28	17	11	-	35.0	10.2
2FA	*Control*	26	16	10	-	37.3	11.3
	Basic	27	18	9	-	37.7	14.0
	Emotion	29	20	9	-	40.0	12.8
	Social	26	10	16	-	35.1	10.8

Statistical Inference Testing Results

Results for the three advice are given in3 tables for each. First, the average and median scores, for all groups at each stage are presented. Then, the distributions for each score, for each video Group are compared at each stage with the Control group using exact Mann-Whitney U-Tests. *U* statistics and significance values are given for each test. Finally, exact Sign Test results comparing scores from each group at each stage with scores from the same group gather before intervention. Here, the number of score decreases, increases, and ties are given (i.e., in the format: Decreases-Increases-Ties), as well as the significance values of the test.

Results for Update Groups

Average and (Median) Scores for Update Groups

			Awareness		*Perceptions*				*Emotions*	
		N	T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*Before*	29	2.2 (2)	1.7 (2)	1.0 (1)	0.8 (0.5)	-1.0 (-1)	-0.9 (-0.5)	6.7 (7)	5.5 (6)
	After	-	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)
	2 Weeks	23	2.3 (3)	1.6 (1.5)	0.9 (1)	0.6 (1)	-0.6 (-0.5)	-0.7 (-1)	5.2 (4)	4.1 (3)
	1 Month	25	2.2 (3)	1.7 (1.5)	1.1 (1)	0.9 (1)	-0.3 (0)	-0.6 (-1)	5.0 (4)	4.0 (3)
Basic	*Before*	24	2.0 (2)	1.9 (2)	0.6 (0.5)	0.4 (0)	-0.5 (-0.5)	-0.8 (-0.8)	7.1 (5)	6.7 (5)
	After	24	2.8 (3)	2.6 (2.8)	1.5 (1.8)	1.5 (1.5)	-0.9 (-1)	-1.4 (-1.5)	11.4 (14.5)	9.6 (11.5)
	2 Weeks	24	2.7 (3)	2.2 (2.5)	1.4 (1.5)	1.2 (1)	-1.0 (-1)	-1.1 (-1)	10.1 (11.5)	8.8 (9.5)
	1 Month	22	2.6 (3)	2.0 (2)	1.3 (1.5)	1.0 (0.8)	-0.7 (-0.8)	-0.8 (-1)	11.5 (15)	10.3 (12)
Emotion	*Before*	26	1.8 (2)	2.1 (2)	0.8 (1)	0.7 (1)	-0.4 (0)	-0.6 (-0.5)	4 (1.5)	2.7 (0.5)
	After	26	2.8 (3)	2.8 (3)	1.5 (1.5)	2.1 (2.3)	-1.1 (-1)	-1.5 (-1.5)	9.4 (10)	7.8 (6.5)
	2 Weeks	22	2.8 (3)	2.6 (2.5)	1.4 (1)	1.6 (1.8)	-0.5 (-0.5)	-1.2 (-1.5)	6.6 (4)	5.4 (2)
	1 Month	20	3.0 (3)	2.5 (2.5)	1.6 (1.5)	1.8 (2)	-0.8 (-0.5)	-1.6 (-1.5)	6.1 (4)	5.1 (3.5)
Social	*Before*	24	1.8 (2)	1.6 (1.5)	0.8 (1)	0.4 (0.3)	-0.6 (-0.5)	-0.3 (0)	7.0 (6)	6.0 (5.5)
	After	24	2.8 (3)	2.4 (2.5)	1.3 (2)	1.6 (2.3)	-0.9 (-1)	-1.1 (-1.5)	11.1 (15)	9.6 (10)
	2 Weeks	21	2.3 (3)	2.0 (2)	1.0 (1)	1.2 (1.5)	-0.5 (0)	-1 (-1)	9.5 (15)	7.8 (9)
	1 Month	23	2.6 (3)	2.2 (2.5)	1.0 (1)	1.1 (1)	-0.5 (-1)	-0.7 (-0.5)	9.3 (12)	8.0 (10)

Mann-Whitney U-Test Results for Update Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Basic	*Before*	282	307.5	277	263	269	343	310	288
		0.31	*0.60*	*0.2*	*0.12*	*0.16*	*0.93*	*0.82*	*0.52*
	After	195.5	168.5	242	227.5	344	234	173.5	185
		0.003	*0.001*	*0.06*	*0.03*	*0.95*	*0.04*	*0.002*	*0.005*
	2 Weeks	213.5	170.5	209	208	225.5	226	124	136
		0.18	*0.04*	*0.15*	*0.15*	*0.28*	*0.29*	*0.002*	*0.004*
	1 Month	205	196.5	260	263.5	236.5	260.5	82	90.5
		0.14	*0.21*	*0.75*	*0.81*	*0.42*	*0.76*	*< 0.001*	*< 0.001*
Emotion	*Before*	278.5	298	309	367.5	272.5	315	257.5	230
		0.13	*0.25*	*0.25*	*0.88*	*0.08*	*0.29*	*0.06*	*0.02*
	After	215	159	245.5	139.5	354.5	234.5	266	286.5
		0.002	*< 0.001*	*0.02*	*< 0.001*	*0.71*	*0.02*	*0.09*	*0.18*
	2 Weeks	173.5	119	178	134	243	172	205.5	204.5
		0.05	*0.003*	*0.09*	*0.005*	*0.83*	*0.06*	*0.54*	*0.51*
	1 Month	139	143	192.5	138	199	128.5	212	212
		0.003	*0.02*	*0.19*	*0.009*	*0.25*	*0.004*	*0.51*	*0.51*
Social	*Before*	253	312.5	347	275	293.5	249	325.5	335
		0.12	*0.67*	*0.99*	*0.19*	*0.33*	*0.07*	*0.85*	*0.97*
	After	187.5	208.5	252	201.5	336.5	273	178	184.5
		0.001	*0.02*	*0.08*	*0.007*	*0.84*	*0.18*	*0.003*	*0.005*
	2 Weeks	226.5	181	221	168	224	221	134	145.5
		0.93	*0.33*	*0.64*	*0.08*	*0.69*	*0.63*	*0.02*	*0.03*
	1 Month	213.5	195	265	256	250.5	284.5	166	156.5
		0.12	*0.08*	*0.65*	*0.52*	*0.45*	*0.96*	*0.02*	*0.009*

Sign Test Results for Update Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*After*	- -	- -	- -	- -	- -	- -	- -	- -
	2 Weeks	3-7-13 *0.34*	10-8-5 *0.82*	8-7-8 *1.0*	11-5-7 *0.21*	10-11-2 *1.0*	9-8-6 *1.0*	13-4-6 *0.05*	12-5-6 *0.14*
	1 Month	4-5-15 *1.0*	10-10-4 *1.0*	8-9-8 *1.0*	9-7-9 *0.80*	5-16-4 *0.03*	7-12-6 *0.36*	14-4-6 *0.03*	13-3-8 *0.02*
Basic	*After*	0-14-10 *< 0.001*	4-17-3 *0.007*	3-17-4 *0.003*	4-14-6 *0.03*	12-6-6 *0.24*	14-4-6 *0.03*	2-16-5 *0.001*	4-14-5 *0.03*
	2 Weeks	1-16-7 *< 0.001*	7-11-6 *0.48*	5-15-4 *0.04*	6-15-3 *0.08*	15-6-3 *0.08*	12-7-5 *0.36*	7-13-3 *0.26*	5-12-6 *0.14*
	1 Month	1-13-8 *0.002*	7-9-5 *0.80*	6-11-5 *0.33*	4-15-3 *0.02*	9-7-6 *0.80*	11-9-2 *0.82*	5-12-4 *0.14*	3-12-6 *0.04*
Emotion	*After*	1-19-6 *< 0.001*	4-18-4 *0.004*	3-20-3 *< 0.001*	2-22-2 *< 0.001*	16-5-5 *0.03*	18-2-6 *< 0.001*	2-18-6 *< 0.001*	1-19-6 *< 0.001*
	2 Weeks	2-14-6 *0.004*	6-13-3 *0.17*	3-14-5 *0.01*	4-15-3 *0.02*	9-10-3 *1.0*	16-5-1 *0.03*	4-11-6 *0.12*	3-10-8 *0.09*
	1 Month	1-14-5 *0.001*	4-12-4 *0.08*	2-14-4 *0.004*	4-15-1 *0.02*	11-7-2 *0.48*	14-2-4 *0.004*	5-12-3 *0.14*	2-12-6 *0.01*
Social	*After*	0-16-8 *< 0.001*	3-16-5 *0.004*	5-13-6 *0.10*	4-18-2 *0.004*	11-6-7 *0.33*	15-4-5 *0.02*	0-13-11 *< 0.001*	3-12-9 *0.04*
	2 Weeks	2-9-10 *0.07*	7-9-4 *0.80*	7-10-4 *0.63*	3-11-7 *0.06*	8-12-1 *0.50*	11-5-5 *0.21*	4-11-6 *0.12*	5-11-5 *0.21*
	1 Month	1-15-7 *0.001*	2-13-8 *0.007*	7-11-5 *0.48*	6-15-2 *0.08*	11-7-5 *0.48*	12-10-1 *0.83*	3-9-11 *0.15*	3-12-8 *0.04*

Results for Password Manager Groups

Average and (Median) Scores for Password Manager Groups

			Awareness		*Perceptions*				*Emotions*	
		N	T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*Before*	30	1.5 (1.5)	2.3 (2.5)	0.5 (0.5)	0.9 (0.8)	-0.1 (0)	-0.2 (0)	7.8 (7)	6.8 (6.5)
	After	-	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)
	2 Weeks	27	1.6 (2)	2.3 (2.5)	0.3 (1)	0.5 (1)	0.1 (0)	-0.1 (0)	7.7 (8)	6.9 (8)
	1 Month	27	1.8 (2)	2.5 (2.5)	0 (0.5	0.4 (1)	-0.1 (0)	-0.2 (0)	7.9 (8)	7.5 (8)
Basic	*Before*	30	1.7 (2)	2.3 (2.5)	0.7 (1)	1.0 (1)	0.2 (0)	0.3 (0)	6.2 (5)	5.5 (4.5)
	After	30	2.5 (3)	2.9 (3)	1.8 (2)	1.6 (2)	-1.0 (-1.3)	-1.1 (-1.5)	12.3 (15)	10 (11)
	2 Weeks	27	2.6 (3)	2.8 (3)	0.9 (1.5)	1.3 (1.5)	-0.7 (-0.5)	-0.5 (-0.5)	10.0 (13)	7.9 (9)
	1 Month	26	2.6 (3)	2.8 (3)	1.1 (1.5)	1.5 (1.8)	-0.5 (-0.5)	-0.5 (-0.5)	11.4 (15)	9.7 (12)
Emotion	*Before*	30	1.7 (2)	2.4 (2.5)	0.9 (1)	0.7 (1)	-0.1 (0)	-0.3 (0)	8.4 (10.5)	7.1 (8)
	After	30	2.3 (2)	3.1 (3)	1.7 (2)	1.7 (2)	-1.2 (-1)	-1.3 (-1.3)	12.2 (15)	10.0 (12)
	2 Weeks	26	2.3 (2)	2.8 (3)	1.5 (2)	1.4 (1.5)	-0.8 (-0.5)	-1.0 (-1)	12.3 (15)	10.7 (12)
	1 Month	23	2.5 (3)	2.8 (3)	1.6 (1.5)	1.7 (2)	-1.0 (-1)	-1.3 (-1.5)	11.1 (15)	10.2 (11)
Social	*Before*	28	1.8 (2)	2.2 (2.3)	0.5 (0.5)	0.6 (0.5)	0 (0)	-0.5 (-0.5)	7.3 (6)	6.2 (4.5)
	After	28	2.5 (3)	2.9 (3)	1.8 (2)	1.7 (2)	-0.6 (-0.8)	-0.9 (-1)	12.8 (15)	10.6 (12)
	2 Weeks	26	2.3 (3)	2.8 (3)	1.3 (1.5)	1.4 (1.5)	-0.3 (-0.5)	-0.3 (-0.5)	11.9 (15)	9.9 (10.5)
	1 Month	22	2.5 (3)	2.8 (3)	1.3 (1.5)	1.4 (1.5)	-0.3 (-0.5)	-0.8 (-1)	9.9 (13)	8.4 (10)

Mann-Whitney U-Test Results for Password Manager Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Basic	*Before*	411.5	448.5	472.5	417.5	414	376	371	383
		0.59	*0.99*	*0.74*	*0.63*	*0.60*	*0.27*	*0.24*	*0.32*
	After	213	311	213.5	262	248	241.5	239	280
		< 0.001	*0.04*	*< 0.001*	*0.007*	*0.004*	*0.003*	*0.001*	*0.01*
	2 Weeks	183.5	270	271.5	224	220.5	284.5	275.5	340
		0.001	*0.10*	*0.11*	*0.01*	*0.01*	*0.16*	*0.12*	*0.68*
	1 Month	193.5	278.5	177.5	174	270	283.5	216.5	272
		0.002	*0.19*	*0.001*	*0.001*	*0.15*	*0.23*	*0.01*	*0.16*
Emotion	*Before*	411.5	438.5	378.5	418	438	436	424	433
		0.58	*0.87*	*0.29*	*0.64*	*0.86*	*0.84*	*0.70*	*0.80*
	After	281.5	259.5	245.5	267.5	236	201.5	243.5	283.5
		0.008	*0.003*	*0.003*	*0.009*	*0.002*	*0.001*	*0.001*	*0.01*
	2 Weeks	225.5	258.5	179.5	240.5	206.5	193.5	185	190.5
		0.02	*0.09*	*0.001*	*0.03*	*0.005*	*0.002*	*0.002*	*0.004*
	1 Month	185.5	271.5	97.5	122	166	126	206.5	222.5
		0.009	*0.44*	*< 0.001*	*< 0.001*	*0.004*	*< 0.001*	*0.04*	*0.09*
Social	*Before*	363	404.5	405	377.5	416	332.5	392.5	391
		0.36	*0.81*	*0.82*	*0.51*	*0.95*	*0.17*	*0.67*	*0.65*
	After	205	281	214	249.5	284.5	256	204.5	228.5
		< 0.001	*0.03*	*0.002*	*0.01*	*0.05*	*0.02*	*< 0.001*	*0.002*
	2 Weeks	219	250.5	216.5	223	283	301.5	196.5	244
		0.01	*0.07*	*0.02*	*0.02*	*0.23*	*0.38*	*0.004*	*0.06*
	1 Month	166.5	230.5	146	166	275	199	234	274.5
		0.004	*0.18*	*0.002*	*0.007*	*0.66*	*0.05*	*0.20*	*0.66*

Sign Test Results for Password Manager Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*After*	- -	- -	- -	- -	- -	- -	- -	- -
	2 Weeks	6-8-13 *0.79*	9-12-6 *0.66*	13-10-4 *0.68*	13-9-5 *0.52*	9-13-5 *0.52*	11-12-4 *1.0*	9-8-10 *1.0*	12-10-5 *0.83*
	1 Month	5-8-14 *0.58*	8-9-10 *1.0*	15-8-4 *0.21*	13-9-5 *0.52*	7-15-5 *0.13*	9-12-6 *0.66*	9-10-8 *1.0*	9-12-6 *0.67*
Basic	*After*	1-18-11 *< 0.001*	5-18-7 *0.01*	3-22-5 *< 0.001*	6-20-4 *0.009*	21-3-6 *< 0.001*	22-2-6 *< 0.001*	0-24-6 *< 0.001*	6-20-4 *0.009*
	2 Weeks	2-20-5 *< 0.001*	4-14-9 *0.03*	7-17-3 *0.06*	5-16-6 *0.03*	15-7-5 *0.13*	17-8-2 *0.11*	3-18-6 *0.001*	8-14-5 *0.29*
	1 Month	1-17-8 *< 0.001*	7-12-7 *0.36*	6-13-7 *0.17*	5-13-8 *0.10*	17-5-4 *0.02*	17-7-2 *0.06*	3-18-5 *0.001*	7-15-4 *0.13*
Emotion	*After*	4-15-11 *0.02*	7-19-4 *0.03*	3-18-9 *0.001*	4-22-4 *0.001*	23-4-3 *< 0.001*	22-4-4 *0.001*	3-19-8 *0.001*	7-18-5 *0.04*
	2 Weeks	3-12-11 *0.04*	6-14-6 *0.12*	5-17-5 *0.02*	8-14-5 *0.29*	17-5-5 *0.02*	17-6-4 *0.04*	5-69-5 *0.03*	6-19-1 *0.02*
	1 Month	1-11-11 *0.006*	5-13-5 *0.10*	4-16-3 *0.01*	2-18-3 *< 0.001*	18-2-3 *< 0.001*	17-4-2 *0.007*	7-13-3 *0.26*	9-13-1 *0.52*
Social	*After*	3-17-8 *0.003*	4-18-6 *0.004*	3-21-4 *< 0.001*	6-19-3 *0.02*	17-6-5 *0.04*	15-9-4 *0.31*	3-18-7 *0.001*	4-17-7 *0.007*
	2 Weeks	5-15-6 *0.04*	4-15-7 *0.02*	7-15-4 *0.13*	6-15-5 *0.08*	13-9-4 *0.52*	10-12-4 *0.83*	2-16-8 *0.001*	6-15-5 *0.08*
	1 Month	3-12-7 *0.04*	8-11-3 *0.65*	4-13-5 *0.05*	6-11-5 *0.33*	12-6-4 *0.24*	10-5-7 *0.30*	5-9-8 *0.42*	7-11-4 *0.48*

Results for 2FA Groups

Average and (Median) Scores for 2FA Groups

			Awareness		*Perceptions*				*Emotions*	
		N	T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*Before*	26	2.0 (2)	2.5 (2.5)	1.2 (1.5)	1.3 (1)	-0.1 (0)	-0.2 (0)	11.1 (15)	9.3 (11)
	After	-	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)	- (-)
	2 Weeks	24	1.9 (2)	2.8 (3)	1.1 (1.3)	1.6 (2)	0 (0)	0 (0)	10.8 (15)	9 (11.5)
	1 Month	24	2.1 (2)	2.8 (3)	1.5 (1.5)	1.5 (1.5)	0 (0.3)	-0.6 (-0.8)	10.5 (15)	9.3 (11)
Basic	*Before*	29	2.2 (2)	2.6 (2.5)	1.5 (1.5)	1.1 (1)	-0.5 (-1)	-0.5 (-0.5)	11.4 (15)	10.2 (12)
	After	29	2.5 (3)	3.0 (3)	2.2 (2.5)	1.8 (2)	-0.8 (-1)	-0.6 (-1)	14.3 (15)	12.4 (13.5)
	2 Weeks	26	2.5 (3)	3.1 (3)	2.1 (2)	1.8 (2)	-0.5 (-1)	-0.5 (-0.8)	13.3 (15)	11.2 (12)
	1 Month	20	2.6 (3)	2.9 (2.8)	1.9 (2)	1.8 (2)	-0.7 (-1)	-0.6 (-1)	12.3 (15)	10.5 (11)
Emotion	*Before*	29	2.3 (3)	3.0 (3)	1.2 (1)	1.3 (1)	-0.3 (0)	-0.4 (0)	8.9 (14)	7.9 (9)
	After	29	2.4 (3)	3.0 (3)	1.7 (2)	1.9 (2)	-0.7 (-1.5)	-0.7 (-1)	10.7 (14)	9.3 (10)
	2 Weeks	27	2.3 (2)	2.7 (3)	1.4 (1.5)	1.5 (1.5)	-0.3 (-0.5)	-0.8 (-1)	11.1 (15)	9.2 (11)
	1 Month	25	2.4 (2)	2.8 (3)	1.5 (1.5)	1.6 (2)	-0.8 (-1)	-1.1 (-1)	11.8 (15)	9.6 (10
Social	*Before*	26	2.1 (2)	2.9 (3)	1.1 (1.5)	1.5 (1.8)	-0.1 (-0.3)	-0.2 (-0.3)	10.1 (13)	8.2 (9)
	After	26	2.8 (3)	3.0 (3)	2.0 (2.5)	1.8 (2.5)	-0.6 (-1)	-1.0 (-1.3)	12.0 (15)	10.1 (11)
	2 Weeks	24	2.8 (3)	2.9 (3)	1.4 (2)	1.6 (2)	-0.9 (-0.8)	-0.9 (-0.8)	12.8 (15)	11.0 (12)
	1 Month	23	2.6 (3)	2.8 (3)	1.6 (2)	1.7 (2)	-0.7 (-0.5)	-0.5 (-0.5)	12.4 (15)	10.4 (11)

Mann-Whitney U-Test Results for 2FA Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Basic	*Before*	343	356	316.5	339	295.5	308	372.5	333.5
		0.55	*0.73*	*0.43*	*0.69*	*0.24*	*0.34*	*0.94*	*0.47*
	After	285	253	178	253	252.5	287.5	236.5	226
		0.09	*0.03*	*0.001*	*0.05*	*0.05*	*0.19*	*0.006*	*0.02*
	2 Weeks	177	277	138	285	227	261	249	269
		0.004	*0.49*	*< 0.001*	*0.60*	*0.10*	*0.32*	*0.17*	*0.40*
	1 Month	156	222.5	165	196	155.5	238	210	222
		0.03	*0.68*	*0.07*	*0.30*	*0.04*	*0.97*	*0.44*	*0.68*
Emotion	*Before*	314	253.5	355.5	348	349	348	311	330.5
		0.26	*0.03*	*0.91*	*0.80*	*0.82*	*0.80*	*0.24*	*0.44*
	After	304.5	276.5	264.5	254.5	254	264.5	358	367
		0.20	*0.08*	*0.08*	*0.06*	*0.06*	*0.09*	*0.74*	*0.87*
	2 Weeks	243	301.5	266.5	308	283.5	230	318.5	315.5
		0.10	*0.67*	*0.28*	*0.76*	*0.45*	*0.08*	*0.91*	*0.88*
	1 Month	248	278.5	279.5	259.5	186.5	214	274	293
		0.27	*0.66*	*0.68*	*0.42*	*0.02*	*0.08*	*0.58*	*0.89*
Social	*Before*	330	241	322	278	321	316.5	297.5	294
		0.94	*0.07*	*0.96*	*0.38*	*0.94*	*0.88*	*0.44*	*0.42*
	After	176.5	240.5	166.5	206.5	256.5	222	284	304.5
		0.001	*0.06*	*0.002*	*0.02*	*0.20*	*0.05*	*0.39*	*0.70*
	2 Weeks	116	284	224.5	269	185.5	200	237	262.5
		< 0.001	*0.94*	*0.19*	*0.69*	*0.03*	*0.07*	*0.24*	*0.60*
	1 Month	185	238.5	240.5	210	194	249.5	227.5	254.5
		0.04	*0.41*	*0.45*	*0.16*	*0.08*	*0.58*	*0.24*	*0.65*

Sign Test Results for 2FA Groups

		Awareness		*Perceptions*				*Emotions*	
		T/F	M-C	INDF	SOCF	INDN	SOCN	Valence	Prosocial
Control	*After*	- -	- -	- -	- -	- -	- -	- -	- -
	2 Weeks	6-3-15 *0.51*	5-8-11 *0.58*	8-4-11 *0.39*	8-6-9 *0.79*	8-11-4 *0.65*	10-10-3 *1.0*	7-7-10 *1.0*	8-10-6 *0.82*
	1 Month	6-6-12 *1.0*	6-9-9 *0.61*	4-9-10 *0.27*	3-7-13 *0.34*	7-10-6 *0.63*	13-6-4 *0.17*	5-7-12 *0.77*	7-14-3 *0.19*
Basic	*After*	3-9-17 *0.15*	8-16-5 *0.15*	2-16-11 *0.001*	3-16-10 *0.004*	15-6-8 *0.08*	14-9-6 *0.41*	0-12-16 *< 0.001*	6-15-7 *0.08*
	2 Weeks	3-8-15 *0.23*	4-12-10 *0.08*	4-11-11 *0.12*	2-11-13 *0.02*	9-10-7 *1.0*	9-12-5 *0.66*	5-10-11 *0.30*	9-12-5 *0.66*
	1 Month	2-5-13 *0.45*	6-9-5 *0.61*	5-7-8 *0.77*	4-8-8 *0.39*	9-6-5 *0.61*	8-7-5 *1.0*	3-6-11 *0.51*	9-8-3 *1.0*
Emotion	*After*	2-3-24 *1.0*	10-7-12 *0.63*	4-14-11 *0.03*	4-14-11 *0.03*	16-6-7 *0.05*	16-7-6 *0.09*	2-10-17 *0.04*	8-14-7 *0.29*
	2 Weeks	6-7-14 *1.0*	13-7-7 *0.26*	12-9-6 *0.66*	8-11-8 *0.65*	14-9-4 *0.41*	15-3-9 *0.008*	2-7-18 *0.18*	8-14-5 *0.29*
	1 Month	3-6-16 *0.5*	11-7-7 *0.48*	7-10-8 *0.63*	4-8-13 *0.39*	17-7-1 *0.06*	16-5-4 *0.03*	3-9-13 *0.15*	7-15-3 *0.13*
Social	*After*	0-16-10 *< 0.001*	11-8-7 *0.65*	2-18-6 *< 0.001*	5-14-7 *0.06*	16-5-5 *0.03*	18-4-4 *0.004*	2-8-15 *0.11*	6-12-7 *0.24*
	2 Weeks	0-14-10 *< 0.001*	9-6-9 *0.61*	6-12-6 *0.24*	9-9-6 *1.0*	15-8-1 *0.21*	17-6-1 *0.04*	2-11-11 *0.02*	5-12-7 *0.14*
	1 Month	3-13-7 *0.02*	9-5-9 *0.42*	4-12-7 *0.08*	6-10-7 *0.45*	14-5-4 *0.06*	12-8-3 *0.50*	2-9-12 *0.07*	5-10-8 *0.30*