2012 IEEE Symposium on Security and Privacy

The Psychology of Security for the Home Computer User

Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska
Computer Science Department
Colorado State University
Fort Collins, CO 80523 U.S.A.
Email: {howe, indrajit, mroberts, urbanska}@CS.ColoState.EDU

Zinta Byrne
Psychology Department
Colorado State University
Fort Collins, CO 80523 U.S.A.
Email: Zinta.Byrne@ColoState.EDU

***Abstract*—The home computer user is often said to be the weakest link in computer security. They do not always follow security advice, and they take actions, as in phishing, that compromise themselves. In general, we do not understand why users do not always behave safely, which would seem to be in their best interest. This paper reviews the literature of surveys and studies of factors that influence security decisions for home computer users. We organize the review in four sections: understanding of threats, perceptions of risky behavior, efforts to avoid security breaches and attitudes to security interventions. We find that these studies reveal a lot of reasons why current security measures may not match the needs or abilities of home computer users and suggest future work needed to inform how security is delivered to this user group.**

***Keywords*-usability and security, home users**

I. Why Study the Home Computer User?

The home computer user is often said to be the weakest link in computer security. Security and privacy threats such as Web cookies and phishing require some form of user complicity or acquiescence. Adequate security does not come with the purchase of the computer but requires additional software, careful settings within applications, appropriate choices of passwords, regular updating of patches, etc. Moreover, as applications are becoming more interesting/useful and businesses are moving away from paper, home computer users are performing more sensitive tasks online and storing more private data on their computers. Anecdotal evidence, surveys, and studies suggest that home computer users often do not adequately understand the threats, or have the time, desire and knowledge to be able to handle them. As large outbreaks of worms and viruses have shown, even systems administrators are not diligent enough in applying patches to improve security [1].

Although home users are frequent targets of attacks[1] and the security software market (primary source of defense for home users) currently brings in more than $4 billion[2], relatively little is still known about how the home user views security threats, privacy threats, and defenses. Various surveys (e.g., [5], [6], [7]) show that many home computer users do not adequately maintain their home systems to support security and often ignore or simply do not act in ways that would keep them secure. Thus, security should be improved overall if developers better understand what influences decisions about security for the home computer user. In this paper, we review studies about the attitudes, perceptions and actions of home computer users. Current defense measures (e.g., patches, anti-virus software, pop-up security warnings) are clearly not working as well as we need; therefore, better knowledge of how users perceive security threats and what the users appreciate about the consequences of their actions can be leveraged to develop more effective interventions and countermeasures.

Whether and how to keep one's computer secure are decisions made by each and every computer user. A survey of 415 home computer users in the U.K. recruited through email and different Web forums [8], [5] showed that 90% of respondents agreed that home users were responsible for the security of their computers. In a followup interview study of 23 participants, Australian users also stated they believed the end-user was responsible for security [9].

Aytes and Connolly [1], [6] identify five factors that influence users' decisions of how to keep their computer's secure: 1) awareness of what constitutes safe practices, 2) awareness of possible negative consequences of not following safe practices, 3) awareness of availability of resources to support safe practices, 4) probability of negative consequences and 5) cost of the consequences. This review divides these factors into two general categories: knowledge of security risks and consequences, and knowledge of defensive security actions (i.e., safe practices). We first discuss some demographics of the home computer user as found in the studies, and follow with what is known about these two categories of factors influencing user behavior. Presenting a cohesive, comprehensive view is impossible as the studies asked different questions, had different goals, solicited participants in different ways and sometimes are temporally disconnected (the oldest study is from 1999, most recent from 2011). Longitudinal studies are lacking. However, we point out commonalities and differences in results and where possible

[1]A 2007 Symantec report states that 95% of attacks were directed at home users [2].

[2]The exact number is difficult to find. This figure probably is for anti-virus software sales overall [3]. The total for security software may be as high at $14 billion this year [4], but because of business sales, it is impossible to tease apart impact of the home user.

DOI 10.1109/SP.2012.23

posit explanations. We conclude with a discussion of gaps in our knowledge of behavior and needed future work. In each case, when a study is introduced, a short description is provided about the number and type of participants and the methodology used (e.g., survey, interview, automated data collection via their computers).

II. The Home Computer User

One of the more difficult aspects of the studies conducted on this topic is that there is no canonical home computer user. Users may be adults performing normal household tasks such as shopping and banking, parents helping their children use educational software, retirees who primarily email their grandchildren, or college undergraduates who have been using computers since pre-school. The population of home users is diverse and huge. Exactly how large worldwide is difficult to know; as an upper bound, Gartner estimates that 2 billion personal computers will be in use by 2014 [10]. For the purposes of this paper, the distinguishing characteristic is that the users are not professionals in computing: they use the computer for all kinds of tasks to support their lives, but they do not develop for it and tend to have little to no formal training in the use of their computer. We also generally limit the discussion to users of computers in the home environment; computers and users in the work environment often have access to IT professionals via their employer and are required to follow employer's rules for the workplace equipment.

A. Demographics/Characteristics from Studies

Studies often focus on a particular user community. For example, Solic and Ilakovac surveyed 39 university faculty from electrical engineering and medical schools who were given laptops by their schools, to assess their attitudes toward security and identify potential differences in these two groups [11]. Friedman et al. [12] conducted semi-structured two hour interviews of 72 adults (ages 19-75) from three different communities (rural in Maine, suburban professional in New Jersey and high-technology in California) to identify what risks concerned them most about Web security and determine whether there were differences between these communities. Diesner et al. [13] surveyed educated users in India because many international corporations are locating their global data centers in India, suggesting that as a country, India may have more access to personal data. Undergraduates are the focus of multiple studies because they tend to have a high level of computer usage/familiarity and are a readily available sample. Aytes and Connolly [6] conducted a wide ranging survey of undergraduates at two different U.S.A. universities to assess their knowledge of risks and the actions they take to address the risks. One purpose of studies comparing two different groups (e.g., the different universities) is to assess generality of conclusions: can the results of one study transfer to larger or different groups of user?

In most cases, basic demographic information was obtained (e.g., age, gender, education), but the reports did not often describe significant effects due to the demographic information. As counter examples, one survey [8] found that women were less likely to rate themselves as advanced users. A survey of 493 users of online shopping services [14] resulted in a model in which "male" and "college graduate" exerted a positive influence on tendency to engage in risky behaviors online. Socioeconomic demographics may also be germane; participants in [9] made comments such as "I don't earn over $40,000 a year so there is no reason for someone to attack my computer . . ." and "I don't think anyone would attack my home computer, there is nothing important on it," suggesting that they believed that only wealthy people are targeted by security threats. Age may also play a significant role. In a study that included both college aged and older adults, the researchers found that older adults tended to perceive a lower risk from a threat involving loss of data confidentiality than college aged adults [15].

Often general information related to their computer use (e.g., how much formal training they had, how much experience they had with the Internet, what operating system/kind of computer they used) was important, but needed to be carefully examined as self-reports were sometimes at odds with other evidence. For example, some respondents with as little as two years of using the Internet claimed to be advanced users [8]. The type of computer/operating system was part of a general trend in usage. Users of Macs [16] and PCs with LINUX [11] tended to use security software at a lower rate, often not at all, because they felt that their operating system choice made them invulnerable.

Home computers are often shared among multiple users, which can make it difficult to tease apart the activities and motivations of the users. One survey found that 30% of respondents had computers used by children up to age 18 [8]. Children may heighten the awareness of privacy issues and cause security issues of their own because they are less likely to be aware of the security consequences of their actions.

In the 2007 U.K. survey, the most common activities for home computers were Web browsing and e-mail (97% and 99% surveyed, respectively), but more than 50% also used their computers for shopping, auctions, instant messaging, education, banking, and work [8]. Similarly, in a 2011 Pew study of computer usage in the U.S.A., the most common activities for adults were e-mail (92% of users), searching for information (92%) and looking for health or hobby information (83%), but more than 50% of the users engaged in other activities such as shopping, watching videos, banking, social networking, etc. [17].

The percentage of people affected by security and privacy problems is significant. In a survey of 1000 people selected through randomized telephone calling in Michigan in 2007,

the problems that the respondents experienced most on their computers were: spam (67%), computer running slower (57%), spyware (42%), computer virus (35%), phishing scams (34%), and new icons or programs appearing on the desktop out of nowhere (25%) [18].

Generally, the studies encompass between 20-500 participants. A few notable exceptions were the Pew Internet studies such as [17] that included 1522 adults, the NCSA/Symantec survey of 3,500 adults [7] and the Florêncio and Herley study of Web password use where the authors obtained data from half a million users over a period of three months by adding an optional module to the Windows Live Toolbar in Summer/Fall 2006 [19].

B. Sources of Information

Various studies report significant gaps in education and knowledge of home users. A significant issue therefore is the user's sources of information: from whom or from where are they learning about computer security and privacy issues and actions? The most common sources of security information in the 2007 U.K. study were found to be public information websites (43% of respondents), IT professionals (43%) and friend or relative (41%) [8]. In the followup in Australia [9], the most common source of advice was the local computer store. An interview-based study of how home users might work with others in setting up and maintaining home computer networks found that because maintaining a home network was so much work and required so much knowledge to do so, users often rely on outsiders (e.g., friends, technicians) to help them troubleshoot problems [20].

In a study from 2004 [6], undergraduates self-reported a high level of knowledge about using email (93% report knowledgeable or expert) and protecting their computers from viruses and crashes (69% are knowledgeable or expert). However, their most common sources of information were friends and co-workers (52%) and personal experience (42%). Only 19% received formal security training/education. In contrast, the NCSA/Symantec survey of 3,500 adults [7] noted that 43% had security training of some type. These differences probably arose from how the users were asked about their sources of information and prior training as well as the demographics of the surveys (undergraduates versus adults) and the time that had elapsed (2004 to 2010).

Considerable effort has been expended by government and commercial entities to produce websites to educate the public; one study [8] revealed relatively low levels of recognition/familiarity of their respondents to four high profile sites in the U.K. (www.getsafeonline.irg, www.itsafe.gov.uk, www.internetsafetyzone.com, and www.bbc.co.uk/webwise). So while users are obtaining information from the Web, it may not always be from carefully vetted sources.

III. Predictive Models

Several studies were designed to assess the accuracy of predictive models of specific security and privacy behaviors. Often the models are extensions of existing social cognitive theories of factors that produce risky behavior in other decision situations, e.g., preventive health [21], crime control, environmental protection. Two types of models are prominent: Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT).

TPB [22] identifies intention as the primary determinant of specific behavior and focuses on three motivational factors that directly predict intention to behave:

1) *Attitude toward the specific behavior:* person's inclination to perform some behavior; is it valued?
2) *Subjective Norms:* person's perception of society's view on whether to perform the specific behavior.
3) *Perceived Behavioral Control:* how capable the person thinks he/she is to perform the specific behavior.

Perceived Behavioral Control is considered quite important because even should a person have the wherewithal to act, his or her perception of his or her own inadequacy may preclude acting. Additionally, Perceived Behavioral Control can be used as a proxy for measures of actual control. Thus, models can include both direct and indirect paths. The model is often quantified as a regression model. Models based on TPB have been used with considerable success (accounting for a good portion of the variance) to predict adoption of a wide variety of behaviors.

PMT [23] was developed to explain how appeals to fear can change behavior. The theory has three components: perceptions of the severity of the threat, probability of its occurrence, and efficacy of the protective response. Perceptions of threat can include both costs of the risky behavior as well as costs of avoiding it, e.g., by not giving out some information, you may not be able to access an online service of interest. Self-efficacy is a person's belief in his or her own ability to produce the intended effects through behaviors [14]. Self-efficacy can be divided into response efficacy (belief the action will be effective) and coping self-efficacy (belief in one's own ability) [24]. The behaviors can be adaptive (protective) or maladaptive (avoidance); a core idea is that high self-efficacy results in adaptive behaviors. As with TPB, the three components can be viewed as factors in factor analysis or regression modeling to predict the intention to behave in the desired manner.

IV. Security Risk and Consequences

In [25], Ryan West summarizes principles of psychology as related to computer security: people underestimate risk, people have limited time and mental resources, security consequences are hard for people to assess because they are abstract and hypothetical and that losses are perceived as higher magnitude than gains. These principles provide an

excellent general starting point to identifying factors that influence home users' understanding of security risk and consequences. User studies have assessed users' knowledge of the range of security and privacy threats, and of what might happen as a consequence of them. In some cases, researchers have tried to capture the cognitive models that users develop to understand the threats, with the goal of improving education by explaining security in terms that users are more likely to understand.

A. Understanding of Threats

People use metaphors or mental models to think about complex processes. Camp et al. [26] collected conceptual models from the security literature and compared how different groups (experts and non-experts) associated these models with key terms from security. The five models[3] were: Physical Safety, Medical Infections, Criminal Behavior, Warfare, and Economic Failure. The security terms were: trojan, keystroke logger, junk mail, virus, worm, hacking, binder, exploit, zombie, authentication, click fraud, password, userid, firewall, backdoor, blacklist, spoofing, address book, honeypot, drive-by-download, dos attack, spam, phishing, spyware, adware, cookies, and identity theft. They used a card sorting procedure in which subjects were asked to assign each term a color that corresponded to one of the models; the subject's ability to do this task was checked by having him or her assign words chosen as synonyms from a thesaurus. The study showed that subjects found some words, e.g., firewall and userID, difficult to categorize. The data also showed considerable disagreement between the experts and non-experts in categorization of words to models, especially as the definition of expert was narrowed to require five years of computer security experience. This study suggested that security experts may have difficulty communicating threats and risk to non-expert users and that other ways of educating users about security are needed.

Mental models of attitudes towards threats can also be assessed as associations between terms. Diesner et al. [13] conducted interviews with a cross-section of 29 educated adults in India to determine their attitudes about privacy and security. Participants were asked 17 open questions about their understanding of privacy and security, their knowledge of risks and protections, and their concerns about availability of personal data on computers. The goal was to determine how much importance/concern was placed on security and privacy. The data were analyzed by identifying and extracting key terms as concepts and then organizing the concepts in a network of relations (in a process called "map analysis"). The resulting networks (mental models) suggested that participants focused on personal information and knowledge as the crux of security and privacy, that security related terms are not central concepts in subjects' minds, and that concerns about privacy and security do not appear as prominent as concepts with positive meanings.

Another approach to understanding how home computer users view threats is to construct "folk models" of their knowledge and perceptions. Wash [16] conducted semi-structured interviews with 23 participants in a first round and 10 in a second round in which he asked about their perception of threats and defensive actions. Participants were found via a snowball sample of home computer users in three cities in the U.S.A. The first round explored familiarity with security problems and countermeasures; the second round introduced hypothetical scenarios and asked participants for their reaction. From the qualitative data, Wash identified four folk models concerning viruses[4]:

- *Bad* reflected low understanding of how viruses were created and a vague notion that viruses could have 'bad' consequences.
- *Buggy Software* characterized viruses as regular software that includes a lot of bad bugs. The software must be intentionally placed on the computer and has consequences similar to that of software with bugs (e.g., crashing, deleting data).
- *Mischief* allowed that viruses are created by malicious hackers and have annoying consequences such as those in the 'Buggy Software' model. Viruses are caused by actively clicking on attachments or by visiting 'bad' parts of the Internet.
- *Crime* viewed the purpose of viruses to be to collect personal information to be used by criminals without otherwise harming the computer. Viruses can be acquired by clicking on attachments, downloaded from websites or actively placed on the computer by hackers.

The group who viewed security as the 'Bad' model were generally unconcerned with the threat. The 'Buggy Software' group were also not concerned with the threat because they avoided downloading software they did not trust. The 'Mischief' and the 'Crime' groups appeared more concerned with the threat. Finally some participants believed multiple of the models. These models suggest that home computer users have little understanding of malware threats.

Three categories of concern (people, information, technology) were found in a study comparing conceptions of Web risks and harms among different communities (rural, suburban, high-tech) in 2002 [12]. *People* reflected concerns about the online experience and social issues, and was further divided into: user's experience, trust, online identity, online interactions, children's welfare and other. *Information* captured the handling and dissemination of data, specifically: quality, management, security, privacy, content, spam and

[3]In [27], the models are described in some detail and another model, Market, is added to the set.

[4]Because all participants used the term "virus" to encompass malicious software, in these models, "virus" referred to a variety of malware including viruses, adware, and spyware.

other. *Technology* referred to harms to the hardware and software, and was divided further into: specific technologies, threat to computer systems and other. The interview allowed participants to describe their own concerns, including if they had none.

Several other trends were noted in the results [12]. First, each community differed in their concerns: 21% of the rural participants had no concerns; all of the participants from other groups had concerns. There were no observed differences in the level of concern about information security and information privacy (21% of rural for both, 46% of suburban for both and 63% of high-tech for both); this suggests that the participants may not have been distinguishing the two. Second, the participants did agree about the importance of a few categories. For each of the groups, the issue with the highest percentage of participants concerned was: "threat to computer systems" (at 38%) for rural and "security" or "privacy" for suburban and high tech (at 46% and 63%, respectively). All three were generally more concerned about "information" than the other two categories. These results can be interpreted to mean that security solutions need to be adjusted to suit the groups or alternatively that the suburban and rural groups may develop more toward those of the high-tech group with increased experience. Given the age of this study, a followup should be conducted to see how the trends have changed.

Semi-structured interviews of 33 people from 15 households had the goal of understanding how home users viewed access to personal files and data and what would constitute an ideal access control policy [28]. The participants were solicited through flyers and distribution lists. The study found that most participants (18 our of 33) were highly concerned about unauthorized access to personal data.

The U.K. survey [5] showed a high self-reported level of understanding of key security threat terms: $> 90\%$ for "virus", "hacker", "firewall" and "identity theft", $> 80\%$ for "spyware", "worm" and "trojan horse", 68% for "phishing". The authors pointed out that although they cast a wide net for recruitment most of the participants reported a higher than average level of education. Paradoxically, the knowledge does not appear to translate into action; the percentage of users who had installed software to address the threats was smaller than their knowledge of the terminology was: 22% lower for spyware, 8% lower for anti-spam installation versus phishing, and 9% lower for firewall.

Unfortunately, self-reported knowledge and understanding of threats may not translate into safe behavior. In a simulation study of phishing attacks [29], even sophisticated users could be fooled by faked websites. The study asked participants to judge a set of 20 websites for whether each was legitimate or a fake. Nine of the websites were selected from actual phishing attacks identified in summer 2005; three were constructed using advanced techniques identified by security organizations that monitor phishing attacks; one website required the user to accept a self-signed SSL certificate, and the remaining seven were legitimate. Participants were given access to a fully functioning website for each using a Firefox browser under Mac OS X; they were told they could interact with the browser as normal and allowed them to open other browser windows if they wished. The 22 participants included students and staff at a U.S.A. university who were given $15 for their time. All participants were familiar with the use of computers and the Web; 86% were in non-technical fields.

In judging the 20 websites, correct identification scores varied from 6 to 18, with a mean of 11.6. Participants who judged only from the content of the website (e.g., logos, designs, information displayed) had the lowest accuracy (mean=7.6). The most successful participants also looked at domain name, prefix of HTTPS and presence of a padlock icon – even when they reported that they did not know what an IP address or SSL was. 15 participants clicked "OK" on the self signed security certificate without reading the warning. Generally, the authors concluded that participants lacked critical computer and security knowledge (e.g., seven had never heard of phishing before), but that more experienced participants could still be fooled by visual deceptions.

B. Perceptions of Risky Behavior

In studies and surveys, risk has been examined as a general characteristic of activities online or with respect to specific behaviors. When asked about their confidence in the overall security of their computers, the U.K. survey found that 70% were satisfied/confident, and that level of confidence was correlated with level of experience (the more experienced, the more confident)[8]. Similarly, in the Online Safety Study in 2010 [7], 85% of the 3,500 respondents felt that their home computers were secure; their primary security/privacy concern was identity theft.

When asked about specific behaviors in a 2004 study of undergraduates [6], fewer than 12% felt there were no negative consequences from the following risky behaviors: opening email attachments, sharing passwords, and not backing up their disks. They were most aware of the problem with email attachments, with all but 4% recognizing the possible danger. They did not, however, think they personally would suffer as 40% estimated that the negative consequences would happen to them "never" or "rarely".

Security measures to discourage unsafe behavior and heighten a user's perception of risk are often designed around cues specific to situations. For example, secure transactions on the Web should be done via an https URL, something a user should look for when banking or shopping. Two studies of students at the University of South Australia examined the effect of graphics in emails to help identify phishing threats [30]. The first study showed 75 students a survey form that contained a risk message and a semantic differential grid (a grid that solicits opinions about charac-

teristics of the message); one group received the form with a graphic embedded behind the message and the other without. The semantic grid collected reactions on three dimensions (evaluation, potency and activity) captured as characteristics such as active versus passive and strong versus weak. They found no significant difference with or without the graphic. A second study tried moving the graphic and also showed no significant difference. Thus, it is hard to influence a user's perception, and graphics may not be the way to emphasize risk in a computer message.

Different online activities incur different levels of risk and exposure to threats. Milne et al. [14] hypothesized that self-efficacy was a strong determinant in a shopper's tendency to engage in risky behaviors online. They developed a protection motivation model based on PMT that relates perceived online threats, perceived likelihood of online threat and self-efficacy to adaptive (actions taken with some business to ensure safety online), maladaptive (avoidance of online shopping), risky (security specific actions that enhance online risk) and protective behaviors (security interventions to mitigate risk). Ultimately, the idea is that if specific factors can be shown to push people away from risky behaviors and toward adaptive and protective behaviors, then these factors might be exploited in training programs. They recruited 449 online shoppers from a commercial opt-in consumer panel and asked them questions to assess the three factors and four types of behaviors. Questions included:

- *Perceived Threat* "I am concerned about having my identity stolen while shopping online." (5 point scale from strongly disagree to strongly agree)
- *Perceived Likelihood* "How likely is it for one's identity to be stolen while shopping online?" (5 point scale from very unlikely to very likely)
- *Adaptive Behavior* "In the past year, have you asked an online business to remove your name and address from any lists they use for marketing purposes?" (yes or no)
- *Maladaptive Behavior* "In the past year, have you avoided online shopping to avoid risk?" (yes or no)
- *Self-Efficacy* "I am skilled at avoiding dangers while shopping online." (5 point scale from strongly disagree to strongly agree)

The risky and protective behaviors were assessed by asking participants to select behaviors from a list of possibilities: 16 protective behaviors such as installing virus checkers and using anonymizers while browsing, and 33 risky behaviors such as saving passwords on computers and downloading unknown files from social networking sites.

Regression models built from the results of the survey showed that self-efficacy had significant positive effects on adaptive and protective behaviors, and significant negative effects on maladaptive and risky behaviors. In other words, users who felt confident in their abilities had a stronger tendency to take actions to protect themselves. For the other two factors, they found that perceived likelihood had a significant effect on adaptive behavior, but perceived threat did not. In contrast, they found that perception of threat exerted a significant positive effect on maladaptive behaviors, but perceived likelihood of threat did not. Neither factor had a significant effect on risky or protective behaviors. These results suggest that online shoppers responded more appropriately to knowledge of probability of negative threats than to knowledge of the threats themselves.

Byrne et al. [15] examined how the presence of specific Internet threats influence users' views of their levels of vulnerability and risk. The Internet threats examined were:

- *Availability:* computer resources are improperly made inaccessible,
- *Integrity:* data on the computer is modified without the user's authorization,
- *Confidentiality:* sensitive information is revealed without the user's approval and
- *Unwitting Accomplice:* user unintentionally spreads the threat to others.

Two levels of each threat (low and high) were represented.

The study used policy-capturing in which 104 subjects were asked to judge cues that were systematically varied across a set of 16 vignettes. Two groups of participants were recruited via flyers in places they were likely to frequent. The two groups, young adults between 18 and 29 years and adults of 50 years or older, were the focus because they were felt to be especially vulnerable to security threats. They were asked questions about their level of basic computer knowledge (two questions on a 6-point scale from "no knowledge" to "extensive"), extensiveness of computer knowledge (eight questions on a 5-point scale from "strongly disagree" to "strongly agree"), self-perception of computer knowledge (one question), frequency of computer usage (one question), and prior exposure to privacy invasions (one question). The experiment was conducted as an online survey; the participants were presented with vignettes corresponding to the four threats and asked to respond to questions about their perceived level of risk (6 point scale from "no risk at all" to "highest level of risk") and vulnerability (6 point scale from "not vulnerable at all" to "extremely vulnerable"). The vignettes were variations on a scenario in which the participant received an email containing an embedded link that would access a dollar-off coupon and then described a series of actions triggered by clicking on the link. The actions corresponded to the threats; for example, to simulate a low availability threat, the act of printing the coupon would cause the Web browser's history to be removed.

The data from the policy-capturing study were analyzed using hierarchical linear modeling to assess the importance of the cues for each participant as well as between participants. The analysis showed that all four threats increased ratings of risk and vulnerability perceptions. Interestingly, it also showed that participants with more extensive computer

knowledge gave more weight to integrity threats than did other participants when rating risk perceptions. Those who reported higher levels of self-perceived computer knowledge gave more weight to threats of integrity when responding to their perceived vulnerability levels. This suggests that better understanding of computers in general may translate to better appreciation for the consequences of risky actions.

One of the services most likely to put users at privacy risk may be Facebook. A 2007 report by Privacy International [31] assessed the privacy practices of 21 Internet service companies; Facebook was one of seven that received an assessment of "substantial and comprehensive privacy threats" (only Google fared worse). User attitudes toward social networking and Facebook have been well studied and, generally, are beyond the scope of this review. However, the results of studies by Debatin et al. [32] and Govani and Pashley [33] highlight the need to consider user perceptions of both risk and benefit when encouraging secure behavior. In [32], 119 undergraduates in the U.S.A. took an online survey of 36 multiple choice questions. The first set of questions asked about their Facebook setup and habits (e.g., how long they had an account, how often they check their account, what types of personal information were in their profile, whether they signed up under their real name). The second set assessed users' privacy practices: familiarity with Facebook's privacy settings, protections on their own profile and when they adjusted the privacy settings. The third set assessed the role of friends: how many friends and what type of friends they accept. The fourth set assessed the perceived benefits of Facebook: "Do you feel that Facebook helps you interact with friends and people?", "Do you think you would have less contact with friends if you didn't have your Facebook account?" and "What role does Facebook play in your everyday life?" (very important/not important). The fifth set assessed the perception of potential risks by asking whether participants had encountered any of 1) unwanted advances, stalking or harassment, 2) damaging gossip or rumors, or 3) personal data stolen/abused by others; participants were asked whether the same problems may have happened to other people. Finally, the participants were asked whether they would change their account setting if they were to hear of such incidents.

The results of the Facebook survey showed that 91% of participants were familiar with the settings and were also likely to restrict their profile privacy settings (77%). However, their restrictions were fairly weak with half restricting to "only friends" and the definition of "friend" comprising a large group of people (38% of participants had > 300 friends, 42% had $100 - 300$ friends). The participants also reported revealing a great deal of personal information on their profiles; 90% included their real name, gender, date of birth and hometown, and $1/3$ provided personal contact information. A paired-samples t-test comparing the perceived benefits to the perceived risks showed a statistically significant difference ($p < .001$) between benefits (higher) over risks. The results also showed that participants were more likely to perceive risks to others' than to themselves and were more likely to change their privacy settings if they personally had an invasion of privacy over hearing of such an incident in others.

Additionally, even when informed of the privacy settings, users may not change their behavior. A pilot study surveyed 50 undergraduates at Carnegie Mellon University, asking about how they used Facebook and its privacy settings [33]. The experiment also downloaded each participant's Facebook profile before and five days after the survey; the "after" profile showed remarkably little change in the contact information that was being included in the participant's profile (e.g., 6.4% drop in primary emails, 8.3% drop in street addresses and no drop in telephone numbers listed). The two Facebook studies suggest that some services are viewed as so essential that users will incur the risk.

V. Defensive Security Actions

Threats to personal security and privacy can be handled through preventative actions or through interventions when problems are encountered. We divide the discussion of studies of users' actions and attitudes into these two activities.

A. Efforts to Avoid Security Breaches

Surveys show mixed results on actions taken to avoid security problems. The survey of users in the U.K. found a high level of installation of security software (93% had anti-virus software, 87% had firewalls, 77% had anti-spyware and 60% had anti-spam), but lower levels of frequently updating the software (from 37% to 63% updated weekly) [8]. A 2006 telephone survey in Michigan [18] found that only 4% of respondents claimed to have no virus protection software, 50% set it up themselves and 41% had it set up by their ISP or others; additionally, 46% claimed to always read privacy statements with only 25% claiming they never or hardly ever read them. A 2010 study in U.S.A. reported a lower level of security software usage and identified a significant discrepancy between self-reports of software security installation (58%) and actual installation (37%)[7]. Together these studies suggest that many users know they should take action but do not follow through.

The access control study of [28] found that 30 out of 33 reported using security measures to avoid unauthorized access such as separate accounts, different passwords, file encryption, being physically present when files are examined, physically separating devices, hiding sensitive files and deleting sensitive data. The authors note that several of these strategies reflect a mismatch between the participants' mental models and the reality of access to files on devices, especially the notion that physical location is key to maintaining access control. As in the mental models of [26], [16], the participants seemed to be applying their mental models

of everyday life (e.g., hiding valuables to ensure physical security) to computer security. The participants wanted fine grained groupings of people and data/file types, read versus write access, logging, accessors asking permission and access based on physical presence. Similar desires were found in another access control study of 20 home users recruited through Craigslist and personal contacts [34].

The study of folk models of security [16] also examined how the folk models related to the kinds of security advice that participants followed. The 12 security actions included three on anti-virus software use, one as a catch-all for other security software, one on email, four on Web browsing and site visiting, and three on computer maintenance. All groups reported that it was important to not click on email attachments. The group that viewed viruses as 'Bad' also indicated that maybe one should use anti-virus software and maybe be careful with software downloads. The group that viewed viruses as 'Buggy Software' also indicated that it was important to be careful with software downloads, it was maybe a good idea to make regular backups and maybe to keep patches up to date. The group that viewed viruses as 'Mischief' indicated that it was important to be careful which websites are visited and to make regular backups; they also thought it might be a good idea to use anti-virus software, keep anti-virus software updated, regularly scan their computer, use other security software, and be careful downloading software. The group that viewed viruses under the 'Crime' model viewed as important the three anti-virus activities, being careful in downloading software, keeping patches up to date and turning off the computer when not in use; they also thought being careful of which websites were visited may be a good idea. If the group description did not mention some security advice, then what remained of the 12 actions was either viewed as unnecessary or offered no opinion. As one moved across the four models, more security advice was considered to be important or helpful. Two actions were ignored by all groups: 1) disabling scripting in Web and email and 2) using good passwords. Based on this study, Wash recommended that education should focus not just on the appropriate actions but also on explaining why they will help.

A model of home system administrators who personally act to secure their home computers was developed to identify the factors that influence adoption of security protections [35]. The model combined TPB with two other models that have been used for explaining technology adoption: Theory of Reasoned Action (TRA) which relates subjective norms and a person's attitudes to the intention to behave and Diffusion of Intention (DoI) which identifies factors that influence the adoption of new ideas. The proposed model included five categories of influences: characteristics of the user (self efficacy of security and self efficacy of computer skills), risk tolerance (computer use and risk awareness), characteristics of innovation (complexity, effectiveness and suitability), social consequences (previous security experience, direct experience with threats and subjective norms) and communication channels (news, friends, vendors and work). These factors were used to predict level of importance and agreement on need to use anti-virus software, anti-spyware software, operating system patches, firewalls, backups and passwords. The model was validated in a self-reporting survey of 77 questions taken by 356 participants who were solicited in snowball sampling starting with solicitations through a charity volunteer mailing list, parents and teachers from a high school, a variety of newsgroups and some businesses. Analysis of the results showed that not all the factors were significant; the pruned model included only seven of the original 14 factors: self-efficacy of security skills, self-efficacy of computer skills, risk awareness, suitability, direct experience, subjective norms and vendors. The lack of influence of the other factors may be due to the fact that the subjects were selected to have been already experienced in maintaining security on their home machines and clearly motivated to do so. The study suggests that this subgroup of home users may have different needs and may respond differently to security measures.

Milne et al.'s study of risk perception of online shoppers [14] collected data about protective and risky behaviors. Their respondents reported high levels of many defensive actions: virus checker installation (86%), passwords with a combination of letters, numbers and symbols (85%), scanning for spyware (84%), clearing browser cache (81%), checking that online forms are secure (81%) and opting out of third party information sharing (80%). The percentages for risky behaviors were lower: saved password on computer (56%), saved credit card information in online store's database (51%), and used social networking sites (45%). There were some inconsistencies between these self-reports; for example, the risky behaviors involving passwords, e.g., used a password found in a dictionary (24%) and used a password that contains personal information (24%), seem to conflict with the high percentage reporting usage of strong passwords. The differences may indicate that participants did not understand what constitutes a strong password.

The policy capturing study of [15] also assessed intention to avoid risky actions by asking after each vignette "If you were to get the message again, how likely are you to click on the link in the email message?" They found that the presence of all four threats lowered respondents' intention to click on the link and that women's intention to click on an embedded link offering a coupon was rated higher than men even when they had been presented with a description of threats that could occur from such action. Also, older adults weighed confidentiality threats less than younger adults. Participants reporting higher levels of basic computer knowledge gave unwitting accomplice threats less attention.

Intention to a particular behavior does not necessarily translate into the particular action. Davinson and Sillence

[36] conducted a four stage study of 64 participants recruited from the Psychology Division at Northumbria University. They examined two factors on intended and actual behavior involving avoidance of fraud on the Internet: informing someone that they have a high or low level of risk and having them play (or not) a game-based educational program. The first stage involved participants taking an online survey that asked about age, gender, Internet use, experience with online financial transactions and experience of fraud. 11 fraud avoiding behaviors were included, such as "I only use websites with the secure padlock icon when shopping online", and were assessed as a 7-point scale from 1=Always to 7=Never. Two susceptibility items asked about how susceptible he or she was and how susceptible others were. Then each participant was assigned a "risk score" that supposedly was calculated from their survey responses, but actually was randomly assigned as either "20% at risk" or "80% at risk of becoming a victim of fraud due to the way you use the Internet". The risk score was accompanied by an information sheet derived from recommendations on the getsafeonline.org and the APACS websites. In the second stage, participants were given a paper survey of their intentions to behave securely over the next 10 days, including the same behaviors as in the first survey. In the third stage, half the participants were asked to complete an interactive game-based training program called "Anti-Phishing Phil" which was developed at Carnegie Mellon University. For the fourth stage, seven days later, the participants were sent email with a survey asking how they had behaved over the previous week.

The safety of participants' behavior was calculated as a summed score over the 11 behaviors, where lower is safer. Interestingly, the results showed a statistically significant drop in the behavior measure between the first stage and subsequent stages *independent* of whether they had been told they had been placed in the low or high risk category at the end of the first stage. However, the behavior measure increased significantly from the second stage to the fourth stage, indicating that although they did exhibit safer behavior than reported in the first stage survey, their intentions did not match what they actually did. The results also showed no effect due to the training. Finally, analysis of the susceptibility reports showed that, at each stage, participants perceived that others were at more risk than was the individual.

Ng and Rahim developed a model of home computer users' intention to practice specific security actions [37]. Their model was based upon prior extensions to TPB that further divided the three factors influencing Intention as follows. Attitude was decomposed as:

- *Perceived Usefulness* was how much a user believes certain actions will help (advantages and disadvantages).
- *Ease of Use* was how simple the user views the action.
- *Compatability* was how well the action fits in with the user's values, experiences and needs.

Subjective Norm was decomposed as:

- *Peer Influence* was how much a user takes action based on peer expectations.
- *Superior's Influence* was how much a user takes action based on expectations from superiors.

Perceived Behavioral Control was decomposed as:

- *Self-Efficacy* was the user's confidence in his/her ability to take the actions.
- *Resource Facilitating Conditions* encompassed the requirements in time and money.
- *Technology Facilitating Conditions* identified technological barriers (compatibility, complexity) that constrain action.

These extensions (called the "Decomposed Theory of Planned Behavior") were developed to explain IT usage [38].

To reflect the switch to security in the home, Ng and Rahim's model did not include Ease of Use, Compatability, Peer Influence, Superior's Influence, Resource Facilitating Conditions and Technology Facilitating Conditions and substituted the following security specific factors:

- *Family and Peer Influence*, as a factor influencing Subjective Norm, was pressure from family and friends to take security actions and reflects the shift from an organization/work environment to the home.
- *Mass Media Influence*, as a second factor influencing Subjective Norm, was whether information gleaned from news outlets, Internet, television, etc. inclines the user to take security actions.
- *Facilitating Conditions*, as the second factor influencing Perceived Behavioral Control, captured the influence of external factors such as time, money and compatibility on whether the user takes the action.

To assess their model, they surveyed 233 undergraduates who were home computer users and asked 75 questions pertaining to three security actions and the factors listed above. The security actions were derived from recommendations made by the United States Computer Emergency Response Team Coordination Center and were:

1) update anti-virus software regularly,
2) back up critical data,
3) use a firewall.

Generally, analysis of the results of the survey supported the model with a few exceptions. Perceived Behavioral Control only exerted a significant effect on Intention for the firewall action; the authors posited that updating software and backing up data are not influenced by Perceived Behavioral Control because the users think they control these actions and because the actions can be set up to be done automatically. Similarly, Facilitating Conditions did not appear to exert a significant effect on Perceived Behavioral Control; the authors suggest that either factors such as

Behavior	SOB	PPB	UOB
Update security patches for OS	.8		
Scan with an anti-spyware program	.8		
Use a pop-up blocker	.8		
Use a spam filter	.7		
Use a firewall	.7		
Erase cookies	.7		
Update virus protection software	.7		
Update security patches for Internet browser	.7		
Scan computer with a browser hijack eraser	.7		
Carefully read license agreement before software download		.8	
Verify identity of a website		.8	
Carefully read website privacy policies before filling in online forms		.7	
Verify a website privacy seal		.7	
Change passwords		.7	
Set up my IM to only accept connections from my buddies		.6	
Back up files regularly		.6	
Increase privacy settings in browser		.6	
Send credit card number over an unsecure connection			.8
Open an email attachment I am not expecting			.8
Send a nasty reply to spam			.8
Click inside a pop-up window that opens unexpectedly in browser			.8
Switch to a different OS			.6
Supply personal information to register at a website			.6

Table I
SIGNIFICANT ONLINE BEHAVIORS IDENTIFIED FROM TABLE 1 IN [24]. RIGHTMOST COLUMNS SHOW THE HIGHEST WEIGHT FOR A CATEGORY OF BEHAVIOR FOUND THROUGH PRINCIPAL COMPONENTS FACTOR ANALYSIS WITH VARIMAX ROTATION.

time and money do not matter as much as ability or that Facilitating Conditions may directly influence Intention. The authors concluded that usefulness of the actions should be stressed in education and mass media should be leveraged to inform users and their peers.

Another study [24] examined intention to perform a variety of self-protective security behaviors. Their model was based on PMT and captured relationships between seven protection motivation variables and specific online safety behaviors. The protection motivation variables were: perceived threat susceptibility, perceived threat seriousness, coping efficacy, response efficacy, perceived benefits of safe behavior, perceived costs of safe behavior and perceived benefits of unsafe behavior. The last two were thought to be negatively related to safe practices; the rest were positively related. Through principal components factor analysis, 23 online behaviors were most closely associated with one of three types of behaviors: Safe Online Behaviors (SOB), Privacy Protection Behavior (PPB) and Unsafe Online Behavior (UOB) (see Table I).

To assess their model, LaRose et al. recruited 576 undergraduates from classes in telecommunications and advertising by offering them extra credit for filling out a survey. Each behavior was presented on a seven point scale ranging from "very likely" to "very unlikely" to be carried out within the next month. Respondents were also asked about threat susceptibility, threat seriousness coping self-efficacy, response efficacy and outcome expectations. Statistical analyses showed that only about half of the expected relationships were significant. Safe online behavior intentions were unrelated to perceived threat susceptibility and to seriousness of threats. However, coping self-efficacy beliefs, perceived efficacy of actions and perceived benefits of safety behaviors were positively related to intentions to practice safe online behaviors. Perceived costs of safe behaviors were unrelated to intentions, while perceived benefits of unsafe behaviors were *positively* related to intention, which may indicate that users still want the benefits of their unsafe behavior and look for ways to mitigate it through other safe behaviors.

The researchers also looked at some social and personality factors. Outcomes that were perceived as enhancing the status of an individual also improved safe behavior intentions. Not surprisingly, users who viewed safety as their responsibility were more likely to engage in safe behaviors and those with a reckless self-concept were less likely. Another factor was whether the users had a regular routine (habit) of following the safe behaviors.

Lu et al. [39] developed and evaluated a model to predict continued use of an online antivirus application (OLA). Their model extended the Technology Acceptance Model (TAM), which predicts users' intention to use technology by characterizing their perception of usefulness (PU) and ease of use (PE), by incorporating perceptions of risk from the technology. In the TAM model, PU directly affects intention to use and PE both directly and indirectly (through PU) affects intention. In the Lu et al. model, perceived risk directly influences intention to use as well as indirectly affecting it through PE; they composed perceived risk from a weighted sum of seven belief variables: physical risk (threat to safety), functional risk (failure of product to perform), social risk (opinion of others), time-loss risk (whether it is a waste of time), financial risk (not worth the cost), opportunity cost risk (selected inferior software) and information risk (not enough knowledge of how to use the software).

To evaluate the extended TAM model, Lu et al. surveyed 1,259 registered users of a trial of Trend Micro OLA (solicited via email and offered an opportunity to participate in a drawing) and asked questions to determine the values of the belief variables. 714 participants indicated that they used only the trial and 107 indicated they used the OLA more than five times subsequently. In examining the differences in the two groups, they found that PU exerted a much more significant influence on attitude/intention than perceived risk for the trial-and-leave group; although PU still exerted a stronger effect than risk for the continuous-use group, the effect was not as significant as for the trial-and-leave-group and perception of risk was found to be an important factor in predicting subsequent use of the OLA. Given that the

participants had already judged that they should try anti-virus software, it seems likely that they were aware of the risk and were instead focusing on the utility of the product.

Undergraduates can exhibit inconsistent behavior between what they know about security and what they actually do to prevent problems [6]. On password security, only 22% report that they never share their passwords, 51% report that they never or rarely change their passwords. On email, 24% report opening email attachments from unknown sources without checking for viruses and 56% report doing so when the source looked to be known. Frequent backups are done by 38%. Interestingly, there was low correlation between taking these actions, suggesting that the group did not divide into cautious and careless, but rather a few pairings that tended to be done together (e.g., checking for viruses in attachments from both known and unknown sources and changing passwords frequently as well as checking for viruses in attachments from known sources). Hence, likely these students were more attuned to particular risks and willing to take action against them, an approach that may arise out of the primary sources of information being their own or friends' experiences with security problems.

Faculty in medicine and electrical engineering who used university supplied (but not maintained) laptops were likely to have security software (anti-virus, anti-spyware, spam filter or firewall) installed, but were lax about backups [11]. More than 92% of those surveyed had some security software installed with anti-virus software being the most common (87% of subjects) and spam filter the least (31% of subjects). These users were highly educated and motivated to protect their portable, employer owned machines.

From a behavioral viewpoint, perhaps the most written about approach to security is password protection. The problems with passwords have been addressed by empirical studies (e.g., [40], [41], [42], [19], [43], [44], [45]), position pieces on the need for alternative approaches (e.g., [46], [47]) and even the popular press (e.g., [48]). The scope of the literature is beyond that of this paper. The primary finding is that while users do understand the merits of strong passwords, current procedures impose too hard a burden on users which in turn has them undermining the safeguards (e.g., re-using passwords, writing or storing passwords in unsecured locations, sharing passwords). Following the rules suggested by some security experts would require the average user to remember a large number of different passwords (estimates of accounts requiring passwords vary from tens to hundreds per user) that may have to conform to different constraints depending on the site (constraints that are designed to make them harder to type and remember). Human memory and patience does not appear to be up to this challenge.

B. Attitudes to Security Interventions

Security countermeasures require time and sometimes cost. The evidence of studies (e.g., [6], [8]) suggests that users either don't see the need and/or are not willing to incur the cost of security measures (too much time or money or loss of access to desired benefits). In [5], 19% of respondents indicated that security software was too expensive.

Downloading software applications is a major source of security breaches because of software bundling. Installation includes notices such as End User Licensing Agreements (EULAs), software agreements and Terms of Service (TOS). Anecdotal evidence supports the observation that users do not read such notices. As a famous case in point, PC Pitstop included a clause in one of its EULAs that offered "special consideration which may include financial compensation" to anyone who contacted them at a particular email address; it took more than 3,000 downloads before anyone sent an email [49].

A study of 31 undergraduates examined the effect of installation notices on decisions to download software [50]. The study presented the participants with the scenario that they were helping a friend set up a new computer and had been asked to install "appropriate" applications from a set of five that had been recommended: Google Toolbar, Webshots, Weatherscope, KaZaA and Edonkey. As part of the installation process, one-third of the participants were presented with the standard EULA, one-third with the EULA plus a Microsoft Windows XP Service Pack 2 warning, and one-third with the EULA plus a customized short notice. The customized notice answered four questions (constructed by the study authors carefully reading the agreements provided with the software): what information is collected, how is this information collected, how is this information used, and how does this program affect your computer. Data were collected about the installations done, and post-study interviews were conducted with each participant. The most important factor influencing download decisions was whether the software was perceived to be "useful". For example, many participants considered file sharing software to be essential and were willing to incur risk for it; although given that they were offered a choice of two in the study, they tended to select the one they perceived incurred the least risk. Brand name trust and prior experience did appear to factor in as 93% installed the Google Toolbar and only 47% installed KaZaA; many participants stated that they had previously had a negative experience with it. The additional notices did appear to improve understanding of the risks (11 out of 21 participants stated that the additional notices had affected their decision to install), but the effect was not significant between the customized notice and the Windows warning. This study suggests that simply improving the notifications is not enough; users may need to be presented with alternatives that satisfy the same utility with less risk.

VI. Recommendations for Future Work

The studies support a set of recommendations about future research and development of security tools for home users.

In particular, we identify six distinct areas that we believe require particular attention.

Choosing a proper methodology for user study: We believe that the methodologies for home user studies need to be broadened. Most of the studies involved self-report surveys. Yet, self reports of taking security and privacy precautions, e.g., downloading patches, protecting passwords, can vary widely between studies. Studies that have been able to verify user's reports on their computers have uncovered lower actual than reported rates of some behaviors [33], [7]. As [37] showed, peer perception does influence how people respond; so some of the responses may reflect more of what the respondent thinks they should be doing than what they actually are (e.g., respondent bias, socially desirable responding). In addition, people are not very good at predicting what they would do in a particular situation. These factors help explain why some of the survey results are contradictory and do not match actual behavior. Whenever possible, self-reporting surveys need to be confirmed by checking intention versus actual behavior.

Another approach is experiments based on simulation – where the participant is put in the actual situation and monitored. The simulation can support a set of user and computer actions that trigger threats of interest. For example, user actions may include emailing, Web browsing, online shopping, social networking, online banking and peer-to-peer activities. Computer actions may include pop-ups asking to download a program, asking for registration at a site in order to proceed, or asking for the user to agree to licensing terms for use of a site. At the end, the participant can be asked about benefits such as convenience, time, access to a greater selection, access to the site, access to the program, overcoming geographic and time boundaries, ease of access, and connecting with multiple people at one time.

A simulation based study can also help us assess the emotional reactions of users to interventions and warnings. The purpose of this assessment is to bypass a participant's responses that may be driven by ego-protection (e.g., "I don't want them to think I'm afraid"), demand characteristics (i.e., participant gives what they think is an expected response), or experimenter bias (i.e., experimenter inadvertently treats participants in a leading manner due to his or her expectations for the study).

Assessing the impact of demographics: A few studies showed differences due to demographics (e.g., [8], [14], [9], [15]). Additionally, some studies hint at effects due to age, interests, location, socioeconomics and education. For example, the majority of studies have been conducted with undergraduate subjects. Given hints from existing studies and intuition about this subject group, one would expect to see significant differences between this group and others. One study [50] indicated that undergraduates consider P2P software to be indispensable, which is probably not the case with older adults. Undergraduates have a level of education, experience with computers and economic stability that is not true of all groups. Another study [9] suggested that socioeconomic factors, such as income, may influence the view of vulnerability. We believe that new studies should cover a broader range of society and identify the commonalities and differences between them in their perceptions of risk, threats, and adaptive behaviors. As a starting point, we suggest studying college age individuals (18–29 years of age) and adults aged 50–64 years. Both these groups are considered vulnerable populations for security threats; studies suggest that seniors are among the most vulnerable demographics for spyware [51].

Assessing the users' understanding of threat and potential consequences of each threat: According to Fox [52] users may not always understand the various security threats and their magnitude as they engage in online behavior. Considerable research has been done on usability of security tools; not enough has been done to elucidate how users understand privacy and security threats, and their potential consequences. Users who lack an understanding of both threat and its consequence may exhibit inappropriate defensive strategies when engaging in online behavior. We believe that a qualitative methodology for assessing user understanding of threat and consequence associated with each threat is most appropriate for this investigation. Qualitative data, which are in the form of words provided by subjects under study, provide rich explanations and descriptions of subjects' perceptions and choices. By asking subjects to provide their own words to answer a question, researchers avoid priming participants, or providing them hints from which to create answers that they believe the researcher wants rather than their own answers [53].

Assessing the factors that influence decision making about security: Security knowledge and high self-efficacy are important determinants of secure behavior. For example, studies such as [24], [35] show that users with high knowledge of computer skills tend to practice safer behaviors and employ more security strategies. Users with a better understanding of computers in general also had a better appreciation of the consequences of risky action [15].

Some studies (e.g., [16], [26]) suggest that many users have incomplete and partially incorrect mental models of security threats, risks and consequences of actions. Even when users have some idea of what they should do, they are often unwilling to incur the costs (cognitive, opportunity and financial) to do so. For example, studies such as [50], [33] show that users are willing to incur higher risk of negative consequences when they really want the service (e.g., Facebook, P2P software). Users are more willing to divulge more personal information when they perceive a positive gain from that information exchange [54]. However, previous studies have not identified levels of gain associated with levels of risk. Such a study will be needed to develop a formula for risk-taking decision-making that can then be

used by an appropriate security tool. To understand risk relative to benefit decision-making, we opine that a scale for assessing perceptions be formulated. Currently no such scale exists for determining which risk computer users are willing to make and for what gain. Hence, the development of such a scale will make a significant contribution to the development of security and privacy protection solutions.

Such information informs the decisions that users make about behaviors online and actions to mitigate security threats. More studies are needed to identify where poor mental models produce poor decisions. What exact data to collect depends on the goal of the study; however, the significant factors found in [14], [24], [35], [32], [37], [39] provide good starting points. Also, research should explore how security tools might allow the user to take calculated risks, while minimizing the damage.

Identifying factors and approaches for improved design of security and privacy software and policies: Education certainly should play a role in encouraging home users to take security precautions, but there is evidence that users are not willing to take the time to do so. For example, a study of 206 undergraduates found that by making most students more aware that online safety was their responsibility, the intention to practice safety online increased (over suggesting it was not their responsibility) except for those not interested in safety issues and who were not confident in their abilities to protect themselves [55]. In light of some of such findings, education may need to be tailored to an individual. In fact, the authors [55] suggested that security education websites might pre-screen visitors and then route them to tailored messages (e.g., utilize computer-adaptive training). Similarly, Davinson and Sillence [36] concluded from their study that participants may have changed their behavior because they believed that the security information they were given had been tailored based on their risk level.

Software and approaches for security and privacy protection need to be better designed to address both current and future needs of home users. Current practice does not appear to be adequate. Home user studies suggest incorporating factors that matter to people (e.g., ease of use, control of personal files); such information should be leveraged to produce approaches that are easily manageable by users and appeal to their abilities and concerns. West [25] suggests having default software settings be more secure and making the activities of security protections more obvious to the user so that they can gain an appreciation of the protection they are producing.

A more ambitious approach is to broaden and integrate the activities of security tools to be more comprehensive in their protection and to reduce the incremental overhead of the current suite of necessary actions. Having to employ different tools for different threats (e.g., installing antivirus software, disabling flash, creating strong passwords) imposes a high burden on home computer users. To the extent possible, protections should be automated and straightforward to understand; safer behavior has been identified in users with automated software updates and habits of safe behavior [24].

Conducting longitudinal studies: Given the rate of change and influence of the Internet, it is difficult to know whether results from 10 years ago still apply. Longitudinal studies could identify the influence of ongoing education (as computer training becomes more common in schools), new technologies (e.g., rise of Twitter), news events (e.g., recent press on the Stop Online Piracy Act) and ongoing efforts to inform the public (e.g., Google's recent email and media notification of its new privacy policy).

VII. Conclusions

Generally, home computer users view others as being more at risk. When they are aware of the threats, home computer users do care about security and view it as their responsibility. However, many studies suggest that users often do not understand the threats and sometimes are not willing or able to incur the costs to defend against them. At least three studies [24], [50], [32] found that users still want the benefits of potentially unsafe behavior. Herley [47] argues that rejection of security advice might actually be a rational choice when the security measures and costs are carefully assessed.

The challenge of user-centered security [56] clearly subsumes some of the issues discussed in this paper; a great deal more needs to be done both in terms of facilitating models of the user and suitable approaches to security that conform to these models. As we recommend in Section VI, user studies need to be broadened and designed to provide more reliable information about what users will actually do, especially investigating the factors that influence home users' decision making. Armed with such information, approaches to security can be more automated and personalizable: suited to the perceptions and capabilities of the person at the keyboard as well as giving them alternatives when their desired action (e.g., downloading P2P software, posting personal information on Facebook) is risky. As Dhamija et al. [29] showed, even experienced users can be fooled.

VIII. Acknowledgements

We thank the anonymous reviewers for their careful reading of the paper and insightful suggestions for changes. This material is based upon work supported by the National Science Foundation under Grant No. 0905232. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] K. Aytes and T. Conolly, "A Research Model for Investigating Human Behavior Related to Computer Security," in *Proceedings of the 9th Americas Conference on Information Systems*, Tampa, FL, August 2003. [Online].

Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1726&context=amcis2003

[2] Symantec, "Trends for January–June 07," *Symantec Internet Security Threat Report*, vol. XII, September 2007. [Online]. Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

[3] T. Team, "Symantec Vaults Above $22 As Andriod Mobile Security Market Booms," Forbes, 2011. [Online]. Available: http://www.forbes.com/sites/greatspeculations/2011/07/24/norton-vaults-above-22-as-android-mobile-security-market-booms

[4] M. Thomas, "Top Anti-Virus Brands Lost Market Share in 2010 as New Entrants Push Up: Gartner." [Online]. Available: http://rtn.asia/583_anti-virus-brands-lost-market-share-2010-new-entrants-push

[5] P. Bryant, S. Furnell, and A. Phippen, *Advances in Networks, Computing and Communications 4*. University of Plymouth, April 2008, ch. Improving Protection and Security Awareness Amongst Home Users.

[6] K. Aytes and T. Connolly, "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational and End User Computing*, vol. 16, no. 3, pp. 22–40, July-Sept 2004.

[7] National Cyber Security Alliance, Norton by Symantec, and Zogby International, "2010 NCSA / Norton by Symantec Online Safety Study," October 2010. [Online]. Available: http://www.staysafeonline.org/sites/default/files/resource_documents/FINAL+NCSA+Full+Online+Safety+Study+2010[1].pdf

[8] S. Furnell, P. Bryant, and A. Phippen, "Assessing the Security Perceptions of Personal Internet Users," *Computers & Security*, vol. 26, no. 5, pp. 410–417, August 2007.

[9] P. Szewczyk and S. Furnell, "Assessing the Online Security Awareness of Australian Internet Ssers," in *Proceedings of the 8th Annual Security Conference: Discourses in Security Assurance & Privacy*, Las Vegas, NV, USA, April 2009.

[10] Gartner, Inc., "Gartner Says More than 1 Billion PCs In Use Worldwide and Headed to 2 Billion Units by 2014," June 2008. [Online]. Available: http://www.gartner.com/it/page.jsp?id=703807

[11] K. Solic and V. Ilakovac, "Security Perception of a Portable PC User (The Difference between Medical Doctors and Engineers): A Pilot Study," *Mediciniski Glasnik*, vol. 6, no. 2, pp. 261–264, August 2009.

[12] B. Friedman, D. Hurley, D. Howe, H. Nissenbaum, and E. Felten, "Users' Conceptions of Risks and Harms on the Web: A Comparative Study," in *Extended Abstracts. Proceedings of the Conference on Human Factors in Computing Systems*, Minneapolis, MN, USA, 2002.

[13] J. Diesner, P. Kumaraguru, and K. Carley, "Mental Models of Data Privacy and Security Extracted from Interviews with Indians," in *Proceedings of the 55th Annual Conference of International Communication Association (ICA)*, New York, NY, USA, May 2005.

[14] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices," *Journal of Consumer Affairs*, vol. 43, no. 3, pp. 449–473, 2009.

[15] Z. Byrne, J. Weidert, J. Liff, M. Horvath, C. Smith, A. Howe, and I. Ray, "Perceptions of Internet Threats: Behavioral Intent to Click Again," in *Proceedings of the 27th Annual Conference of the Society for Industrial and Organizational Psychology*, San Diego, CA, April 2012.

[16] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond, Washington, USA, 2010.

[17] Pew Research Center, "What Internet Users Do Online — Pew Research Center's Internet & American Life Project," October 2011. [Online]. Available: http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activites-Total.aspx

[18] Schulman, Ronca & Bucuvalas Inc., "Michigan State University Internet Safety Survey," August 2007. [Online]. Available: https://www.msu.edu/~isafety/finalreport.pdf

[19] D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," in *Proceedings of the 16th International Conference on World Wide Web*, Banff, Alberta, Canada, 2007.

[20] R. Grinter, K. Edwards, M. Newman, and N. Ducheneaut, "The Work to Make a Home Network Work," in *Proceedings of the 9th European Conference on Computer Supported Cooperative Work*, Paris, France, September 2005.

[21] B. Y. Ng, A. Kankanhalli, and Y. Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, 2009.

[22] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, 1991.

[23] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology: Interdisciplinary and Applied*, vol. 91, no. 1, pp. 93–114, September 1975.

[24] R. LaRose, N. Rifon, S. Liu, and D. Lee, "Understanding Online Safety Behavior: A Multivariate Model," in *Proceedings of the 55th Annual Conference of the International Communication Association*, New York, NY, USA, 2005.

[25] R. West, "The Psychology of Security," in *Communications of the ACM*, vol. 51, no. 4, April 2008, pp. 34–41.

[26] J. Camp, F. Asgharpour, and D. Liu, "Experimental Evaluations of Expert and Non-expert Computer Users' Mental Models of Security Risks," in *Proceedings of Workshop on the Economics of Security*, Pittsburgh, PA, USA, June 2007.

[27] L. J. Camp, "Mental Models of Privacy and Security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, Fall 2009.

[28] M. L. Mazurek *et al.*, "Access Control for Home Data Sharing: Attitudes, Needs and Practices," in *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, Atlanta, GA, April 2010, pp. 645–654.

[29] R. Dhamija, J. Tygar, and M. Hearst, "Why Phishing Works," in *Proceedings of the Conference on Human Factors in Computing Systems*, Montreal, Canada, April 2006.

[30] M. Pattinson and G. Anderson, "How Well Are Information Risks Being Communicated to Your End-users?" *Information Management and Computer Security*, vol. 15, no. 5, 2007.

[31] Privacy International, "A Race to the Bottom: Privacy Ranking in Internet Service Companies – A Consultation Report," June 2007. [Online]. Available: https://www.privacyinternational.org/article/race-bottom-privacy-ranking-internet-service-companies

[32] B. Debatin, J. P. Lovejoy, A.-K. Horm, and B. N. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication*, vol. 15, pp. 83–108, 2009.

[33] T. Govani and H. Pashley, "Student Awareness of the Privacy Implications When Using Facebook," 2005. [Online]. Available: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

[34] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in Access Right Assignment for Secure Home Networks," in *Proceedings of 5th USENIX Workshop on Hot Topics in Security*, Washington, DC, USA, August 2010.

[35] W. A. Conklin, "Computer Security Behaviors of Home PC Users: A Diffusion of Innovation Approach," Ph.D. dissertation, University of Texas at San Antonio, Department of Information Systems and Technology Management, August 2006.

[36] N. Davinson and E. Sillence, "It Won't Happen to Me: Promoting Secure Behaviour Among Internet Users," *Computers in Human Behavior*, vol. 26, pp. 1739–1747, 2010.

[37] B. Y. Ng and M. A. Rahim, "A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security," in *Proceedings of the 9th Pacific Asia Conference on Information Systems*, Bangkok, Thailand, July 2005.

[38] S. Taylor and P. A. Todd, "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research*, vol. 6, no. 2, pp. 144–176, 1995.

[39] H.-P. Lu, C.-L. Hsu, and H.-Y. Hsu, "An Empirical Study of the Effect of Perceived Risk upon Intention to Use Online Applications," *Information Management & Computer Security*, vol. 13, no. 2, pp. 106–120, 2005.

[40] A. Adams and M. A. Sasse, "Users Are Not the Enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, December 1999.

[41] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password Memorability and Security: Empirical Results," *IEEE Security & Privacy*, pp. 25–31, September/October 2004.

[42] G. Notoatmodjo and C. Thomborson, "Passwords and Perceptions," in *Proceedings of the 7th Australasian Conference on Information Security*, Darlinghurst, Australia, 2009.

[43] P. G. Inglesant and M. A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," in *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, Atlanta, GA, USA, 2010.

[44] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering Stronger Password Requirements: User Attitudes and Behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. New York, NY, USA: ACM, 2010.

[45] E. Hayashi and J. I. Hong, "A Diary Study of Password Usage in Daily Life," in *Proceedings of the 29th Annual Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada, May 2011.

[46] D. A. Norman, "THE WAY I SEE IT: When Security Gets in the Way," *Interactions*, vol. 16, no. 6, pp. 60–63, November 2009.

[47] C. Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," in *Proceedings of the 2009 Workshop on New Security Paradigms*, Oxford, UK, 2009.

[48] J. A. Miller, "Identity Crisis: What's My Favorite Dessert? Only My Bank Knows for Sure," *Smithsonian Magazine*, October 2011.

[49] L. Magid. It Pays to Read License Agreements. [Online]. Available: http://www.pcpitstop.com/spycheck/eula.asp

[50] N. Good *et al.*, "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware," in *Proceedings of the 1st Symposium On Usable Privacy and Security*, Pittsburgh, PA, USA, July 2005.

[51] S. Fox, "Are 'Wired Seniors' Sitting Ducks?" Pew Internet & American Life Project, Data Memo., April 2006. [Online]. Available: http://www.pewinternet.org/pdfs/PIP_Wired_Senior_2006_Memo.pdf

[52] ——, "Online Threats and Fears are Changing Consumer Behavior," Pew Internet & American Life Project, October 2005. [Online]. Available: http://www.pewinternet.org/ppt/Fox_IAPP_2005.pdf

[53] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*, 2nd ed. Thousand Oaks, CA: Sage Publication, 1994.

[54] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, vol. 19, 2000.

[55] R. LaRose, N. Rifon, and R. Enbody, "Promoting Personal Responsibility for Internet Safety," *Communications of the ACM*, vol. 51, no. 3, March 2008.

[56] M. E. Zurko, "User-Centered Security: Stepping up to the Grand Challenge," in *Proceedings of the 21st Annual Computer Security Applications Conference, (ACSAC 2005)*, Tucson, AZ, USA, December 2005, pp. 187–202.