Social Cybersecurity:  
Understanding and Leveraging Social Influence to Improve End-User Security Sensitivity

Sauvik Das  
Human-Computer Interaction Institute  
School of Computer Science  
Carnegie Mellon University

Ph.D. Thesis Proposal  
March 7th, 2016

Thesis Committee  
Jason I. Hong (chair) [HClI, CMU]  
Laura A. Dabbish (co-chair) [HClI, CMU]  
Jeffrey P. Bigham [HClI, CMU]  
J.D. Tygar [University of California, Berkeley]
Abstract

Despite substantial improvements made by the usable privacy and security community at raising the general populace’s awareness of, motivation to use, and knowledge of how to use security and privacy tools (i.e., their security sensitivity), much security advice remains ignored and many security tools remain underutilized. In this thesis, I argue that this low security sensitivity can partially be explained by the fact that traditional security and privacy behaviors can have myriad social consequences. For example, by using two-factor authentication, one might also be perceived as “paranoid” or as someone with something to hide. Yet, to date, little theoretical work in usable privacy and security has applied social science theory to understand how these potential social consequences affect people’s security sensitivity. Likewise, little systems work in usable privacy and security has considered the social consequences of security tool design, nor have many security tools been developed with social principles in mind.

To bridge this gap in the literature, I will begin to build a theory of social cybersecurity and apply these theoretical insights to create interventions and security tools that improve people’s security sensitivity. Specifically, through a series of observational studies, I will construct both qualitative and quantitative models of behavior to explore how and why social factors influence security sensitivity and, in turn, the diffusion of security tool adoptions through a social network. I will then conduct a series of random experiments to test if these observational insights can be leveraged to enhance security sensitivity. I will then distill these observational and experimental results into a set of concrete design guidelines and recommendations for the effective use of social influence to increase security sensitivity and to improve security and privacy tools. Finally, to begin exploring the design space of social cybersecurity systems, I will design, implement, and evaluate a socially compatible security system, Thumprint. In a field deployment, I will use Thumprint as a design probe to better understand how the introduction of a “social” cybersecurity system affects security practices and social dynamics.

Concretely, this thesis will provide the following contributions: (i) an initial theory of social cybersecurity, developed from both observational and experimental work, that explains how social factors affect people’s security sensitivity—i.e., their awareness of, motivation to use, and knowledge of how to use security tools; (ii) a set of design recommendations for creating better, more socially compatible security and privacy systems; and, (iii) the design, implementation and evaluation of a system that leverage these design recommendations to explore the design space of social cybersecurity systems.
# Table of Contents

Abstract ................................................................................................................................................. 2

Chapter 1: Introduction .......................................................................................................................... 5

Chapter 2: Background and Related Work .......................................................................................... 8
  Security Sensitivity ............................................................................................................................... 8
  Social Influence and Security Sensitivity ............................................................................................ 8
  Gaps and Opportunities ....................................................................................................................... 10

  Summary ............................................................................................................................................... 12
  Motivation ............................................................................................................................................ 12
  Methodology ....................................................................................................................................... 12
    Semi-Structured Interviews .................................................................................................................. 12
    Recruitment ....................................................................................................................................... 13
    Data Coding and Analysis .................................................................................................................. 14
  Results ................................................................................................................................................ 15
    Social Triggers in Driving Behavior Change ...................................................................................... 16
  Discussion ........................................................................................................................................... 21
    Opportunities .................................................................................................................................... 21
    Future Work ...................................................................................................................................... 22

Chapter 4: Understanding How Security Information Is Communicated ....................................... 24
  Summary ............................................................................................................................................... 24
  Motivation ............................................................................................................................................ 24
  Methodology ....................................................................................................................................... 24
    Data Coding and Analysis .................................................................................................................. 25
  Results ................................................................................................................................................ 25
    Catalysts for Security Related Communication .............................................................................. 25
    Conversation Goals .......................................................................................................................... 28
    Identifying a typology of communications: The Interaction of catalysts and goals ..................... 28
  Discussion ........................................................................................................................................... 33
    Opportunities .................................................................................................................................... 33
    Future Work ...................................................................................................................................... 34

Chapter 5: How Social Influences Affects Security Tool Diffusion .............................................. 35
  Summary ............................................................................................................................................... 35
  Motivation ............................................................................................................................................ 35
  Hypotheses .......................................................................................................................................... 36
    Social Diffusion and Friend Diversity ................................................................................................. 36
    Social Diffusion and Observability .................................................................................................... 36
    Social Diffusion on Security Adoptions ............................................................................................. 36
  Methodology ....................................................................................................................................... 37
  Results ................................................................................................................................................ 39
    How exposure to friends from distinct social circles relates to adoption ......................................... 39
    How social influence affects the adoption of security tools ............................................................ 41
    Summary of Results As They Relate to Hypotheses ......................................................................... 45
  Discussion ........................................................................................................................................... 45
  Future Work ....................................................................................................................................... 46
Chapter 6: Increasing Security Sensitivity with Social Proof

Summary...................................................................................... 48
Motivation.................................................................................... 48
Experiment .................................................................................. 49
  Methodology ............................................................................. 49
  Dataset ................................................................................... 53
Hypotheses .................................................................................. 54
Results ....................................................................................... 55
  Summary of Results from Initial Experiment........................... 58
Follow-up Study With Survey to Gauge Sentiment and Awareness ............................................................................. 58
  Methodology ............................................................................. 58
  Results ................................................................................... 59
General Discussion ..................................................................... 60
Future Work .............................................................................. 61

Chapter 7: Proposed work.......................................................... 62
Proposed Observational Work..................................................... 62
  Viral Security Behavior Surveys .............................................. 62
  Security Information Dissemination Surveys ......................... 63
Proposed Experimental Work...................................................... 64
  Social & Contextual Privacy Notifications .............................. 64
Proposed System Development Work ........................................ 66
  Thumprint .............................................................................. 66
Summary & Expected Contributions .......................................... 69

Chapter 8: Timeline .................................................................... 71
References .................................................................................. 72
Chapter 1: Introduction

In early 2013, the Associated Press's Twitter account was compromised through a password phishing scheme, and erroneously tweeted that President Obama was injured in a bombing [82]. In response, stock prices plummeted [56], adversely affecting thousands. Moreover, this incident could have been easily prevented with the use of two-factor authentication: A security tool, available at that time, that requires entry of a random code generated on one's phone in addition to a password when authenticating [44]. This incident is just one example of how the underutilization of available security and privacy tools remains a large, outstanding problem.

In our age of increasing connectivity, it is critically important for the widespread awareness of and appropriate use of security and privacy (S&P) tools to protect our rich, deeply personal data and resources. Accordingly, there have been many efforts in both industry and academia seeking to address the underutilization of S&P tools. Among academics, there has been a deep focus on improving the usability of existing S&P tools (e.g., [43,45,67,81]), inventing new S&P tools that were made to be usable (e.g., [17,34,36,42,69]), as well as better communicating information about S&P risks and options to counter-act those risks through warnings and notifications (e.g., [8,25,26,29,30]).

Likewise, large, online user-facing companies like Facebook and Google are investing a lot in the construction of security and privacy tools to provide people with a multitude of options to secure their accounts and protect their data. For example, Facebook offers a suite of optional, end-user facing security tools such as Login Notifications (e-mail/SMS notifications of login attempts), Login Approvals (two-factor authentication) and Trusted Contacts (enlisting friends to help with account recovery), while Google has invested considerable effort in improving reactive and preventative warnings to keep consumers safe from privacy and security threats.

Nevertheless, despite these substantial and important usability improvements, the awareness and adoption of these tools remains relatively low [18,44]. For example, at least in 2013, the adoption rate, among Facebook users, was less than 10% for Login Notifications, less than 2% for Login Approvals and Trusted Contacts [19]. Similarly, a field study on the effectiveness of browser warnings found that as many as 70% of users bypass certain security and privacy warnings [3].

The question remains: Why does the awareness and adoption of security and privacy tools remain low among lay people? Prior work offers a number of reasons. Some prior work suggests that many believe they are in no danger of experiencing a security breach [1] and are unaware of both threats and the security tools available to protect against those threats. Other work suggests that many choose not to use security tools and follow security advice because doing so is often antagonistic towards the immediate goal of end users—a complex password that usually requires three attempts to get right prevents a user from doing what she actually wants to do: e.g., authenticating into social media. Herley further argues it may even be economically rational for users to ignore security advice, as the expected cost, in time, of a lifetime of following security advice might actually be higher than the expected loss a user would suffer if his account actually was compromised [39]. Thus, many people are unmotivated to behave securely. Still others suggest that security tools are simply too difficult to use [66,81], so many people do not have the knowledge required to operate them. Taken together, it appears that the lack of what we call security sensitivity—the awareness of motivation to use, and knowledge of how to use security and privacy tools—is a large barrier to increasing the uptake of security tools and the following of security advice.

In this thesis, I argue that one reason security sensitivity remains relatively low among the general populace is that we do not yet understand the social processes underlying people's decisions to communicate about security and adopt security tools. In other words, security behaviors—as any human behavior—should be viewed within the context of a social system. Indeed, the social psychology literature illustrates that social influence, or our ability to affect other people's perceptions and behaviors with our words and actions [15], plays a central role in how people behave—even specifically in changing their behavior or adopting a new technology or idea [15,62]. Rogers' highly influential diffusion of innovations work, for example, has shown that social influence drives technology adoption [62]. Likewise, another popular model for explaining how technology
gets adopted and sees widespread use, the Technology Acceptance Model [20], identifies social influence as a key factor in driving new technology adoption.

Social processes, thus, should undoubtedly affect one’s decision to follow security advice or adopt a privacy tool. For example, prior work has shown that people who encrypt email can be perceived as “paranoid” by others [32], which, in turn, suggests that the early adopters of some S&P tools may disenfranchise the tool and inhibit others from adopting the tool themselves. Conversely, the principle of social proof—that we look to others for cues on how to behave, especially when we are uncertain [15]—suggests that if people see many examples of others using a S&P tool, they should be more inclined to use the tool themselves. Understanding this tension between disenfranchisement and social proof, and especially how it interacts with the particular design of different security tools, might be pivotal in determining people’s motivation to use a S&P tool. Similarly, how people communicate with each other about S&P tools and behaviors might be pivotal in determining people’s awareness and knowledge of available S&P tools. Taken together, these illustrative examples show that social processes might significantly impact all layers of the security sensitivity stack—awareness, motivation, and knowledge. Yet, to date, little theoretical work in usable privacy and security has applied social science theory to understand how social processes affect security sensitivity.

In turn, this lack of theoretical insight has precluded systems work that considers the social consequences of S&P tool design. As a result, few security tools have been developed with social principles in mind. For example, authentication tools have traditionally only served (i) large organizations, like militaries, who have strict security needs and only loosely trust individual members of the organization and (ii) individuals who trust no one else. Thus, authentication tools have been largely isolating, forcing people into a “me vs. the world” mindset where no one outside of the user, herself, can be trusted. Accordingly, it is difficult to share access to devices and resources without violating the security assumptions of a system. Furthermore, many authentication tools treat all “non-users” as the same, whether that non-user is the user’s spouse who wants to use a phone’s map application for navigation or a cracker with the intention of stealing the user’s personal data. Yet, there is increasing evidence that people do, in fact, want to share access to their personal devices and resources with others [37,72]. Families, for example, collectively own a number of devices—such as game consoles, smart appliances, and computers—to which they would like shared access without the need for strict security, because they largely trust each other and already have a lot of physical security. Thus, there remains a great but largely untapped opportunity for innovation in constructing socially compatible S&P tools that can potentially increase people’s security sensitivity.

To bridge these gaps in the literature, I propose to build an initial theory of social cybersecurity and apply these theoretical insights to create interventions and security tools that improve people’s security sensitivity. Specifically, through a series of observational studies, I will construct both qualitative and quantitative models of behavior to explore whether and how social factors influence security sensitivity and S&P tool adoption. I will then conduct a series of experiments to test if these observational insights can be leveraged to enhance security sensitivity. I will then distill these observational and experimental results into an initial set of design recommendations for the effective use of social influence to improve S&P tools. Finally, with these social design recommendations in mind, I will design, implement, and evaluate a socially compatible security system and gauge how it affects security sensitivity and social dynamics.

The remainder of this document outlines the theoretical background of my work (chapter 2), my initial explorations into constructing a theory of social cybersecurity using both observational and experimental work (chapters 3-6), and, finally, my proposed work: to expand upon my theoretical contributions with additional observational studies and experimentation, as well as to demonstrate the practical application of these theoretical insights by designing, implementing and evaluating a social cybersecurity system, Thumprint (chapters 7-8). Specifically, this thesis will follow the outline depicted by the following image:
Social Cybersecurity

Preliminary Work

Observational Analysis
- Behavior + Communication Interviews
- Diffusion analysis
- Behavior + Communication Surveys

Experimental Testing
- Social Proof Experiment
- Social + Contextual Notifications Experiment

System Development
- Thumprint

Proposed Work
Chapter 2: Background and Related Work

Security Sensitivity

Prior work in usable privacy and security alludes to at least three reasons underlying why much security advice is ignored and many security tools remain unused: lack of awareness, motivation, and knowledge. First, many users lack the awareness of security threats and the tools available to protect themselves against those threats. For example, a study by Adams and Sasse found that insufficient awareness of security issues caused users to construct their own model of security threats that are often incorrect, resulting in security breaches [2]. Stanton and colleagues found that a lack of awareness of basic security principles even influenced “experts” to make security mistakes, such as using a social security number as a password [73]. Users who are unaware of a threat cannot take measures to avoid the threat, and users who are not cognizant of the tools available to protect themselves from these threats cannot use those tools to actively defend themselves.

Second, users—even those who are aware of security and privacy threats and the preventive tools that combat those threats—often lack the motivation to utilize security features to protect themselves [2,26]. The lack of motivation to use security features is not entirely surprising, as stringent security measures are often antagonistic towards the specific goal of the end user at any given moment [24,66]. For example, while a user might want to access her Facebook, a complex password that usually requires three attempts to get right prevents her from accessing Facebook for an intolerable amount of time [25]. Thus, users often reject the use of security and privacy tools when they expect or experience them to be weighty [2,32,41,66].

Furthermore, many security threats remain only an abstract threat to most individuals [2,38,59]: Bob may know, conceptually, that there are security risks to using the same simple password across accounts, but does not believe that he is, himself, in danger of experiencing a security breach. Additionally, this perspective may be economically rational, as the expected cost, in time, of a lifetime of following security advice might actually be higher than the expected loss a user would suffer if his account actually was compromised [39]. Finally, the benefits of security features are often invisible, as users are often not cognizant of the absence of a breach that otherwise would have occurred without the use of a security or privacy tool. In all, it is unsurprising that many users lack the motivation to explicitly use security tools: to do so would mean to incur a frustrating complication to everyday interactions in order to prevent an unlikely threat with little way to know whether the security tool was actually effective.

Third, security tools are often too complex to operate for even aware and motivated end-users, suggesting that users often do not have the specialized knowledge to actually utilize security tools [81]. Indeed, there is a wide gulf of execution for most security features for most users. For example, many users cannot distinguish legitimate vs. fraudulent URLs, nor forged vs. legitimate email headers [22]. Also, a study revealed how security features in Windows XP, Internet Explorer, Outlook Express, and Word applications are difficult for users [31]. And, Wash found that many people hold “folk” models of computer security that are often misguided, and use these incorrect models to justify ignoring security advice [78].

In sum, prior work in usable privacy and security suggests that there are at least three large obstacles inhibiting the widespread use of security and privacy tools: the awareness of security threats and tools, the motivation to use security tools, and the knowledge of how to use security tools (see Error! Reference source not found.). We refer to this layered stack as security sensitivity for ease of discussion, as it encapsulates how likely a user is to seek information about and use security tools. Note, however, that the concept is not necessarily novel, as prior work has alluded to such a stack in security specifically [26], and in the adoption of technology more generally [21,62].

Social Influence and Security Sensitivity

Efforts have been made at improving all parts of the security sensitivity stack—for example, through games for security education [71], browser extensions to make people more aware of phish [83], more effective user interfaces for security tools [23], and simpler ways to authenticate [17]. Security sensitivity, nevertheless, could be much higher. The question is: how?
Prior work in cognitive psychology highlights the influential nature of social proof in driving human behavior. For example, lots of prior work has demonstrated the potency of the concept of “social proof”—or our tendency to look to others for examples of how to act in uncertain circumstances [13,15]. For example, Milgram, Bickman, and Berkowitz [55] demonstrated the social proof principle when they showed that simply getting a small crowd of people—the more, the better—to look up at the sky on a busy sidewalk caused others to do the same. Still other work has shown how social interventions can be powerfully effective at driving human behavior: for example, at reducing household energy consumption by showing people their neighbors’ reduced energy consumption [68], reducing hotel guests’ wasteful use of towels by showing them previous patrons chose to be less wasteful [33], and even in eliminating young children’s phobia of dogs by showing them film clips of other children playing with dogs [6].

Other work highlights the significant effect of social processes in the adoption of technology, specifically. For example, in his seminal work on the diffusion of innovations, Rogers claimed that new technology gets widely adopted through a process by which it is communicated through members of a social network [62]. Rogers argued that primarily subjective perceptions, not scientific or empirical fact, get communicated through social channels, and that these perceptions are key to the success of an innovation. He further outlined that preventative innovations—or innovations, like security and privacy tools, that prevent undesirable outcomes from happening in the future—typically have low adoption rates, probably because of their lack of observability, or the invisibility of their use and benefits. More recent studies on online platforms such as Facebook have similarly alluded to the potency of social proof. Kramer [49] showed that users were more likely to share emotional content matching the emotional valence of content shared by friends in the past few days, and Burke and colleagues [9] showed that social learning plays a substantial role in influencing how newcomers to Facebook use the platform. Notably, Bond and colleagues [7] found that simply showing people that their Facebook friends voted was sufficient to increase voter turnout in the 2010 U.S. Congressional elections.

Taken together, the background literature suggests that social influence strongly affects people’s behaviors and decisions; likely, also their security-related behaviors and decisions. And, indeed, prior work has alluded to the importance of social processes in raising security sensitivity. For example, DiGioia and Dourish [23] suggested that “social navigation”—or people’s inclination to look for cues on how to act—can be used to raise users’ security sensitivity by showing them other users’ actions in context. Rader et al.’s study on stories as informal lessons about security suggests that storytelling
increases awareness of and motivation to guard against security threats [58]. On the other hand, social processes can also lower security sensitivity and/or encourage unsafe practices. For example, Singh et al. outlined the common practice of sharing passwords and PINs [72]. Gaw et al. [32] found that many people believed that use of security tools was an indication of paranoia, unless the user had an obvious reason for doing so. If there is a stigma of paranoia attached to using security features, then it is possible that social influence can also work against security sensitivity (e.g., “only paranoid people encrypt their e-mail, and I’m not paranoid”).

In fact, because security tool usage is often invisible, rarely communicated, and generally undesired [15, 24], it may be that social processes, left unchecked, work against security sensitivity more often than not. Indeed, prior work in usable privacy and security suggests that many security features remain unused because stringent security measures are often antagonistic towards the specific goal of the end user at any given moment [66]. For example, while a user might want to check her e-mail, a complex password that usually requires three attempts to get right prevents her from checking her e-mail. Thus, people often reject security features when they expect or experience them to be weighty [2]. Consequently, typically only people who are especially dedicated to protecting their information use interruptive security features, and we know from prior work that non-experts may perceive these early adopters as “paranoid” [32]. More formally, because early adopters of security features are likely to be perceived by others as behaviorally different (e.g., either paranoid, or in possession of expert knowledge), non-experts may perceive an illusory correlation [12], or an exaggerated relationship, between security feature usage and this behavioral difference. In turn, as non-experts consider themselves different from those who use security features, they may reject the use of security features. Moreover, this illusory correlation should only strengthen as more of these security-enthusiast early adopters use the feature because of the “availability heuristic”—a mental shortcut that biases people’s judgments towards what is more frequently recalled [76].

The upshot of all of this is that the subjective perceptions of a security feature that propagates through social channels may work against its adoption, at least until enough of a potential adopter’s behaviorally similar friends start using the feature so that its use becomes normative.

**Gaps and Opportunities**

While there is a host of rich prior work in social psychology highlighting the importance of social influence in driving human behavior, and a host of rich prior work in usable security highlighting the reasons why end-users avoid using security tools, the background literature explicitly exploring how social processes affect privacy and security decisions remains surprisingly thin.

Indeed, to my knowledge, little work has looked at how social influence affects security sensitivity, and, in turn, enacts behavior changes related to privacy and security, or how people generally communicate about security and privacy (outside of Rader et al.’s study on security storytelling [58]). Yet, understanding how social influence affects security related behavior change and communication could improve our understanding of why security sensitivity remains as low as it is, and could even help inform the design of social interventions that raise security sensitivity. Thus, there is a strong need for more observational work to build up an initial theory of how social processes affect security and privacy behaviors and communications.

Similarly, while much background work alludes to the potential efficacy of social proof in heightening security sensitivity, there is a substantial lack of work testing this potential. Part of the problem is that security feature usage has historically been kept secret to preserve the privacy of individual feature-users. Still, as social channels are the primary way through which innovations spread [61], the hiding of social meta-data surrounding security feature usage has undoubtedly inhibited both the widespread adoption of security features and research in studying social cues as a way to heighten security sensitivity. The little empirical data we do have about the effects of social influence on security related behavior change comes from work that only treated the social dimension in passing. Egelman and colleagues [28] included a social condition in their study on the effects of various types of password meters on convincing people to create stronger passwords. They found that a “peer pressure” password meter that showed participants how strong their passwords were relative to other “users” performed no better in increasing the strength of participants’ composed passwords, as
compared to a standard password meter that told participants whether their passwords were “weak”, “medium” or “strong”. However, Egelman and colleagues’ “peer pressure” password meter measured participants’ passwords relative to strangers’ passwords for a completely different service, and provided little feedback as to whether a given meter reading was important enough to act upon (is it good or bad that my password is better than 50% of “others”?). In addition, their social intervention could only have an affect on participants’ motivation—not awareness or knowledge.

Thus, there is a strong need for more experimental work to investigate the presence and strength of a causal link between social proof and security sensitivity.

Finally, few security tools have been designed to be “social”—i.e., with an understanding of the social consequences of security tool use or with the intention of leveraging social processes to maximize their adoption. For example, even though people frequently share passwords and PINs [37,72], few security tools have been developed to be inclusive. Rather, most existing security solutions support sharing access through ad-hoc solutions, if at all: e.g., by having people create a “guest PIN” that they have to separately remember, or by sharing their original password or PIN which affords guests unrestricted access. Likewise, few security tools are built to be observable, so that their use can be seen by others (to maximize social spread) without compromising the user’s security. Also, few tools allow people to act on their deep sense of responsibility for their friends and loved ones security. Thus, there is a strong need for more system development work that explores and iterative evaluates “social” security and privacy tools.

For my dissertation work, I intend to bridge these gaps in theory and practice. I will contribute observational work exploring how social influence affects security tool adoptions and behaviors. I will also contribute experimental work in which I will directly test how modulating social proof affects people’s security sensitivity. Finally, I will implement and evaluate a social cybersecurity tool designed with the social principles I uncovered from my prior work and my initial experimental and observational work.

Summary
The first step in making security more social is to build a theory for social cybersecurity—or, to understand the relationship between social influence and security adoption, and to identify areas where current security tools can be improved with social modifications. To build this understanding, I employed both in-depth qualitative and large-scale quantitative research methods. In this chapter, I present some formative work in which I used semi-structured interviews to ask people of various ages and backgrounds about their security-related behavior changes and communications [1]. I found that social factors were key drivers of security-related behavior change, accounting for nearly half of all reported behavior changes (e.g., using a PIN on one's phone or enabling a Facebook security tool). The most prevalent social catalyst for security related behavior change was observing friends—people often started using security tools after observing friends and/or strangers use those same tools. Unfortunately, few security tools are built for this form of passive observability, and are thus unable to spread in this powerful and social way.

Motivation
Much prior work in usable privacy and security has looked at improving all parts of the security sensitivity stack—for example, through games for security education [71], browser extensions to make users more aware of phish [83], more effective user interfaces for security tools [48], and faster or simpler ways to authenticate users [75]. Security sensitivity, nevertheless, remains low.

I argue that part of the problem is that we do not yet understand the social processes underlying people's decisions to communicate about security and adopt security tools. In other words, security behaviors—as any human behavior—should be viewed within the context of a social system. Indeed, the social psychology and sociology literature illustrates that social influence, or our ability to affect other people's perceptions and behaviors with our words and actions [15], plays a central role in how people behave—even specifically in changing their behavior or adopting a new technology or idea [15,62]. Rogers' highly influential diffusion of innovations work, for example, has shown that social influence drives technology adoption [62]. Social processes, thus, should undoubtedly affect a user's decision to follow security advice or adopt a security tool.

Nevertheless, the effect of social influence on decisions people make about security and privacy remains relatively understudied. Indeed, we do not yet know how social influence affects behavior change with regards to security and privacy. Understanding how social influence affects security related behavior change and communication should improve our understanding of why security sensitivity remains low, and, in turn, may help inform the design of social interventions and tools that can raise security sensitivity. To that end, I conducted a retrospective interview study aimed at investigating the following research questions:

**RQ1:** What role does social influence play in an individual's decisions to use, discontinue use, and explore security tools and privacy settings?

**RQ2:** Under what circumstances do people communicate about security and privacy?

However, as these two research questions are fairly distinctive and inform distinctive directions for future work, in this chapter, I will focus on our findings with respect to **RQ1**. In Chapter 4, I will more deeply explore our interview findings with respect to **RQ2**.

Methodology
Semi-Structured Interviews
We constructed an IRB approved semi-structured interview protocol to probe participants about recent security related behavior changes. We elected a semi-structured approach so that we could concretize the discussion by directing participants' memories towards changes in behavior, while
still allowing participants the flexibility to expand on the their undoubtedly unique experiences. Our interview protocol probed participants about recent changes in (1) mobile authentication, or whether and why participants enabled, disabled, or changed authentication on their smartphones (e.g., from PIN to Password); (2) application installation and uninstallation, or whether and why participants decided to uninstall or halt installing applications because of privacy and security concerns; and, (3) online privacy settings in social media, or whether and why participants changed their privacy settings on the social media platform they most commonly used. We chose to explore these three categories to uncover general trends across different types of security tools, and we chose these three categories specifically because they represented a broad range of behaviors representative of common security and privacy decisions made by most people on a fairly regular basis.

If participants reported a specific security-related behavior change, we asked them to explain further how the change was catalyzed—specifically, to discern between social and non-social catalysts for behavior change. Either way, we asked participants to explain, in detail, the context surrounding their decision to enact the change: Was the change brought about by a personal negative experience, or because of an article they read online? If they heard about a security incident through a friend, how did the friend broach the conversation? And, if a social process drove the change, we asked participants to clarify how the social process manifested—for example, did they seek out advice, or did a friend offer them unsolicited advice? We also asked participants whether and why they did or did not share their concerns, advice, or behavior change with anyone else.

We iteratively refined our protocol by piloting it with 5 people. All interviewers participated in the pilots in order to mitigate variation in delivery across interviewers and interview sessions. Questions that participants could not easily answer (e.g., hypotheticals) were culled through these iterations. Ultimately, our interview lasted approximately 45 minutes, and interviewees were compensated $10 to participate.

Recruitment
We recruited participants from CBDR¹, an online recruitment tool that pairs research participants from Pittsburgh with research projects of interest. Participants were required to own a smartphone running Android or iOS, be an active user of any social media service, and be at least 18 years old. We went through three rounds of recruitment to recruit a variety of occupations and ages across our sample. For example, in our first round of recruitment, we predominantly interviewed students in their mid-twenties. Thus, in subsequent recruitment rounds, we specifically recruited older non-students. We stopped recruiting additional participants once we believed we had sufficient diversity in occupation, age, and security proficiency to capture a large cross-section of experiences with security-related behavior change and communication. In our case, we appeared to reach this point after interviewing 19 participants—indeed, after the first 15, every additional participant echoed experiences very similar to those previously reported by others.

Our participants ranged in age from 20 to 54 years old (m=28.5, sd=10). Seven out of the 19 participants were female. Furthermore, as we tried to recruit participants from diverse backgrounds, 10 of our participants were non-students from many different professional backgrounds. All participants used an Android (n=12) or iOS (n=7) smartphone and were frequent Facebook users. Fifteen of the 19 participants reported using Facebook daily, while the remaining 4 reported that they checked Facebook at least a few times every week. shows an overview of participants.

---

¹ http://cbdr.cmu.edu/index.asp
We recorded and transcribed, with consent, each interview, and used a qualitative data analysis program called Dedoose \(^2\) to analyze the anonymized transcripts. We partitioned each transcript into a set of excerpts comprising all instances of an *action taken*, a *decision made*, or, more generally, a *behavior changed* related to security or privacy. A representative example of behavior changes is P18’s decision to rub-off the smudges on his Android device after a friend demonstrated that the smudges on his screen makes it easy for others to “crack” his Android 9-dot pattern:

> “What I’ve been doing, I believe, after that scare with the nine dot, pretty much every time I turn off my phone, I put it in the pocket, I just kind of rub, just rub the smears off so you can’t really see what direction I was going.” (P18)

---

\(^2\) http://www.dedoose.com

---

<table>
<thead>
<tr>
<th>Age</th>
<th>Gender</th>
<th>Race</th>
<th>Occupation</th>
<th>Phone OS</th>
<th>Phone Auth.</th>
<th>Social Media Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>28</td>
<td>Male</td>
<td>African American</td>
<td>Customer Service</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P2</td>
<td>22</td>
<td>Female</td>
<td>Asian</td>
<td>Unemployed</td>
<td>iOS</td>
<td>None</td>
</tr>
<tr>
<td>P3</td>
<td>22</td>
<td>Female</td>
<td>African American</td>
<td>Student</td>
<td>iOS</td>
<td>PIN</td>
</tr>
<tr>
<td>P4</td>
<td>22</td>
<td>Male</td>
<td>African American</td>
<td>Student</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P5</td>
<td>27</td>
<td>Female</td>
<td>Asian</td>
<td>Unemployed</td>
<td>iOS</td>
<td>None</td>
</tr>
<tr>
<td>P6</td>
<td>29</td>
<td>Male</td>
<td>White</td>
<td>Software Developer</td>
<td>iOS</td>
<td>None</td>
</tr>
<tr>
<td>P7</td>
<td>54</td>
<td>Female</td>
<td>White</td>
<td>Administrative Assistant</td>
<td>iOS</td>
<td>PIN</td>
</tr>
<tr>
<td>P8</td>
<td>31</td>
<td>Male</td>
<td>Indian</td>
<td>Unemployed</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P9</td>
<td>30</td>
<td>Male</td>
<td>White</td>
<td>Software Developer</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P10</td>
<td>37</td>
<td>Male</td>
<td>White</td>
<td>Graphic Designer</td>
<td>Android</td>
<td>9-dot</td>
</tr>
<tr>
<td>P11</td>
<td>54</td>
<td>Male</td>
<td>African American</td>
<td>Chef</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P12</td>
<td>20</td>
<td>Female</td>
<td>African American</td>
<td>Student</td>
<td>iOS</td>
<td>None</td>
</tr>
<tr>
<td>P13</td>
<td>24</td>
<td>Female</td>
<td>Indian</td>
<td>Graduate Student</td>
<td>Android</td>
<td>None</td>
</tr>
<tr>
<td>P14</td>
<td>25</td>
<td>Male</td>
<td>Indian</td>
<td>Graduate Student</td>
<td>Android</td>
<td>PIN</td>
</tr>
<tr>
<td>P15</td>
<td>21</td>
<td>Male</td>
<td>Indian</td>
<td>Graduate Student</td>
<td>Android</td>
<td>9-dot</td>
</tr>
<tr>
<td>P16</td>
<td>22</td>
<td>Male</td>
<td>Indian</td>
<td>Graduate Student</td>
<td>Android</td>
<td>9-dot</td>
</tr>
<tr>
<td>P17</td>
<td>34</td>
<td>Male</td>
<td>Asian</td>
<td>Unemployed</td>
<td>iOS</td>
<td>None</td>
</tr>
<tr>
<td>P18</td>
<td>20</td>
<td>Male</td>
<td>African American</td>
<td>Student</td>
<td>Android</td>
<td>9-dot</td>
</tr>
<tr>
<td>P19</td>
<td>20</td>
<td>Male</td>
<td>White</td>
<td>Student</td>
<td>Android</td>
<td>9-dot</td>
</tr>
</tbody>
</table>

*Table 1. Interview participant demographics, occupations, use of authentication on their mobile phones, as well as social media usage.*
The second set of excerpts was a collection of all specific instances of communication about security and privacy, which we will refer to as the communications. An example excerpt comes from P14. After he received spam mail from a friend's e-mail account, he mentioned:

“I told my friend that this is something weird that came from your account. This is not what you would be probably into.” (P14)

In total, from our 19 transcripts, we extracted \( n=114 \) behavior change excerpts. Excerpts were usually just answers to pointed questions, but to ensure robustness, two of the research group mutually agreed on all partition points for each excerpt.

We used these excerpts as our units of analysis—though, occasionally, we aggregated data across participants where it made sense (e.g., in determining how many participants actually changed their behavior as a result of a social process). We used an iterative, open coding process [54] to code the data, constructing codes where patterns naturally emerged and refining the codes iteratively until we reached consensus. Our goal was to understand the effect of social influence in driving behavior changes—which, in turn, means understanding the effect of social influence in modulating security sensitivity.

Concretely, two researchers independently and openly coded a random subset of 20\% of the excerpts. These openly generated codes were collaboratively synthesized into a set of high-level codes that three of the research team then used to code the remaining excerpts. Upon completion, the coding team discussed potential extensions to the coding scheme that arose from coding the new examples. If a change to the scheme was made, the coding team re-coded the full set of excerpts with the new scheme. We required two coding iterations to come to consensus.

From the 20\% overlap of excerpts, overall inter-coder agreement was 85\% (calculated as the number of overlapping excerpts where codes matched divided by the total number of overlapping excerpts). In cases of discrepancies, the coders discussed the discrepancies until agreement was reached, following standard practice. Inter-coder agreement for each applied code can be found in Error! Reference source not found., and all exceeded the 0.7 threshold commonly held to be acceptable in qualitative research [54].

<table>
<thead>
<tr>
<th>Code</th>
<th>Inter-Coder Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Change: Social or Non-Social</td>
<td>0.93</td>
</tr>
<tr>
<td>Behavior Change: Trigger Event</td>
<td>0.87</td>
</tr>
<tr>
<td>Behavior Change: Raised Awareness</td>
<td>0.87</td>
</tr>
<tr>
<td>Behavior Change: Raised Motivation</td>
<td>0.80</td>
</tr>
<tr>
<td>Behavior Change: Raised Knowledge</td>
<td>0.80</td>
</tr>
</tbody>
</table>

*Table 2. Inter-coder rating agreement on 20\% of the behavior change excerpts.*

Results

First, we wanted to know if social processes often drove security related behavior changes, so we coded each behavior change excerpt as being driven by a social or non-social process. Excerpts were coded as being driven by a social process when the reason for the behavior change was social, and, importantly, if the social process was clearly reported by the participant in the transcript. For example, when asked about why he first enabled a PIN on his iPhone, P6 stated:

“When I first had a smartphone I didn’t have a code, but then I started using one because everyone around me I guess had a code so I kind of felt a group pressure to also use a code.” (P6)

As the underlying reason for the behavior change was a social process (observing one's friends) and was stated as such, we coded that behavior change as social. An example of a non-social behavior change comes, again, from P6. When asked why he changed his Twitter password, P6 responded:
“Diversification of passwords. I had the same password for every service so I wanted to pick a stronger password for... the service, yeah.” (P6)

While P6 could have learned about the need for password diversification from friends, as he did not explicitly confirm this speculation, we coded the excerpt as non-social.

In all, out of the 114 behavior change excerpts, we coded a substantial 48 as being explicitly driven by some form of social influence. Furthermore, most participants (17 out of 19) reported at least one action taken, decision made, or behavior changed that was driven by social influence. Of note, however, is that the 48 examples of socially driven behavior change did not come uniformly from all of our participants. Notably P2 and P10 reported the largest number of socially driven changes at eight, each. It is important to keep this bias in mind in any quantitative interpretation of our findings.

In all, these results suggest that social influence already plays a strong role in driving security and privacy related behavior change—even without any explicit social interventions. Next, we wanted to understand when and how social influence is effective at driving these behavior changes.

Social Triggers in Driving Behavior Change

To explore when social influence drove behavior change, we open coded the triggers for behavior change excerpts coded as "social". We found five primary social triggers for behavior change: observing friends, social sensemaking, pranks and demonstrations, experiencing security breaches, and sharing access. Table 3 lists all triggers, their frequency and their description.

Next, to answer how social processes enacted behavior change, we also coded whether or not the socially driven behavior change examples in our dataset affected any part of the security sensitivity stack. Specifically, we asked the following:

<table>
<thead>
<tr>
<th>Trigger</th>
<th>N</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observed friends</td>
<td>14</td>
<td>Observing people around them engaging in a particular security behavior and emulated those people.</td>
<td>“So when I was an undergrad I’ve been using it since then. And this four digit everybody started using it and it was a hype. And we had it.” (P14)</td>
</tr>
<tr>
<td>Social sensemaking</td>
<td>9</td>
<td>Discussing concerns with friends/loved ones to determine the right behavior.</td>
<td>“I mean, like, one of my friends told me that you could alter the privacy settings so that, like, not everyone can look up your profile and not everyone can, like, try sending messages to you.” (P15)</td>
</tr>
<tr>
<td>Prank/Demonstration</td>
<td>8</td>
<td>Friends/loved ones hacked into his/her account, demonstrating they were insecure.</td>
<td>“Yeah, like my laptop was in my room. I walked out of my room and someone walked by and saw my Facebook and thought it would be funny to put something up.” (P19)</td>
</tr>
<tr>
<td>Security breach</td>
<td>6</td>
<td>Someone hacked into his/her account or information was shared too widely.</td>
<td>“I did change that within the past week. The girlfriend was reading all of my mail, which is also a privacy concern” (P10)</td>
</tr>
<tr>
<td>Sharing access</td>
<td>3</td>
<td>Sharing access to a device or account with another person leading to need for better security.</td>
<td>“There are sometimes when you have to tell your friends what is my PIN number because they are a very good friend of yours and they have to make a call and I can’t go every time and just unlock this for them.” (P14)</td>
</tr>
</tbody>
</table>

Table 3. Social triggers for behavior change derived from our iterative open coding process.
**Raised Awareness**: Did the social process raise the participant’s awareness of a new threat and/or security tool?

**Raised Motivation**: Did the social process raise the participant’s motivation to protect him or herself against a security threat?

**Raised Knowledge**: Did the social process raise the participant’s knowledge of how to use a security tool or method?

Importantly, we only answered “yes” to those questions if the social process mentioned in the excerpt was the reason for the heightened security sensitivity. For example, P16 mentioned that his Facebook account getting “hacked” resulted in him changing many of his passwords every 6 months at the advice of his friends, who he sought out for advice after the incident. In this example, the social process of P16 speaking with his friends raised his knowledge but not his awareness or motivation. It was the non-social process of experiencing a breach that raised his awareness and motivation.

For most (44 of 48) reported examples of socially driven behavior change, we found that the social process triggering the behavior change did, in fact, raise some form of security sensitivity. In fact, many examples raised all points of the security sensitivity stack. For example, P18 recalled advice he received on password composition after asking his friend to share a password:

“When I was working this summer, one of my co-workers told me about the whole algorithm thing. One, it just helps you I guess have different passwords. It helps you recall them easier based on I guess have different passwords. I guess you can cater, you can change your algorithm, depending on I guess want what you want to be in it. But ever since I started using it.” (P18)

In this example, the social process of P18 asking his friend about how to compose a password increased his awareness of a new method of password composition, his motivation to update his own method of password composition, and his knowledge of how to improve his method of password composition. In the text to follow, we describe each social trigger we found in our data for security related behavior change. Furthermore, as a descriptive aid, we plotted how frequently different social triggers raised the different components of security sensitivity in Figure 2.

![Figure 2. The number of times each social trigger for behavior change reported by our sample raised any of the three parts of the security sensitivity stack: awareness, motivation, or knowledge.](image-url)
Observing friends (14/48 examples)

Most frequently, our participants reported changing their behavior after observing the actions of friends or others around them. In other words, participants changed their behavior after finding social proof—or, cues on how to act based on the actions of others [15]. For example, one participant in our sample adopted the 9-dot authentication method on his Android phone because his friends also used it. Additionally, as previously illustrated, P6 adopted a PIN because he felt “group pressure” to do so after observing everyone around him use authentication. This finding appears to be well supported by the background literature on technology adoption, which lists observability as a key criteria for an innovation to spread rapidly through social channels [62].

In certain cases, other forms of social influence apart from social proof appeared to be at play—specifically the social influence concepts of liking, or our tendency to follow the advice of those we like and those like us, and authority, or our tendency to follow the advice of those we consider to be authority figures [15]. For example, one participant indicated that she adopted a PIN code for her iPhone wholly because her mother, who she considered technically savvy, also had a PIN:

“His mother has-- she had an iPhone before I did, so she always had the block on hers, so I just kind of the... I think just because I saw her doing it, so it kind of just felt like it was something I had to do too.” (P3)

Observation influenced behavior change for mobile authentication more often than the other specific topics we asked about in our interviews, probably because it is relatively easy to observe others authenticating onto their phones compared to observing others update their social media privacy settings or uninstall an app.

Looking at Figure 1, participants who observed others use security tools often were themselves motivated to start using those tools (11/14 examples). Furthermore, participants often became more aware of security tools after observing others’ using those tools (9/14), but only occasionally gained knowledge of how to use the observed tools and methods by observing others (5/14).

Social Sensemaking (9/48 examples)

The second most frequent social trigger reported by our sample was social sensemaking—or, the process of making sense of a security system, tool, or threat by discussing concerns with others. We termed these triggers social sensemaking because they were similar in form and purpose to discussions, observed by Weick et al., among members of an organization who attempted to resolve uncertainty about recent novel events in their environment [80].

Participants often reported having discussions to resolve ambiguity in news and hearsay about security. The aim of these discussions was usually to find the correct or appropriate way to act to achieve the desired level of privacy or security within a system or with a security tool. In many cases, these discussions were prompted by a sudden infusion of uncertainty—for example, news articles about a novel security threat or gossip about anomalous security breaches others had experienced. Participants discussed these novel threats with others to share information about the threat, assess its veracity, and determine whether and how to change their behavior in response. For example, one participant in our dataset reported becoming more restrictive with posting to Facebook in response to a sudden, alarming, but unclear threat of all timeline posts becoming public:

“So yeah. I recently, like, a day or two, day before yesterday, I went through an ordeal. I don’t know if it’s fake or it’s real, but somebody mentioned that all his private messages, they became public. Like, his messages with a friend. And it was like he had never thought of putting it on wall. And it suddenly opened his Facebook and everything was on his... I don’t know if it’s a real thing. And somebody mentioned in a comment that it happened with him as well, few days back.” (P16)
P16’s example is another illustration of social proof based social influence affecting an individual’s security behavior: facing an ambiguous threat, P16 observed his friends for cues on how to act.

Social sensemaking also occurred when a participant wanted to understand a particular function within a system—for example, Facebook privacy settings. This need for specific information resulted in discussion and information sharing that exposed novel functionality or methods for protecting oneself against threats—often increasing participants’ knowledge about the system (5/9 examples) and eventually leading to behavior change as a result. For example, one participant updated his privacy settings after a discussion that revealed novel system functionality:

“I mean, like, one of my friends told me that you could alter the privacy settings so that, like, not everyone can look up your profile and not everyone can, like, try sending messages to you. As in you can go to the privacy settings tab. And then, you could actually change it. Because I didn’t know that you could do it, before. I mean, I just thought that it was default that everyone could look at your profile.” (P15)

Social sensemaking also made participants more aware of available security tools (9/9), and the discussions would frequently motivate participants to act on their newly acquired knowledge (6/9).

Prank/Demonstration (8/48 examples)

The third most prevalent social trigger for the behavior changes reported by our participants was pranks and demonstrations—i.e., friends or loved ones cracking participant’s accounts and devices as a prank, or to demonstrate that they were being insecure. Often, these pranks were explicit demonstrations to prove to the victim that their current security strategy or behavior was insecure. For example, one participant in our sample described a co-worker breaking into his phone to show the vulnerabilities of 9-dot authentication:

“One of my, when I was interning, engineering company, one of my friends and a fellow intern came to my desk, just unlocked my phone. I was surprised. I was like, “Hey, how’d you do it?” He put it against the sunlight and he saw I guess the smudges my finger left. He just followed the direction. Yeah, he had access to my phone.” (P18)

Other prank examples reported were simply driven by opportunity—for example, a friend gaining unauthorized access to the participant’s account because they left their Facebook account open on an unprotected device. Indeed, several of our participants were motivated to change their security behavior after their friends accessed their social media accounts and posted embarrassing information on their behalf. For example, one participant experienced this type of prank after leaving his laptop open and unprotected in his dorm room:

“Besides just my friends getting into my phone or on my Facebook and that’s more from just me leaving my Facebook open or something if I walk out of the room and they just put up a funny status or something like or even just look through my messages or something like that. But nothing too threatening, more like practical joking side of it. But once that happens, I usually change my password immediately as would all of my other friends would too.” (P19)

Pranks appeared to be quite effective at raising participants’ security sensitivity. In all cases (8/8 examples), participants were made aware of a security threat and, in most cases, participants were instantly motivated (6/8) to update their behaviors to prevent a reoccurrence of the prank. Pranks aimed at demonstrating insecure behavior were also effective at raising participants’ knowledge (5/8), as they were often followed up with direct or indirect lessons to prevent the breach from reoccurring—for example, the screen smudge “hack” reported by P18 taught him to wipe out the smudges from his phone screen periodically.
Experienced a security breach (6/48 examples)

Another prominent social trigger was experiencing a security breach—when participants or someone they knew had an account or device accessed by a stranger, or otherwise had information shared with unintended parties. In these examples, the victims of a security breach solicited advice from friends and loved ones, simultaneously spreading awareness (3/6 examples) of a new security threat, and motivating (4/6) behavior changes by grounding it in a real example of harm.

One participant initiated a new practice of updating his password on a monthly basis following his Facebook account getting breached, because his friend recommended that course of action:

“Because once I got my account hacked. And I was [doing my] bachelor’s in a city, so yeah. After that I was more precautious regarding the same. And I’ll keep changing my password, so on a monthly basis [because] My friends, actually they recommended me to do so. Like there’s one of my friends used to do it. He said it’s better to be safe than sorry, so…” (P16)

Sharing access (3/48 examples)

Another general social trigger was behavior change triggered by sharing a device or account with a friend or loved one—for example, modifying a password after allowing a friend to check their phone. These changes were a reflexive response to the fact that what participants desired to generally be private was now more widely available because of a transient need to share access. For example, one participant let her son use her phone and updated the passcode afterwards:

“One of my boys wanted to use my phone for something so I gave them my passcode. And not that I have anything that I don’t care for them to see or anything, but after they did that then I changed it again because I just didn’t want anybody to just-- I don’t care if it's them or not. I don’t want them to just be able to pick up my phone and do what they want with it.” (P7)

While these triggers rarely raised awareness (0/3 examples) or knowledge (0/3), they seemed to be motivate participants to make a change (3/3).

Other triggers (8/48 examples)

Eight other instances of behavior change reported by our sample were triggered by other experiences, usually conversations or recommendations—for example, an authority figure recommending the use of authentication, as mentioned by P8 when asked why he first enabled mobile authentication:

“I think my boss at the time had it and he recommended it, because he leaves his phone at his desk.” (P8)

Likewise, P10 mentioned adopting anti-virus software after receiving a recommendation from a friend who he considered a security expert, and P13 mentioned that she stopped using Google Chrome for financial transactions because two of her security expert friends informed her that the version of Chrome she used insecurely stored information. These recommendations often raised participants’ awareness of, motivation to use and knowledge of how to use a new security tool.

Importantly, however, recommendations from authority figures didn’t always result in behavior change. P13, for example, mentions that she ignored her boss’s advice to have different passwords for different accounts because it would be hard to remember all those passwords. Nevertheless, the advice did raise her awareness of proper security practices.

P7 reported re-activating the PIN for her iPhone because a family member asked her why she deactivated it in the first place, urging her to reconsider. The conversation didn’t raise her awareness or knowledge, but re-upped her motivation to use a security tool with a bit of social proof.
Interestingly, another participant mentioned installing anti-virus software on her laptop simply because she felt guilty, after conversing with others who attended her university's cybersecurity awareness fair, for not using software that her school provided:

“I also felt guilty that I have all this free stuff I could install to protect my computer, and all this stuff I could do that’s smart and I wasn’t taking it.” (P12)

The guilt inspired behavior change reported by P12 is emblematic of the reciprocity principle of social influence, which suggests that people are more likely to follow the suggestions of those who did them a favor—even an unsolicited one [15].

Importantly, one participant reported how a social process urged her against behavior change (but was still responsible for a decision she made about security). P17 mentioned that she did not follow her security-expert husband’s advice to delete unused and obscure online accounts because she noticed that her friends, who did not follow the advice, never experienced a security breach:

“I don’t think it will be dangerous. Maybe I didn’t see this kind of news or my friend didn’t get some trouble when they didn’t set password. Like, my friends sometimes they usually have a lot of different accounts, the same as me. But they didn’t get any trouble. So I think maybe it will not be dangerous.” (P17)

In this way, P17’s friends’ lack of a security breach offered her social proof that it’s okay to ignore her husband’s security advice.

Discussion

In summary, we interviewed 19 participants about specific, recent security and privacy related behaviors they had taken. From these interviews, we extract and analyzed 114 examples of behaviors changed, actions taken, or decisions made related to security and privacy. Our results introduce a typology of social interaction around cybersecurity behavior. First, we confirmed that social processes are an important influence on cybersecurity behavior change—indeed, a large number of behavior changes (48 / 114) reported by our sample were driven at least partially through social processes. Specifically, we identified five common social triggers for security related behavior change—observing and learning from friends, social sensemaking (discussing ambiguous security threats with friends to determine the relevance of the threat and a clear course of action), pranks and demonstrations, experiencing a security breach and sharing access to a device with others. Furthermore, all social triggers for behavior change reported by our sample appeared to heighten security sensitivity in some way—either by increasing participants’ awareness of a new threat or security tool, motivating participants to protect themselves, or increasing participants’ knowledge of how to protect themselves. These findings lend some support to the notion that social influence, especially in the form of social proof, authority, liking, and reciprocity, can be potent in raising security sensitivity—a result that bolsters the implications of prior work [32,58,72].

Opportunities

Our results also highlight some opportunities to leverage social processes to drive security-related behavior change:

Creating teachable moments out of negative experiences. Our results emphasize the influential nature of a specific negative experience in raising the security sensitivity and, in turn, changing the cybersecurity behavior of victims and those around them. Interestingly, friends and loved ones appeared to at least indirectly take advantage of this fact, often breaking into others’ accounts to prove to that person that s/he was not fully protected. This notion of pranking by friends and family can also be considered as an effective way to create a teachable moment, something that past work on PhishGuru has found to be effective in teaching people about phishing attacks [50]. In other cases, pranks were not necessarily meant to directly educate victims, but were used as a form of hazing. Either way, the breach elicited a similar reaction—both the victims of these pranks and the people around them who they shared the experience with became more aware of and motivated to address their own security vulnerabilities.
**Creating more observable security tools.** The observability of security features and methods also proved to be important in driving behavior changes through social processes. Indeed, observing friends was the most frequent social trigger for behavior change. Nevertheless, most security features and methods are inherently unobservable and were rarely surfaced in our interviews—password composition methods, for example. When P18 learned of a new way to compose passwords from his friend, he immediately started utilizing this new composition policy. However, only two of our participants mentioned talking about password composition policies, suggesting that there is room for improvement in leveraging social processes to raise security sensitivity.

However, simply increasing the observability of all security features may not be the best solution. First, security settings have historically been private—and for good reason. Indeed, past work by Gaw et al. [32] found that people who encrypted e-mail were often considered paranoid unless they were in a role where they handled sensitive company data, suggesting an illusory correlation [12] between security feature usage and paranoia. Indeed, as early adopters of security features are likely those who are especially concerned about their security—and, thus, are the most likely to be considered as paranoid by lay users—it is possible that making security decisions and behaviors perfectly observable might work against security sensitivity. First, potential adopters may look at the present adopter list and find tenuous *social proof* that only “paranoid” people use a security feature. Second, we also saw evidence that social processes can work against a user following advice if it seems like none of their friends are affected by a threat—for example, it is possible that when a useful security feature has few present adopters, potential adopters might see the absence of adoption as social proof against using the feature.

To best leverage observability, therefore, it seems that we should create security tools that are more visual and amenable to conversation, such that non-experts can passively raise their *awareness* and *motivation* by observing their friends, and then raise their *knowledge* by asking about security.

**Creating security tools that facilitate sharing access with others.** Finally, several participants mentioned sharing access to accounts and devices as a prompt to change their authentication secrets. While the result of updating one’s password after sharing one’s device with others is desirable, this practice suggests a broader weakness of many present security tools—the assumption that people would never want to share their accounts and devices with others temporarily or regularly. As pointed out by prior work on home data sharing [53] and password usage in daily life [37], as well as illustrated by our own interviews, this assumption of non-sharing is flawed. Thus, in addition to making security tools more *observable* it seems that we should also make these tools more *socially inclusive* to better support these sharing practices. In turn, by making security more socially inclusive, we may also combat the perception of “paranoia” associated with security tool usage [18,32].

**Future Work**

The results from this interview study shows the influential nature of social proof on affecting security related behavior change. However, our sample, although representative in many respects, is primarily from the US and young. Furthermore, as we solicited participants from only one online recruitment source, and in so doing we could have introduced a systematic bias into our results—our participants were the type that generally volunteers for research projects. This means our results may not necessarily widely generalize, as is the case with most qualitative research.

Thus, one fruitful avenue to bolster these results is to examine whether the patterns and relationships identified in our data persist in a larger, representative sample of technology users. In Chapter 7, I discuss in more detail some proposed work to generalize the findings from this interview study to a broader, more representative sample of internet technology users.

Now that we know that social influence affects security behaviors, it would also be pertinent to apply social network analysis theory to better understand whether and how security behaviors diffuse through social networks. In Chapter 5, I discuss one such project I undertook with Facebook.

Finally, these findings inform the design of systems and interventions that *leverage* social influence processes to raise security sensitivity. For example, a key finding from our interviews was that the
observability of security tool greatly facilitates its spread through social channels. Nevertheless, most security tools are not observable, leaving little room for social spread and learning. Future work could introduce simple manipulations to increase the observability of security tools and measure their effect on behavior change, for example. In Chapter 6, I discuss one such project I undertook with Facebook. In Chapter 7, I discuss a few "social" security tools I plan to design, implement, and evaluate with the insights from this interview and other work in mind.
Chapter 4: Understanding How Security Information Is Communicated

Summary
I showed that social influence appears to be a key driver of people’s security and privacy behaviors. A number of these social catalysts for behavior change, however, required active communication between multiple people about security tools and/or threats. Accordingly, I next investigated whether and how people communicate about security. In this chapter, I report on results from the second half of the same interview study in which we investigated communications about security and privacy. From these data, we construct a typology of security communications—specifically, we categorize a number of conversations that differ primarily in catalyst and goal. We learned that communications about security are scarce, with many participants, including several security experts, reporting that they did not talk much about security at the risk of being boring or sounding preachy. The few conversations about security that did happen, though, were mostly to warn others of security threats or to teach others about how to protect themselves from a threat. Thus, it seems that people feel accountable for the security and privacy of their loved ones, and it is this feeling of accountability that seems to prompt many conversations about security and privacy.

Motivation
In the previous chapter, I showed that social influence is a powerful tool to affect security and privacy related behavior change. But, it remains unclear: How prevalent is socially driven security-related behavior change? Socially driven change is the result of an interaction between two or more individuals—but those interactions are rare in the domain of security and privacy. Indeed, when asked why he didn’t share his concerns about the U.S. government’s pervasive surveillance (NSA PRISM) program, one our participants stated: “That’s one thing I will never talk about.” Similarly, when asked about whether he has warned friends about a malicious smartphone application he uninstalled, another stated: “Especially online. In person, it depends on the context. It does become a boring subject.” The realization that conversations about security remain rare—and, thus, so too does the potential for socially driven behavior change related to security—begged the question: Under what circumstances do conversations about cybersecurity occur? In this chapter, I explore the second research question we asked in our interview study:

*RQ2: Under what circumstances do people communicate about security and privacy?*

Methodology
In the same semi-structured interview in which we asked participants about specific security-related behaviors they undertook and the reasons they made those changes, we also asked participants if they could recall specific conversations they had about security and privacy. For example, if a participant mentioned a that a conversation she had was the reason she started using a PIN, we further probed that participant to provide more details about the conversation—e.g., who told her to use a PIN? How did that conversation start? In addition, to capture security-related conversations that did not fit into our pre-constructed themes of mobile authentication, app installation, and social media privacy settings, we also asked participants more open-ended questions about conversations related to security and privacy. Did they ever share information about security or privacy? If so, what did they share, with whom, and why? These more general questions were asked at the end of the interview.

By focusing on specific conversations about security and privacy (e.g., “I told my mother to update her privacy settings”), rather than general conversations (e.g., “People usually tell me to update my password”), we were often able to uncover the specific context of a conversation (e.g., a catalyst and goal for the conversation).

To reiterate, we recruited 19 participants to interview from the greater Pittsburgh area with CBDR and iteratively refined our interview protocol with 5 pilot participants before conducting the actual interview. Our participants ranged in age from 20 to 54 years old (*m*=28.5, *sd*=10), and seven were female. For more specific details about participant recruitment, demographics, and compensation,
please refer to the Methodology section of Chapter 3: A Typology of How Social Influence Affects Security Behaviors, as these insights are obtained from the same interview study as that of Chapter 3.

Data Coding and Analysis
To reiterate the previous chapter, we recorded and transcribed, with consent, each interview, and used a qualitative data analysis program called Dedoose to analyze the anonymized transcripts. However, for this analysis, we identified excerpts pertaining to specific instances of communication about security and privacy. An example excerpt comes from P14—after he received spam mail from a friend’s e-mail account, he mentioned:

“I told my friend that this is something weird that came from your account. This is not what you would be probably into.” (P14)

We classified this excerpt as a communication excerpt because the participant explicitly mentioned conversing with a friend about something that could have implications for privacy or security. In total, from our 19 transcripts, we extracted n=118 communication excerpts. Excerpts were usually just answers to pointed questions, but to ensure robustness, two of the research group mutually agreed on all partition points for each excerpt.

We used these excerpts as our units of analysis—though, occasionally, we aggregated data across participants where it made sense (e.g., in determining how many participants reported having a certain type of conversation). We used an iterative, open coding process [54] to code the data, constructing codes where patterns naturally emerged and refining the codes iteratively until we reached consensus. Ultimately, our goal during the coding process was to better understand the triggers and reasons underlying communications about security and privacy.

Concretely, two researchers independently and openly coded a random subset of 20% of the communications excerpts. These openly generated codes were collaboratively synthesized into a set of high-level codes that three of the research team then used to code the remaining excerpts. Upon completion, the coding team discussed potential extensions to the coding scheme that arose from coding the new examples. If a change to the scheme was made, the coding team re-coded the full set of excerpts with the new scheme. We required two coding iterations to come to consensus.

From the 20% overlap of excerpts overall inter-coder agreement was 79% (calculated as the number of overlapping excerpts where codes matched divided by the total number of overlapping excerpts). In cases of discrepancies, the coders discussed the discrepancies until agreement was reached, following standard practice. Inter-coder agreement for each applied code can be found in Table 4. Inter-coder agreement of codes on a 20% random sample of communication excerpts, and both exceeded the 0.7 threshold commonly held to be acceptable in qualitative research [54].

<table>
<thead>
<tr>
<th>Code</th>
<th>Inter-Coder Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication: Catalyst</td>
<td>0.71</td>
</tr>
<tr>
<td>Communication: Reason</td>
<td>0.86</td>
</tr>
</tbody>
</table>

Table 4. Inter-coder agreement of codes on a 20% random sample of communication excerpts.

Results
To understand the conditions under which conversations about security and privacy occur, we open coded excerpts about communication to surface triggering events for the interaction (catalysts) and the goal of the conversation (conversation goal).

Catalysts for Security Related Communication
We observed six primary catalysts for security related conversations, as summarized in Table 5. Below, we summarize each of these conversation catalysts in turn.
Negative experiences (33/118)

Negative experiences were by far the most common catalyst for security conversations reported by our participants. These negative experiences could take many form, but often involved at least one of the conversation partners directly experiencing a security or privacy breach themselves. Indeed, many participants reported having conversations with friends and loved ones after experiencing a security breach. For example, one participant sought advice from friends after she received a friend request, on Facebook, from a fake profile using her own picture:

“Yes, my data got stolen. My photo got stolen on Facebook. I spoke to a couple of my friends. The only thing I could do was report abuse.” (P6)

Observing insecure or non-private behaviors (15/118)

Often, participants reported starting a conversation in response to observing what they believed was non-secure behavior, such as a friend or family member oversharing on social media:

“One of the reasons we talked about it is because I saw so many people post things on Facebook. A lot of times it’s unnecessary things, you know, like just what they did today, “Oh, I had an amazing day,” or, “I had a great dinner,” and I was just...” (P20)
In this case, a participant, P5, observed her connections on Facebook engaging in what she considered “oversharing.” This observed behavior prompted her to initiate a conversation with her husband to understand why people engaged in this non-private behavior.

**Sense of accountability (15/118)**

A sense of social accountability also frequently prompted conversations about security. Curiously, this sense of accountability was not limited to any one social role. Rather, we observed that many different entities who held many different social roles all appeared to feel a sense of accountability for others’ security and privacy. For example, parents lectured their children about security and privacy best practices:

> “When I was younger, I remember my parents always telling me, like I’m sure everyone’s parents tell them, to be very careful about who they give their Social Security number to. So, that’s always like in my head, like if someone asks me for that, I’m just like, uh, no.” (P14)

Likewise, managers informed their employees about how to manage company data because it was a part of their responsibilities. One participant described this type of interaction with his boss:

> “When I was at work, I was given some sensitive documents, and I was told I couldn’t send them over e-mail. I had to use a flash drive to move them over, encrypt them, then send them in e-mail.” (P18)

Curiously, even large organizations, such as entire universities, appeared to feel a sense of accountability for its students. For example, one student talked about her university providing security solutions and advice in an annual security fair that she attended:

> “They give us LoJack and all these different things you can get at the computer center. So we did talk about that. Like, locking up our computers and changing our passwords and stuff and being careful with the Wi-Fi.” (P12)

**Reading news (15/118)**

Unsurprisingly, news articles or other press about security and privacy breaches also frequently triggered conversations. For example, one participant read and subsequently shared an article on social media about how over sharing could lead to identity theft and, more darkly, black market organ trading:

> “I know there’s like news talking about girls they are just so crazy about telling people on the social media where they are every minute, what they are doing every minute. So some criminals they actually use the information and just like kind of how do you say they found the girl according to her shared information online every minute. [...] So I shared this article just to let my friends see just don’t do it very often because I saw some of my friends on Facebook she did this really often like telling everybody what she was doing and what she had and where she was and like that.” (P2)

This link between online and offline crime can potentially make the consequences of poor computer security and online privacy practices more concrete—if extreme.

**Configuring settings (14/118)**

Another frequent conversation catalyst about security and privacy was the need to configure security and privacy settings on a new device, application or account. For example, one participant reported asking a friend for advice when a Facebook application asks for access to protected information:
“So there are many applications and Facebook would say that if you want to access them, there’s a pop-up saying, “Allow,” like, it will access all your information and stuff. So I asked him if I should go for it or not, and he tells me if it’s worth going. Like, “Is it reliable or not?” (P16)

In general, participants frequently started conversations when setting or re-setting Facebook privacy settings (P13, P14, P16). In addition, many participants reported parents or older friends initiating conversations when they were setting up new computers or social media profiles for the first time (P4, P10, P15).

Observing novel behavior (11/118)

Finally, people appeared to initiate conversations about security or privacy after observing novel behaviors—for example, a new, visually appealing authentication technique. Indeed, one participant was stopped in a coffee shop and asked about the 9-dot authentication on his Android phone:

“We were just sitting in a coffee shop and I wanted to show somebody something and [they said], “My phone does not have that,” and I was like, “I believe it probably does.” (P10)

In general, most security and privacy behaviors are designed to be invisible which prevents lay people from observing what experts do to protect their security. As a result, there are few vectors for lay people to converse with experts about their security habits and behaviors.

Conversation Goals

Conversations typically have agendas or goals. Thus, we next coded our 118 communication exceptions for conversation goals to better understand what people wanted to achieve from the conversation. Was it to warn others about potential threats, edify others about security tools or seek advice on how to configure security settings? During our open coding process, we identified seven distinct types of conversation goals, summarized in Table 6 below.

<table>
<thead>
<tr>
<th>Goal</th>
<th>N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify or warn</td>
<td>32</td>
<td>Notify or warn others of a potential security or privacy threat.</td>
</tr>
<tr>
<td>Prank or Demonstrate</td>
<td>5</td>
<td>Demonstrate insecure behavior by hacking into a friend’s account or device.</td>
</tr>
<tr>
<td>Share solutions</td>
<td>14</td>
<td>Share solutions, tools, and best practices (e.g., sharing how one composes his/her own password).</td>
</tr>
<tr>
<td>Vent</td>
<td>8</td>
<td>Seek social support / commiserate the experience.</td>
</tr>
<tr>
<td>Offer advice</td>
<td>19</td>
<td>Offer specific advice to others (e.g., update privacy settings, change password).</td>
</tr>
<tr>
<td>Seek advice</td>
<td>18</td>
<td>Ask for specific advice about security / privacy.</td>
</tr>
<tr>
<td>Storytelling</td>
<td>12</td>
<td>Topic was interesting/shocking/otherwise made for a good story.</td>
</tr>
</tbody>
</table>

| Table 6. Conversation goals derived from our iterative open coding process. |

Identifying a typology of communications: The Interaction of catalysts and goals

Thus far, we have identified a set of conversation catalysts and goals. The interaction between these catalysts and goals affords us a typology of security and privacy communications. To construct this typology, we started by cross-tabulating catalysts and conversation goals. The results are shown below in Table 7:
For brevity, we focus here on the six most prevalent and interesting combinations, summarized in Table 8. These six combinations grouped into two broad categories of conversations, distinct in terms of their catalyst, focus and goal—warnings and teachings.

<table>
<thead>
<tr>
<th>Name</th>
<th>N</th>
<th>Catalyst</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warnings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cautionary tales</td>
<td>10</td>
<td>Negative experience</td>
<td>Notify / warn</td>
</tr>
<tr>
<td>Targeted warnings</td>
<td>7</td>
<td>Insecure behavior</td>
<td>Notify / warn</td>
</tr>
<tr>
<td>Spreading the news</td>
<td>8</td>
<td>News article</td>
<td>Notify / warn</td>
</tr>
<tr>
<td>Teachings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lectures</td>
<td>8</td>
<td>Sense of accountability</td>
<td>Offer advice</td>
</tr>
<tr>
<td>Configuration help</td>
<td>8</td>
<td>Configuration</td>
<td>Seek advice</td>
</tr>
<tr>
<td>Social learning</td>
<td>5</td>
<td>Novel behavior</td>
<td>Share solution</td>
</tr>
</tbody>
</table>

Table 8. The most frequent conversations about security and privacy, based on the catalyst and content.

Using this typology of security and privacy related conversations, we have enough context to answer our second research question: *under what circumstances do conversations about cybersecurity occur?*
Warnings

Warnings were meant to raise awareness of a specific, immediate threat that had come to the attention of the conversation initiator. These warnings took three forms, varying in their catalysts, but resulted in a notification about a novel threat: cautionary tales, targeted warnings, and spreading the news.

Cautionary tales (10/118 examples)

The most common catalyst-goal combination reported by our participants was what we called cautionary tales—a conversation triggered by a negative experience on the part of the conversation initiator or someone close to the initiator, with the goal of warning friends and loved ones about the threat. These conversations often involved sharing information about a recent security breach so that others could judge if their accounts or information were in any danger. In several cases the conversation was a response to an out-of-character behavior on the part of a friend or family member. For example, when asked about why he decided to reach out to his friend about a potential security breach, P11 mentioned:

“Because, when I opened the e-mail, it said that they were, I think, they were in England and they didn’t have enough money to come back to the States so can you send us some money, wire us some money, over, yeah. And if I’m not mistaken, I was probably the first to contact them that they were hacked. I’m like, ‘This isn’t right. Something strange’” (P11)

In other words, a specific negative experience (i.e., receiving odd requests for money from a friend via e-mail), triggered P11 to reach out to this friend to caution that friend about his email account was likely breached. In other cases, participants relayed cautionary tales to others who were not, themselves, part of the incident. For example, after his girlfriend illicitly accessed his e-mail account, P10 spoke to his friends to let them know that she may have read their conversations:

“It was just like, ‘Hey, [my girlfriend’s] been reading through our mail, like our conversations and stuff,’ [...] She probably read some of our conversations, not like she’s going to get into your accounts.” (P10)

Targeted warnings (7/118 examples)

Another common conversation we observed was one in which a conversation initiator issued someone a warning about potential security or privacy threats after observing that someone engaged in what they believed was risky behavior—what we call targeted warnings. For example, one participant described a friend warning her about the danger of not having a passcode:

“I was having a conversation with somebody and they were saying, ‘Don’t you have your passcode on there anymore?’ And I said, ‘No, it’s a pain in the butt.’ And they said, ‘Well, it’d probably be a good idea if you- especially if you like leave it lay around on your desk or something like that. Or even if you’re out in the evening and you have it on your purse, which most people now when they’re out they have this thing right on the table where they are that somebody doesn’t come by and grab it or whatever. That way they can do whatever they want with it.’” (P7)

In this example, P7 conveys a story about how someone told her, after noticing that she no longer used a PIN on her iPhone, that her behavior could result in a number of security breaches.

Spreading the news (8/118 examples)

News articles about security breaches often resulted in conversations we refer to as spreading the news—conversations where the initiator attempted to warn friends and loved ones about a security threat outlined in a news article. These conversations sometimes included advice on how to change behavior to protect oneself from the new threat, but were usually just meant to raise awareness that
a threat existed. For example, one participant talked about his contacts on Twitter discussing stories about Facebook privacy concerns without giving advice:

“Oh. Yes. People have said constantly on Twitter about how Facebook, it’s not private anymore. Which is ironic, because neither is Twitter. So I’ve seen that, but no one has showed a article about being secure like with NSA and stuff.” (P4)

As with other warnings, these conversations were often motivated by a desire to protect. For example, one participant described sharing a link to an article, through social media, about a credit card breach in order to warn her loved ones to be careful. Indeed, when asked why she shared one such news article, P2 said:

“To ask my beloved to actually pay attention to these things, to make sure they’re okay. Their bank accounts are okay, if they actually do some shopping that day.” (P2)

Conversations prompted by news articles also sometimes led to sharing best practices or details of privacy and security behaviors.

“We were just generally sitting around and somebody was like, ‘Oh, this is an article about Facebook privacy stuff again. Let’s look at it’ ‘Do you use this,’ or ‘I use that,’ and ‘Oh.’ So really just comparing notes is the best way I can put it. Like we weren’t overly scrutinizing each other’s things. But like ‘I found this to be effective.’” (P10)

In all of these examples, a news article about a potential security breach triggered a conversation between participants and their contacts. In all cases, the purpose of the conversation was primarily to make just others aware of the issue—thus, these conversations were less directed and driven than cautionary tales or targeted warnings.

Teachings

Apart from warnings, the other broad category of conversations we uncovered was teachings. Whereas warnings were meant to inform participants about threats, teachings were meant to share security best practices or demonstrate to others how to protect themselves from security and privacy threats. In contrast to warnings, teachings focused on sharing specific information about behaviors to enact rather than just information. Another difference was that whereas warning conversations were almost always reactive (i.e., triggered by an immediate threat or news about that threat), teachings were both reactive (i.e., meant to solve an immediate problem) and proactive (i.e., meant to avoid future threats). Within teachings, we identified three common conversations: lecturing, configuration help, and social learning.

Lectures (8/118 examples)

Lectures occurred when conversation initiators offered security and privacy advice to those for whom they felt accountable—for example, parents and children, or managers and employees. For example, parents often advised young and college-bound children not to over share on Facebook. Older children, however, tended to be the ones lecturing their parents about security best practices. Indeed, when asked if he shared security advice with others, one adult participant said:

“I mean, I’ve spoken to my mom and dad about it. Like, I’ve told them, like, because I’ve told them to also use the same features that I do. Like having screen locks for phones and being more careful about passwords. And not logging into public computers and just leaving them without signing out.” (P8)

P8’s advice to his parents is a good example of proactive advice—advice about security given even in the absence of an immediate threat. This example is also illustrative of another theme that often
arose with teachings: a sense of accountability. P8 felt accountable for the security of his parents, which in turn prompted these conversations.

Another type of lecture was managers lecturing employees about best practices to protect company data. For example, when asked why she updated her e-mail password, one participant said:

"Actually, this advice was given to me by my manager, with whom I used to work. So he's the one who told me about this. He was like you should change your password because it contains confidential information." (P13)

Similarly, another participant described his boss asking him to encrypt confidential files and transmit them physically on a USB flash drive rather than through email (P18).

**Configuration help (8/118 examples)**

Often, teaching conversations were triggered by a conversation initiator soliciting advice on how to configure security and privacy settings for a new device or account—what we called configuration help conversations. For example, one participant described helping his mother set up her new laptop with the appropriate security settings to keep her information safe (P19). Another participant described encouraging his mother to enable 9-dot authentication on her new Android phone to make sure no one else could access it. When asked why, P15 responded:

"I mean, just the same reason that people shouldn't just look into her phone. Because, like, if it does not have a button, anyone can just, like, unlock and look at her messages and stuff." (P15)

While not directly the trigger for this conversation, this excerpt is again illustrative of the sense of accountability that people feel for their loved ones' security and privacy.

Broadly, configuration help conversations were about setting up Facebook privacy settings (P1, P3, P4, P8, P19). For example, P19 describes how her mom asked for her help with enacting specific privacy related behaviors on Facebook.

"my mom...doesn't really know how to do Facebook that much so she'll ask me questions about it, in general, like how to post or, I guess, how to remove herself from something or certain things like that. So, I guess, I have given her advice in a way, just given her a few basic steps of set this as this just so you don't have-- you're not completely open and public." (P19)

**Social learning (5/118 examples)**

Finally, while they were not very frequent among our participants, one of the more effective conversations at enacting behavior changes we uncovered were social learning conversations. In these conversations, conversation initiators observed novel security or privacy behaviors or tools and asked those who enacted those behaviors or used those tools questions about those behaviors or tools. For example, some participants asked others about novel ways to construct passwords (P9, P10, P18) or a new type of authentication (P8). For example, P18 asked a friend about sharing his Amazon account password, prompting the friend to share his password composition method:

"When I was working this summer, one of my co-workers told me about the whole algorithm thing. One, it just helps you I guess have different passwords. It helps you recall them easier based on I guess the type of profile. I guess you can cater, you can change your algorithm, depending on I guess what you want to be in it. But ever since I started using it." (P18)

Typically, our more security-savvy participants reported that they did not often share their own security behaviors with their less security-savvy friends and loved ones because they feared the topic was too boring. However, social learning conversations presented opportunities for experts or early adopters to share their solutions for solving common security problems.
Discussion
In analyzing the 118 conversations about security and privacy reported by our participants, we uncovered six common conversation catalysts (Table 5. Conversation catalysts derived from our iterative open coding process.) and seven common conversation goals (Table 6). From these catalysts and goals, we constructed an initial typology for conversations about security and privacy in which we identified six of the more common and interesting catalyst-goal contexts (Table 8). In turn, this typology enabled us to answer our research question: *under what circumstances do people generally talk about privacy and security?*

Broadly, the answer to this question appears to be: to warn or to teach others. Most commonly, our participants reported conversations about privacy and security to be educational experiences—either in sharing or receiving information about a novel security threat, or in sharing or receiving advice about how to solve a specific security problem or security best practices. *Observability*, again, *appeared to be a key driver of conversations*—be it experts witnessing *insecure* behavior or non-experts witnessing *novel* behavior. These findings reaffirm the notion that social processes contribute to the modulating of security sensitivity, as these conversations often raised any or all of awareness, motivation or knowledge about security—warnings typically by raising awareness and motivation, and teachings typically by raising awareness and knowledge.

Opportunities

**Create more opportunities for social learning.** One type of conversation that raised all parts of the security sensitivity stack—*social learning*—was not very prevalent despite its efficacy. Indeed, social learning conversations may represent the ideal context under which social influence *can* affect security sensitivity—novices interested in learning about security voluntarily ask for information from experts, thereby raising their awareness, motivation and knowledge. In turn, experts are willing to share their information and don't feel that their efforts are wasted, as was implied by several of the security savvy participants we interviewed when asked why they don't share information about threats more often (P4, P9). One way to increase opportunities for social learning may be to increase the *observability* of security tools and behaviors. Indeed, the few social learning conversations that *did* occur were triggered when people saw novel security behaviors or tools in practice (e.g., one participant reported being asked, by a stranger, about Android 9-dot authentication at a café because it looked interesting).

**Facilitate experts’ sharing of security advice with others.** Unfortunately, many of our participants alluded to an illusory correlation [12] between security feature usage and paranoia, referring to their expert friends as “hyper-secure” (P5) and their actions as going “above and beyond” (P18) or “nutty” (P1). Perhaps as a result of this negative perception towards those with high security sensitivity, many of the security savvy participants we interviewed mentioned that they avoided sharing *proactive* information with their friends because the topic seemed socially inappropriate or unwelcome—as too preachy, for example. There is, thus, a substantial missed opportunity for experts to share knowledge with novices that only appears to be overcome when novices observe and query about interesting, novel behavior by the expert. Apart from increasing the observability of security tools and behaviors to create more opportunities for social learning conversations, another way to facilitate experts’ sharing of security advice might be to create tools for experts to share their knowledge *anonymously* (e.g., so they can share this information without incurring any perceived losses to social capital) or *indirectly* (e.g., by generally sharing their behaviors for others to view at their own leisure, but not as a directed message at any specific time).

**Create security tools that allow people to act on their sense of accountability.** Many conversations about security and privacy were triggered by a sense of accountability participants felt for the security of their loved ones. Yet, few security and privacy tools exist that allow participants to act on this sense of accountability—for example, tools that allow people to audit their loved ones security and privacy configurations. From the literature on usable privacy and security, we know that it is difficult to get people motivated enough to enact security and privacy behavior changes for their own sake [40]. Our results indicate, however, that it may be easier to get people motivated enough to help their loved ones enact security and privacy behavior changes.
Future Work
The results from this interview study illustrates how and why conversations about security and privacy happen. However, our sample, although representative in many respects, is primarily from the US and young. Furthermore, as we solicited participants from only one online recruitment source, and in so doing we could have introduced a systematic bias into our results—our participants were the type that generally volunteers for research projects. This means our results may not necessarily widely generalize, as is the case with most qualitative research. Thus, one fruitful avenue to bolster these results is to examine whether the patterns and relationships identified in our data persist in a larger, representative sample of technology users. In Chapter 7, I discuss in more detail some proposed work to generalize the findings from this interview study to a broader, more representative sample of internet technology users.

Our results are also limited to the communication and interaction instances participants could recall during our interview session—the so-called recall problem that afflicts retrospective interview studies [54]. In Chapter 7, I discuss some proposed work using surveys in response to breaking security news to capture people’s decisions to share information about security and privacy as they make those decisions.
Chapter 5: How Social Influences Affects Security Tool Diffusion

Summary
The interview study results offered initial evidence that social influence affects security behavior and tool adoption. However, it had two large limitations: (i) it was limited in its scale with only 19 participants, and (ii) it relied upon participants’ memory of their behaviors. In this chapter, to get a clear and more empirical understanding of how social influence affects security tool adoption, I report on a large scale investigation of how three optional security tools diffused through the social networks of 1.5 million Facebook users. My results confirm the findings that social influence can affect security tool adoption both positively and negatively. Specifically, the directionality and magnitude of the effect of social influence on any potential adopter’s likelihood of adopting a security tool is modulated at least by: (i) the number of the potential adopter’s friends who currently use the tool and (ii) the design of the security tool itself. Indeed, at low levels of adoption, negative social proof appears to disenfranchise the tool from further adoption, while at high levels of adoption, positive social proof appears to increasingly encourage further adoptions. Furthermore, security tools that are observable and socially inclusive are far more amenable to social spread. Taken together, these results offer an explanation for why many security tools are rarely used despite improvements to usability: most security tools are designed to be unobservable and socially exclusive, and thus the early adopters of these tools tend to disenfranchise their use, thus inhibiting further adoption.

Motivation
In the previous chapters, I reported on a rich, albeit small-scale interview study in which we showed that social influence plays a pivotal role in security related behavior change and security tool adoption. However, our results suggested that social proof can have contradictory effects.

Sometimes social proof appears to promote adoption of security technology and behaviors—especially when the tools and/or behaviors being diffused are highly novel or observable [11]. Indeed, as we know from a rich body of prior work in social psychology research, social proof can be an effective motivator for behavior change. This holds true even for behaviors, like security behaviors, that are not immediately or even directly gratifying—for example, conserving energy, reusing hotel towels, or preserving natural parks.

At other times, social proof appears to stifle the adoption of security technology because security tools tend to be preventative, intrusive, and associated with paranoia [18,32]. Indeed, if only ‘experts’ or people who are perceived as paranoid initially use a security tool, lay people might develop an illusory correlation [12] between using a security tool and paranoia that disenfranchises the use of a security tool.

Taken together, it appears that social influence can be both a helpful and harmful force in security-tool adoption, but we do not yet fully understand the parameters under which it is helpful or harmful. In addition, we do not know how social influence plays out unadulterated “in the wild”—the examples reported by our interview participants are subject to recall bias where only especially memorable instances were reported. Thus, to have a clearer understanding of how social forces affect security tool adoption, as well as to understand when positive social proof drives adoption and when negative social proof stifles adoption, I next analyzed how the adoption of three Facebook security tools—Login Notifications, Login Approvals and Trusted Contacts—diffused through the social networks of 1.5 million people [2]. The specific research questions we were trying to answer with this work were:

Q1. In practice, does social influence have a detectable effect on one’s likelihood to adopt a security tool?

Q2. If so, what factors affect the directionality and magnitude of the effect of social influence on security tool adoption?
Hypotheses
With big data observational research, it is easy to find significant effect sizes and retrofit hypotheses after the results are known. To avoid falling into this trap and better frame our methodology, we first surveyed the prior literature in social psychology, social network analysis and usable security in order to develop believable hypotheses.

Social Diffusion and Friend Diversity
Earlier work suggests that exposure to novel information on social networking sites increases information diffusion through social channels [5], but that these diffusion chains are most effective when the seed information is shared by many different sources [5,74], especially when the information is intended to enact behavior change [10,11]. Ugander and colleagues [77] extended this result, finding that people who were invited to join Facebook through e-mail recommendations from their friends were more likely to join if the recommenders were from distinct social contexts—i.e., receiving an invitation from a school friend and a family member was more convincing than receiving invitations from two different family members. Romero and colleagues [63] found that the “persistence” of the information being spread—or, the marginal likelihood that content will be re-shared after one more exposure—is also important in determining whether content will be diffused. Specifically, controversial topics—like information about security, say—require repeated exposure from many sources before they are diffused. These considerations led us to hypothesize:

H1: People with exposure to tool-adopting friends from many distinct social contexts will be more likely to use that tool than others with exposure to the same number of tool-adopting friends from fewer distinct social contexts.

Social Diffusion and Observability
It is well established that not all behavior diffuses equally [10,11], and the adoption of technology is no different. Thus, efforts have been made to model the factors that influence the adoption of technology. Rogers [61], in his seminal work on the diffusion of innovations, argued that new technology gets widely adopted through a process by which it is communicated through members of a social network. Rogers argues that primarily subjective perceptions get communicated through social channels, and that these perceptions are key to the success of an innovation. He further outlines that preventative innovations—or innovations, like security tools, that prevent undesirable outcomes from happening—typically have low adoption rates, in part because of their low observability, or the invisibility of their use and benefits. Finally, in my own prior work reported in Chapter 3: A Typology of How Social Influence Affects Security Behaviors and Chapter 4: Understanding How Security Information Is Communicated, I found that the observability of security tools and behaviors was a key factor in driving the adoption of security tools. In fact, I found that of all social catalysts for behavior change, observing others use security tools was the most prevalent.

H2: More observable security tools will more effectively diffuse through social channels than less observable security tools.

Social Diffusion on Security Adoptions
Prior work in psychology and the application of social influence implies that if many of one's friends and acquaintances use a security tool, one should be more likely to use that security tool herself. This is the basic premise of social proof—that we look to each others for cues on how to behave when we are uncertain [15]. Yet, we see some counter examples of this premise in the usable security literature. Indeed, Gaw and colleagues [32] found that many non-experts perceived others who used e-mail encryption as “paranoid”, a perception that inhibited their own use of e-mail encryption. In our interview study, we found that non-expert participants were similarly aversive towards using security tools, and spoke of their security-expert friends as being “nutty” or going “above and beyond”.

Thus, it appears that social proof does not always have the expected effect on security tool adoption. We believe, in fact, that because security tool usage is often invisible, rarely communicated, and
generally undesired [39,66], social proof can act against the adoption of a security tool at early stages of adoption.

Indeed, prior work in usable privacy and security suggests that many security tools remain unused because stringent security measures are often antagonistic towards the specific goal of the end user at any given moment [66]. For example, while a user might want to check her e-mail, a complex password that usually requires three attempts to get right prevents her from checking her e-mail. Thus, people often reject security tools when they expect or experience them to be weighty [2]. Consequently, typically only people who are especially dedicated to protecting their information use interruptive security tools, and we know from prior work that non-experts may perceive these early adopters as “paranoid” [32]. More formally, because early adopters of security tools are likely to be perceived by others as behaviorally different (e.g., either paranoid, or in possession of expert knowledge), non-experts may perceive an illusory correlation [12], or an exaggerated relationship, between security tool usage and this behavioral difference.

In turn, as non-experts consider themselves different from those who use security tools, they may reject the use of security tools. Moreover, this illusory correlation should only strengthen as more of these security-enthusiast early adopters use the tool because of the “availability heuristic”—a mental shortcut that biases people’s judgments towards what is more frequently recalled [76].

The upshot is that the subjective perceptions of a security tool that propagates through social channels may be tainted into working against its adoption, at least until enough of a potential adopter’s behaviorally similar friends start using the tool so that its use becomes normative.

In other words, there may be a non-linear relationship between one’s exposure to tool-adopting friends and one’s likelihood to adopt a security tool. Specifically, if a potential adopter is only exposed to few, early-adopter friends who use a security tool, it is possible that he might find social proof that a security tool should not be used (because of an illusory correlation), and the strength of this negative social proof should increase with the number of these tool-adopting friends (because of the availability heuristic). On the other hand, once a potential adopter is exposed to many tool-adopting friends, especially those that are similar to himself, he might find social proof that a security tool should be used (because of the positive effects of homophilous networks on technology adoption [8]), and the strength of this positive social proof should increase with the number of his tool-adopting friends.

**H3:** When a potential adopter is exposed to many tool-adopting friends, he will be more likely to adopt a security tool than those with fewer tool-adopting friends.

**H4:** When a potential adopter is exposed to few tool-adopting friends, he will be less likely to adopt a security tool than those with even fewer tool-adopting friends.

### Methodology

In the summer of 2013, I was intern on the Facebook Data Science team\(^3\), which afforded me access to the anonymized and aggregated security tool adoption patterns of Facebook users. To test our hypotheses, we monitored security tool adoptions for the following three Facebook security tools:

1. **Login Approvals**—A tool that requires adopters to enter a separate code, usually generated on or sent to the adopter’s smartphone, in addition to their password when they attempt to authenticate;  
2. **Login Notifications**—A tool that notifies adopters, via e-mail or SMS, when their account is accessed from previously unseen browsers and devices; and,  
3. **Trusted Contacts**—A tool that allows an adopter to specify three to five friends who can verify her identity if she forgot her password and cannot access her e-mail. We investigated multiple security tools to avoid drawing conclusions specific to any one tool, as well as to empirically evaluate the hypothesis that the design

\(^3\) [https://www.facebook.com/data](https://www.facebook.com/data)
of a security tool (e.g., its observability) may play a role in its diffusion [21]. Furthermore, we chose these three tools because of their diversity and colocation within the “security settings” page on Facebook.

For 12 days in late 2013, we collected data from a random subset of people who use Facebook and newly adopted one of the aforementioned security tools: Login Approvals, Login Notifications, or Trusted Contacts. In total, we collected data from n=250,000 people per tool (750,000 adopters overall)—the positive examples of tool adopters in our dataset. Then, for each day and tool, we also obtained a random sample of an equal number of people who had not adopted that tool up to that day—negative examples of tool adopters. In total, we had n=1,500,000 people across all twelve days, three tools (Login Approvals, Login Notifications, Trusted Contacts), and two tool usage states (i.e., uses or doesn’t use).

For all people in our sample, we also collected a set of variables that we believed could have affected one’s decision to adopt a security tool. These variables fell under four categories: demographic variables that described individual characteristics such as age and gender; behavioral variables that described activity on Facebook, such as posts shared and deleted; network variables that described one’s social network, such as friends’ average age and gender diversity; and, social proof variables that described how many and which of a person’s friends had adopted any of the aforementioned security tools up to the day during which the data was collected. In Table 9, we provide a full list of variables included in our analysis. All data was de-identified prior to our analysis.

<table>
<thead>
<tr>
<th>Demographic Variables</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of the individual.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Self-reported gender: male or female.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friend count</td>
<td>Count of the individuals number of friends with Facebook accounts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account length</td>
<td>Days that have passed since the individual activated his account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Days active in last 30</td>
<td>Days the individual was active on Facebook in the past 30 days.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Network Variables</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean friend age</td>
<td>Average age of the individual’s Facebook friends.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friend age entropy</td>
<td>Shannon entropy of the individual’s Facebook friends’ ages.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percent male friends</td>
<td>Percentage of the individual friends that are male.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mean friends’ account length</td>
<td>Average number of days an individual’s Facebook friends have used Facebook.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friend country entropy</td>
<td>Shannon entropy of countries from which the user has friends.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mean number of friends among friends</td>
<td>Average number of Facebook friends among an individual’s Facebook friends.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavioral Variables (all aggregated across the week prior to data collection)</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Posts Created</td>
<td>Number of posts created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posts Deleted</td>
<td>Number of posts deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comments Created</td>
<td>Number of comments created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comments Deleted</td>
<td>Number of comments deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likes</td>
<td>Number of likes given.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friends Added</td>
<td>Number of friends added.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friends Removed</td>
<td>Number of friends removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photos Added</td>
<td>Number of photos added.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Videos Added</td>
<td>Number of videos added.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Proof Variables</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of friends who use Login Approvals</td>
<td>Percent of friends who use the Login Approvals security tool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percent of friends who use Login Notifications</td>
<td>Percent of friends who use the Login Notifications security tool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percent of friends who use Trusted Contacts</td>
<td>Percent of friends who use the Trusted Contacts security tool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of diverse social contexts</td>
<td>Number of social contexts from which friends who use security tools originate.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 9. Collected tool descriptions. These variables were all collected per individual.*

We selected people who newly adopted security tools because security tool adoptions were not time-stamped in our data, so it would be otherwise impossible to know who, between two people, adopted
a security tool first. For someone who newly adopted a security tool on a given day, however, we knew that all friends of their friends who used that tool adopted it before that day.

Notably, we could not measure how security tool adoptions diffused—i.e., we did not alter the observability of security tool usage and initiation. Rather, we simply control for other factors that also affect security tool adoption, such that we can compare the tool adoption rate of two sub-populations that differ primarily in their exposure to friends who have adopted a security tool. We do not believe this limitation to be stifling—understanding the channels through which social diffusion occurs is separate from our goal of understanding its ultimate effect on security tool adoption.

Finally, all data collection complied with Facebook's terms of use and data use policy and was performed in aggregate so that we were not privy to any individual's information. Furthermore, as our data was observational, we believe our analysis constituted minimal risk to those in our sample.

Results
How exposure to friends from distinct social circles relates to adoption

Analysis method

First, we wanted to test the hypothesis that people with security-tool adopting friends from many distinct social circles should be more likely to adopt a security tool than those with the same number of tool-adopting friends from fewer distinct social circles. To do so, we estimated a logistic regression model for each security tool. These regressions modeled the strength of the relationship between a person's likelihood to adopt a security tool and the number of distinct social contexts from which his tool-adopting friends originated. Note that we define a “distinct social context” as a distinct connected component in one’s friend graph, following similar definitions used in prior work [29].

As linear regression analysis assumes independence in the response variable (in our case, whether or not someone in our sample adopted a security tool), we only included a balanced subset of our full sample into the regressions after eliminating people in our sample who happened to be Facebook friends with one another. This reduced sample consisted of n=65,000 positive and negative examples of tool adopters for each of our three tools, resulting in n=130,000 people for each regression, all of whom were not friends with one another.

In running these regressions, we controlled for the demographic, social network and behavioral variables described in Table 9. In addition, we also controlled for the number of one's tool-adopting friends, so that the coefficient for the number of distinct social contexts variable can be interpreted after controlling for a potential adopter’s number of tool using friends.

Analysis Results

The coefficient for the number of distinct social contexts variable for each logistic regression is shown in Error! Reference source not found., while the full regression table is shown in Table 10. These coefficients represent a change in “log-odds”, or \( \ln \frac{P}{1-P} \), where \( P \) represents the probability that an individual adopted the security tool. A positive coefficient implies that the log-odds ratio increases, or that an increase in the variable increases the likelihood that a person adopts the tool, \( P \). A negative coefficient implies the opposite. Furthermore, each variable was centered and scaled, such that its coefficient represents the expected change in log-odds that a person uses a tool given a one standard deviation increase in the predictor variable, holding all other numerical variables at their means and categorical variables at their baselines. Additionally, larger absolute coefficient values imply a stronger relationship between the IVs and DVs.

Thus, from Figure 3 and Table 10, we can see that the number of diverse social contexts variable positively correlated with the adoption of every security tool \((b_{\text{LA}}=+0.15, p<2e-16; b_{\text{LB}}=+0.03, p<2e-16; b_{\text{TC}}=+0.088, p<2e-16)\). This finding offers support for \( \text{H1} \)—people with friends from more diverse social contexts (e.g., high school friends, college friends, family) who use a security tool should be more likely to adopt that tool themselves than those with tool-adopting friends from fewer distinct social contexts. In other words, it is not just the number of one's friends who use a security tool that matters; these friends should be independent of one another for the effect to be strongest.
In addition, the discrepancy of effect size across tools offers some support for H2—that more observable security tools will be more effectively diffused through social channels. Indeed, the absolute effect size of the number of diverse social contexts variable is largest, by far, for Trusted Contacts (the most observable tool, $b_{TC} = +0.88$), then for Login Approvals (the next most observable, $b_{LA} = +0.15$) and finally lowest for Login Notifications (the least observable tool, $b_{LN} = +0.03$).
Indeed, Login Notifications are private messages that are not very observable, and are thus difficult to passively diffuse via social channels. Thus, while having many different friends use Login Notifications may make for a more convincing case for a potential adopter to use the tool, the case is unlikely to be made. Login Approvals are more observable than Login Notifications in that friends who are collocated with an adopter will see the additional authentication step it requires, which in turn may passively provide these friends with social proof to use Login Approvals [18]. This modest increase in observability appears to correlate with a modest increase in the effect size of the number of diverse social contexts variable. Finally, the Trusted Contacts tool sends out a notification to each of one’s friends who was specified as a Trusted Contact, thus substantially increasing its visibility in a direct way and, in turn, correlating with a substantial increase in effect size. It is also possible that the social nature of the tool—in enlisting friends to help recover one’s account—lends itself to amplified social diffusion.

In summary, our regression analysis provides us with support for H1 and limited support for H2, but we have yet to test H3 and H4—that the tool-adoption rate of one’s current set of friends will moderate whether the effect of social proof will be positive or negative on one’s own likelihood to adopt that security tool. Unfortunately, linear regression analysis is limited in that it does not consider this form of non-linearity in the relationship between predictor and response. Furthermore, regression analysis confounds homophily-based diffusion with social-influence based diffusion [4,70]. In other words, because similar people cluster together as friends, we cannot tell if co-adoption of a tool is due to one friend influencing another or because both friends share an interest.

**How social influence affects the adoption of security tools**

**Analysis Methodology**

Thus, to test H3 and H4, we ran an adapted version of matched propensity sampling analysis [4]. Matched propensity sampling is a form of causal inference that helps us differentiate tool adoption due to homophily from tool adoption due to social influence. It distinguishes between homophily and social influence by comparing the tool adoption rates of two sets of people who are equally likely to have a fixed proportion of friends who have adopted a security tool, where one set actually does have the fixed proportion of friends who have adopted this tool and the other set does not. People in the former set are “exposed” to their tool-adopting friends at this fixed rate, while those in the latter set are “unexposed.”

Exposed and unexposed individuals are matched, in pairs, based on a “propensity score” computed from a set of covariates $Z$ that are theorized to represent homophily-based diffusion [64]. We used a logistic regression to calculate the propensity score as suggested by prior work [4], and the covariates included in the model were the demographic, behavioral, and social network variables listed in Table 9. As we are not concerned about estimating exact coefficients and their variances with the logistic regressions in this analysis, we are able to break the independence assumption and include the full set of 1.5 million users in our sample.

Unfortunately, as we could not capture the security expertise of those in our sample, there remains some form of “latent homophily” for which we do not control. However, the demographic, behavioral, and social network variables for which we control likely predict security expertise, so we believe this limitation to be minimal.

By matching exposed and unexposed individuals who have the same likelihood of being exposed, we can take the difference in tool adoption rates between the exposed and the unexposed as evidence of the effect of social influence. Indeed, after the propensity matching process, the only theoretical difference between these two sets of people are that the exposed set has a certain proportion of friends who use a security tool and those in the unexposed set do not. If social influence has no effect, we should see the same rate of adoption for the exposed and unexposed, whereas if social influence has a positive or negative effect, we should see that exposed individuals adopt the tool at a higher or lower rate, respectively.

We specified five empirical exposure conditions for each security tool—Login Approvals, Login Notifications, and Trusted Contacts—with each exposure condition representing whether or not the
user was at least in the 1st percentile, the 21st percentile, the 41st percentile, the 61st percentile, or the 81st percentile in the percent of friends who use tool variable, or the total percentage of their friends who used a security tool at the day of data collection. Notably, a potential adopter could count as "exposed" at some levels but not others.

Figure 4 depicts the values of the percent of friends who use tool variable that qualified for “exposure” under E1 through E5, with actualized values for these conditions shown in Table 11. Concretely, an individual is exposed in E1 for Login Approvals if at least 0.2% of her friends adopted the tool, because that puts her at least at the 1st percentile of people whose friends have adopted the tool.

<table>
<thead>
<tr>
<th>Percentile</th>
<th>Approvals</th>
<th>Notifications</th>
<th>Trusted Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>1st</td>
<td>0.2%</td>
<td>2.0%</td>
</tr>
<tr>
<td>E2</td>
<td>21st</td>
<td>0.8%</td>
<td>7.3%</td>
</tr>
<tr>
<td>E3</td>
<td>41st</td>
<td>1.3%</td>
<td>10.0%</td>
</tr>
<tr>
<td>E4</td>
<td>61st</td>
<td>1.8%</td>
<td>12.3%</td>
</tr>
<tr>
<td>E5</td>
<td>81st</td>
<td>2.7%</td>
<td>15.1%</td>
</tr>
</tbody>
</table>

Table 11. Exposed condition prerequisites for each security tool. For example, if a user is “exposed” at E3 for login approvals, at least 1.3% of her friends must have adopted login approvals at the time of data collection.

Likewise, she is exposed in E5 for Login Approvals if at least 2.7% of her friends adopted the tool.

We chose five exposure conditions uniformly spaced across the distribution of the percent of friends who use tool variable to get a detailed map of the relationship between exposure to friends who have adopted a security tool and one’s own likelihood to adopt that tool at different levels of exposure. This map should help us evaluate both H3 and H4—specifically, H3 predicts a higher adoption rate for the exposed relative to the unexposed at high exposure conditions because of positive social proof, whereas H4 predicts a higher adoption rate for the unexposed at low exposure conditions because of negative social proof—specifically, an illusory correlation between the attributes of early adopters (e.g., “paranoid”, “nutty”, “expert”) and the security tool itself.

Analysis Results

Figure 5 shows the rate of feature adoption for exposed and unexposed individuals for all three features across all five exposures. In interpreting the results of the matched propensity analysis in Figure 5, we note the following: (i) If social influence has any effect on the adoption of a security feature at a particular level of exposure, we should see a significant difference in the adoption rates of exposed and unexposed individuals; (ii) If social influence has a positive effect on the adoption of a security feature at a particular level of exposure, then we should see that exposed individuals have a significantly higher adoption rate than the unexposed; and, (iii) If social influence has a negative
effect on the adoption of a security feature at a particular level of exposure, we should see that exposed individuals have a significantly lower adoption rate than the unexposed.

First, as we show in Table 12, below, all of the differences in adoption rate between the exposed and unexposed were significant, suggesting that irrespective of the security feature and level of exposure to friends who use that feature, social influence appears to have a significant effect on one’s likelihood to adopt a security feature. This finding strongly supports our smaller-scale qualitative results, explained in Chapters Chapter 3: A Typology of How Social Influence Affects Security Behaviors and Chapter 4: Understanding How Security Information Is Communicated, that surfaced social influence as a key factor in the adoption of security features [18].

For Login Notifications, we see that people who are exposed to a certain proportion of feature-using friends appear to be less likely to adopt those features than people who are unexposed for all levels of exposure we tested. Thus, in our sample, even people with a higher-than-average proportion of feature-adopting friends (i.e., those exposed at E4-E5 who are at least at the 61st percentile) were themselves less likely to use Login Notifications than people who had fewer friends who used those features. It appears, therefore, that exposure to friends who use Login Notifications stifles the adoption of Login Notifications, a finding that supports H4—that social influence will have a negative effect on feature adoption at low exposure levels—but conflicts with H3—that social influence will have a positive effect on feature adoption at high exposure levels.

We see just the opposite trend for Trusted Contacts, however: even at E1, the lowest level of exposure, exposed individuals are significantly more likely to adopt Trusted Contacts than the unexposed. In other words, it seems that any exposure to friends who use Trusted Contacts substantially increases one’s own likelihood to adopt that feature, a finding that supports H3 but contradicts H4.

Table 12. Chi square significance tests for the difference in adoption rate between exposed and unexposed individuals across all exposure conditions and all security features. All differences significant, \( p < 2e^{-16} \).

<table>
<thead>
<tr>
<th></th>
<th>Approvals</th>
<th></th>
<th>Notifications</th>
<th></th>
<th>Trusted Contacts</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N ( \chi^2, \text{df}=1 )</td>
<td>N ( \chi^2, \text{df}=1 )</td>
<td>N ( \chi^2, \text{df}=1 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1</td>
<td>5852</td>
<td>1553</td>
<td>25061</td>
<td>13743</td>
<td>4995</td>
<td>491</td>
</tr>
<tr>
<td>E2</td>
<td>122765</td>
<td>4994</td>
<td>518907</td>
<td>172603</td>
<td>105156</td>
<td>11742</td>
</tr>
<tr>
<td>E3</td>
<td>240061</td>
<td>3104</td>
<td>1014159</td>
<td>174619</td>
<td>205541</td>
<td>29775</td>
</tr>
<tr>
<td>E4</td>
<td>228905</td>
<td>140</td>
<td>963824</td>
<td>93771</td>
<td>196397</td>
<td>42022</td>
</tr>
<tr>
<td>E5</td>
<td>111092</td>
<td>1976</td>
<td>468147</td>
<td>18828</td>
<td>95393</td>
<td>34665</td>
</tr>
</tbody>
</table>

Figure 5. Feature adoption rates, plotted for each security feature for each exposure condition, for both exposed and unexposed individuals. Exposed feature adoption rates are plotted as red circles, and unexposed feature adoption rates are plotted as blue triangles.
Finally, for Login Approvals, we see exactly the nuanced, thresholded relationship we predicted. At lower levels of exposure, unexposed individuals are more likely than the exposed to adopt the feature, but at the highest level of exposure, exposed individuals are more likely to adopt the feature—a finding that supports both H3 and H4.

Thus, we have three security features for which adoption is significantly affected by social influence, but for which the effect of social influence appears to manifest differently. For Login Notifications, it appears that social influence is a categorically negative force on its adoption, for Trusted Contacts it is a categorically positive force, and for Login Approvals, the direction of its effect is based on a threshold level of exposure a potential adopter has to friends who already use that feature. What could explain the differences in the effect of social influence across these features?

**Theoretical vs. Empirical Exposure Threshold**

The matched propensity sampling analysis only reflects the effect of social influence on the adoption of a feature at its rate of adoption at the time of data collection. Indeed, our exposure conditions were based on an empirical division of the percent of friends who use feature variable; therefore, it is possible that there is a theoretical exposure greater than E5 where social influence could have a positive effect on the adoption of Login Notifications. Indeed, for Login Notifications, exposure at E5—at which about 15% of one’s friends use Login Notifications—may not yet be at the threshold where H3 predicts social influence should have a positive effect on its adoption.

To test this possibility, we must observe how the adoption rate difference between the exposed and unexposed varies across exposure conditions. We plot these differences in Figure 6, by subtracting the unexposed adoption rate from the exposed adoption rate. From this plot, we can understand the marginal effect of social influence on adoption at higher exposure conditions. In interpreting Figure 6, we note the following: (i) If unexposed individuals are more likely than the exposed to adopt a feature at a certain level of exposure, then the value of the difference will be negative, whereas it will be positive if exposed individuals are more likely to adopt the feature than the unexposed; and, (ii) If the value of the difference increases (moves up) at higher exposure conditions, then the marginal effect of having more friends who use a security feature on that feature’s adoption is positive, whereas if the value of the difference decreases (moves down), then the marginal effect is negative.

From Figure 6, we see that the value of the difference between exposed and unexposed adoption rates increases (moves up) constantly, for all three features, from E1 to E5. For Login Notifications and Login Approvals, the initial adoption rate advantage of unexposed individuals gradually
diminishes at higher levels of exposure. In fact, the advantage is ultimately in favor of exposed individuals for Login Approvals at E5, when the difference shifts from negative to positive. For Trusted Contacts, the advantage starts with exposed individuals and simply gets larger at higher levels of exposure. Thus, at higher levels of exposure, the likelihood for exposed individuals to adopt any of the security features grows at a rate faster than the unexposed. It seems likely, therefore, that there is a theoretical exposure higher than E5 where exposed individuals are more likely to adopt Login Notifications than the unexposed—as would be predicted by H3. Unfortunately, we did not have a large enough number of people at a high enough exposure to empirically confirm this prediction from the data in our random sample.

It is tempting to also apply this logic to entertain a theoretical exposure lower than E1 at which the effect of social influence is negative for Trusted Contacts. However, as the exposure threshold for E1 for Trusted Contacts is just 0.1%, the theoretical and empirical exposure lower bounds are essentially the same—i.e., having at least one friend who uses the feature. Thus, while it seems like H3 may be true even for Login Notifications, it seems likely that H4 may not be true for some features—social influence does not have to be a negative force at low exposure conditions.

**Individual Feature Attributes**

Another consideration in interpreting the differences in the effect of social influence across security features is the individual attributes of each feature. Specifically, as H2 suggests, more observable security features should be more positively affected by social influence.

The threshold beyond which the effect of social influence toggles from negative to positive appears to be inversely proportional to the observability of the feature, lending further support for H2. Indeed, the threshold is “lowest” for Trusted Contacts in that the threshold seems to be at its theoretical lowest possible value of having just one friend who uses the feature. The threshold is next lowest for Login Approvals at E5—or when approximately 2.7% of ones friends use the security feature. Finally, the threshold is highest for Login Notifications at a level of exposure higher than E5, if such a threshold exists at all.

It makes intuitive sense that the threshold of friends required for negative social proof to be overcome by positive social proof should be lower for more observable features. If our reasoning for H4 is correct, negative social proof is the result of stereotypes and generalizations that may be overcome if potential adopters can see, concretely, that security feature usage is not necessarily limited to those who they may consider “paranoid” or who have an unachievable level of specialized knowledge about security.

**Summary of Results As They Relate to Hypotheses**

In summary, the results from our matched propensity sampling analysis lends additional support to H2 and conditional support to H3 and H4. Specifically, the prediction, of H3 and H4, that the direction of the effect of social influence on a potential adopter’s likelihood to adopt a security feature will shift at a threshold appears to be true for Login Approvals and is likely true for Login Notifications. For Trusted Contacts, however, it appears that social influence has a positive effect on its adoption, regardless of the level of exposure. Furthermore, the observability of a security feature appears to at least partially moderate the presence and value of this threshold.

**Discussion**

We analyzed whether and how security feature adoptions diffused through the social networks of 1.5 million people who use Facebook. These results provide large-scale empirical evidence that social influence does affect the adoption of security tools, and can do so in both a positive or negative direction. This directionality and magnitude of the effect of social influence on security tool adoption are dependent on at least three factors.

**First, the current level of adoption among a potential adopter’s friends affects their own likelihood to adopt the tool.** While the magnitude of this effect varied across tools, the presence of the effect was consistent across tools. Specifically, for Login Notifications, people who were unexposed to a certain percentage of friends who already used the tool were more likely to use the tool than those who were exposed to that same percentage of friends who already used the tool—for
all tested levels of exposure. In other words, social proof had a negative effect—the early adopters of Login Notifications appeared to disenfranchise the tool. For Login Approvals, the same was true up until the highest levels of exposure at which point the exposed were more likely to adopt the tool than the unexposed. In other words, social proof has a negative effect until a certain critical threshold of a potential adopter’s friends start using the tool, at which point it starts having a positive effect. Finally, for Trusted Contacts, we saw a completely different trend: For all levels of exposure, those who were exposed were more likely to use Trusted Contacts than those who were unexposed. In other words, social proof had a positive effect even at the lowest levels of exposure. While each tool was affected differently by social influence, for all three tools, at higher levels of exposure, the difference in adoption rate between those who were and were not exposed got greater. Thus, social influence was always trending towards a more positive effect on tool adoption at higher levels of adoption.

Second, the difference in adoption trends across tools suggests that the design of a security tool strongly affects its potential for social diffusion. Specifically, using Rogers’ Diffusion of Innovations [60] theory and my own prior qualitative work as a lens, it may be that Trusted Contacts has two advantages, in its potential for social spread, over Login Notifications and Login Approvals. First, its use is more observable—whereas use of Login Notifications and Login Approvals is private, enabling Trusted Contacts requires a user to specify three to five friends to help with account recovery. These specified “trusted contacts” are, in turn, notified that they have been entrusted with this role and thus its use is broadcast. Second, Trusted Contacts is more socially inclusive. Whereas Login Notifications and Login Approvals are used to exclude others from access and may thus be indicative of distrust [1], Trusted Contacts is uniquely social—it allows friends to provide security, and may thus be more indicative of trust. Indeed, it allows friends to be accountable for each other’s security, which, as suggested in the results of our interview study, is something that many present-day security tools are sorely lacking.

Third, exposure to friends from more diverse social contexts who use a security tool may increase one’s likelihood to adopt a security tool. Indeed, for all three security tools, controlling for the number of one’s friends who used a security tool, people who had exposure to friends from more diverse social contexts who used a security tool was had a higher likelihood of adopting the security tool themselves.

To summarize, it seems that security tool adoption does depend on social influence, but only positively for tools that are observable, socially compatible and/or widely adopted by many distinct social circles within a potential adopter’s social network.

Future Work
The results from this interview study provides empirical evidence that social influence powerfully affects one’s decision to adopt a security tool and that the design of a security tool affects its potential for social spread. However, the question remains: how can leverage the power of social influence to increase the awareness and adoption of security tools?

Our results suggest that having friends from many social circles that use a security feature is strong social proof that a security feature should be used. Thus, one method to maximize the social spread of security features may be to target people from distinct social contexts and offer them personalized incentives to try security tools in hopes that their use of those tools will propagate through their extended social networks. I will not try this approach in my proposed work, but it does present a fruitful opportunity for future experimental work.

It also appears that individual attributes of a security feature can affect its spread. Therefore, security tool designers should be mindful of the fact that use of a security feature can have social consequences. If, as prior work suggests, use of security tools can be seen as a sign of paranoia, then designing security features like Trusted Contacts that draw friends in, can be seen, and feel trusting and collaborative rather than isolating may make it easier to convince people to use security features. In Chapter 7, I discuss some proposed work in where I plan to design, implement and evaluate a set of example security tools with these design dimensions in mind. In Chapters 6 and 7, I also discuss some experimental work (or proposed experimental work) in which I increase the observability of
security and privacy tool usage and test how that increased observability affects non-adopters’ awareness and adoption of those tools.

In Chapter 7, I also discuss some future theory-building work in which I plan to enumerate and empirically validate the design dimensions of security tools that affect its potential for social spread. I have already mentioned two—observability and social compatibility. The goal of this line of work will be to provide a “social checklist” for security tool designers to evaluate whether their tools adequately consider social design dimensions.
Chapter 6: Increasing Security Sensitivity with Social Proof

Summary

In Chapters 3-5, I constructed both qualitative and quantitative models of how social influence affects security behaviors and tool adoptions. From these models, we identified that the observability of these behaviors and tools were key to their social propagation. These initial studies were limited in that they were entirely observational, however—and thus it is difficult to claim causality. Building on these findings and opportunities, I next wanted to experimentally test whether increasing the observability of security tool usage would, in fact, increase people's awareness and adoption of those tools. I once again partnered with Facebook to conduct this experiment. As a part of Facebook's annual security-awareness campaign, we showed 50,000 people who use Facebook one of eight announcements promoting the use of the same three security tools we studied in the previous chapter—Login Approvals, Login Notifications and Trusted Contacts. Seven of the announcements had a social proof cue: i.e., some descriptive text that informed viewers about the fact that some number of their direct friends already used the security tools we were promoting. These social proof cues varied in their specificity (i.e., the exact number of friends to just 'some' friends) and framing (e.g., "Over X friends" vs. "Only X friends"). The eighth announcement was a non-social control. Our results were unambiguous: the social announcements all significantly out-performed the non-social control, increasing clicks on the announcement by 37% and thereby also increasing the number of security tool adoptions by 30%.

Motivation

Looping back to the introduction of this proposal, one of the largest problems in computer security is the need for higher awareness and use of available security tools. From Chapters 3, 4, and 5, I demonstrated that social influence plays a key role in people's awareness and use of available security tools, and identified that security tools and behaviors that were more observable might more easily spread via social channels. This finding is line with prior work in social psychology and sociology. Indeed, Rogers, in his seminal Diffusion of Innovations [60], lists observability as one of the five key factors in determining whether a technology will see widespread use. Similarly, studies by Milgram and colleagues [55] and Cialdini and colleagues [14,15,33] also highlight the concept of social proof—or the tendency for one to try and emulate what she can see others around her doing.

Historically, however, security feature usage has been kept confidential to preserve an individual security-tool-user's privacy. While this privacy is important, as using a security tool can also have negative connotations such as being "paranoid" [32] or "nutty" [Chapter 3: A Typology of How Social Influence Affects Security Behaviors], this hiding of security feature use has both stifled the social diffusion of security features and made it difficult to test the effect of social interventions on increasing people's security sensitivity. Furthermore, it has been difficult if not impossible to answer these questions because of the lack of data associating security tool adoptions with social meta-data. Consequently, the security community has overlooked a potentially fruitful avenue for increasing security sensitivity, as there is a dearth of empirical data conclusively linking social-proof based interventions to heightened security sensitivity. Today, with the rich and high-complete social meta-data on platforms such as Facebook, we can design simple social cues that show non-adopters social proof that their friends use security tools.

In the following chapter, I share some of the first results experimentally testing whether increasing the observability of security tool usage does indeed increase the awareness and adoption of security tools [3]. Along with colleagues, I designed a set of 7 security announcements with social proof cues that can preserve the privacy of individuals who use security tools while still providing their friends with positive social proof in favor of using the tools. All social announcements informed viewers that their friends used "additional" security tools, but the seven variations differed in their specificity (i.e., showing viewers exactly how many of their friends used security features versus just saying that "some" of their friends used security features) and framing (i.e., using keywords such as "only" or "over" to prime viewers' interpretation of the text). To run this experiment in an ecologically valid setting, I again teamed up with Facebook's Site Integrity team to promote the security tools we studied in Chapter 5: How Social Influences Affects Security Tool Diffusion: Login Notifications, Login
Approvals and Trusted Contacts. The specific research questions we wanted to answer in this experiment were:

Q1. Does increasing the observability of security tool usage drive the awareness and adoption of security tools?

Q2. Does the framing of social information affect the exploration and adoption of security tools? If so, which framings work – those that suggest that many of a friends have already started using security tools, or those that suggest that few have already started using security tools and that the viewer should be among the first?

Q3. Does the specificity of the social proof cue matter? In other words, is it enough to inform viewers that “some friends” use security tools, or is it only effective if they see a specific number?

We ran two experiments. In our first experiment, we tested all of the eight announcements we designed to test whether and which social proof cues yielded the highest click-through rates and follow-up adoptions. In our second experiment, we re-ran only our best performing social conditions and also asked participants to answer a short survey to test whether providing social proof cues in an announcement influenced people’s perceptions of the security tools we promoted—namely, whether a viewer believed the tools were sufficient to address their security concerns.

Experiment
In our initial experiment, we showed 50,000 people who use Facebook one of eight announcements, pinned at the top of their Facebook newsfeed, informing them about the availability of extra security features on Facebook. Seven of these announcements included a social cue informing viewers that their friends also used security features, but varied in their specificity (i.e., showing the exact number of friends versus just saying “some” friends) and framing (i.e., priming the interpretation of the social cue with keywords such as “only” and “over”). None of the announcements revealed any information about individual tool users, however, thus providing aggregated social proof without surfacing who was using which tools. We measured whether the nature of the text in the announcement (social vs. non-social, the framing and specificity of the social proof text) led to greater exploration of available security features and greater adoption of security features—or, increased awareness of and motivation to use security features, respectively.

Methodology
People in our sample who logged on to Facebook between November 4th, 2013 and November 8th, 2013 were shown one of eight announcements informing them that they could use extra security features to protect their Facebook accounts. The announcements were rendered at the top of their newsfeeds—the portion of Facebook’s user interface where people are directed when they first log in, where they see an assortment of content shared by their friends (see Figure 7). All announcements contained a call-to-action button (labeled “Improve Account Security”) that directly linked people who clicked on the button to an interstitial that explained the benefits of the three security features we promoted (described below) and allowed viewers to enable the features.

Announcements were shown at most three times to the same person over the course of the four days, in order to mitigate the effect of greater exposure to those who were more active.

Experiment Groups
We designed and implemented four social framings to test not only whether and how social-proof cues can increase people’s security sensitivity, but also if the specificity and framing of those cues matter. We refer to these framings as “Over”, “Only”, “Raw”, and “Some”. The “Over” framing informed viewers that more than a certain number or percent of their friends use extra security features, priming viewers to interpret the social cue as there being abundant social proof that others they know use security features: i.e., “many people do this, so I should too.” The “Only” framing takes a contrasting approach, framing the social cue in a manner that suggests that only a few of a viewer's
friends use security features so they should be among the first of their friends to secure their account. The “Raw” framing eliminates subjectivity in the framing altogether and simply presents the viewer with the quantity of her friends who use security features. Finally, the “Some” framing is ambiguous: informing viewers only that a positive number of their friends use security features.

The “Over”, “Only”, and “Raw” framing had two forms: a number form where the number of the viewer’s security-feature using friends was rendered in the announcement, and a percentage form where the percentage of the viewer’s security-feature using friends was rendered in the announcement. In total, thus, there was one control group, two “Over” framing groups, two “Only” framing groups, two “Raw” framing groups, and one “Some” framing group, for a total of \(1+2+2+2+1=8\) experimental groups. The eight experimental groups are summarized in Table 13, and an image of each of these announcements is shown in Figure 8.

**Sample**

We selected a random sample of \(n=50,000\) people from the U.S. who used Facebook in English, were at least 18 years old, logged on to Facebook at least once in the month preceding the experiment, had at least 10 friends who enabled one of the promoted security features, and had not enabled any one of the security features we were promoting. We evenly assigned the \(n=50,000\) people in our sample into one of the aforementioned eight experiment groups, amounting to 6,250 people per group. This assignment was mostly random, with the constraint that people assigned to the Over condition had to have at least 10% of their friends who enabled security features, and people assigned to the Only conditions had to have fewer than 10% of their friends who enabled security features. Our participants were 40 years old on average (s.d., 16), and 68% were women, suggesting that our sampling criteria had a bias towards older females. Notably, our sampling criteria was also biased towards active, non-security experts, but we do not believe this to be a stifling limitation given that active, non-security experts are the intended target for interventions aiming to heighten security sensitivity, as these people potentially face the greatest risk of having their accounts compromised.
Finally, the $n=50,000$ sample size we selected for our experiment comfortably exceeded the 4,000 participant sample size suggested by a power analysis for generalized linear models [16], with 26 coefficients, a significance level of 0.001, a power of 0.999, and a very modest effect size of 0.02—i.e., a prediction that the best social announcement will only introduce 2% more clicks relative to the control condition. In practice, we expected the effect size to be greater than 2%, but we selected a low effect size for the power analysis to get an upper bound on the number of users we needed to obtain significant results for our experiment. The 26 coefficients in our model comprised of the 18 variables described in Table 14, in addition to seven categorical variables representing the experimental conditions, and one intercept variable.

<table>
<thead>
<tr>
<th>Group</th>
<th>Prompt Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>You can use security settings to protect your account and make sure it can be recovered if you ever lose access.</td>
</tr>
</tbody>
</table>
| Over (#/%) | Over X of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access.  
[Note: X rounded down to nearest 5th (e.g., 108 becomes 105)] |
| Only (#/%) | Only X of your friends use extra security settings. Be among the first to protect your account and make sure it can be recovered if you ever lose access. |
| Raw (#/%) | X of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access. |
| Some   | Some of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access. |

Table 13. Prompt text in announcement across all 8 experimental groups. Some social groups have templates that are filled in with either the number or percentage of a user's security feature-using friends.

Promoted Security Features

We decided to promote the following three security features in our initial campaign:

**Login Notifications**: A security feature that informs users, via text and/or e-mail, whenever their Facebook account is accessed under suspicious circumstances: e.g., from a city the person had not previously visited.

**Login Approvals**: A two-factor authentication security feature that requires users to enter a randomly generated security code (sent to or generated on their phone) in addition to their passwords in order to authenticate.

**Trusted Contacts**: A security feature that allows users to specify 3-5 friends who can vouch for the user’s identity if she forgets her Facebook account password and cannot access her e-mail.

We selected these three security tools because they were the same set of tools we studied in the previous chapter, as well as because they were all co-located within the “security settings” menu context in Facebook’s user interface. We chose to promote three security tools to avoid drawing conclusions specific to any single security tool, and because these tools represented a wide range of definitions for “security features”—with Login Notifications simply informing people of potential breaches, Login Approvals adding an extra step to the authentication process, and Trusted Contacts asking people to draw in their friends to help protect their accounts.
1. **Control**

   ![Keep Your Account Safe](image)
   
   **Keep Your Account Safe**
   
   You can use security settings to protect your account and make sure it can be recovered if you ever lose access.
   
   **Improve Account Security**

2. **Raw #**

   ![Keep Your Account Safe](image)
   
   **Keep Your Account Safe**
   
   108 of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access.
   
   **Improve Account Security**

3. **Over %**

   ![Keep Your Account Safe](image)
   
   **Keep Your Account Safe**
   
   Over 20% of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access.
   
   **Improve Account Security**

4. **Some**

   ![Keep Your Account Safe](image)
   
   **Keep Your Account Safe**
   
   Some of your friends are using extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access.
   
   **Improve Account Security**

5. **Only #**

   ![Keep Your Account Safe](image)
   
   **Keep Your Account Safe**
   
   Only 108 of your friends use extra security settings. Be among the first to protect your account and make sure it can be recovered if you ever lose access.
   
   **Improve Account Security**

---

*Figure 8. Screenshots of each of the social framings and the control announcements in our experiment. In total we had 8 announcements. Not pictured is the Raw %, Over # and Only % announcements, but they look similar to their counterparts pictured above.*
Dataset

We measured click-through rate for each announcement, as well as the short-term and long-term adoption rate of the promoted security features up to a week and 5 months after running the experiment, respectively. We used click-through rate on the announcement as a proxy for raising awareness (as people who clicked on the announcement were taken to explore the promoted security features), and adoption rate as a proxy for raising motivation (as people who adopted security features must have gained the motivation to enact a behavior change). We could not measure the differential effects of the announcements on knowledge, however, as all announcements led viewers to the same interstitial with the same information.

In addition, we collected each viewer’s number of friends who used any of the three security tools we were promotion, along with a set of behavioral (e.g., frequency of posts and comments), demographic (e.g., age, gender) and social network descriptor (e.g., mean friend age, mean friend-of-friend count) control variables that we expected might affect click-through rate and security feature adoption among our sample. These variables are described in Table 14.

### Table 14

<table>
<thead>
<tr>
<th>Demographic Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of the user.</td>
</tr>
<tr>
<td>Gender</td>
<td>Self-reported gender: male or female.</td>
</tr>
<tr>
<td>Friend count</td>
<td>Count of the user’s number of friends.</td>
</tr>
<tr>
<td>Account length</td>
<td>Days that have passed since the user activated his/her account.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Network Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean friend age</td>
<td>Average age of friends.</td>
</tr>
<tr>
<td>Friend age entropy</td>
<td>Shannon entropy of friend ages.</td>
</tr>
<tr>
<td>Percent male friends</td>
<td>Percentage of friends that are male.</td>
</tr>
<tr>
<td>Mean friends’ account length</td>
<td>Average number of days the user’s friends have used Facebook.</td>
</tr>
<tr>
<td>Friend country entropy</td>
<td>Shannon entropy of countries from which the user has friends.</td>
</tr>
<tr>
<td>Mean friend of friend count</td>
<td>Average number of friends of friends.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavioral Variables (all aggregated across the week prior to data collection)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posts Created</td>
<td>Number of posts created.</td>
</tr>
<tr>
<td>Posts Deleted</td>
<td>Number of posts deleted.</td>
</tr>
<tr>
<td>Comments Created</td>
<td>Number of comments created.</td>
</tr>
<tr>
<td>Comments Deleted</td>
<td>Number of comments deleted.</td>
</tr>
<tr>
<td>Friends Added</td>
<td>Number of friends added.</td>
</tr>
<tr>
<td>Friends Removed</td>
<td>Number of friends removed.</td>
</tr>
<tr>
<td>Photos Added</td>
<td>Number of photos added.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature-using friends</td>
<td>Number of friends who use security features.</td>
</tr>
</tbody>
</table>

Table 14. Collected feature descriptions and distributions for the n=50,000 people in our sample. † Approximate values.
Hypotheses
Cialdini’s [15] concept of social proof suggests that when we are confronted with making a decision where we are uncertain of the appropriate course of action—like adopting a security tool, say—we look to our friends and those around us for cues on how to act. Combined with Rogers [61] assertion that observability—or, the visibility of the use and benefits of an innovation—is critical to the widespread adoption of an innovation, our own finding that the observability of security tool usage is a major positive factor in security and privacy related behavior change, we predicted:

**H1:** Social announcements will have higher click-through rates than the non-social control.

Extending the idea that social proof is more convincing when people see larger groups conforming to an action [55], we also predicted:

**H2a:** People with more security-tool using friends will be more likely to click on the announcement.

**H2b:** People with more security-tool using friends will be more likely to adopt a security tool, both in the short and long-term.

Similarly, we predicted experiment groups that rendered higher values or otherwise suggested that more rather than fewer of the viewer’s friends used security features would be more effective at getting users to click on the announcement and explore security features. Thus, we expected that “number” conditions would have higher click-through rates than their “percent” counterparts, as the former generally render higher numbers in the announcement (e.g., 20 friends vs. 20/400=5% of friends). Furthermore, as the “Raw” framing rendered the highest values, followed by the “Over” and then the “Only” framing, we expected that the click-through rates for these framings would fall in that order as well.

**H3a:** The “number (#)” context conditions will have higher click-through rates than their “percent (%)” counterparts.

**H3b:** The “Raw” framing will have the highest click-through rate, followed by the “Over” and then “Only” framings.

Next, as one of the driving forces for social proof is a search for a clear course of action in an unclear circumstance [15], we also suspected that clearer, more informative messages would be more effective at driving click-through rate.

**H4:** More specific social framings will have higher click-through rates. Thus, the “Some” context will have the lowest click-through rate.

For short-term adoptions, we expected that the effects of social conditions would be muted. Indeed, while it is cheap—in terms of time and effort—for people to explore and gather information about security features, it can be expensive for them to actually activate those features. For example, activating Login Approvals would require people to spend an extra few seconds every time they “logged in” to their Facebook accounts. Taken together with the previous finding that people generally only enact security and privacy related behavior change after personally experiencing or hearing about a threat [18], and Egelman and colleagues’ finding that a “peer pressure” password meter did not raise people’s motivation to create stronger passwords relative to a non-social password meter [28], we expected that, in the short term, there would be no difference in security feature adoption rate among those who view social and non-social announcements.

**H5:** The adoption rate for the promoted security features should be about the same for those who view a social or a non-social announcement in the week following the experiment.
On the other hand, we expected that there should be a long-term increase in the overall security feature adoption among users in the social condition. While our experiment lacked a strong catalyst for security behavior change, we expected that people in the social conditions might more strongly retain the information that extra security features are available for when they do encounter a compelling catalyst (e.g., hearing about a security breach on the news or through a friend). As a number of highly publicized security vulnerabilities were surfaced in the five months following the experiment (including the widely publicized “Heartbleed” bug in OpenSSL [84]), we arrived at:

H6: The adoption rate for the promoted security features should be higher for those who view a social announcement compared to those who viewed a non-social announcement in the 5 months following the experiment.

Results
Out of the 50,000 people in our sample, 46,235 logged in to Facebook within the duration of the experiment and were shown an announcement. Across all conditions, 5971 (13%) people clicked on the announcement to explore the promoted security features, while 1873 (4%) people adopted one of the promoted security features within the following week, and 4555 (9.9%) within the following five months. In Table 15, we show an aggregated breakdown of clicks and adoptions across experiment groups. The raw data suggests that all social conditions had higher click-through rates than control, the best social announcements elicited higher adoption rates in the short and long term, and the “Raw #” announcement generally performed best of all.

<table>
<thead>
<tr>
<th>Group</th>
<th>N</th>
<th>Clicked</th>
<th>Adopted</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raw #</td>
<td>5862</td>
<td>846</td>
<td>280</td>
<td>623</td>
</tr>
<tr>
<td>Some</td>
<td>5828</td>
<td>835</td>
<td>243</td>
<td>602</td>
</tr>
<tr>
<td>Over #</td>
<td>5770</td>
<td>779</td>
<td>248</td>
<td>547</td>
</tr>
<tr>
<td>Only #</td>
<td>5668</td>
<td>748</td>
<td>225</td>
<td>548</td>
</tr>
<tr>
<td>Over %</td>
<td>5761</td>
<td>724</td>
<td>223</td>
<td>557</td>
</tr>
<tr>
<td>Only %</td>
<td>5708</td>
<td>714</td>
<td>221</td>
<td>555</td>
</tr>
<tr>
<td>Raw %</td>
<td>5953</td>
<td>730</td>
<td>225</td>
<td>573</td>
</tr>
<tr>
<td>Control</td>
<td>5685</td>
<td>595</td>
<td>208</td>
<td>550</td>
</tr>
<tr>
<td>Social vs. Non-Social</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Control</td>
<td>40550</td>
<td>4376</td>
<td>1665</td>
<td>4005</td>
</tr>
<tr>
<td>Social Number vs. Social Percent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td>17300</td>
<td>2373</td>
<td>753</td>
<td>1718</td>
</tr>
<tr>
<td>Percent</td>
<td>17422</td>
<td>2168</td>
<td>669</td>
<td>1685</td>
</tr>
<tr>
<td>Social Contexts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raw</td>
<td>11815</td>
<td>1576</td>
<td>505</td>
<td>1196</td>
</tr>
<tr>
<td>Over</td>
<td>11531</td>
<td>1503</td>
<td>471</td>
<td>1104</td>
</tr>
<tr>
<td>Only</td>
<td>11376</td>
<td>1462</td>
<td>446</td>
<td>1103</td>
</tr>
</tbody>
</table>

Table 15. Clicks and adoptions by experimental conditions. “N” represents the number of users who viewed the announcement. “ST” stands for short term, and “LT” stands for long term. These values are strictly descriptive. Statistical tests used and significance is mentioned where relevant in the text.

To statistically test whether and how the existence of, specificity, and framing of the social cue in the announcement affected click-through rate and security feature adoption, we ran three logistic regressions for clicks, short-term adoptions, and long-term adoptions. The response variables for our three models were, respectively, binary values representing (i) whether or not an individual had clicked on the announcement they were shown, (ii) whether or not an individual had adopted any of the three promoted security features in the 7 days following our experiment, and (iii) whether or not an individual had adopted any of the three promoted security features in the 5 months following the experiment. Our independent variable was which of the eight social announcement an individual had seen, and we also included, as controls, the behavioral, demographic, and social network descriptor variables listed in Table 14. For the two adoption models, we included an additional control
representing whether or not an individual had actually clicked on the announcement they were shown to "improve account security".

In Table 16, we show the logistic regression coefficients for our independent variables predicting clicks, short-term adoptions and long-term adoptions. Coefficients in Table 16 represent a change in "log-odds", or \( \ln \frac{P}{1-P} \), where P represents the probability that the user clicked on the announcement or adopted one of the three security features, depending on the model. A positive coefficient implies that the log-odds ratio increases, or that the variable for the coefficient increases the likelihood that the viewer clicked on the announcement or adopted a security feature. A negative coefficient implies the opposite. Furthermore, all variables are centered and scaled, such that the coefficient for each variable represents the expected change in log-odds that an individual uses a feature given a one standard deviation increase in the predictor variable, holding all other numeric variables at their means and categorical variables at their baselines. Additionally, larger absolute coefficient values imply a stronger relationship between the independent and dependent variables.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Clicked</th>
<th>Adopted 7-day</th>
<th>Adopted 5-month</th>
</tr>
</thead>
<tbody>
<tr>
<td>† Group: At Least #</td>
<td>0.29 *</td>
<td>-0.07 *</td>
<td>-0.13</td>
</tr>
<tr>
<td>† Group: At Least %</td>
<td>0.21 *</td>
<td>-0.12 *</td>
<td>-0.06</td>
</tr>
<tr>
<td>† Group: Only #</td>
<td>0.26 *</td>
<td>-0.16 *</td>
<td>-0.09</td>
</tr>
<tr>
<td>† Group: Only %</td>
<td>0.19 *</td>
<td>-0.12 *</td>
<td>-0.05</td>
</tr>
<tr>
<td>† Group: Raw #</td>
<td>0.36 *</td>
<td>-0.01 *</td>
<td>-0.001</td>
</tr>
<tr>
<td>† Group: Raw %</td>
<td>0.17 *</td>
<td>-0.15 *</td>
<td>-0.06</td>
</tr>
<tr>
<td>† Group: Some</td>
<td>0.35 *</td>
<td>-0.18 *</td>
<td>-0.03</td>
</tr>
<tr>
<td>Tool-using friends</td>
<td>0.09 *</td>
<td>0.17 *</td>
<td>0.20 *</td>
</tr>
<tr>
<td>Intercept</td>
<td>-2.16 *</td>
<td>-5.23 *</td>
<td>-2.62 *</td>
</tr>
<tr>
<td>Age</td>
<td>-0.01</td>
<td>-0.19 *</td>
<td>-0.18 *</td>
</tr>
<tr>
<td>Gender: Male</td>
<td>-0.03</td>
<td>-0.06 *</td>
<td>-0.13 *</td>
</tr>
<tr>
<td>Account length</td>
<td>0.11 *</td>
<td>0.03</td>
<td>0.03</td>
</tr>
<tr>
<td>Friend count</td>
<td>-0.16 *</td>
<td>-0.06 *</td>
<td>-0.15 *</td>
</tr>
<tr>
<td>Mean friend age</td>
<td>0.14 *</td>
<td>-0.16 *</td>
<td>-0.24 *</td>
</tr>
<tr>
<td>Friend age entropy</td>
<td>0.03</td>
<td>0.28 *</td>
<td>0.26 *</td>
</tr>
<tr>
<td>Percent male</td>
<td>0.02</td>
<td>0.08</td>
<td>0.13 *</td>
</tr>
<tr>
<td>Mean friends days since confirmed</td>
<td>0.007</td>
<td>0.003</td>
<td>-0.08 *</td>
</tr>
<tr>
<td>Friend country entropy</td>
<td>0.04 *</td>
<td>0.04</td>
<td>0.03</td>
</tr>
<tr>
<td>Mean number of friends of friends</td>
<td>-0.04</td>
<td>-0.09 *</td>
<td>-0.09 *</td>
</tr>
<tr>
<td>Posts created</td>
<td>0.05</td>
<td>0.02</td>
<td>-0.02</td>
</tr>
<tr>
<td>Posts deleted</td>
<td>-0.008</td>
<td>0.02</td>
<td>-0.002</td>
</tr>
<tr>
<td>Comments created</td>
<td>0.09</td>
<td>0.07 *</td>
<td>0.10 *</td>
</tr>
<tr>
<td>Comments deleted</td>
<td>0.07</td>
<td>-0.13 *</td>
<td>-0.01</td>
</tr>
<tr>
<td>Friends added</td>
<td>-0.003</td>
<td>0.004</td>
<td>0.02</td>
</tr>
<tr>
<td>Friends removed</td>
<td>-0.004</td>
<td>0.01 *</td>
<td>0.02</td>
</tr>
<tr>
<td>Photos added</td>
<td>0.03 *</td>
<td>0.004</td>
<td>0.03</td>
</tr>
<tr>
<td>Clicked on Announcement</td>
<td>N/A</td>
<td>4.38 *</td>
<td>1.94 *</td>
</tr>
</tbody>
</table>

† Baseline: Control, * p < 0.05

Table 16. Coefficients for the three regressions predicting clicks, feature adoptions up to a week after the experiment, and feature adoption up to 5 months after the experiment. Bolded coefficients are of interest.

For example, the tool-using friends variable (i.e., the number of one's friends who use security features) coefficient for the "clicks" model is 0.09; thus, a one standard deviation increase in this variable increases the log-odds that a viewer clicks on the announcement by 0.09, and the actual odds by \( e^{0.09} = 1.09 \). More concretely, our model predicts that someone with 80 security feature-using friends (one standard deviation above the mean) is 9% more likely to have clicked on the security announcement, compared to the average person in our sample.

From Table 16, we can see that, relative to the control condition, all social experiment conditions do elicit higher click-through rates for announcements, as evidenced by the positive and significant coefficients for every experiment condition coefficient. The "Raw #" (b_click=0.36, p<0.001) condition had the highest click through rate, at 14.4%—a substantial 37% increase relative to control. Even the
least effective social condition—the “Raw %” ($b_{clicked}=0.17$, $p<0.001$) condition—significantly enhanced click-through rate relative to control, up to 12.3%. There does, therefore, appear to be strong evidence in favor of $H_1$—that all social conditions will improve click-through rate relative to the control condition. The effect is both significant and substantial.

There is also support for both $H_{2a}$ and $H_{2b}$—that people with more security-tool using friends will be more likely to click on the announcement and adopt a promoted security tool. The tool-using friends variable ($b_{clicked}=0.09$, $p<0.05$; $b_{adoptions}=0.17$, $p<0.05$; $b_{adoptions-smo}=0.20$, $p<0.001$) has a large and positive coefficient for all three models, suggesting that viewers who see that more of their friends use optional security tools are more likely to click on the announcement and actually adopt a security tool relative to the average person in our sample (with all numeric variables at the mean and categorical variables at the baseline).

The data, however, is not as clear in its support for the hypothesis that social framings that suggest more rather than fewer of a viewer’s friends use security tools will be more effective at driving click-through rate on the security announcement. There does appear to be support for $H_{3a}$—that number conditions will outperform percent conditions in driving click-through rate on the security announcement. Indeed, all number conditions significantly outperformed all percent conditions, and, in aggregate, number conditions elicited 7% more clicks than percent conditions ($\chi^2(1, n=34,722)=12.3$, $p=0.0004$). However, we found no support for $H_{3b}$—that the “Raw” framing would outperform the “Over” framing, which, in turn, would out perform the “Only” framing in driving click-through rate. While the aggregated click-through rate of these framings do fall into the expected sequence (Raw=13.3%, Over=13.0%, Only=12.9%), the difference is not significant despite massive power ($\chi^2(2, n=34,722)=1.2$, $p=0.54$).

Thus, while social announcements that suggest that more rather than fewer of a viewer’s friends are currently using extra security features can be more effective at getting people to click on the announcement, the specific framing of the social text does not appear to significantly impact its click-through rate.

Relatedly, we found evidence to contradict $H_4$—that ambiguous social framings such as the “Some” framing will be less effective at driving click-through rate for the announcement. In fact, the “Some” ($b_{clicked}=0.35$, $p<0.001$) framing is the second most effective group in driving click-through rate, after the “Raw #” ($b_{clicked}=0.37$, $p<0.001$) condition, with an overall click-through rate of 14.5%.

We derived $H_4$ from a simple understanding of social proof—if people look to their friends for cues on how to act during periods of uncertainty, then ambiguous cues are probably less effective than clear cues. However, in reality, the ambiguity appears to elicit more interest in the announcement than most of the more specific social framings. Perhaps this finding can be explained by the intuition that people may overestimate the number of their friends who use security features when it is left ambiguous. Future work can validate this hypothesis by looking at the discrepancy between people’s perceptions of the number of their friends who use security tools relative to the actual number of their friends who use security tools.

Next, there appears to be support for $H_5$—that social prompts will not be significantly more effective at driving feature adoption in the short-term than non-social prompts. Indeed, all of the coefficients for the social conditions are insignificant in the short-term adoptions model in Table 16. We expected this result for two reasons: (1) people usually only adopt security tools after experiencing a “catalyst” for security behavior change—for example, in the form of experiencing a security breach or hearing about a security breach [18], and (2) the social text is not reinforced in the security interstitial where people must actually make the decision to adopt a security feature—thus, as with Egelman and colleagues’ study [28], potential adopters are not given enough social context at the moment of potential behavior change—for example, who among their friends use what security tools.

More surprising, however, is that this negative result holds even for long-term adoptions, disconfirming $H_6$—that social announcements will be significantly more effective at driving security feature adoption in the long term relative to the non-social announcement. In the 5 months following the experiment, a number of widely publicized security vulnerabilities that could have served as
catalysts for security behavior change were highly publicized (e.g., Heartbleed [84], the iOS SSL bug [85]). Nevertheless, there was no significant difference in adoption rate between those who saw the social and non-social announcements, perhaps because the social announcements were not more memorable. We also note, however, that H6 may in fact be valid, but only with respect to relevant security threats that are presented on time and in context: Activating Login Approvals would not be a direct answer to Heartbleed or the iOS SSL bug, so the latter may not have easily triggered a memory of the former.

Importantly, the immediate cascading effects of raising people’s awareness of security features should not be ignored. While there is no significant difference in the rate of feature adoption between people who clicked on either the social or non-social announcement, as significantly more people clicked on the social announcements, many more people who saw social announcements also actually adopted security features. Indeed, from Table 15, we can see that 280 of 5862 (4.8%) people shown the “Raw #” announcement adopted one of the promoted security features over the 7 days following the experiment, compared to just 208 of 5685 (3.7%) people shown the non-social announcement ($\chi^2(1, n=11,547)=8.7, p=0.003$). In other words, significantly more people who saw a social announcement adopted the promoted security features because significantly more people clicked on the social announcements.

Summary of Results from Initial Experiment
We found that increasing the observability of security tool usage can be effectively used to increase both awareness of and adoption of available security features. Furthermore, this effect increases with the number of the viewer’s friends who use security tools. While neither the framing of a social cue nor its specificity appeared to have a large effect on raising click-through rate, social announcements that rendered the number of a viewer’s friends that used security tools, rather than the percent of the same, elicited higher click-through rates. On the other hand, we found no evidence that the social proof cues we tested, which were aggregated and anonymous, were more effective than a non-social announcement at raising a viewer’s motivation to use the promoted security features. Indeed, the rate of feature adoption among viewers who clicked on any of the announcements were non-significantly different despite massive statistical power.

Follow-up Study With Survey to Gauge Sentiment and Awareness
To more concretely measure whether our announcements increased people’s awareness of available security features, we ran a second deployment of our best performing announcements from the initial experiment and collected survey responses.

Methodology
We re-ran a second campaign of our experiment with a separate set of n=50,000 people, randomly sampled among across users who used Facebook in English, logged in to Facebook at least once in the past month, and had at least 10 friends who used security features. People in our sample were shown one of three announcements mirroring the announcements in the previous experiment: the unambiguous “raw number” social condition, the ambiguous “some” social condition, and the non-social control condition—all exactly matching the corresponding condition from the initial experiment. All announcements were once again outfitted with an “Improve Account Security” button that, when clicked, would navigate the clicker to an interstitial that explained the promoted security tools, as well as allowed viewers to enable the same. The follow-up study ran between December 20th and December 22nd, 2013.

In this second campaign, we also asked people to complete a short survey with the following 3-point Likert-scale question: Facebook provides me with the necessary security settings to protect my account (i.e., the “Provides security tools” statement). We decided to ask this question to test whether social information in the announcement influenced people’s perceptions of the security tools we promoted—namely, whether a viewer believed the tools were sufficient to address their security concerns.

We had three methods to solicit survey responses. First, we surveyed people who fully navigated through the interstitial (i.e., the “interstitial” solicitation group). We separately sent the survey to
people who saw an announcement but never clicked on it (i.e., the “viewed announcement” solicitation group), and also to a random sample of 80,000 people who used Facebook in English, logged in to Facebook at least once in the past month, and who never viewed any of our security announcements (i.e., the “holdout” solicitation group).

In total, we had 2814 responses to our survey. Table 17 shows a tabulation of the how many users per experimental condition and survey solicitation method.

<table>
<thead>
<tr>
<th></th>
<th>Holdout</th>
<th>Non-Social</th>
<th>Raw #</th>
<th>Some</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interstitial</td>
<td>0</td>
<td>498</td>
<td>226</td>
<td>254</td>
</tr>
<tr>
<td>Viewed Announcement</td>
<td>0</td>
<td>127</td>
<td>72</td>
<td>67</td>
</tr>
<tr>
<td>Holdout</td>
<td>788</td>
<td>322</td>
<td>214</td>
<td>246</td>
</tr>
</tbody>
</table>

*Table 17. Number of survey responses per solicitation method (rows) and experimental group (columns).*

**Results**

Table 18 shows the coefficients for a proportional-odds logistic regression [35] predicting the likelihood of an individual selecting a higher value of agreement with the “Provides security tools” statement previously explained. Coefficients in Table 18 represent a change in “log-odds” that the user selected “neutral” over “disagree” or “agree” over “neutral” as a response to one of the questions. We included the viewer’s experiment group as well how they were solicited to complete the survey as independent variables, and included the behavioral, demographic and social network descriptor variables described in Table 14 as controls.

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Provides security tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>† Group: Non-Social</td>
<td>-0.08</td>
</tr>
<tr>
<td>† Group: Raw #</td>
<td>-0.19</td>
</tr>
<tr>
<td>† Group: Some</td>
<td>-0.16</td>
</tr>
<tr>
<td>Δ Solicitation: Interstitial</td>
<td>1.04 *</td>
</tr>
<tr>
<td>Δ Solicitation: Viewed Announcement</td>
<td>0.16</td>
</tr>
<tr>
<td>Feature-using friends</td>
<td>-0.13</td>
</tr>
<tr>
<td>Age</td>
<td>0.04</td>
</tr>
<tr>
<td>Gender: Male</td>
<td>0.15</td>
</tr>
<tr>
<td>Account length</td>
<td>0.20 *</td>
</tr>
<tr>
<td>Friend count</td>
<td>0.25 *</td>
</tr>
<tr>
<td>Mean friend age</td>
<td>-0.14</td>
</tr>
<tr>
<td>Friend age entropy</td>
<td>0.07</td>
</tr>
<tr>
<td>Percent male</td>
<td>0.03</td>
</tr>
<tr>
<td>Mean friends days since confirmed</td>
<td>-0.57 *</td>
</tr>
<tr>
<td>Friend country entropy</td>
<td>0.005</td>
</tr>
<tr>
<td>Mean number of friends of friends</td>
<td>-0.08</td>
</tr>
<tr>
<td>Posts created</td>
<td>0.02</td>
</tr>
<tr>
<td>Posts deleted</td>
<td>-0.07</td>
</tr>
<tr>
<td>Comments created</td>
<td>-0.06</td>
</tr>
<tr>
<td>Comments deleted</td>
<td>0.05</td>
</tr>
<tr>
<td>Friends added</td>
<td>0.05</td>
</tr>
<tr>
<td>Friends removed</td>
<td>-0.05</td>
</tr>
<tr>
<td>Photos added</td>
<td>-0.001</td>
</tr>
</tbody>
</table>

† Baseline: Holdout; Δ Baseline: Holdout, *p < 0.05

*Table 18. Coefficients for the two proportional-odds logistic regressions predicting agreement with the trustworthy and protection statements.*

† Baseline: Holdout; Δ Baseline: Holdout, *p < 0.001

Just as in the previous study, a positive coefficient implies that the log-odds ratio increases, or that the variable for the coefficient increases the likelihood that the user selected “neutral” over “disagree” or “agree” over “neutral”. A negative coefficient implies the opposite. Furthermore,
predictor variables were centered and scaled, such that each coefficient represents the expected change in log-odds that the user selected a higher value response given a one standard deviation increase in the predictor variable, holding all other numerical variables at their means and categorical variables at their baselines.

From Table 18, there appears to be no significant effect of viewing any of the security announcements on people’s agreement with Facebook providing necessary security features, helping to explain why we saw the same adoption rate among both those who saw social and non-social announcements. Indeed, none of the coefficients for the “Group” variable were significant.

On the other hand, people who actually clicked on the announcement and navigated through the security interstitial were significantly and substantially more likely to agree with the “Provides security tools” statement ($b$=1.04, $p<0.001$) statement. Thus, while showing people security announcements with social information does not appear to directly affect people’s sentiment towards Facebook’s security tools, social announcements drive more people to the security interstitial and thus can at least indirectly raise their awareness or available security tools and their belief that those security tools are effective.

General Discussion
In a nutshell, our results suggest that social proof is a promising approach to increase people’s security sensitivity, but it is not a panacea. People who saw announcements with social proof cues that increased the observability of security tool usage were more likely to click on the announcement. Clicking on this announcement, in turn, increased viewers’ (i) awareness of available security tools, (ii) their likelihood to adopt one of those tools, and (iii) their sentiment towards the efficacy of the promoted tools. However, the aggregated, impersonal social information we showed people only seemed to raise their interest in exploring security features—we did not find strong evidence that the social proof cues, themselves, were more effective than a non-social announcement in increasing people’s likelihood of actually adopting one of the promoted security tools (though our results do not prove the opposite, either).

**Aggregate social proof cues can raise people’s interest in exploring available security tools.** The positive effect of these social announcements on click-through rate is especially strong when viewers have many friends who use security tools and when that information is rendered directly in the announcement, as with our “Raw #” announcement—a finding aligning with both the concept of social proof [15] and the diffusion of innovations [61]. This result suggests that the positive effect of these social cues will strengthen over time as more and more people start using security tools (and thus higher and higher numbers will be rendered in the announcement). We also found evidence that social announcements indirectly appeared to increase viewers’ belief that the security features they needed to secure their accounts were available. Indeed, people who viewed a social announcement were far more likely to click on the announcement and navigate through the resulting security interstitial, and people who navigated through the security interstitial far more likely to agree that Facebook provided them with necessary security tools.

**However, these social proof cues, alone, were not more effective at getting people who clicked on the announcement to actually adopt a promoted security tool.** Thus, used alone, the social announcements we tested appeared to be no better than a non-social announcement at raising users motivation to adopt the promoted security features. This finding holds true in both the short and long term, even through a number of widely publicized security vulnerabilities including Heartbleed [84] and the iOS SSL implementation bug [85] that could have been potential catalysts for security behavior change [18]. Nevertheless, as more people who saw a social announcement clicked on the announcement and explored the promoted security tools, significantly more people who saw a social announcement adopted one of the promoted security features. There was, thus, an indirect increase in security tool uptake as a result of showing people a social announcement.

**Social proof cues might be more effective if more personal and shown in context.** Importantly, our findings do not suggest that social cues are ineffective at raising people’s motivation to use security tools. Rather, our null result at raising motivation was likely an artifact of the fact that the prompts we tested were aggregated, out of context and not very informative. For example, showing
someone an announcement that 100 of her friends use security tools does not inform her why those friends use security tools, which security features are being used (or for what purpose), who among her friends are using those security features, and whether or not her friends would actually recommend using those tools. In other words, our absence of results in raising motivation may be due to lack of compensation for an invalid context—i.e., asking people to consider extra security tools when they are not really thinking about security. Accordingly, motivation to adopt security tools might be best driven by a paired approach of security threat detection followed by a timely delivery of a security announcement with social cues.

Taken together, in this experiment, I have provided some experimental evidence that simple social proof cues can be used to raise peoples’ security sensitivity—specifically, their awareness of available security tools. Furthermore, using these simple social cues may have the additional indirect benefits of raising security tool adoption and people’s sentiment towards the promoted tools, as well. Care should be taken, however, to sparingly surface these announcements so that people do not get desensitized to them. For example, to maximize the efficacy of a campaign to raise security sensitivity, social announcements should probably only be shown once every few months to people who already have many friends who use the security tools promoted in a campaign.

Future Work

Our results suggest that social proof cues that raise the observability of security tool usage among one’s friends is promising at raising people’s interest in exploring optional security tools. However, we found no evidence that the cues we tested were effective, by themselves, at raising people’s motivation to use those tools. Furthermore, we did not test whether social proof cues could increase people’s knowledge of security tool and behaviors. Accordingly, these results offer a number of fruitful opportunities for future work.

First, it is possible that the reason our social cues were ineffective at raising motivation is because they were presented out-of-context, because they were impersonal, and because they provided no context as to whether or not the friends who used those security tools would recommend using those tools. In Chapter 7, I discuss some proposed work in which I plan to run a similar experiment, outside of the Facebook context, with more personal social proof cues that are presented in-context (e.g., after the user has seen an article about security or privacy). I also plan to run this experiment with participants from both within and outside of the U.S. to explore if people from different cultural origins respond differently to social proof cues.

This work also does not speak to the efficacy of social proof in increasing people’s knowledge of how to use security tools and behaviors. In Chapter 7, I will discuss a thread of research in which we will aim to experimentally evaluate whether social proof can be used to increase people’s knowledge of security through sharable internet quizzes.

Finally, while this work increased the observability of security tool usage with announcements, the tools themselves remain unaltered and unobservable. In Chapter 7, I discuss some proposed work in which I plan to build and evaluate a few example “social” cybersecurity tools with the theoretical insights I derived from my initial theorybuilding work in mind: specifically, that security tools should be observable, socially inclusive, and allow people to be more accountable for the security of their friends and loved ones.
Chapter 7: Proposed work

My preliminary work on social cybersecurity offers empirical evidence that social factors are not only key to understanding why security tools remain little known and scarcely used, but that they can also be leveraged to increase people’s awareness of, motivation to use and knowledge of how to use security tools—i.e., their security sensitivity. This prior work has focused on two threads of research: observational research to understand how social factors affect security sensitivity “in the wild” (Chapters 3-5), and experimental work that validates the causal links between social proof and security sensitivity (Chapter 6). Nevertheless, there remain a number of open questions that I hope to address in my proposed work. Accordingly, in my proposed work, I intend to expand on these two threads of research as well as spawn a new thread of research: system development. In the following subsections, I describe my proposed work across all three threads of research. Figure 9 summarizes how my proposed work and preliminary work fits into the broader theme of social cybersecurity.

![Diagram of Social Cybersecurity]

**Figure 9. Summary of preliminary and proposed work in this thesis. I propose to do additional observational analysis, experimental testing and develop a social cybersecurity system for my thesis.**

**Proposed Observational Work**

**Viral Security Behavior Surveys**

Based on my preliminary work in Chapter 3: A Typology of How Social Influence Affects Security Behaviors, I introduced a typology of social catalysts for security-related behavior change. However, as with most qualitative studies, it is restricted in its generalizability: we recruited only from Pittsburgh, and only 19 people. Thus, this typology is unlikely to be exhaustive. Furthermore, the relative frequency of these social catalysts is unclear—how often is security related behavior change
a result of a social catalyst? And, among those that are, which catalysts are most frequent? Finally, to fit within an hour, the interview study was necessarily direct in its definition of security behaviors. Indeed, we asked participants specifically about mobile authentication, application installations, social media privacy, and password construction in order to keep the discussion grounded on actual experiences as opposed to hypotheticals. But, there are other security behaviors that should be affected by social influence: for example, the use of secure messengers. These unstudied behaviors, in turn, might be spread through social catalysts we have not yet captured in our typology.

To address these and other limitations, I propose to run an additional study: a large-scale survey in which I will seek to generalize the social catalysts typology we uncovered in our initial interview with a larger, more representative sample of internet users. The survey will mimic our interview study in structure. We will ask participants about recent security-related behavior changes across a broad set of security and privacy behaviors—including the four we asked about in our interviews. This broader set of security and privacy behaviors will be defined by reviewing the background literature on end-user facing security behaviors, but might include, for example: providing fake information on account creation forms, using onion routing, or encrypting communications / using secure messengers. Participants who answer affirmatively to enacting at least one of these behaviors will be asked to elaborate on why. Specifically, they will be presented with our initial typology of catalysts for behavior change and asked to select if any of them apply. They will also be provided an “Other” option in case none of our existing categories apply, and, if so, they will be asked to briefly explain. If participants select a social catalyst, e.g., “observing others”, they will also be asked to define who were the other parties involved and the context surrounding the triggering event (again, through multiple selection check-box options derived from our interview study results). We will also collect some meta-information from participants, such as their demographics (age buckets, self-identified gender) as well as a measure of their security and privacy knowledge and attitudes (with, for example the Security Behaviors Intention Scale [27] and the IUIPC [52]).

I will run the study on a number of online participation pools to get a more representative sample of internet users. These online participation pools will include Amazon’s Mechanical Turk and participants found through advertisements on Facebook and Google Search. I will also run a shorter version of the survey on Google Consumer Surveys. The target sample will include participants from at least the U.S. and India to get perspectives from cultures that have previously been shown to have differing privacy and security attitudes [46].

The results from this survey should afford us a number of additional insights that we could not capture in the initial interview study. Specifically, the expected contributions of this proposed work should include:

- The frequency of socially triggered security behavior change for recent security behaviors
- The relative frequency of different social catalysts for behavior change.
- An expansion of our initial typology of social catalysts for behavior change, or a validation of our initial typology as being exhaustive (less likely).
- A correlational analysis relating various meta-variables to the frequency of socially triggered security behavior changes and the relative frequency of different social triggers. The meta-variables I plan to test include: a participant’s country of origin, their security and privacy knowledge, their security and privacy concern, and their demographic background.

**Security Information Dissemination Surveys**

Based on the same interview study, in Chapter 4: Understanding How Security Information Is Communicated I introduced a typology of security related conversations that people have with others. However, this work is also limited in its generalizability given that we were only able to interview 19 people, and because many of the conversations that people reported having were directly related to the behaviors we were studying. But, I suspect that there are other conversations about security not specifically related to the security behaviors we studied. Furthermore, in our interview study, participants responses were necessarily biased by recency. Indeed, we specifically asked participants to recall their most recent conversations about security and privacy. Accordingly, there may be many other conversations about security that participants have throughout their lives.
that were not well represented by the typology I introduced in Chapter 4: Understanding How Security Information Is Communicated.

To get a more wholistic understanding of how social factors influence people's knowledge about security, I propose to run an additional study: a series of surveys in response to breaking news events about security. Often, there are news stories about security breaches (e.g., the Sony hack), government announcements about security (e.g., the 2015 Obama administration's State of the Union address), or new security and privacy technology (e.g., the Google privacy checkup). In our interview study, we identified that these news articles about security are often how participants learn information about security or at least inspire conversations about security through which they learn. My goal with this supplementary study is to better understand these conversations that are triggered by security news—specifically, how people hear about this news (e.g., do they hear about it from others or do they seek out the information) as well as if and why they reshared this information.

For a subset of security-related news stories, we will run a survey shortly after the publishing of the articles to capture whether participants have heard about these stories and, if they have, how and from who they heard about these stories as well as if and why they reshared the story with others. We will ask participants whether they heard about a particular news incident and, if they answer affirmatively, ask them two "knowledge" questions which we will craft for each news story. These knowledge questions will ask participants simple semantic information about the events and will serve to validate their responses. Participants will then be asked how they heard about the story. The sources will include a variety of options based on the typology I defined in Chapter 4. If participants pick a social source (e.g., social media or someone else), we will ask for more information about who was that social source as well as how the social source shared the information. We will then ask participants if they, themselves, reshared the information with anyone. If they did, we will ask who they shared the information with, why, and how. We will also collect some meta-information from participants, such as their demographics (age buckets, self-identified gender) as well as a measure of their security and privacy knowledge and attitudes (with, for example the Security Behaviors Intention Scale [27] and the IUIPC [52]).

I will run the surveys about 7-days after the initial news incident on Amazon's Mechanical Turk. I will solicit 100 responses per article, and expect to run it for as many articles as our funds will allow over the course of the next few months. The target sample will include participants from the U.S. [46].

The results from this survey should afford us a number of insights that we could not capture in the initial interview study. Specifically, the expected contributions of this proposed work include:

- A rough understanding of how many people hear about different security news events.
- An understanding of how people hear about these incidents: whether from conversations or specifically seeking the stories out.
- An understanding of why and how people reshare security news information.
- A correlational analysis relating various meta-variables to how people get security news and whether they reshare that news. The meta-variables I plan to test include: a participant's security and privacy knowledge, their security and privacy concern, and their demographic background.

Proposed Experimental Work

Social & Contextual Privacy Notifications

People often ignore security and privacy notifications: especially preventative notifications that are not shown in response to an immediate threat. Examples of preventative notifications include announcements promoting the use of new security tools and announcements about updates to privacy policies. One reason people ignore these warnings may be because they provide little perceived value. In a large-scale field investigation of the types of mobile notifications people receive, prior work has found that people primarily find value in two types of notifications: social notifications that inform people of what their friends have said and done, and contextual notifications that inform people of something relevant to the here and now [65]. The same work showed that people least value notifications about "system updates". Most present security and privacy
notifications, especially those that are preventative rather than reactive, are more like the latter than the former.

My own initial experimental work in Chapter 6: Increasing Security Sensitivity with Social Proof reinforces the intuition that showing people social cues in preventative security announcements should significantly increase click-throughs on those announcements. However, there were a number of limitations with that work that offer fruitful opportunities for further exploration.

First, in that work, I was focused directly on measuring changes to objective behaviors. Accordingly, there was a missed chance to better explain the underlying mechanism that should have driven the behavioral measures: changes in perceived value. As such, in follow-up work, it would be pertinent to directly measure perceived value to more concretely establish the relationship between social cues - > perceived value - > behavior change.

Second, I was only able to test impersonal and out-of-context social cues. Knowing that "Jason H., Laura D., Jeff B., and Doug T." did something should have a measurably distinct effect on perceived value than knowing that "4 of your friends" did something. Similarly, getting a notification about updating your password after reading an article about cracked passwords should also have a greater effect on perceived value than getting the same notification after just logging into Facebook.

Third, there was no information presented about whether friends recommended the promoted security tools. It may be that if people saw direct recommendations from their friends, then they would perceive even more value from the social cue than if they just saw what their friends did.

Fourth, I only tested these social cues with people from the U.S., when there is a host of literature that suggests that social cues are more or less effective across people from different cultures.

Finally, I only tested social cues from one contributing social group: friends. There may be many other social groups that yield effective results, such as privacy and security experts, or other people who share a similar demographic or context (e.g., other males, other people who read Gizmodo).

Accordingly, I propose an additional experiment to fully or partially address the aforementioned limitations and further our knowledge of how social cues interact with the perceived value of security and privacy notifications to drive security and privacy behaviors and decision making.

The experiment will run on Mechanical Turk over two sessions and employ some light deception. I will be promoting a security/privacy tool, as I did in the Facebook experiment. However, participants, from both India and the U.S., will be recruited under the pretense of completing a study designed to understand what affects people's decisions to share online articles. Under this pretense, in the first session participants will be asked to provide some information about their close friends and expert friends names. They will also be asked to provide some demographic information. There will be two sessions. They will then go through a distractor task in which they will read an article and answer some distractor questions about it (such as whether they would share it with the friends they earlier named).

Participants will be invited to come back for a second session a few days later. They will be presented with one of two articles: one group will read an article about a security/privacy tool we will promote, and the other group will read an article unrelated to security and privacy. While reading their assigned article, participants will be interrupted with a notification promoting the selected security/privacy tool. The notifications will vary in: contributing social group (e.g., named close friends, demographically similar people, named expert friends) and social action (i.e., trending or recommended). I will track a variety of behavioral metrics of participants' interacting with the notification. After participants dismiss the notification, they will be redirected to a questionnaire in which they will be asked questions to gauge their comprehension of the notification as well as their perceived value of the notification.

In my analysis, I will test: (1) how contributing social group, country of origin, social action and contextual relevance affected perceived value and (2) how perceived value correlates with
comprehension and click-through rate. Through this experiment, I expect the following contributions:

- A definition of and a validated scale to measure the perceived value of security and privacy notifications.
- An understanding of how contributing social group, country or origin, social action and contextual relevance affects the perceived value of security and privacy notifications.
- An understanding of how perceived value correlates with comprehension of and behavioral response to security and privacy notifications.

**Proposed System Development Work**

My initial observational and experimental work offers at least three broad insights relevant to the design of more socially compatible security and privacy tools: observability, inclusiveness and stewardship. To recap, security tools should be designed to be observable so that their use can spread through social proof; when possible, they should be inclusive so that their use is a sign of trust in friends and loved ones rather than unfounded paranoia; and, when possible, they should allow for people to act as stewards for their loved one's security and privacy. Grounded on these theoretical insights, I hope to design, implement and evaluate a novel security tool to explore the design space of social cybersecurity.

**Thumbprint**

Robust authentication is an essential component of all secure spaces and systems [36]. Yet, authentication research has traditionally served just two types of users: (1) large organizations that have a strict need to keep out unauthorized individuals; and, (2) individuals who need to restrict access to only themselves for sensitive accounts, such as bank accounts and password managers. Accordingly, there has been a heavy focus in authentication research on having strict outsider rejection—i.e., forbidding access from malevolent entities—to the exclusion of everything else. However, this unilateral focus on outsider rejection is not socially compatible, and has resulted in tools that underserve small, local groups of individuals who collectively own or share resources and largely trust each other.

Three examples of these underserved groups are families who share game consoles and smart appliances like the Nest thermostat; small research labs who share access to office supplies; and, student organizations who collectively own sports equipment. The shared resources of these local groups typically have significant physical security: they are generally in homes or university campuses, which automatically reject most dangerous outsiders through centuries of anti-burglary regulation. As a result, while strict outsider rejection remains important for these groups, it should not be prioritized to the exclusion of all other needs. Usability, of course, is always important. Any authenticator should be fast and simple if it is to see widespread use. But, what else?

Despite the prevalence of these local group units, their authentication needs have scarcely been studied in their own right. Nevertheless, through a survey and synthesis of the existing literature on social psychology and usable security, I identified at least four considerations outside of outsider rejection that should be important.

First is **facilitating shared responsibility**. Responsibility for the well-being of the group is often distributed across many or all members [47,51], so individuals may be resistant to weighty security solutions that require a large personal investment. Accordingly, outsider rejection should not come at the price of large personal investments of effort from individual group members. Second is **member identification**, which allows for audit logs, tiered access to resources, and personalization. Indeed, social group structures vary widely [79]. If group structures are hierarchical, then members with higher status may require greater access than those with lower status. To afford this functionality, individuals should be identifiable. Nevertheless, individual identification should not come at the expense of **inclusiveness**. Requiring individuals to keep track of their own secrets to access shared group resources is cumbersome and could lead to non-compliance [53]. Furthermore, it is contradictory to require individual secrets to access shared resources: Rather, groups should have a shared secret that reinforces group bonds. Fourth, groups that are built off of a common-
identity (e.g., tennis clubs), rather than a common bond (e.g., families, close friends), also likely have a lot of churn; i.e., they might frequently gain new members and lose old members [57]. For these groups, it should be easy to share access with new members while also facilitating revoking access from old members. However, there remains a need to uncover new and empirically validate the aforementioned local group authentication needs, as well as to understand the relative importance of these needs for different groups. In practice, local groups are diverse, and different types of groups will weigh certain needs higher than others. For example, families sharing Xboxes might care a lot about individual identification, whereas small work groups sharing office supplies might care a lot about sharing and revoking access from new and old members.

One thing that is certain is that few existing security solutions support the aforementioned needs as core functionality. Presently, there are two approaches local groups must take to protect their shared resources: (1) individual members must independently authenticate with their own “secrets” (e.g., by swiping their personal keycard or entering their own password), or (2) every group member is given a single shared secret (e.g., a physical key or a group password/PIN). Both of these solutions fall short. The first solution provides individual identification but is not inclusive, nor does it make it easy to share and revoke access between new and old members, nor does it facilitate shared responsibility (individuals can slack in creating a strong secret and thus compromise the whole group’s security). The second solution is inclusive and evenly distributes responsibility, but does not identify individuals. It is sometimes easy to share access (e.g., by sharing a password, but not if using physical keys and there are more members than keys). And, it is generally difficult to revoke access (e.g., it might require tracking down old members who have physical keys). Thus, there is a need for new security solutions that better meet the security needs of local groups.

To bridge these gaps in both theory and practice, I propose Thumprint. With Thumprint, groups create a single shared group secret by “thumping” a small, solid object on a surface instrumented with an accelerometer and microphone. The “secret” is the combination of the object being thumped and the manner in which it is thumped. Thumprint should still be able to identify individual group members by the unique way in which they enter the group secret. Thumprint should also be easy to share given its observability. An existing group member with administrative privileges can simply show new a new group member the group secret, upon which time the new member can register herself by entering the group secret a number of times. Revoking access should be as simple as mapping an identified users’ privileges to no access. Furthermore, security responsibility is equally shared across all group members and does not require any individual to invest a disproportionate amount of effort to ensure the group’s security. I plan to run two evaluations of Thumprint: a technical evaluation and a social evaluation.

Technical Evaluation
The purpose of the Technical evaluation will be to answer the following questions:

• Can different thumprints be reliably distinguished from each other?
• Can individuals consistently replicate their own thumprints?
• How successfully can pre-registered users who are entering the same thumprint be distinguished from one another?
• How successfully can non-registered users with different capabilities simulate group members?

To answer these questions, I will run a series of lab studies. First, I will collect a set of small, solid everyday objects that have different material properties and recruit a number of individual participants to create a host of simple and complex thumprints. I will also video record them entering
these thumprints. In a subsequent session at least one day later, I will have participants re-enter their thumprints. I will also have participants replicate other participants’ thumprints with different affordances to simulate various local adversaries. For example, some participants will be given the video recording and the exact token used while others will be given only the correct token used with no video recording. I will then run a series of offline analyses to answer the aforementioned research questions. Specifically, I will do the following to answer each question:

**Can different thumprints be reliably distinguished from each other?**

I will create a multi-class classification model to distinguish between different thumprints. A unique thumprint will be considered to be any thumprint consisting of the same object and thumping pattern entered by a particular participant. Models will be trained on an 80% split of the data, and tested on the remaining 20% split.

**Can individuals consistently replicate their own thumprints?**

I will train a one-class classifier on a participants thumprint registration attempts from the first session, and test it on her attempts from a subsequent session.

**How successfully can pre-registered users who are entering the same thumprint be distinguished from one another?**

I will train a multi-class classification model consisting of some number of users entering the same Thumprint (defined as the same object thumped in the same way). The model will, again, be trained on an 80% random split of the available data and tested on a 20% split.

**How successfully can non-registered users with different capabilities simulate group members?**

I will train a mutli-class classification model consisting of some number of users entering the same Thumprint. I will also train a one-class classifier for each individual participant. I will then take the “adversary” attempts from the study and run them through the multi-class classifier to obtain the group member that the adversary best replicates, and then test the adversarial attempt against the one-class classifier of that group member. I will gauge how many times an adversary can succesfully “fool” the one-class classifier, and compare the success rate across different adversaries.

The technical evaluation will be useful in identifying whether or not Thumprint is feasible as well as what signal processing methodologies need to be implemented in real time in order to get Thumprint to work in a field deployment. My preliminary tests have already shown that Thumprint appears to be feasible. In an initial study in which we recruited 15 participants to create a set of simple (objects thumped regularly at the center of the screen) and complex thumprints (objects thumped in a unique pattern), we were able to distinguish between different objects thumped in the same way by the same participant with close to 96% precision and recall, between up to 15 different participants entering the same simple thumprint with 98% precision and recall, and between 2 participants entering the same complex thumprint with 100% precision and recall. This result needs to be extended to participants entering their thumprint across multiple sessions, however. Furthermore, I still need to run a comprehensive analysis of adversarial success rates.

**Social Evaluation**

Based on the results of this technical evaluation, I will implement a version of Thumprint that should work in real time. The instrumented sensor surface will be an Android smartphone or tablet, which will connect, via bluetooth, to an electronically operated lock (e.g., a Lockitron). Once I have a working version of Thumprint that works in real time, I plan to run a social evaluation. The goal of the social evaluation will be to answer the following open questions:

- What do local groups require and value in group authentication? How and why do these requirement vary between groups?
- How do local groups currently meet their group authentication needs and where do these solutions fall short?
- How do local groups create and use Thumprint? How does use of an inclusive group authenticator affect group social dynamics, if at all?
• Does Thumprint better meet local group security needs? If not, where does it fail and how can it be improved?

To answer these questions, I propose to run an interview study, followed by a field deployment. The first study is an interview study. The purpose of this study is to understand the security needs of local groups with different group structures and contexts, as well as how these groups use existing security solutions to meet those needs. I will first recruit a variety of local groups and speak to individual group members in a 30-minute interview session. From these interviews, I hope to validate the list of security needs I uncovered from my initial survey of the literature review as well as uncover previously unknown needs. I will use this understanding to direct my implementation of a functional prototype of Thumprint. However, given that local groups have existing security practices that are shaped by their familiarity with current solutions, it is not enough to ask them about their needs—their thoughts will be based on their experience with these existing solutions.

Accordingly, I will next use Thumprint as a design probe in a field study with the recruited groups. I will install Thumprint on a low-stakes protected space for each of the groups: e.g., on a door to a kitchenette. The groups will use Thumprint as a means to access this low-stakes protected space for a number of weeks. During the field deployment, I will run an experience sampling survey pinging the group members several times a week to identify any problems, feature requests, or other notable experiences they had with Thumprint. At the end of the field study, I will bring in each group for an exit interviews where they will be afforded a chance to expand on their reported experiences. Specifically, I will look for instances where Thumprint broke down, caused tension or otherwise notably impacted people's experience accessing the shared space. This study should provide actionable insights on what is important for inclusive, group authenticators. In addition, it is conceivable that the study will serve as a stimulus for local groups to conceive of access needs they previously had not considered.

Summary & Expected Contributions

To summarize, through my proposed work, I expect to expand on all three aspects of my social cybersecurity work: observational theory building, experimental testing and system development. For my proposed observational theory building work, I will run a series of surveys to generalize my results from the interview study I reported in Chapter 3: A Typology of How Social Influence Affects Security Behaviors and Chapter 4: Understanding How Security Information Is Communicated. Specifically, I'm hoping to validate and expand upon the typology I introduced for social catalysts of security related behavior change, as well as the types of conversations people have about security and their resulting effects on security sensitivity. For my proposed experimental testing work, I will evaluate the effect of personalized social proof, contextual relevance, cultural origin, and the interaction between these factors on people's perceived value of a preventative security notification. As well, I will test the relationship between perceived value, comprehension and behavior. Finally, for my proposed system development work, I will design, implement and evaluate an observable and inclusive local group authenticator: Thumprint. I will recruit local groups to use Thumprint in a field study, and then evaluate whether and how Thumprint better meets the authentication needs of local groups, how it can be improved, and, finally, if using a more inclusive authenticator affects group social dynamics.

Based on the findings of my proposed and foundational work (reported in Chapters 3-6), I will conclude with a set of actionable insights and guidelines on how (not) to use social processes to increase security sensitivity, as well as a set of recommendations for security tool designers to consider in making new security tools that are more socially compatible. Thus, my expected contributions are three fold:

(i) an initial theory of social cybersecurity, developed from both observational and experimental work, that explains how social factors affect people's security sensitivity;

(ii) a set of design guidelines and recommendations for adequately leveraging social processes to increase security sensitivity, as well as to create more socially compatible security and privacy systems; and,
(iii) the design, implementation and evaluation of a system that leverages these design recommendations to explore the design space of social cybersecurity systems.
Chapter 8: Timeline

<table>
<thead>
<tr>
<th>Month</th>
<th>Activities</th>
</tr>
</thead>
</table>
| January 2016 | Viral Behavior Surveys  
February 2016 | Information Dissemination Surveys  
March 2016 | Social + Contextual Notifications Experiment Analysis  
April 2016 | Viral Behavior Surveys Analysis  
|            | Information Dissemination Surveys Analysis  
| March 2016 | Thumprint technical evaluation  
| April 2016 | Thumprint technical evaluation  
| May 2016   | Submit Thumprint technical paper to UIST  
| June 2016  | Thumprint real-time development  
|            | Submit Social + Contextual Notifications Experiment to CCS  
| July 2016  | Thumprint real-time development  
| August 2016| Submit Information Dissemination Surveys + Viral Behavior Surveys to CSCW  
| September 2016 | Thumprint social evaluation  
| October 2016| Submit Thumprint social evaluation paper to CHI  
| November 2016| Writing dissertation / applying for jobs  
| December 2016| Writing dissertation / applying for jobs  
|            | Defense  

References


43. Maritza Johnson, Serge Egelman, and Steven M Bellovin. 2012. Facebook and Privacy: It’s
Complicated Categories and Subject Descriptors. *Proc. SOUPS'12.*


