Stories as Informal Lessons about Security

Emilee Rader
emilee@msu.edu

Rick Wash
wash@msu.edu

Brandon Brooks
brook205@msu.edu

Department of Telecommunication, Information Studies, and Media
Michigan State University
East Lansing, MI

ABSTRACT

Non-expert computer users regularly need to make security-relevant decisions; however, these decisions tend not to be particularly good or sophisticated. Nevertheless, their choices are not random. Where does the information come from that these non-experts base their decisions upon? We argue that much of this information comes from stories they hear from other people. We conducted a survey to ask open- and closed- ended questions about *security stories* people hear from others. We found that most people have learned lessons from stories about security incidents informally from family and friends. These stories impact the way people think about security, and their subsequent behavior when making security-relevant decisions. In addition, many people retell these stories to others, indicating that a single story has the potential to influence multiple people. Understanding how non-experts learn from stories, and what kinds of stories they learn from, can help us figure out new methods for helping these people make better security decisions.

Categories and Subject Descriptors

H.5.m [**Information Interfaces and Presentation**]: Miscellaneous; H.1.2 [**Models and Systems**]: User/Machine Systems—*Human Factors*

General Terms

Human Factors,Security

Keywords

mental models, security stories, storytelling, stories

1. INTRODUCTION

The United States National Academy of Engineering has declared Cybersecurity to be one of its *Grand Challenges*[1]. Among many issues related to cybersecurity that they identify, one of the most important is understanding how non-expert users think about and manage information security tasks. These are people without significant technical or security training who routinely use computing technology, and they must make decisions on a regular basis that affect the security of the systems they interact with. In fact, the vast majority of home computers and personal computing devices are administered by people who have little security knowledge or training.

In addition, everyday computing is becoming more complex, not simpler, as it becomes ubiquitous. *Home computer security* doesn't just refer to the devices in someone's home office anymore—computing technology is increasingly blending in with all parts of our daily lives. Non-expert users have at their disposal a whole ecosystem of devices such as smartphones, tablets and music players, in addition to desktop and laptop computers. These devices may be subject to even greater risk due to the rise of the apps model, in which downloading and using potentially unsafe software from unknown third party developers is becoming an every day activity. And since it seems that in the very near future practically any consumer device available for purchase will be network-ready, from televisions to toasters[2], the contexts in which security choices and behaviors must take place will continue to expand, and to indirectly affect many other people. All of this means that both the need to manage one's computer security, and the complexity of that task, are increasing for non-expert users.

Unfortunately, managing the security of a computer system is a very difficult task for non-experts. The main reasons that novice users cite for improper security stem from a lack of knowledge and understanding: "43% claimed not to understand the threats, 38% claimed they did not know how to use security packages, 35% indicated that they did not know how to secure their computer, and 32% indicated that they did not know about the threats" [13].

Wash [25] examined how non-expert computer users think about information and computer security threats, and how that thinking leads to security practices. He identified eight different "folk models" of computer security threats—four different ways of thinking about what a computer virus is, and four different ways of thinking about hackers—that non-expert computer users use when thinking about computer security issues. These folk models are over-simplifications of the real world, but provide a basis for security decision making by non-experts.

[1] `http://www.engineeringchallenges.org/cms/8996/9042.aspx`

[2] See the Texas Instruments SimpleLink WIFI CC3000

Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13, 2012, Washington, DC, USA.

However, it is not clear how these people learn the folk models that they use in their decision making. Ideally, the information in folk models would come from security experts in formal training sessions; but we suspect that few people attend formal security training, and even those that do rarely remember everything in the lessons.

Rather, we suspect that people learn much of what they know by hearing *stories about computer security.* We explore this intuition by asking a number of non-expert users to tell us stories they heard about computer and information security. We describe these stories and the important role they play in how non-experts learn about security concepts and security threats. In addition, we describe how those stories might affect computer security thinking and behavior.

2. RELATED WORK

One of the biggest challenges these computer users face is operating these computers securely. There is a large ecosystem of threats, and a large percentage of these threats specifically target home computer users. According to the US Census Bureau, there are over 81 million households in the United States that have a computer with Internet access in their home; this represents almost 70% of all households in this country [24]. Symantec, a computer security vendor, analyzed the security threats they addressed in 2006 and found that "from the 2249 new threats identified during the first 6 months of 2006, 86% were aimed at home users [2]." Most home computers are administered by non-experts; thus, these threats are particularly problematic for people who don't fully understand the security implications.

Non-expert users frequently try to avoid security decisions by relying on other people or on software to help them maintain proper security, because they feel like they don't have the skills to do it themselves. They find ways to delegate the responsibility for security to some external entity which could be technological (like a firewall), social (another person or IT staff), or institutional (like a bank)[12]. However, despite this delegation of responsibility, many users still make numerous security-related decisions on a regular basis. The literature does not explain how those decisions get made; rather, it focuses mostly on the anxiety the decisions create. Cormac Herley [17] argues that when non-expert users reject security advice, it is often rational to do so. He writes that security experts provide advice that ignores the costs of the users' time and effort, and therefore overestimates the net value of security.

Wash found that home computer users have a variety of different "mental models" of security threats [25]. Mental models describe how a user thinks about a problem; it is the model in the person's mind of how things work. People use these models to make decisions about the effects of various actions [18]. For example, some believed that hackers are mischievous teenagers showing off for their friends. Others believed that hackers are criminals out to steal financial and identity information. All of the respondents he interviewed were motivated to take positive security actions, but only for the threats they believed existed. Users who believe that hackers are teenaged troublemakers were likely to install firewall and other security software to keep them out, while the users who saw hackers as criminals frequently believed that they were not rich or important enough to be a target, and therefore didn't need to secure their computers.

Security experts differ sharply from non-experts in how they think about security. Gross and Rosson [15] studied what security knowledge end users, who were not directly responsible for security but had access to sensitive information, possessed in the context of large organizations. Users' security knowledge was "neither comprehensive nor sufficient" to maintain proper security, but common security actions such as locking the screen when away were better understood and practiced. All participants were aware of some sensitive information they had access to, and knew to protect it and to be wary of being tricked into revealing it (social engineering). Gross and Rosson also noted that their participants frequently conflated security and functionality failures. Asghapour et al. [6] conducted a card sorting experiment in which participants were instructed to match words with a set of computer security related concepts. They found that experts and non-experts show sharp differences in which analogy (medical, crime, etc.) they felt the concepts were closest to, and hypothesized that analogies might function as mental models.

Some usable security researchers believe that the software is simply too complex to operate securely [10]. We believe that users are intentionally choosing actions that leave them insecure. This is not because they are being tricked by social engineering (though that sometimes happens), but rather because people honestly believe that they are doing what is necessary to protect their computers. The question remains, though: where do people learn about security?

Where do people learn security?.

There are a number of places where people seem to learn about computer and information security concepts. The most obvious place to learn about security is personal experience; some people have personal experience with security problems (such as having a virus on their computer), and that teaches them about potential security threats. Home computer users often do not have a lot of examples around them of security problems that they can use to learn how to react, or security experts to learn from. Actual security situations people encounter are infrequent, and not always recognized as security situations until it is too late. For example, when a person is the victim of identity theft, rarely can they trace the information back to how it was originally stolen. Thus, identifying this as a security problem does not help the person learn how to better *protect* against identity theft, just how to *cope* after the fact.

Another place that people learn about security is formal education: classes and training seminars about computer security. There has been much effort devoted to training users in organizations to be more secure, and some researchers have investigated the effects of different kinds of training programs and security policies on security outcomes [4, 11]. Microsoft has an extensive online resource for teaching users all about computer security [1]. Many organizations including Microsoft, CERT and US-CERT include lists of advice for being more secure. This approach has many parallels in other domains; for example, many organizations are also working hard to educate consumers about environmentally-friendly activities and goods. However, these approaches are most effective when the desired behavior changes are not very difficult or costly to adopt, and often produce only modest, short-term improvements [23]. Home computer users are rarely interested in learning the details of how security software works in order to make appropriate security deci-

sions. Often, the details are so complicated that users get frustrated and don't really understand enough.

The Management Information Systems (MIS) literature has several examples of research projects that approach computer security behaviors from an "adoption" perspective; these researchers suggest that people adopt security behaviors much in the same way as they might adopt a new technology. They seek to understand psychological characteristics that lead people to adopt security behaviors, and how these characteristics interact with the messages about security that home computer users might receive [26, 5, 20, 27]. However, these studies do not go into detail about the process by which security behaviors spread among people.

Learning From Stories.

If people are not learning what they need to know to make good security-relevant decisions from formal education (classes and seminars taught by experts) or from guidelines and training materials produced by experts, then how do they know what to do when faced with a situation in which they need to act? Non-experts face these decisions every day — from choosing whether to click on a link in Facebook, to which requests for information they should or should not respond to — and they must take action when they do. In general, when people don't know how how to act in a given situation, they either fall back on what little they already know, or they look to others around them to figure out how they should behave [9].

However, computer security situations are different from, say, the experience of going to traffic court for the first time, in that there is rarely somebody else with more experience in the same situation that one can look to for guidance. Instead, human beings are able to learn about things they have not personally experienced by hearing narratives about those situations described by others. These narratives — stories told by other people — are an important component of our ability to learn about the world around us and behave appropriately [8]. Stories people tell about each other, sometimes labeled "gossip" (a word with culturally negative connotations), constitute observational learning and help us avoid others' mistakes [7].

Stories about others reveal useful information about how our culture and society operate; it is easier to make our way through our complex world if we can learn from the experiences of others, and stories are a vehicle for this information. In an exploratory study of gossip, Baumeister et al. [7] found that most instances of gossip people could remember hearing were about people personally known to the participant (85%). People find gossip most interesting when it is about people similar to them [21], and model their behavior after people they perceive to be similar to them [14]. This is evidence that people do indeed learn about how to behave from the experiences of similar others. In addition, stories that arouse emotion, such as stories about bad things that happened to acquaintances, are more likely to be remembered and passed on [22, 16].

3. METHODS

To better understand how stories about security inform people's thinking and behavior, we conducted a short survey in December 2011 and January 2012. This survey asked respondents to think about a number of stories that they had heard about security-related issues, and then choose one story which they could easily recall details about. Then we asked them a number of questions about this story, including where they heard the story and from whom, what the story was about, and what kinds of reactions they had to the story. This study was approved as minimal risk by our Institutional Review Board. (The survey instrument is available as an appendix.)

We asked students in 5 different undergraduate telecommunications classes to respond to the survey. We received a total of 301 usable responses[3], from approximately 728 potential respondents[4] (41% response rate). Respondents ranged in age from 18 to 38, but the vast majority were between 18 and 23. All but 10 were full-time students. There were 179 male (59%) and 119 female (40%) respondents. These demographics approximately reflect the demographics of students in this major, and therefore we believe we achieved a representative sample of such students. Respondents who completed the entire survey received extra credit.

Respondents were given extra credit as an incentive. They were free to leave any answer blank that they didn't want to answer, and this did not affect whether they received the incentive. We cleaned the data, removing any respondents who didn't answer a sufficient quantity of the questions (about 70% of questions) or who showed evidence of not taking the survey seriously (such as choosing the same answer for a majority of questions and having a very long completion time).

We believe that undergraduates are an interesting sampling frame to study storytelling about security. Current undergraduates have grown up with computers their whole lives, and thus are familiar with their use. However, most of them are not experts in computing or in security, and therefore need to learn about managing computer security in some other way, much like the rest of the population. Only 37 of our 301 respondents reported working in a technology-related job or having computer security training.

Note that this survey *assumes* that people tell stories about security. However, we didn't assume what types of stories people tell, nor what types of responses people have to these stories. This survey does not allow us to determine whether or how often stories are told. It does allow us to make claims about what kinds of stories are told, how people react to those stories, and whether these people chose to retell the stories. That said, simply asking respondents to tell us a "story about computer security" doesn't work; pilot testing indicated that people had trouble understanding this prompt, even when they had numerous computer security related stories they could tell us. We included high-level,

[3]Cases in which questions were completed but the survey was not submitted at the end were excluded, as were cases where respondents did not enter a security story, did not indicate the class in which they were enrolled, or indicated that they were not a student. In addition, 6 cases were removed because logs from the online survey indicated these respondents took over 8 hours to complete the survey; the average completion time was 20.56 minutes. Finally, 21 cases were removed because the story the respondents entered was not a story at all. For instance, #2 "I didn't have a story" or #194 "n/a" or #166 "Go to see the movie 'the social network' bro!"

[4]Some students may be in more than one class. We kept only the first response from students who took the survey more than once. 728 is a high estimate; for legal reasons we cannot know which students were enrolled in multiple classes.

one-word examples of what kinds of stories qualify as computer security stories in the prompt. Thus, respondents told stories that frequently fit these examples. The fact that stories are somewhat similar to these examples is not surprising; however, the proportion of stories that fit each example is not a result of this prompting. Our findings about the types of stories told should be interpreted relative to the set of stories implied by the prompt that includes security threats (like hackers and viruses), security protections (anti-virus and firewalls) and unusual circumstances (unwanted popups or mysterious Facebook posts). See the appendix for the full prompt.

We explored the data post hoc looking for patterns that could indicate priming effects (i.e., if we mention friend as a source first, does that bias people toward stories from friends?) and found little evidence of strong priming effects.[5]

4. RESULTS

We received a total of 301 stories from our respondents, which involve a wide variety of different computer and information security threats. The stories were heard in a variety of contexts, but most of them were heard in informal contexts from family and friends. Most stories that respondents reported have a lesson or moral that the story was intended to convey, about a fairly serious threat. Almost half of these stories where then retold by the respondent to others, mostly family and friends. Most respondents indicated that they changed their thinking about security issues, and their behavior, as a result of hearing the story they reported. We elaborate on these results below, and believe that together, these results illustrate how stories that people tell each other are very important in shaping and understanding computer security behaviors.

4.1 Stories Are Informal Lessons

We asked respondents to type their story into the survey form. We also asked a number of closed-ended questions about the content of the stories, to help us understand what they were about. A member of the research team made a first pass through the stories and made a list of topics by which they might be categorized. Upon examination of this list, we discovered six distinct topics in the stories. Two members of the research team then coded all of the stories using definitions for these topics that the research team agreed upon in advance. We calculated inter-coder reliability using Cohen's κ. The number of stories per topic and inter-coder reliability are included in Table 1. Finally, the coders met to resolve any disagreements and produce a final categorization of stories into topics.

Stories Are About Security Incidents.

The stories that respondents reported hearing spanned six security-related topics. Stories could be about more than one topic, with the exception of "Other"; if a story was designated as "Other" by definition it was not also about one of the other topics. For each topic, we include below an exemplar story that represents common characteristics of stories about that topic (see the Appendix for additional example stories). These stories are primarily about security incidents that happened (such as break-ins, phishing, and viruses) rather than being about consequences (theft) or security precautions (passwords, firewalls).

Table 1: The number of stories that were coded for each topic group, along with inter-rater reliability κ for the coding process

Topic	*# stories*	*Cohen's κ*
PC Effects	95	0.86
Breaking In	59	0.70
Theft	75	0.78
Spam	37	0.79
Phishing	53	0.81
Other	62	0.68

PC Effects: Many of our respondents told a story about how someone's computer was acting strangely because of a security problem, and how that person took action to fix it. The strange behavior included things like lost information, slow performance, or a computer that died or wouldn't start. "Viruses" were commonly blamed for these behaviors, and frequently the stories included computers that became completely useless as a result and had to be repaired by an expert or replaced entirely. Example: "My friend was just doing normal stuff online. He went to a site he was unfamiliar with. What he did there I am not so sure maybe he downloaded some music or something. His computer was then full of viruses such as child pornography. His computer was basically a piece of metal. He couldn't do anything that involved the internet. When he tried to get on the internet it immediately closed and he couldn't do anything." (#114)[6]

Breaking In: A number of respondents told a story that included a description of consequences from someone having broken into a computer or system. This includes account or profile information that was changed, sending uncharacteristic messages, or reports of a "hack" or unauthorized access. A system at any scale could be attacked, from a personal computer to service provider. "Hackers" were often blamed for break-ins, but "viruses" were also implicated in the stories. Example: "My friend called me and told me her Facebook had been hacked. She was not sure who had broken into it but she logged on and somehow a mass virus link was posted on all of her freinds walls. Some of her pictures were deleted and she called me to warn me not to go on her profile or click on the link on my wall." (#10)

Theft: A story was considered to be about *Theft* when there was evidence in the story that personal information or money had been taken, or unauthorized use of credit cards had taken place. This often was reported to have occurred when someone used a credit card to make a purchase online, or had been taken in by a phishing scam. Stories that mentioned consequences to "hacks" of service providers were often coded as Theft as well. Example: "So my friend attempted to purchase some anti virus software from a website. It was a website she never been on before. More then the listed amount was withdrawn from her account and she realized her identity had been stolen by a fraud from the

[5]We thank the anonymous reviewers for suggesting we look into this.

[6]All stories are represented exactly as typed into the survey, including grammatical errors, spelling errors, and capitalization issues. Numbers in parentheses with # in front of them that precede or follow stories are respondent IDs.

website." (#129)

Spam: A number of the stories included mentions of sending or receiving unwanted messages of any kind. Typically, these stories involved the user unknowingly clicking on a link in social media or email, and then being notified by one of their email contacts that they had received a strange message. Example: "My sister's teacher confronted my sister in her class the other day, because she received an email that contained a message about viagra and other prescription pills. My sister, unknowingly, downloaded some sort of file or email and it began spreading throughout her address book to everyone including my parents, other family members, teachers and her friends. She's not sure which email it was or how to stop it, but it just keeps sending them." (#224)

Phishing: Stories about Phishing all included a request for information involving a computer (i.e., not a phone phishing scam), usually personal or financial information, that the person would have been able to opt-out of by not answering. Phishing stories ranged from emails impersonating banks, to more elaborate attempts by individuals chatting up unsuspecting users on Facebook or in online games. Example: "My friend sat next to me during class looking very disheartened. i had asked her what had happened and she stated that her facebook had been hacked by an unknown user. i then asked how this could have happened, and she stated that hours before she had opened an email for her facebook password. And hours later it had been hacked. I recall telling her to contact the networking site and tell them what had happened to try and get her profile back. she did so and obtained her facebook account once again." (#471)

Other: This category included stories that do not contain enough detail to be coded using any of the above codes, or about something that is not computer security. If this code was applied, no other codes could be used for that story. Example: "It was a few years ago and I was in the kitchen with my mother. She was on the phone with my uncle, who told her that his computer had been hacked by someone. I don't recall exactly what the hacker did or how it turned out, but it's still scary to think about." (#88)

Two pairs of codes that appeared often were *Breaking In* and *Theft* (24 times), and *Phishing* and *Theft* (32 times). This seems to indicate that threats from outside perpetrators often come with consequences in terms of loss of information or money. Only 15 of the 95 stories coded as *PC Effects* were coded something else as well, which seems to indicate that the stories convey the idea that PC effects are not caused by other users (unlike breaking in, spam, or phishing), although the stories indicate that PC effects do come from the users' own actions (clicking links, downloading files, etc.) Only 1 story included both *PC Effects* and *Theft*, indicating that one's own actions are rarely associated with loss of information or money.

Stories are heard informally from family and friends.

Most of the stories that our respondents recounted were heard in very informal settings. 70% of the stories were heard at home, at a friends house, or in a coffee shop. 55% of the stories were told face-to-face, and a total of 69% were told using direct, person-to-person communication such as instant messaging or direct email. 64% of the stories were told by family or friends. People tended to report stories that they originally heard a long time ago; 40% of the stories were over a year old, and 71% were heard more than a month ago.

Together, these results indicate that storytelling about security issues is a very informal thing that happens among people who are relatively close.

Table 2: Facts about the Content of Stories

Story Content	
95%	Believed to be True
55%	About Family and Friends
51%	Autobiographical
18%	About Strangers
35%	Ended "well"
29%	Ended "badly"
72%	Have a lesson
	54% "Always do" something
	32% "Never do" something

Stories are lessons about everyday people facing moderately serious threats.

Most of the stories in our sample were told about friends and family (55%), and 18% were told about strangers. Most of the remaining stories were told about organizations or organizational representatives like IT workers. Slightly over half (51%) of the stories were autobiographical in nature. In other words, most of the stories were about fairly normal people, and often it was people known to the listener.

On a scale of 1–5, the seriousness of the threats in the story averaged 3.65, which is somewhere between "Serious (3)" and "(4)". 29% of the stories ended badly for the protagonist, and 35% ended well for the protagonist. This indicates that these stories are about only moderately serious security issues that can frequently be recovered from.

72% of the stories reported here have a lesson embedded in them; respondents reported that these stories were told with the perceived purpose of conveying a lesson of something that a person should always do or never do. In 54% of stories, this lesson was something you should always do, and in 32% of the stories, the lesson was something you should never do. It seems that people tell stories about security issues to convey lessons and educate people that they know.

Additionally, 95% of respondents believe that the story they reported in this survey is a true story. This does not necessarily mean the event as represented in the story actually happened in the way that it was described; however, we take this as evidence that people trusted the story and the person they heard it from.

Table 2 summarizes what we know about the content of the reported stories.

Lessons Learned.

To better understand what lessons respondents took away from these stories, we explicitly asked the open-ended question, "What did you learn from this story?" We used an inductive qualitative coding approach to analyze the answers. Inductive or open coding involves bottom-up grouping and sorting answers into themes. This is in contrast to the multiple-coder content analysis approach we used to categorize the stories into topics, we used an inductive approach here. This approach allows us to see patterns we didn't know in advance we would be looking for – aspects of the responses that would allow us to look deeper than the more easily defined identified topics present in the stories.

The coding process involved identifying similar answers and grouping them together into higher-level themes. The unit of analysis was the entire answer; a few answers contained more than one idea or thought, and these multi-thought answers were grouped together with the idea they contained that was least-well-represented in the data.

We did not start out with a priori themes or a theoretical framework in mind, nor did we have a particular number of themes we were looking for. However, we did start with a goal: to summarize and describe similarities across respondents' answers. When two answers seemed to contain a similar lesson they were grouped together, and a sub-theme was started. Evidence for similarity ranged from two answers that were nearly identical (as in #412: "Don't click on sketchy links" and #3: "Don't click on weird links") to answers that were understood to express a similar sentiment in different words (as in #428: "Make sure you choose a well-trusted antivirus program to protect your computer from spyware and threats" and #46: "Make sure I keep a virus protection on my computer at all times"). Answers that were difficult to interpret or unrelated to computer security were not included in this analysis. As the groupings grew, we checked subsequent additions to each sub-theme against the answers that were already there to ensure consistency.

Dangerous Place: One theme that emerged in the "lessons" respondents provided was a general sentiment that the Internet is a dangerous place, and people must try to be secure and protect themselves. Lessons that were grouped under this theme included mentions of high-profile "hacking" incidents like the Sony Playstation hack (#54: "Don't trust Sony with my info. Yeah."), the idea that anyone unknown to you on the internet can't be trusted (#473: "I learned not to talk to strangers, especially online"), and a general feeling that one is always vulnerable (#28: "Learn that there are always vulnerabilities no matter how hard you try to secure yourself"). A few respondents reported that they learned there was nothing they could do to protect themselves (#391: "Hope that I don't get hacked").

The answers provided by respondents indicate that the stories contained lessons about the importance of protecting oneself, but that these lessons were vague and not necessarily actionable, such as #78: "To get security software" or #227: "Make sure that you have protection for your computer" or #121: "To not be stupid and recognize when a virus is attempting to harm your computer". Some lessons were actionable, however, such as #87: "Buy Macs because people can't get into them" and #325: "I learned when setting up a wireless network, always make sure it is locked with a password only you have access to". Finally, several respondents expressed the feeling that it is a bad idea to be too trusting online (for example, #270: "Never reply to emails that have ridiculous claims about money and jobs", and #473: "I learned not to talk to strangers, especially online").

The lessons respondents reported included two specific ways people might protect themselves: practicing safe password habits, and using antivirus. These included choosing good passwords (#386: "Have a strong password"), not giving away passwords (#160: "To not give away passwords! And to protect yourself from hackers"), changing passwords often (#195: "Change my passwords on a regular basis"), and not saving passwords on websites and applications (#238: "To not have my passwords saved on things on the web"). Lessons related to antivirus software included directives to use antivirus (#428: "Make sure you choose a well-trusted antivirus program to protect your computer from spyware and virus threats"), and keep virus definitions up-to-date (#140: "Always update your antivirus software when you are supposed to. Especially don't let your software expire!").

Specific Threats: A second high-level theme described lessons about particular activities in which threats are perceived to be prevalent, and how to avoid problems in these areas: email, downloading files, surfing the web, and online shopping.

Regarding email, the lessons focused on a general idea that one must make sure an email is safe before opening it, but contained vague and sometimes contradictory suggestions for how to tell if this is true (#460: "Don't open suspicious emails, even if they are from a family member or friend"; #251: "Don't trust emails from people you do not know"; #366: "To always verify if the email is real").

Directives related to surfing the web were equally vague; most took the format of "Don't click on [shady adjective] links", where the shady adjectives were things like "unknown" (#479), "spam" (#357) , "sketchy" (#412), and "random" (#161). Facebook in particular was identified in several lessons as someplace that one should be careful when clicking on links (#110: "Not to open links on Facebook even if they are sent from friends").

There was also a general sentiment in some lessons that downloading files is a risky activity, especially when this activity may be illegal (#331: "Don't use Limewire or Napster"). But for the most part, lessons about downloading files did not contain specific information for how to recognize when a particular download might be a problem before problems arise (#395: "Don't go to sketchy websites and download things").

Online shopping was specifically addressed as an activity that might put one at risk, and the lessons in this subtheme were more specific than for email, clicking on links, and downloading. For example, lessons mentioned assessing the credibility of an online shopping site based on the URL (#211: "Check the URL address of a site in which you're giving away personal information"), looking for signs that a website is secure (#280: "To always check if the website is a secure one"), and not shopping online at unfamiliar websites (#129: "Don't purchase from unfamiliar websites").

Private Information: Finally, a third theme that emerged was specifically about phishing and other similar scams that involve giving away one's personal information when one should not. These lessons did not pertain to specific activities during which one is at risk, but rather that there is certain information that should not be made public or given

Table 3: Content influences on changes in thinking and behavior

	Change in Behavior		*Change in Thinking*	
(Intercept)	0.27		2.27	
Contains a lesson	2.33	**	0.26	.
Seriousness of threat (scale)	1.14		0.15	**
Autobiographical	1.79	*	0.15	

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Coefficients for Change in Behavior are from a logistic regression, and represent the odds ratio for whether there is a change in behavior. Coefficients for Change in Thinking are from an OLS regression, and represent the change on a 1-5 likert scale in the amount of change in thinking. Seriousness of threat is a 5-point Likert scale.

away. Examples include #322: "To be very careful about the information I post online"; #402: "To not share personal information"; #120: "To not post my entire date of birth or the state where I'm from on Facebook"; and #174: "That you should not give your credit card info away via online". A sub-theme in this area specifically covered the idea that someone who asks for this information is up to no good (#324: "That the bank won't ask you for your information through email").

4.2 Stories Change Both Security Thinking and Behavior

Our respondents reported that these security stories frequently changed both their thinking about security issues, and their behavior with respect to security. 52% of respondents said that they changed their behavior as a result of hearing the story they reported. 94% of the respondents reported changing the way they think about security after hearing the story. 33% reported changing their thinking "a lot", while 46% reported "moderate" changes in thinking.

People who changed their behavior reported signficantly larger changes in their thinking. The mean change in thinking for respondents who did NOT report a change in behavior was 2.86 on a 1-5 Likert scale, where 5 represents "A Lot" of change in thinking; for respondents who reported a change in behavior, the change in thinking was 3.30 (p=0.0346). Since this is survey data, we cannot say if there is a causal relationship, and if so, which direction it is. But this association between changing thinking and changing behavior makes sense. The Theory of Planned Behavior [3] would suggest that people change their thinking about security issues, and then subsequently change their behavior as a result of this change in thinking. Cognitive Dissonance theory suggests that the behavior change may come first, and then thinking is altered to be more inline with the person's behavior. Either way, thinking and behavior are strongly related, which suggests that stories from people that change either one (or both!) are important.

In the rest of this section, we look at what properties of these stories influence whether people change their behavior as a result of hearing this story, and how much people change their thinking as a result of hearing this story. Note: we are not establishing causality as a result of correlations between survey items. Rather, we asked respondents to identify which stories *caused* changes in thinking or behavior; the causal relationship is perceived by the respondent. We then identify correlations between those stories and other properties of the stories (such as the content of the story or the identity of the person who told the respondent the story). Almost all of these properties, with the exception of emotional reaction to the story, exist before the respondent reacted to the story by changing his or her behavior and/or thinking. Therefore, if there is a causal relationship, it is the property of the story causing the change in thinking or behavior; however, there could still be unmeasured additional variables that cause both.

Story Content is Important.

Unsurprisingly, the content of the story is important; some stories are associated with a higher probability of change in behavior and other stories are associated with greater changes in thinking. While this general fact is not surprising, we are able to dig deeper into this and identify what properties of stories are most commonly associated with the changes in behavior and thinking that respondents reported happened after they heard the stories.

As mentioned above, 72% of the stories reported contain a lesson. These stories with lessons are much more likely to cause a change in behavior; our estimates indicate that stories with a lesson have over twice as high of odds of causing a change in behavior than stories without a lesson. Additionally, stories with lessons are associated with larger changes in thinking than stories without lessons. These lessons appear to be important for subsequent changes in behavior and in thinking.

Stories that describe a more serious threat tend to be associated with larger changes in thinking. This makes sense; more serious threats are more likely to be taken seriously, and thought about more, than less serious threats. However, more serious threats appear to make little difference for whether the story causes a change in behavior. People reported changing their behavior for both serious and not-so-serious threats.

Stories that are autobiographical—that are about the person who originally told the story to the respondent—are more likely to cause a change in behavior. The odds of changing behavior are about 79% higher for autobiographical stories than for stories about other people. It isn't clear why this would be the case; it could be that autobiographical stories ring true and are more credible. It could also be that autobiographical stories have more details about potential behavior changes that people can learn from. Autobiographical stories are somewhat associated with a change in thinking, but we cannot be sure as our estimate is not statistically significant.

Who and Where Matters.

The context around the story also seems to have an important influence on whether the story is associated with reported behavior change, and how much the story changes thinking. In particular, who tells the story, and where the story is told seems to be important.

Stories that are told in a home context seem to be more strongly associated with respondents changing their behavior. The odds that a story told in a home context leads to behavior change are 95% higher than the odds that a story told in a formal context such as an office or school leads to behavior change. This could be because certain types of stories are more likely to be told in home contexts, and those

Table 4: Source influences on changes in thinking and behavior

	Change in Behavior		*Change in Thinking*
(Intercept)	0.21		2.50
Home Context	1.95	.	0.28
Knowledgable Source	1.40	**	0.11

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Coefficients for Change in Behavior are from a logistic regression, and represent the odds ratio for whether there is a change in behavior. Coefficients for Change in Thinking are from an OLS regression, and represent the change on a 1-5 Likert scale in the amount of change in thinking. Home context is compared to a baseline of a formal context such as school or work. Knowledgable source is a 5-point Likert scale.

Table 5: Emotional influences on changes in thinking and behavior

	Change in Behavior		*Change in Thinking*	
(Intercept)	0.27		1.83	
Happy	0.91		0.07	
Sad	0.64	.	0.15	
Anxious	1.88	*	0.24	*
Anger	1.84	**	0.19	*

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Coefficients for Change in Behavior are from a logistic regression, and represent the odds ratio for whether there is a change in behavior. 1.0 means no change in behavior; > 1 is an increased probability of changing behavior, while < 1 is a decreased probability. Coefficients for Change in Thinking are from an OLS regression, and represent the change on a 1-5 likert scale in the amount of change in thinking. All four emotions are scales made up of multiple questions from Kay and Lovelock [19]; Cronbach's alpha: Happy=0.55, Sad = 0.69, Anxious=0.73, Anger=0.82.

types of stories are more likely to cause behavior changes. Or it could be that people pay more attention to stories that they hear casually, or from people they interact with in more casual contexts like homes. We were unable to find another variable in our data that explains why home contexts are associated with greater behavior change. Home contexts also seem to be associated with greater changes in thinking; however, we cannot be confident in this because our estimate is not statistically significantly different than zero (p=0.107) and has a large standard error (0.17).

Stories that are told by more knowledgable people are more likely to lead to changing security behaviors. A one point increase on a 5-point Likert scale measurement of security knowledge of the storyteller is associated with an approximately 40% increase in the odds of behavior change. However, more knowledgable people have only a small (and not statistically significant) effect on how much people change their thinking.

Emotional Reactions Influence Change.

Stories commonly evoke emotional reactions on the part of the listener. Different stories may evoke different emotional reactions. We asked the respondent to answer a few questions about what kinds of emotional reactions they experienced when hearing their story. Based on existing work by Kaye and Lovelock [19], we grouped the emotions into four categories: happy reactions, sad reactions, anxiety-producing reactions, and anger-producing reactions.

Stories that produced more anxiety or anger were much more likely to lead to a change in behavior. A one point increase in anxiety on a 5-point Likert scale is associated with an 88% increase in the odds of changing behavior. Likewise, a one point increase in anger is associated with an 84% increase in the odds of changing behavior. These are strong associations, and are statistically significant. That anxiety reactions induce behavior change makes sense; if you are worried about some security threat after hearing a story, it would make sense that you would want to protect yourself from it. Anger, however, is less obvious. Stories that make you angry are associated with a similar magnitude of behavior change.

Interestingly, stories that lead to a sad reaction are associated with less behavior change. A one-point increase on a 5-point Likert scale of sadness is associated with a 36% decrease in the odds of the story causing a change in behavior. Sad stories don't seem to provoke the kinds of reactions that cause behavior change.

Much like behavior change, both anxiety and anger are associated with changes in security thinking.

These results about emotional reactions are just correlations. It isn't clear if the emotional reaction played a causal role in changing behavior or thinking, or if some other property was more important. The effect that these emotional reactions have on thinking and behavior cannot be explained by the properties of the content of stories that we measured; however, there are many aspects of the stories that we were not able to measure that may lead to both strong emotional reactions and to behavior change.

Stopping, Starting, and Paying Attention.

Respondents who reported changing their behavior as a result of hearing the story were also asked to describe one thing they started doing differently, in an an open-ended question: "Please describe one thing you started doing differently after hearing this story." 152 respondents indicated that they changed their behavior, so only 152 respondents answered this question. 57 of these answers were virtually identical to the answers to the question, "What did you learn from this story?" discussed above, and so those responses were removed prior to the analysis of these responses. A similar process to the inductive, bottom-up coding described above was also separately used to analyze the responses to this question.

In general, respondents reported that they stopped doing some behaviors, started other behaviors, and paid more attention to things they previously did not think about or were not aware of.

Some behaviors, like online shopping and downloading files, were perceived as more risky after hearing the story, and respondents reported that they stopped doing these things (#127: "Stopped browsing for free samples online"; #242: "Ceased to order things online"). Respondents reported that they removed information from their online account and social media profiles, (#4: "I withdrew as much of my info from my AOL account as was possible while still remaining a user") and no longer allowed software and web applications to save passwords (#44: "Making sure my computer did not remember any of my passwords"). Finally, a

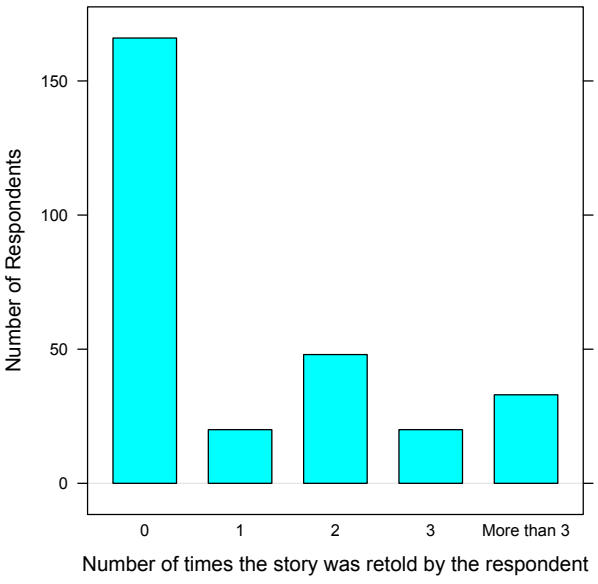

Figure 1: Histogram of How Many Times a Person Retold Their Story

few respondents reported that they stopped going to Facebook (#110: "I pretty much stopped using Facebook") and visiting potentially harmful websites (#150: "I made sure I was never on websites that I wasn't supposed to be on").

Respondents also reported starting activities and behaviors intended to help them be more secure. These respondents indicated in their answers that they had "outsourced" the responsibility to security software in some way, usually by downloading and installing "virus protection" or antivirus (#371: "We downloaded Norton antivirus software. It helped make the computer secure and make everybody feel better"). Other respondents reported taking a more active role by making sure they kept the software updated (#450: "I upgraded my antivirus software and periodically make sure it is up to date") and by initiating scans of files they download (#448: "Started scanning torrent contents before opening. Also reading torrent comments"). One respondent indicated that he or she began keeping other software up-to-date as well (#427: "After learning about how this type of infection works, I started keeping any programs or web plugins up to date that I could...").

Passwords were another area in which respondents reported behavior change. Respondents reported changing passwords (#341), specifically to something "longer" (#103), "unique" across multiple sites (#379), or "random" (#236). (These clearly line up with the lessons participants reported learning about passwords.) Finally, one respondent (#143) reported memorizing passwords rather than writing them down.

Finally, respondents reported that they began to notice and pay attention to things differently than before hearing the stories. This included reading emails more carefully so as to evaluate the risk (#356: "Reading more carefully the subject line in emails") and deleting mails that might potentially be harmful (#270: "Deleting emails that I knew were totally false and potentially dangerous to the safety of my computer"), and keeping an eye on bank accounts and credit card statements (#408: "I watch my account very well and I also made sure my credit card companies are watching my account for any unusual activity").

Table 6: Facts about How Stories Spread

Hearing Stories		*Retelling Stories*	
70%	In home contexts	87%	In home contexts
69%	F2F + Email + IM	89%	F2F
64%	**By** family / friends	97%	**To** family / friends
71%	Heard > 1 month ago	47%	Retold within a day
40%	Heard > 1 year ago	90%	Retold within a week
		43%	Are retold
		11%	Retold more than 3x

4.3 Stories are Retold to Others

45% of our respondents reported telling this story to other people. This is important, because a story has more potential for impact if it is heard by more people. The stories that our respondents heard varied widely in how much they were retold. 11% of the respondents reported retelling the story more than 3 times! Figure 1 describes how frequently our respondents retold the story they heard to others.

When people retell stories, they tend to do so very quickly. 47% of the people who retold did so within a day of hearing the story, and 90% retold the story within a week of originally hearing the story. Presumably, they retell the story while it is still fresh in their head and relevant to the world. However, this is an interesting contrast to the finding above that most of the stories told to us by the respondents are more than a month old. It seems that our respondents retell stories very quickly, but remember them for months or years after originally hearing them. Table 6 contains more information about where stories are heard and how stories are retold.

When people retell stories about security, they almost always retell them in home contexts (87% of retellers), through face-to-face interaction (89% of retellers), and retell them to family and friends (97% of retellers). These numbers are striking in how extreme they are; even though only 64% of stories are heard from family and friends, 97% are retold to family or friends! It seems that when people hear a story that is worth retelling, they turn to family and friends and tell the story in a casual, face-to-face way.

Serious Lessons are Retold.

Stories that contain a lesson are much more likely to be retold than stories without a lesson. Our estimates (Table 7) indicate that the odds of retelling a story with a lesson are 230% higher than the odds of retelling a story that doesn't have a lesson. This translates to approximately a 20% increase in the probability retelling for stories that contain a lesson.

Stories that are about more serious threats are also more likely to be retold. A one point increase (on a 5-point Likert scale) in the seriousness of a threat increases the odds of retelling by approximately 30%. Together, these two results suggest that the kinds of stories that are retold are frequently stories that have lessons about serious security

Table 7: Content influences on the probability of retelling

	Retelling	
(Intercept)	0.167	
Contains a lesson	2.30	**
Seriousness of threat (scale)	1.30	*
Autobiographical	1.07	

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Coefficients are from a logistic regression, and represent the odds ratio for whether the respondent retold the story. Seriousness of threat is a 5-point likert scale. The other two variables are yes/no variables.

Table 8: Source influences on the probability of retelling

	Retelling	
(Intercept)	0.29	
Casual Context	0.88	
Knowledgable Source	1.41	**

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Coefficients are from a logistic regression, and represent the odds ratio for whether the story was retold. Casual context is compared to a baseline of a formal context such as school or work. Knowledgable source is a 5-point Likert scale.

threats. If a story provides advice on how to deal with a serious security problem, then people are more likely to repeat the story to others.

Stories from Knowledgable People are Retold.

Stories that were told by a more knowledgable source are more likely to be retold. A one point increase on a 5-point Likert scale of how much the source knows about security is associated with a 40% increase in the odds of retelling the story. In other words, a story told by someone with an expertise of 4 has on average a 17% higher probability of being retold than a story with an expertise of 2.

It isn't clear why more stories from knowledgable sources are retold. It could be that more knowledgable sources are trusted more, and therefore have more credibility. It also could be that more knowledgable sources tell stories that have more details that make them easier to believe. Future work will follow up on this question.

5. DISCUSSION AND IMPLICATIONS

People tell stories about security, informally to family and friends, that are about specific security incidents. These stories matter for security. They usually contain lessons about security, and people change both the way they think and the way they behave in response to those lessons. And the stories spread; many people retell these stories they've heard to others they are close to.

Stories about security seem to be an overlooked aspect of the security "education" that non-experts receive. People seem to be using these stories to find guidance about how to think about a number of security threats, and to better understand what these potential threats are. Looking at the stories, it appears that the advice they learn is similar to traditional expert advice (from sources such as Microsoft[7], NCSA[8], and US-CERT[9]). Advice from stories frequently contain few specific explanatory details about what happened and why, but it includes more information about why that advice is important. The lessons in the stories are not necessarily bad for security. Indeed, most of the security lessons that our respondents reported seem like sensible, if vague, security advice.

One limitation of this study is that we asked people to report their most salient security story. It is possible that people can more easily remember stories with severe or surprising consequences, rather than stories with good advice. Or, it may be that people can most easily remember stories containing lessons, and that is why we see so many. Our results should not be taken to be representative of the population of stories about security. Rather, we have learned that people frequently are able to tell to us—and by extension, to others as well—stories that they heard informally, affected their thinking and behavior, and that they retold. The most salient stories are the most likely ones to be retold and to spread through the population of people.

From reading the stories, we suspect that another value that the stories have is that they convey the complexity and difficulty of security. Often, security advice from experts comes across as very black-and-white (e.g. "choose good passwords and you will be safe"); however, these stories from our respondents frequently illustrated how much more complicated and situational protecting one's personal computing devices can be. This is an interesting juxtaposition with the explicit lessons we asked our respondents to articulate, which mostly sounded like black-and-white repetitions of standard security advice. We wonder if stories, with all of their contradictions, might actually be better for helping people recognize and deal with security problems after they occur than they are for providing proactive, preventative security advice. Future studies will test this hypothesis.

The stories that people hear from each other influence behavior, by helping people behave in a more secure fashion. Although few of the reported behavior changes are major changes, they do all seem to be working toward increased security. Also, we believe that these stories help to change people's mental models; in other words, stories influence how people think about and perceive security threats and the possible choices they have to respond to threats.

We found a strong relationship between changes in thinking and changes in behavior; this suggests further research to discover whether using stories to change people's understanding of security issues can help them make more secure choices. It is interesting that some things, like the seriousness of the threat in the story, affect thinking and behavior differently. We currently do not have a good theory as to why this happens; following up on this and finding out why it affects thinking but not behavior may help us understand better why people make the decisions they do.

Security knowledge and behavior is influenced by things that happen outside work, school, or other computing contexts. This suggests that stories and storytelling are a new opportunity for intervention above and beyond the ways we currently are trying to influence people's security choices.

[7] `http://www.microsoft.com/security`, retrieved Mar 9, 2012
[8] `http://www.staysafeonline.info/`, retrieved Mar 9, 2012
[9] `http://www.us-cert.gov/cas/tips/`, retrieved Mar 9, 2012

We may be able to help people tell more stories, or tell stories that have more useful lessons. Or we can help stories reach more people than just friends and family by creating a story sharing website. Indeed, social networking sites like Facebook show that people can and do tell stories to each other online; maybe we can harness that to help spread useful security stories?

Storytelling seems to be different than traditional methods of persuasion. It isn't clear that people perceive security as something you do like "eating healthy" or "going green"; rather, security is something that non-expert users deal with in an irregular fashion. Storytelling also seems to happen in a very informal context, and informal contexts usually have more ability to influence behavior[9]. People may not feel like they are being "sold" something by these stories, since the stories come from someone they presumably know and trust. As such, trying to persuade people to be more secure might not work. Rather, this suggests a new approach to addressing computer security management. We should focus on creating or shaping stories to give people the intellectual tools they need to make secure choices, so that when they face security decisions, they are able to make good ones.

6. ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1116544 and CNS-1115926. We also thank Kimberly Setili, Jacob Solomon, and Alcides Velasquez for helping code responses to open-ended questions.

7. REFERENCES

[1] Microsoft Security: The Latest in Computer Security. `http://www.microsoft.com/security/default.aspx`.

[2] Symantec Internet Security Threat Report: Trends for January 06–June 06. Technical report, Symantec, 2006.

[3] I. Ajzen. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50:179–211, 1991.

[4] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4):432–445, June 2010.

[5] C. Anderson. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *Citeseer*, 34(3):613–643, 2010.

[6] F. Asgharpour, D. Liu, and L. Camp. Mental models of computer security risks. In *Workshop on the Economics of Information Security (WEIS)*, 2007.

[7] R. F. Baumeister, L. Zhang, and K. D. Vohs. Gossip as Cultural Learning. *Review of General Psychology*, 8(2):111–121, 2004.

[8] J. Bruner. The narrative construction of reality. *Critical inquiry*, 18(1):1–21, 1991.

[9] R. B. Cialdini. *Influence: Science and Practice*. Prentice Hall, 5th edition, 2008.

[10] L. F. Cranor. A Framework for Reasoning About the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSec)*, 2008.

[11] N. F. Doherty, L. Anastasakis, and H. Fulford. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6):449–457, Dec. 2009.

[12] P. Dourish, R. E. Grinter, J. Delgado De La Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, Sept. 2004.

[13] S. Furnell, P. Bryant, and A. Phippen. Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5):410–417, Aug. 2007.

[14] N. J. Goldstein, R. B. Cialdini, and V. Griskevicius. A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels. *Journal of Consumer Research*, 35(3):472–482, 2008.

[15] J. Gross and M. Rosson. Looking for Trouble: Understanding End-User Security Management. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology*, pages 30–31, 2007.

[16] C. Heath, C. Bell, and E. Steinberg. Emotional Selection in Memes: The Case of Urban Legends. *Journal of Personality*, 81(6):1028–1041, 2001.

[17] C. Herley. So Long , And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *NSPW '09 Proceedings of the 2009 New Security Paradigms Workshop*, 2009.

[18] P. Johnson-Laird, V. Girotto, and P. Legrenzi. Mental Models: A Gentle Guide for Outsiders, 1998. `http://icos.groups.si.umich.edu/gentleintro.html`.

[19] R. Kay and S. Loverock. Assessing emotions related to learning new software: The computer emotion scale. *Computers in Human Behavior*, 24(4):1605–1623, July 2008.

[20] N. Kumar, K. Mohan, and R. Holowczak. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46(1):254–264, Dec. 2008.

[21] F. T. McAndrew and M. A. Milenkovic. Of Tabloids and Family Secrets: The Evolutionary Psychology of Gossip. *Journal of Applied Social Psychology*, 32(5):1064–1082, May 2002.

[22] K. Peters, Y. Kashima, and A. Clark. Talking about others: Emotionality and the dissemination of social information. *European Journal of Social Psychology*, 39(2):207–222, 2009.

[23] L. Steg. Promoting household energy conservation. *Energy Policy*, 36(12):4449–4453, Dec. 2008.

[24] US Census. Current Population Survey, Computer Use and Ownership Supplement, 2009. `http://www.census.gov/population/www/socdemo/computer.html`.

[25] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–16. ACM, 2010.

[26] M. Workman, W. Bommer, and D. Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6):2799–2816, Sept. 2008.

[27] M. E. Zurko. User-Centered Security: Stepping Up to the Grand Challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 187–202. Ieee, 2005.

APPENDIX

A. EXAMPLE STORIES FOR EACH TOPIC

PC Effects.

#22: "I know a guy who told me of this virus that can get into your computer that is embedded in an email or can be hidden in a flash drive that when is connected or email opened will go in and wipe your flash drive and ultimately crash your computer. He told me really only way to monitor and protect yourself is to only open emails from people that you know and to only use your flash drive."

#233: "My friend was on his laptop surfing the internet and his laptop suddenly shut off. He tried turning back on again and the screen wouldn't turn back on. He called tech support and they told his it was a virus that had destroyed his computer. He had to send it in so he could get a new one."

#328: "My family was going to visit my grandparents and when we arrived, my grandpa told us about how their computer had been acting funny and not working as well. Within the couples days before we came to visit, it had even stopped powering completely up or down when they would go to use it. On the day we went to visit it was determined it had somehow got a virus and was no longer good to use."

#377: "My friend decided he wanted to watch some inappropriate videos and went to a shady site. He did not have a firewall or any sort of anti virus so his computer got infected. His computer slowly got worse and worse until he couldn't handle it and took it to his parents. His parents did not know what to do and before they could figure it out, the computer died."

Breaking In.

#7: "So guess what i heard. i heard that the playstation network got hacked by a random group of hackers. They don't even know how to track them down or who they are because they did all of their organizing on 4chan, and the way their system wipes itself clean at a frequent rate so there is no trace of who they are. They completely shut down their system and hacked into peoples profiles. The system was down for a few days."

#176: "My parents told me there was this Hacker that was getting the credit card information from people who ordered through this restaurant online and then buying a whole bunch of expensive things and the people didn't get their money back and had to go through a whole big mess to get their credit straightened out."

#289: "So one of my friends downloaded a free trial of a pretty neat indie game, and wanted to get the full version. He didn't want to pay for the game, and wasn't very computer savvy, so he decided to google "free version of x-game". He clicked the first website that came up which had a list of "free keys" for every single game you could think of. He downloaded the file, unzipped it, and the next thing you know, a hacker was into his computer. He started messaging him on his own aim account through his own name, messing with his files, and installing software. He immediately shutdown his computer, pulled out the Ethernet cable, and restarted. Eventually he called a friend and he told him to go into safe mode and gave him a fix for the specific virus."

Theft.

#5: "I was in class when someone start talking about them having to get a new card because someone tried to switch her credit card Numbers or something like that. She had bought a pair of earring off a site she had never heard off before but she really like the earring. All in all, he card stopped working because he bank had security protection and she called to see why her card was not working and they told her. After that she never bought anything from a weird website again. It scared her!"

#326: "Within the last year, this summer I believe Playstation Network got hacked into. The hackers stole peoples credit card information because people have to pay to use this system. I haven't really heard much about it since relatively soon after this happened, but I believe they were shut down for a little bit trying to make their systems more secure."

#446: "A man put all of his personal information on his computer, such as his social security number and bank account numbers. His computer got hacked and the hacker was able to steal his identity and used his credit cards and got into his bank accounts. He could have avoided this by securing his information or not having it on there at all."

Spam.

#3: "It appears that Facebook has gotten yet another virus and people are posting weird things onto their friends walls without them knowing. So if you get a notification about someone posting on your wall be careful and not directly click on it or else your Facebook might get hacked or a virus"

#391: "My friend had randomly been selected by the hacker who hacked his school email account. and was sending out viruses to every person in his email address. THe person was also trying to send a serious virus to the school that would crash the entire system. The school eventually shut down his email account and gave him a new one hoping that the attempt did not happen again they also never found the hacker."

#460: "I was on the phone with my mom the other day and asked her about a strange email that she had sent me that was talking about working online and how I should apply. I almost clicked on the link but because I don't want to work this semester I decided not to. My mom said she was so glad that I didn't open it because apparently it was spam and was being sent to all of her contacts whom notified her that this was going on even before I had. Thankfully, her computer was not affected by the email."

Phishing.

#12: "Hey, guess what happened to my roommate? She logged onto her facebook and saw that she had chat boxes open to people she hasn't talked to in years (and she never did!) she noticed that she was asking them weird security questions that are normally the ones that people answer for their password protection (What street did you grow up on? What was your first car? etrc.)In the end, she had to change her password and warn ppl to not answer the hackers question."

#115: "A friend was playing the online game, and ended becoming friends with another player. Both of them ended up as being really close in the game and talk about each other's personal life. When this player asked for my friend's

password to level up his character when he wasn't on, my friend thought that was a good idea and did exactly that. A few days later, my friend found that this guy stole his items. Maybe a day or two after that, he found that his IP address had been banned from the game."

#344: "I heard there was an email going around that looks like it comes from your bank. They ask you for your account and credit card information. Do NOT respond to it or click on the link. It is a scam and they are only looking for access to your account to steal your information and your money. The bank already has your information so they have no need to ask for it. They will also never terminate your account for such a reason."

B. APPENDIX B: SURVEY QUESTIONS

Data collected: 2011/11/28 – 2011/12/09 and 2012/01/23 – 2012/02/03

Sample: n = 301, college students, age 18 and older.

INSTRUCTIONS In this survey, we are interested in things you have heard about or learned from others related to protecting your computer and yourself from computer security threats.

These threats might include things like hackers, viruses, identity theft, shady URLs in spam emails, etc. It can be very hard sometimes to tell when you are facing a computer security threat- –symptoms might include when your computer is slow or freezes unexpectedly, when programs won't close, or lock up, unwanted popup windows, spam email, posts appearing in your Facebook account without your permission or knowledge, or other undesirable computer issues.

Sometimes people cope with these threats by using tools such as anti-virus or firewall software, or by making sure to back up their data, or not clicking links or installing apps from people they don't know or trust.

DEFINITION For this research project, we are particularly interested in things you have heard or learned about computer security through stories from OTHER PEOPLE, such as something told to you by a friend, coworker or acquaintance, social media sites like Facebook, blogs and newspapers, or any other sources you can think of. We are NOT interested in something that happened to you personally—only stories you've heard related to computer security that are mostly about other people.

THREATS First, to help you start to remember any stories related to computer security that you might have heard, please name as many different kinds of computer security problems or threats that you can think of.

LEARNING Next, think of all of the different ways you have learned about how to protect yourself and your computer from computer security problems or threats, and make a list of these below.

STORY_LIST Take a moment to think back to times in the past when you remember being told or reading about a story related to computer security.

Please make a list of as many of these stories as you can remember, using only a couple of words to describe each story (you may want to read over your answers to the previous questions to jog your memory).

STORY Finally, please choose one story for which you can most easily recall details about where you were and what happened when you heard or read the story. You will be answering further questions about this story in the rest of the survey. In a sentence or two, briefly summarize what happened.

SOURCE_PAST How long ago did you hear or read the story?

Within the last day	3
Within the last week	28
Within the last month	43
Within the last year	92
Longer than one year ago	122
NA's	13

SOURCE_CONTEXT Where were you when you heard or read the story?

Don't remember	11
At a coffee shop	1
At a friend or relative's house	37
At home	174
At work	10
In a computer lab	2
In class	42
In the library	6
NA's	18

SOURCE_MEDIUM Via what medium did you hear or read the story?

In person (face-to-face)	165
Phone	13
Text message	4
Chat (instant messaging)	3
Video chat	2
Email	21
Blog post	4
Social network site (Facebook, Twitter, etc.)	23
Print news media (physical newspaper, magazine, etc.)	5
Broadcast news media (TV, Radio, etc.)	19
Online news media (CNN.com, Yahoo News, etc.	27
Don't remember	4
Other	11

SOURCE From what source did you hear or read the story?

Family member	79
Friend	113
Acquaintance	7
Coworker or Boss	3
IT or Computer Repair Person	5
Stranger	8
News Institution	34
Don't Remember	14
Other	37
NA's	1

SOURCE_EXPERT How knowledgeable do you think the source you selected above is about computer security? Please rate the source's knowledge from 1 (Not Knowledgeable) to 5 (Very Knowledgeable).

1	17
2	40
3	66
4	73
5	52
NA's	53

RETELL Did you tell, send, post, or otherwise share this story with anybody else?

Yes	135
No	166

RETELL_NUMBER Approximately how many times did you share the story?

1	20
2	48
3	20
More than 3	33
Don't remember	14
NA's	166

RETELL_CONTEXT In what context did you share the story (select all that apply)?

At work	26
At home	84
At a friend or relative's house	73
In class	44
In the library	0
At a coffee shop	2
In a computer lab	6
Don't remember	7
Other	6

RETELL_MEDIUM What medium did you use to share the story (select all that apply)?

In person (face-to-face)	120
Phone	34
Text message	22
Chat (instant messaging)	19
Video Chat	1
Email	9
Blog post	3
Social network site (e.g. Facebook, Twitter, etc.)	25
Print news media (newspaper, magazine, etc.)	1
Broadcast news media (TV, Radio, etc.)	0
Online news media (CNN.com, Yahoo News, etc.)	0
Don't remember	1
Other:	1

RETELL_SOURCE With whom did you share the story (select all that apply)?

Family member	87
Friend	113
Acquaintance	17
Coworker or Boss	21
IT or Computer Repair person	3
Stranger	2
News Institution	1
Don't Remember	2
Other:	4

RETELL_TIME How long after you first heard or read the story did you first share it with others?

Within one day	64
Within one week	57
Within one month	10
Within one year	0
Longer than one year	2
Don't Remember	2
Other	0

RETELL_WHY Please briefly describe why you shared this story with others.

CONTENT_PROTAGONIST Who or what was the "main character" (the protagonist) in the story (select all that apply)?

Family member	69
Friend	101
Acquaintance	18
Coworker or Boss	6
IT or Computer Repair person	5
Stranger	54
News Institution	5
Don't Remember	14
Other:	51

CONTENT_SOURCE Was this story about the same person who told the story to you?

Yes	154
No	129
Don't Remember	12
Other	5
NA's	1

CONTENT_THREAT How serious was the threat or problem? Please rate the severity from 1 (Not Serious At All) to 5 (Very Serious).

Not Serious (1)	10
(2)	55
Serious (3)	81
(4)	73
Very Serious(5)	82

CONTENT_ENDING Did the story end well or badly for the main character? Please rate the outcome from 1 (Very Well) to 5 (Very Badly).

Very Well (1)	47
(2)	58
Neither well nor badly (3)	107
(4)	54
Very Badly (5)	33
NA's	2

CONTENT_SUCCESS In general, was the story about something you should ALWAYS do (e.g., wash your hands after using the bathroom), or something you should NEVER do (e.g., stick your tongue to a frozen flagpole)?

Always do	56
Never do	121
Both	41
Neither	82
NA's	1

CONTENT_MORAL What did you learn from this story?

REACT_EMOTION This story made me feel:

	Not at all	Somewhat	Mostly	Extremely	NA's
Satisfied	176	74	38	10	3
Disheartened	88	119	78	14	2
Anxious	102	127	60	10	2
Irritable	129	83	71	15	3
Excited	237	34	20	6	4
Dispirited	134	117	34	12	4
Insecure	108	122	48	19	4
Frustrated	101	86	78	32	4
Curious	68	103	105	23	2
Helpless	148	99	34	16	4
Nervous	127	101	56	16	1
Angry	118	84	61	35	3

REACT_CHANGE Did you start doing anything differently to try to protect yourself from computer security threats or problems after hearing this story?

Yes	154
No	145
NA's	2

REACT_CHANGE_HOW Please describe one thing you started doing differently after hearing this story:

REACT_TRUE Do you believe this story actually happened?

Yes	285
No	3
Don't Know	13

REACT_MORAL Please briefly summarize what you feel the main point or "moral" of the story might be:

REACT_THREATS How much do you think hearing this story has affected the way you think about computer security threats? Please rate it from 1 (A Lot) to 5 (Not At All): *[Reverse Coded]*

A lot (1)	33
(2)	54
Moderately (3)	138
(4)	59
Not at all (5)	17

FULL_STORY At the beginning of the survey, you entered this brief summary of a story, you remembered being told or reading about, related to a computer security threat or problem. Below, please write the story as if you were telling it to a friend. Use as much detail as you can, including any thoughts or recollections you might have had about what happened as you were filling out the survey.

AGE What is your age?

GENDER What is your gender?

Female	119
Male	179
NA's	3

RACE What is your Race? Indicate one or more races that you consider yourself to be (select all that apply):

American Indian or Alaska Native	5
Asian or Pacific Islander	25
Black or African-American	36
Hispanic or Latino	17
White	224
Other:	4

MOTHER_EDUCATION What is the last grade or class your mother completed in school?

2	None, or grades 1-8
0	High school incomplete (grades 9-11)
44	High school graduate (grade 12, GED certificate)
10	Technical, vocational school AFTER high school
87	Some college, no 4-year degree
115	College graduate (B.S., B.A., 4-year degree)
34	Post-graduate
7	I Don't Know
0	Other
2	NA's

STUDENT Are you a full- or part-time student?

Yes, full-time student	291
Yes, part-time student	10
No, not a student	0
Other	0

COMPUTERS What kinds of computing devices have you used in the past week (select all that apply)?

Desktop Computer	137
Laptop Computer	295
Smart Phone (e.g. iPhone, Android phone)	220
Tablet PC (e.g. iPad)	50
Game Console	153
Other:	14

ACTIVITIES Which of the following activities have you done in the past week (select all that apply)?

Social Networking	291
Email	299
Watch Streaming Video (e.g. Netflix)	249
Chat (instant messaging)	227
Texting	293
Download smartphone apps	162
Play online games	171
Online Banking	190
Shopping Online	176
Turn in Class Assignments	278

DIGITAL_LITERACY_Q1 How familiar are you with the following Internet-related items? Please rate your familiarity with each term below from None (no understanding) to Full (full understanding).

	None	Little	Some	Good	Full	NA's
Modem	9	55	78	94	65	0
Browser	1	15	42	110	132	1
Server	6	36	84	113	62	0
ISP	44	75	82	56	43	1
HTML	10	41	80	97	71	2
"BCC" in email	79	74	66	28	54	0
Flaming	134	67	45	18	37	0
Spam	5	37	61	93	105	0
Spider	160	73	40	8	20	0
Boolean expression	148	53	39	20	41	0
MP3	1	8	33	88	170	1
JPG	7	17	39	91	146	1
XML	69	62	60	49	60	1
Natural Language	107	68	59	39	26	2
.gov ("dot gov")	15	32	60	81	113	0
Click-through	76	71	62	39	52	1
Usenet	121	80	53	12	33	2
Cookie	22	57	67	83	72	0
DNS Parking	154	70	43	9	23	2
Mirror site	133	60	41	23	42	2
P3P	158	73	37	14	19	0
Meta-tag	169	71	25	12	22	2
Shareware	118	58	46	38	40	1
Newsgroup	112	68	56	27	36	2
PDF	5	15	37	101	143	0

DIGITAL_LITERACY_Q2 In terms of your Internet skills, do you consider yourself to be . . . .

Not at all skilled	0
Not very skilled	16
Fairly skilled	155
Very skilled	108
Expert	21
NA's	1

HIGHTECH Have you ever worked in a "high tech" job such as computer programming, IT, or computer networking?

Yes	37
No	260
Other	4

COMP_TYPE What type of computer do you use most often?

Mac	172
PC	123
Other	6