Folk Models of Home Computer Security

Rick Wash
Michigan State University
East Lansing, MI 48824-1212
wash@msu.edu

ABSTRACT

Home computer systems are insecure because they are administered by untrained users. The rise of botnets has amplified this problem; attackers compromise these computers, aggregate them, and use the resulting network to attack third parties. Despite a large security industry that provides software and advice, home computer users remain vulnerable. I identify eight 'folk models' of security threats that are used by home computer users to decide what security software to use, and which expert security advice to follow: four conceptualizations of 'viruses' and other malware, and four conceptualizations of 'hackers' that break into computers. I illustrate how these models are used to justify ignoring expert security advice. Finally, I describe one reason why botnets are so difficult to eliminate: they cleverly take advantage of gaps in these models so that many home computer users do not take steps to protect against them.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*evaluation/methodology,user-centered design*; H.5.3 [**Information Interfaces and Presentation**]: Group and Organization Interfaces—*collaborative computing*

General Terms

Human Factors, Security

Keywords

Home Security, Mental Models, Folk Models

1. INTRODUCTION

Home users are installing paid and free home security software at a rapidly increasing rate.[1]. These systems include anti-virus software, anti-spyware software, personal firewall software, personal intrusion detection / prevention systems, computer login / password / fingerprint systems, and intrusion recovery software. Nonetheless, security intrusions and the costs they impose on other network users are also increasing. One possibility is that home users are starting to become well-informed about security risks, and that soon enough of them will protect their systems that the problem will resolve itself. However, given the "arms race" history in most other areas of networked security (with intruders becoming increasingly sophisticated and numerous over time), it is likely that the lack of user sophistication and non-compliance with recommended security system usage policies will continue to limit home computer security effectiveness.

To design better security technologies, it helps to understand how users make security decisions, and to characterize the security problems that result from these decisions. To this end, I have conducted a qualitative study to understand users' *mental models* [18, 11] of attackers and security technologies. 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 [17].

In particular, I investigate the existence of folk models for home computer users. Folk models are mental models that are not necessarily accurate in the real world, thus leading to erroneous decision making, but are shared among similar members of a culture[11]. It is well-known that in technological contexts users often operate with incorrect folk models [1]. To understand the rationale for home users' behavior, it is important to understand the decision model that people use. If technology is designed on the assumption that users have correct mental models of security threats and security systems, it will not induce the desired behavior when they are in fact making choices according to a different model.

As an example, Kempton [19] studied folk models of thermostat technology in an attempt to understand the wasted energy that stems from poor choices in home heating. He found that his respondents possessed one of two mental models for how a thermostat works. Both models can lead to poor decisions, and both models can lead to correct decisions that the other model gets wrong. Kempton concludes that "Technical experts will evaluate folk theory from this perspective [correctness] – not by asking whether it fulfills the needs of the folk. But it is the latter criterion [...] on which sound public policy must be based." The same argument holds for technology design: whether the folk models are correct or not, technology should be designed to work well with the folk models actually employed by users.[2]

[1]Despite a worldwide recession, the computer security industry grew 18.6% in 2008, totaling over $13 billion according to a recent Gartner report [9]

Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA USA

[2]It may be that users can be re-educated to use more correct mental models, but generally it more difficult to re-educate

For home computer security, I study two related research questions: 1) *Potential threats*: How do home computer users conceptualize the information security threats that they face? 2) *Security responses*: How do home computer users apply their mental models of security threats to make security-relevant decisions?

Despite my focus on "home computer users," many of these problems extend beyond the home; most of my analysis and understanding in this paper is likely to generalize to a whole class of users who are unsophisticated in their security decisions. This includes many university computers, computers in small business that lack IT support, and personal computers used for business purposes.

1.1 Understanding Security

Managing the security of a computer system is very difficult. Ross Anderson's [2] study of Automated Teller Machine (ATM) fraud found that the majority of the fraud committed using these machines was not due to technical flaws, but to errors in deployment and management failures. These problems illustrate the difficulty that even professionals face in producing effective security.

The vast majority of home computers are administered by people who have little security knowledge or training. Existing research has investigated how non-expert users deal with security and network administration in a home environment. Dourish et al. [12] conducted a related study, inquiring not into mental models but how corporate knowledge workers handled security issues. Gross and Rossum [15] also studied what security knowledge end users posses in the context of large organizations. And Grinter et al. [14] interviewed home network users about their network administration practices.

Combining the results from these papers, it appears that many users exert much effort to avoid security decisions. All three papers report that users often find ways to delegate the responsibility for security to some external entity; this entity could be technological (like a firewall), social (another person or IT staff), or institutional (like a bank). Users do this because they feel like they don't have the skills to maintain proper security. However, despite this delegation of responsibility, many users still make numerous security-related decisions on a regular basis. These papers do not explain how those decisions get made; rather, they focus mostly on the anxiety these decisions create.

I add structure to these observations by describing how folk models enable home computer users to make security decisions they cannot delegate. I also focus on differences between people, and characterize different methods of dealing with security issues rather than trying to find general patterns. The folk models I describe may explain differences observed between users in these studies.

Camp [6] proposed using mental models as a framework for communicating complex security risks to the general populace. She did not study how people currently think about security, but proposed five possible models that may be useful. These models take the form of analogies or metaphors with other similar situations: physical security, medical risks, crime, warfare, and markets. Asghapour et al. [3] built on this by conducting a card sorting experiment that matches these analogies with the mental models of uses. They found that experts and non-experts show sharp differences in which analogy their mental model is closest to.

Camp et al. began by assuming a small set of analogies that they believe function as mental models. Rather than pre-defining the range of posssible models, I treat these mental models as a legitimate area for inductive investigation, and endeavor to uncover users' mental models in whatever form they take. This prior work confirms that the concept of mental models may be useful for home computer security, but made assumptions which may or may not be appropriate. I fill in the gap by inductively developing an understanding of just what mental models people actually possess. Also, given the vulnerability of home computers and this finding that experts and non-experts differ sharply [3], I focus solely on non-expert home computer users.

Herley [16] argues that non-expert users reject security advice because it is rational do to so. He believes that security experts provide advice that ignores the costs of the users' time and effort, and therefore overestimates the net value of security. I agree, though I dig deeper into understanding how users actually make these security / effort tradeoffs.

1.2 Botnets and Home Computer Security

In the past, computers were targeted by hackers approximately in proportion to the amount of value stored on them or accessible from them. Computers that stored valuable information, such as bank computers, were a common target, while home computers were fairly innocuous. Recently, attackers have used a technique known as a 'botnet,' where they hack into a number of computers and install special 'control' software on those computers. The hacker can give a master control computer a single command, and it will be carried out by all of the compromised computers (called zombies) it is connected to [4, 5]. This technology enables crimes that require large numbers of computers, such as spam, click fraud, and distributed denial of service [26]. Observed botnets range in size from a couple hundred zombies to 50,000 or more zombies. As John Markoff of the *New York Times* observes, botnets are not technologically novel; rather, "what is new is the vastly escalating scale of the problem" [21].

Since any computer with an Internet connection will be an effective zombie, hackers have logically turned to attacking the most vulnerable population: home computers. Home computer users are usually untrained and have few technical skills. While some software has improved the average level of security of this class of computers, home computers still represent the largest population of vulnerable computers. When compromised, these computers are often used to commit crimes against third parties. The vulnerability of home computers is a security problem for many companies and individuals who are the victims of these crimes, even if their own computers are secure [7].

1.3 Methods

I conducted a qualitative inquiry into how home computer users understand and think about potential threats. To develop depth in my exploration of the folk models of security, I used an iterative methodology as is common in qualitative research [24]. I conducted multiple rounds of interviews punctuated with periods of analysis and tentative conclusions. The first round of 23 semi-structured interviews was conducted in Summer 2007. Preliminary analysis proceeded throughout the academic year, and a second round

a society than it is to design better technologies.

of 10 interviews was conducted in Summer 2008, for a total of 33 respondents. This second round was more focused, and specifically searched for negative cases of earlier results [24]. Interviews averaged 45 minutes each; they were audio recorded and transcribed for analysis.

Respondents were chosen from a snowball sample [20] of home computer users evenly divided between three midwestern U.S. cities. I began with a few home computer users that I knew in these cities. I asked them to refer me to others in the area who might be information-rich informants. I screened these potential respondents to exclude people who had expertise or training in computers or computer security. From those not excluded, I purposefully selected respondents for maximum variation [20]: I chose respondents from a wide variety of backgrounds, ages, and socio-economic classes. Ages ranged from undergraduate (19 years old) up through retired (over 70). Socio-economic status was not explicitly measured, but ranged from recently graduated artist living in a small efficiency up to a successful executive who owns a large house overlooking the main river through town. Selecting for maximal variation allows me to document diverse variations in folk models and identify important common patterns [20].

After interviewing the chosen respondents, I grew by potential interview pool by asking them to refer me to more people with home computers who might provide useful information. This snowballing through recommendations ensured that the contacted respondents would be information-rich [20] and cooperative. These new potential respondents were also screened, selected, and interviewed. The method does not generate a sample that is representative of the population of home computer users. However, I don't believe that the sample is a particularly special or unusual group; it is likely that there are other people like them in the larger population.

I developed an (IRB approved) face-to-face semi-structured interview protocol that pushes subjects to describe and use their mental models, based on formal methods presented by D'Andrade [11]. I specifically probed for past instances where the respondents would have had to use their mental model to make decisions, such as past instances of security problems, or efforts undertaken to protect their computers. By asking about instances where the model was applied to make decisions, I enabled the respondents to uncover beliefs that they might not have been consciously aware of. This also ensures that the respondents believe their model enough to base choices on it. The majority of each interview was spent on follow-up questions, probing deeper into the responses of the subject. This method allows me to describe specific, detailed mental models that my participants use to make security decisions, and to be confident that these are models that the participants actually believe.

My focus in the first round was broad and exploratory. I asked about any security-related problems the respondent had faced or was worried about; I also specifically asked about viruses, hackers, data loss, and data exposure (identity theft). I probed to discover what countermeasures the respondents used to mitigate these risks. Since this was a semi-structured interview, I followed up on many responses by probing for more information. After preliminary analysis of this data, I drew some tentative conclusions and listed points that needed clarification. To better elucidate these models and to look for negative cases, I conducted 10 second-round interviews using a new (IRB approved) interview protocol. In this round, I focused more on three specific threats that subjects face: viruses, hackers, and identity theft.

For this second round, I also used an additional interviewing technique: hypothetical scenarios. This technique was developed to help focus the respondents and elicit additional information not present in the first round of interviews. I presented the respondents with three hypothetical scenarios and asked the subjects for their reaction. The three scenarios correspond to each of the three main themes for the second round: finding out you have a virus, finding out a hacker has conpromised your computer, and being informed that you are a victim of identity theft. For each scenario, after the initial description and respondent reaction, I added an additional piece of information that contradicted the mental models I discovered after the first round. For example, one preliminary finding from the first round was that people rarely talked about the creation of computer viruses; it was unclear how they would react to a computer virus that was created by people for a purpose. In the virus scenario, I informed the respondents that the virus in question was written by the Russian mafia. This fact was taken out of recent news linking the Russian mafia to widespread viruses such as Netsky, Bagle, and Storm.[3]

Once I had all of the data collected and transcribed, I conducted both inductive and deductive coding of the data to look both for predetermined and emergent themes [23]. I began with a short list of major themes I expected to see from my pilot interviews, such as information about viruses, hackers, identity theft, countermeasures, and sources of information. I identified and labeled (coded) instances when the respondents discussed these themes. I then expanded the list of codes as I noticed interesting themes and patterns emerging. Once all of the data was coded, I summarized the data on each topic by building a data matrix [23].[4] This data matrix helped me to identify basic patterns in the data across subjects, to check for representativeness, and to look for negative cases [24].

After building the initial summary matrices, I identified patterns in the way respondents talked about each topic, paying specific attention to word choices, metaphors employed, and explicit content of statements. Specifically, I looked for themes in which users differ in their opinions (negative case analysis). These themes became the building blocks for the mental models. I built a second matrix that matched subjects with these features of mental models.[5] This second matrix allowed me to identify and characterize the various mental models that I encountered. Table 7 in the Appendix shows which participants from Round 2 had each of the 8 models. A similar table was developed for the Round 1 participants.

I then took the description of the model back to the data, verified when the model description accurately represented the respondents descriptions, and looked for contradictory evidence and negative cases [24]. This allowed me to update the models with new information or insights garnered by following up on surprises and incorporating outliers. This was an iterative process; I continued updating model de-

[3] `http://www.linuxinsider.com/story/33127.html?wlc=1244817301`

[4] A fragment of this matrix can be seen in Table 5 in the Appendix.

[5] A fragment of this matrix is Table 6 in the Appendix.

scriptions, looking for negative cases, and checking for representativeness until I felt that the model descriptions I had accurately represented the data. In this process, I developed further matrices as data visualizations, some of which appear in my descriptions below.

2. FOLK MODELS OF SECURITY THREATS

I identified a number of different folk models in the data. Every folk model was shared by multiple respondents in this study. The purpose of qualitative research is not to generalize to a population; rather, it is to explore phenomenon in depth. To avoid misleading readers, I do not report how many users possessed each folk model. Instead, I describe the full range of folk models I observed.

I divide the folk models into two broad categories based on a distinction that most subjects possessed: 1) models about viruses, spyware, adware, and other forms of malware which everyone refered to under the umbrella term 'virus'; and 2) models about the attackers, referred to as 'hackers,' and the threat of 'breaking in to' a computer. Each respondent had at least one model from each of the two categories. For example, Nicole[6] believed that viruses were mischievous, and hackers are criminals who target big fish. These models are not necessarily mutually exclusive. For example, a few respondents talked about different types of hackers and would describe more than one folk model of hackers.

Note that by listing and describing these folk models, in no way do I intend to imply that these models are incorrect or bad in any way. They are all certainly imcomplete, and do not exactly correspond to the way malicious software or malicious computer users behave. But, as Kempton [19] learned in his study of home thermostats, what is important is not how accurate the model is but how well it serves the needs of the home computer user in making security decisions.

Additionally, there is not "correct" model that can serve as a comparison. Even security experts will disagree as to the correct way to think about viruses or hackers. To show an extreme example, Medin et al. [22] conducted a study of expert fishermen in the Northwoods of Wisconsin. They looked at the mental models of both Native American fishermen and of majority-culture fishermen. Despite both groups being experts, the two groups showed dramatic differences in the way fish were categorized and classified. Majority-culture fishermen grouped fish into standard taxonomic and goal-oriented groupings, while Native American fishermen groups fish mostly by ecological niche. This illustrates how even experts can have dramatically different mental models of the same phenomenon, and any single expert's model is not necessarily correct. However, experts and novices do tend to have very different models; Asgharpour et al. [3] found strong differences between expert and novice computer users in their mental models of security.

Common Elements of Folk Models.

Most respondents made a distinction between 'viruses' and 'hackers.' To them, these are two separate threats that can both cause problems. Some people believed that viruses are created by hackers, but they still usually saw them as distinct threats. A few respondents realized this and tried to describe the difference; for example at one point in the interview Irving tries to explain the distinction by saying "The hacker is an individual hacking, while the virus is a program infecting." After some thought, he clarifies his idea of the difference a bit: "So it's a difference between something automatic and more personal." This description is characteristic of how many respondents think about the difference: viruses are usually more programatic and automatic, where hacking is more like manual labor, requiring the hacker to be sitting in front of a computer entering commands.

This distinction between hackers and viruses is not something that most of the respondents had thought about; it existed in their mental model but not at a conscious level. Upon prompting, Dana decides that "I guess if they hack into your system and get a virus on there, itÕs gonna be the same thing." She had never realized that they were distinct in her mind, but it makes sense to her that they might be related. She then goes on to ask the interviewer if she gets hacked, can she forward it on to other people?

This also illustrates another common feature of these interviews. When exposed to new information, most of the respondents would extrapolate and try to apply that information to slightly different settings. When Dana was prompted to think about the relationship between viruses and hackers, she decided that they were more similar than she had previously realized. Then she began to apply ideas from one model (viruses spreading) to the other model (can hackers spread also?) by extrapolating from her current models. This is a common technique in human learning and sensemaking [25]. I suspect that many details of the mental models were formed in this way. Extrapolation is also useful for analysis; how respondents extrapolate from new information reveals details about mental models that are not consciously salient during interviews [8, 11]. During the interviews I used a number of prompts that were intended to challenge mental models and force users to extrapolate in order to help surface more elements of their mental models.

2.1 Models of Viruses and other Malware

All of the respondents had heard of computer viruses and possessed some mental model of their effects and transmission. The respondents focused their discussion primarily on the effects of viruses and the possible methods of transmission. In the second round of interviews, I prompted respondents to discuss how and why viruses are created by asking them to react to a number of hypothetical scenarios. These scenarios help me understand how the respondents apply these models to make security-relevant decisions.

All of the respondents used the term 'virus' as a catch-all term for malicious software. Everyone seemed to recognize that viruses are computer programs. Almost all of the respondents classify many different types of malicious software under this term: computer viruses, worms, trojans, adware, spyware, and keyloggers were all mentioned as 'viruses.' The respondents don't make the distinctions that most experts do; they just call any malicious computer program a 'virus.'

Thanks to the term 'virus,' all of the respondents used some sort of medical terminology to describe the actions of malware. Getting malware on your computer means you have 'caught' the virus, and your computer is 'infected.' Everyone who had a Mac seemed to believe that Macs are 'immune' to virus and hacking problems (but were worried anyway).

[6]All respondents have been given pseudonyms for anonymity.

	Bad	*Buggy Software*	*Mischief*	*Support Crime*
# Subjects	5	9	12	6
Creator	Unspecified	Bad people	Mischievous hackers	Criminals
Purpose of viruses	Unspecified	No purpose	Cause mischief; cause annoying problems	Gather information for identity theft
Effects of infection	General notion of bad things happening	Same effects as buggy software, but more extreme	Annoying problems with computers	No direct harm to computer; stolen information
Method of transmission	"Catch" viruses; miscellaneous methods of catching them	Must be manually downloaded and executed	Passive "catching" by visiting shady websites or opening shady email	Spread automatically, or installed by hackers

Table 1: Summary of folk models about viruses, organized by model features

Overall, I found four distinct folk models of 'viruses.' These models differed in a number of ways. One of the major differences is how well-specified and detailed the model was, and therefore how useful the model was for making security-related decisions. One model was very under-specified, labeling viruses as simply 'bad.' Respondents with this model had trouble using it to make any kind of security-related decisions because the model didn't contain enough information to provide guidance. Two other models (the *Mischief* and *Crime* models) were fairly well-described, including how viruses are created and why, and what the major effects of viruses are. Respondents with these models could use them to extrapolate many different situations and use them to make many security-related decisions on their computer. Table 1 summarizes the major differences between the four models.

2.1.1 Viruses are Generically 'Bad'

A few subjects had a very under-developed model of viruses. These subjects knew that viruses cause problems, but these subjects couldn't really describe the problems that viruses cause. They just knew that they were generically 'bad' to get and should be avoided.

Respondents with this model knew of a number of different ways that viruses are transmitted. These transmission methods seemed to be things that the subjects had heard about somewhere, but the respondents did not attempt to understand these or organize them into a more coherent mental model. Zoe believed that viruses can come from strange emails, or from "searching random things" on the Internet. She says she had heard that blocking popups helps with viruses too, and seemed to believe that without questioning. Peggy had heard that viruses can come from "blinky ads like you've won a million bucks."

Respondents with this model are uniformly unconcerned with getting viruses: "I guess just my lack of really doing much on the Internet makes me feel like IÕm safer." (Zoe) A couple of people with this model use Macintosh computers, which they believe to be "immune" to computer viruses. Since they are immune, it seems that they have not bothered to form a more complete model of viruses.

Since these users are not concerned with viruses, they do not take any precautions against being infected. These users believe that their current behavior doesn't really make them vulnerable, so they don't need to go to any extra effort. Only one respondent with this model uses an anti-virus program, but that is because it came installed on the computer. These respondents seem to recognize that anti-virus software might help, but are not concerned enough to purchase or install it.

2.1.2 Viruses are Buggy Software

One group of respondents saw computer viruses as an exceptionally bug-ridden form of regular computer software. In many ways, these respondents believe that viruses behave much like most of the other software that home users experience. But to be a virus, it has to be 'bad' in some additional way. Primarily, viruses are 'bad' in that they are poorly written software. They lead to a multitude of bugs and other errors in the computer. They bring out bugs in other pieces of software. They tend to have more bugs, and worse bugs, than most other pieces of software. But all of the effects they cause are the same types of effects you get from buggy software: viruses can cause computers to crash, or to "boot me out" (Erica) of applications that are running; viruses can accidentally delete or "wipe out" information (Christine and Erica); they can erase important system files. In general, the computer just "doesn't function properly" (Erica) when it has a virus.

Just like normal software, viruses must be intentionally placed on the computer and executed. Viruses do not just appear on a computer. Rather than 'catching' a virus, computers are actively infected, though often this infection is accidental. Some viruses come in the form of email attachments. But they are not a threat unless you actually "click" on the attachment to run it. If you are careful about what you click on, then you won't get the virus. Another example is that viruses can be downloaded from websites, much like many other applications. Erica believes that sometimes downloading games can end up causing you to download a virus. But still, intentional downloading and execution is necessary to be infected with a virus, much the same way that intentional downloading and execution is necessary to run programs from the Internet.

Respondents with this model did not feel that they needed to exert a lot of effort to protect themselves from viruses. Mostly, these users tried to not download and execute programs that they didn't trust. Sarah intentionally "limits herself" by not downloading any programs from the Internet so she doesn't get a virus. Since viruses must be actively executed, anti-virus program are not important. As long as no one downloads and runs programs from the Internet, no virus can get onto the computer. Therefore, anti-virus programs that detect and fix viruses aren't needed. However, two respondents with this model run anti-virus software just in case a virus is accidentally put on the computer.

Overall, this is a somewhat underdeveloped mental model of viruses. Respondents who possessed this model had never really thought about how viruses are created, or why. When asked, they talk about how they haven't thought about it,

and then make guesses about how 'bad people' might be the ones who create them. These respondents haven't put too much thought into their mental model of viruses; all of the effects they discuss are either effects they have seen or more extreme versions of bugs they have seen in other software. Christine says "I guess I would know [if I had a virus], wouldn't I?" presuming that any effects the virus has would be evident in the behavior of the computer. No connection is made between hackers and viruses; they are distinct and separate entities in the respondent's mind.

2.1.3 Viruses Cause Mischief

A good number of respondents believed that viruses are pieces of software that are intentionally annoying. Someone created the virus for the purpose of annoying computer users and causing mischief. Viruses sometimes have effects that are often much like extreme versions of annoying bugs: crashing your computer, deleting important files so your computer won't boot, etc. Often the effects of viruses are intentionally annoying such as displaying a skull and crossbones upon boot (Bob), displaying advertising popups (Floyd), or downloading lots of pornography (Dana).

While these respondents believe that viruses are created to be annoying, they rarely have a well-developed idea of who created them. They don't naturally mention a creator for the viruses, just a reason why they are created. When pushed, these respondents will talk about how they are probably created by "hackers" who fit the *Graffiti* hacker model below. But the identity of the creator doesn't play much of a role in making security decisions with this model.

Respondents with this model always believe that viruses can be "caught" by actively clicking on them and executing them. However, most respondents with this model also believe that viruses can be "caught" by simply visiting the wrong webpages. Infection here is very passive and can come from just from visiting the webpage. These webpages are often considered to be part of the 'bad' part of the Internet. Much like graffiti appears in the 'bad' parts of cities, mischievous viruses are most prevalent on the bad parts of the Internet.

While most everyone believes that care in clicking on attachments or downloads is important, these respondents also try to be careful about where they go on the Internet. One respondent (Floyd) tries to explain why: cookies are automatically put on your computer by websites, and therefore, viruses being automatically put on your computer could be related to this.

These 'bad' parts of the Internet where you can easily contract viruses are frequently described as morally ambiguous webpages. Pornography is always considered shady, but some respondents also included entertainment websites where you can play games, and websites that have been on the news like "MySpaceBook" (Gina). Some respondents believed that a "secured" website would not lead to a virus, but Gail acknowledged that at some sites "maybe the protection wasn't working at those sites and they went bad." (Note the passive tense; again, she has not thought about how site go bad or who causes them to go bad. She is just concerned with the outcome.)

2.1.4 Viruses Support Crime

Finally, some respondents believe that viruses are created to support criminal activities. Almost uniformly, these respondents believe that identity theft is the end goal of the criminals who create these viruses, and the viruses assist them by stealing personal and financial information from individual computers. For example, respondents with this model worry that viruses are looking for credit card numbers, bank account information, or other financial information stored on their computer.

Since the main purpose of these viruses is to collect information, the respondents who have this model believe that viruses often remain undetected on computers. These viruses do not explicitly cause harm to the computer, and they do not cause bugs, crashes, or other problems. All they do is send information to criminals. Therefore, it is important to run an anti-virus program on a regular basis because it is possible to have a virus on your computer without knowing it. Since viruses don't harm your computer, backups are not necessary.

People with this model believed that there are many different ways for these viruses to spread. Some viruses spread through downloads and attachments. Other viruses can spread "automatically," without requiring any actions by the user of the computer. Also, some people believe that hackers will install this type of virus onto the computer when they break in. Given this wide variety of transmission methods and the serious nature of identity theft, respondents with this model took many steps to try to stop these viruses. These users would work to keep their anti-virus up to date, purchasing new versions on a regular basis. Often, they would notice when the anti-virus would conduct a scan of their computer and check the results. Valerie would even turn her computer off when it is not in use to avoid potential problems with viruses.

2.1.5 Multiple Types of Viruses

A couple of respondents discussed multiple types of viruses on the Internet. These respondents believed that some viruses are mischievous and cause annoying problems, while other viruses support crime and are difficult to detect. All users that talked about more than one type of virus talked about both of the previous two virus folk models: the mischievous viruses and the criminal viruses. One respondent, Jack, also talked about a third type of virus that was created by anti-virus companies, but he seemed like he felt this was a conspiracy theory, and consequently didn't take that suggestion very seriously.

For the respondents with multiple models, they generally would take all of the precautions that either model would predict. For example, they would make regular backups in case they caught a mischievous virus that damaged their computer, but they also would regularly run their anti-virus program to detect the criminal viruses that don't have noticeable effects. This fact suggests that information sharing between users may be beneficial; when users believe in multiple types of viruses, they take appropriate steps to protect against all types.

2.2 Models of Hackers and Break-ins

The second major category of folk models describe the attackers, or the people who cause Internet security problems. These attackers are always given the name "hackers," and all of the respondents seemed to have some concept of who these people were and what they did. The term "hacker" was applied to describe anyone who does bad things on the

Internet, no matter who they are or how they work.

All of the respondents describe the main threat that hackers pose as "breaking in" to their computer. They would disagree as to why a hacker would want to "break in" to a computer, and to which computers they would target for their break ins, but everyone agreed on the terminology for this basic action. To the respondents, breaking in to a computer meant that the hacker could then use the computer as if they were sitting in front of it, and could cause a number of different things to happen to the computer. Many respondents stated that they did not understand how this worked, but they still believed it was possible.

My respondents described four distinct folk models of hackers. These models differed mainly in who they believed these hackers were, what they believed motivated these people, and how they chose which computers to break in to. Table 2 summarizes the four folk models of hackers.

2.2.1 Hackers are Digital Graffiti Artists

One group of respondents believe that hackers are technically skilled people causing mischief. There is a collection of individuals, usually called "hackers," that use computers to cause a technological version of mischief. Often these users are envisioned as "college-age computer types" (Kenneth). They see hacking computers as sort of digital graffiti; hackers break in to computers and intentionally cause problems so they can show off to their friends. Victim computers are a canvas for their art.

When respondents with this model talked about hackers, they usually focused on two features: strong technical skills and the lack of proper moral restraint. Strong technical skills provide the motivation; hackers do it "for sheer sport" (Lorna) or to demonstrate technical prowess (Hayley). Some respondents envision a competition between hackers, where more sophisticated viruses or hacks "prove you're a better hacker" (Kenneth); others see creating viruses and hacking as part of "learning about the Internet" (Jack). Lack of moral restraint is what makes them different than others with technical skills; hackers are sometimes described as people as maladjusted individuals who "want to hurt others for no reason." (Dana) Respondents will describe hackers as "miserable" people. They feel that hackers do what they do for no good reason, or at least no reason they can understand. Hackers are believed to be lone individuals; while they may have hacker friends, they are not part of any organization.

Users with this model often focus on the identity of the hacker. This identity – a young computer geek with poor morals – is much more developed in their mind than the resulting behavior of the hacker. As such, people with this model can usually talk clearly and give examples of who hackers are, but seem less confident in information about the resulting break-ins that happen.

These hackers like to break stuff on the computer to create havoc. They will intentionally upload viruses to computers to cause mayhem. Many subjects believe that hackers intentionally cause computers harm; for example Dana believes that hackers will "fry your hard drive." (Dana) Hackers might install software to let them control your computer; Jack talked about how a hacker would use his instant messenger to send strange messages to his friends.

These mischievous hackers were seen as not targetting specific individuals, but rather choosing random strangers to target. This is much like graffiti; the hackers need a canvas and choose whatever computer they happen to come upon. Because of this, the respondents felt like they might become a victim of this type of hacking at any time.

Often, victims like this felt like there wasn't much they could to do protect themselves from this type of hacking. This was because respondents didn't understand how hackers were able to break into computers, so they didn't know what could be done to stop it. This would lead to a feeling of futility; "if they are going to get in, they're going to get in." (Hayley) This feeling of futility echoes similar statements discussed by Dourish et al. [12].

2.2.2 Hackers are Burglars Who Break Into Computers for Criminal Purposes

Another set of respondents believe that hackers are criminals that happen to use computers to commit their crimes. Other than the use of the computer, they share a lot in common with other professional criminals: they are motivated by financial gain, and they can do what they do because they lack common morals. They would "break into" computers to look for information much like a burglar will break into houses to look for valuables. The most salient part of this folk model is the behavior of the hacker; the respondents could talk in detail about what the hackers were looking for but spoke very little about the identity of the hacker.

Almost exclusively, this criminal activity is some form of identity theft. For example, respondents believe that if a hacker obtains their credit card number, for example, then that hacker can make fraudulent charges with it. But the resondents weren't always sure what kind of information the hacker was specifically looking for; they just described it as information the hacker could use to make money. Ivan talked about how hackers would look around the computer much like a thief might rummage around in an attic, looking for something useful. Erica used a different metaphor, saying that hackers would "take a digital photo of everything on my computer" and look in it for useful identity information. Usually, the respondents envision the hacker himself using this financial information (as opposed to selling the information to others).

Since hackers target information, the respondents believe that computers are not harmed by the break-ins. Hackers look for information, but do not harm the computer. They simply rummage around, "take a digital photo," possibly install monitoring software, and leave. The computer continues to work as it did before. The main concern of the respondents is how the hacker might use the information that they steal.

These hackers choose victims opportunistically; much like a mugger chooses his victims, these hackers will break into any computers they run across to look for valuable information. Or, more accurately, the respondents don't have a good model of how hackers choose, and believe that there is a decent chance that they will be a victim someday. Gail talks about how hackers are opportunistic, saying "next time I go to their site they'll nab me." Hayley believes that they just choose computers to attack without knowing much about who owns them.

Respondents with this belief are willing to take steps to protect themselves from hackers to avoid becoming a victim. Gail tries to avoid going websites she's not familiar with to prevent hackers from discovering her. Jack is careful to

	Graffiti	*Burglar*	*Big Fish*	*Contractor*
# Subjects	8	13	9	3
Identity of hacker(s)	Young technical geek	Some criminal	Professional criminal hackers	Young technical geek
Level of organization	Solo, or to impress friends	Unspecified	Part of a criminal organization	Solo, but a contractor for criminals
Reason for break-ins	Cause mischief	Look for financial and personal information	Look for financial and personal information	Look for financial and personal information
Effects of break-ins	Lots of computer problems; requires reinstall	Possible harm to computer; exposure of personal information	No harm to computer; exposure of personal information	Exposure of personal information
Target(s)	Anyone; doesn't matter	Opportunistic; could be me	Not me; only looking for rich or important people	Not me; looking for large databases of info
Am I a target?	Possibly	Possibly	No	No

Table 2: Summary of folk models about hackers, organized by model features

always sign out of accounts and websites when he is finished. Hayley shuts off her computer when she isn't using it so hackers cannot break into it.

2.2.3 Hackers are Criminals who Target Big Fish

Another group of respondents had a conceptually similar model. This group also believes that hackers are Internet criminals who are looking for information to conduct identity theft. However, this group has thought more about how these hackers can best accomplish this goal, and have come to some different conclusions. These respondents believe in "massive hacker groups" (Hayley) and other forms of organization and coordination among criminal hackers.

Most tellingly, this group believes that hackers only target the "big fish." Hackers primarily break into computers of important and rich people in order to maximize their gains. Every respondent who holds this model believes that he or she is not likely to be a victim because he or she is not a big enough fish. They believe that hackers are unlikely to ever target them, and therefore they were safe from hacking. Irving believe that "I'm small potatoes and no one is going to bother me." They often talk about how other people are more likely targets: "Maybe if I had a lot of money" (Floyd) or "like if I were a bank executive" (Erica).

For these respondents, protecting against hackers isn't a high priority. Mostly they find reasons to trust existing security precautions rather than taking extra steps to protect themselves. For example, Irving talked about how he trusts his pre-installed firewall program to protect him. Both Irving and Floyd trust their passwords to protect them. Basically, their actions indicate that they believe in the speed bump theory: by making it slightly hard for hackers using standard security technologies, hackers will decide it isn't worthwhile to target them.

2.2.4 Hackers are Contractors Who Support Criminals

Finally, there is a sort of hybrid model of hackers. In this view, hackers the people are very similar to the mischievous graffiti-hackers from above: they are college-age, technically skilled individuals. However, their motivations are more intentional and criminal. These hackers are out to steal personal and financial information from people.

Users with this model show evidence of more effort in thinking through their mental model and integrating the various sources of information they have. This model can be seen as a hybrid of the mischievous graffiti-hacker model and the criminal hacker model, integrated into a coherent form by combining the most salient part of the mischievous model (the identity of the hacker) and the most salient part of the criminal model (the criminal activities). Also, everyone who had this model expressed a concern about how hacking works. Kenneth stated that he doesn't understand how someone can break into a computer without sitting in front of it. Lorna wondered how you can start a program running; she feels you have to be in front of the computer to do that. This indicates that these respondents are actively trying to integrate the information they have about hackers into a coherent model of hacker behavior.

Since these hackers are first and foremost young technical people, the respondents believe that these hackers are not likely to be identity thieves. They believe that the hackers are more likely to sell this identity information for others to use. Since the hackers just want to sell information, the respondents reason, they are more likely to target large databases of identity information such as banks or retailers like Amazon.com.

Respondents with this model believed that hackers weren't really their problem. Since these hackers tended to target larger institutions like banks or e-commerce websites, their own personal computers weren't in danger. Therefore, no effort was needed to secure their personal computers.

However, all respondents with this model expressed a strong concern for who they do business with online. These respondents would only make purchases or provide personal information to institutions they trusted to get the security right and figure out how to be protected against hackers. These users were highly sensitive to third parties possessing their data.

2.2.5 Multiple Types of Hackers

Some respondents believed that there were multiple types of hackers. Most of the time, these respondents would believe that some hackers are the mischievous graffiti-hackers and that other hackers are criminal hackers (using either the burglar or big fish model, but not both). These respondents would then try to make the effort to protect themselves from both types of hacker threats as necessary.

It seems that there is some amount of cognitive dissonance that occurs when respondents hear about both mischievous hackers and criminal hackers. There are two ways that respondents resolve this: the simplest way to resolve this is to

believe that some hackers are mischievous and other hackers are criminals, and consequently keep the models separate; a more complicated way is to try to integrate the two models into one coherent belief about hackers. This latter option involves a lot of effort making sense of the new folk model that is not as clear or as commonly shared as the mischievous and criminal models. The 'contractor' model of hackers is the result of this integration of the two types of hackers.

3. FOLLOWING SECURITY ADVICE

Computer security experts have been providing security advice to home computer users for many years now. There are many websites devoted to doling out security advice, and numerous technical support forums where home computer users can ask security-related questions. There has been much effort to simplify security advice so regular computer users can easily understand and follow this advice.

However, many home computer users still do not follow this advice. This is evident from the large number of security problems that plague home computers. There is a disagreement among security experts as to why this advice isn't followed. Some experts seem to believe that home users do not understand the security advice, and therefore more education is needed. Others seem to believe that home users are simply incapable of consistently making good security decisions [10]. However, none of these explanations explain which advice does get followed and which advice does not. The folk models described above begin to provide an explanation of which expert advice home computer users choose to follow, and which advice to ignore. By better understanding why people choose to ignore certain pieces of advice, we can better craft that advice and technologies to have a greater effect.

In Table 3, I list 12 common pieces of security advice for home computer users. This advice was collected from the Microsoft Security at Home website[7], the CERT Home Computer Security website[8], and the US-CERT Cyber-Security Tips website[9], and much of this advice is duplicated across websites. This advice represents the distilled wisdom on many computer security experts. This table then summarizes, for each folk model, whether that advice is important to follow, helpful but not essential, or not necessary to follow.

To me, the most interesting entries indicate when users believe that a piece of security advice is not necessary to follow (labeled 'xx' in the table). These entries show how home computer users apply their folk models to determine for themselves whether a given piece of advice is important. Also interesting are the entries labeled '??'; these entries indicate places where users believe that the advice will help with security, but do not see the advice as so important that it must always be followed. Often users will decide that following advice labeled with '??' is too costly in terms of effort or money, and decide to ignore it. Advice labeled '!!' is extremely important, and the respondents feel that it should never be ignored, even if following it is inconvenient, costly, or difficult.

[7] `http://www.microsoft.com/protect/default.mspx`, retrieved July 5, 2009

[8] `http://www.cert.org/homeusers/HomeComputerSecurity/`, retrieved July 5, 2009

[9] `http://www.us-cert.gov/cas/tips/`, retrieved July 5, 2009

3.1 Anti-Virus Use

Advice 1–3 has to do with anti-virus technology: Advice #1 states that anti-virus software should be used; #2 states that the virus signatures need to be constantly updated to be able to detect current viruses; and #3 states that the anti-virus software should regularly scan a computer to detect viruses. All of these are best practices for using anti-virus software.

Respondents mostly use their folk models of viruses to make decisions about anti-virus use, for obvious reasons. Respondents who believe that viruses are just buggy software also believe it is not necessary to run anti-virus. They think they can keep viruses off of their computer by controlling what gets installed on their computer; they believe viruses need to be executed manually to infect a computer, and if they never execute one then they don't need anti-virus.

Respondents with the under-developed folk model of viruses, who refer to viruses as generically 'bad,' also do not use anti-virus software. These people understand that viruses are harmful and that anti-virus software can stop them. However, they have never really thought about specific harms a virus might cause to them. Lacking an understanding of the threats and potential harm, they generally find it unnecessary to exert the effort to follow the best practices around anti-virus software.

Finally, one group of respondents believe that anti-virus software can help stop hackers. Users with the burglar model of hackers believe that regular anti-virus scans can be important because these burglar-hackers will sometimes install viruses to collect personal information. Regular anti-virus use can help detect these hackers.

3.2 Other Security Software

Advice #4 concerns other types of security software; home computer users should run a firewall or more comprehensive Internet security suite. I think that most of the respondents didn't understand what this security software did, other than a general notion of providing "security." As such, no one included security software as an important component of their mental model. Respondents who held the graffiti-hacker or burglar-hacker models believed that this software must help with hackers somehow, even though they don't know how, and would suggest installing it. But since they do not understand how it works, they do not consider it of vital importance. This highlights an opportunity for home user education; if these respondents better understood how security software helps protect against hackers, they might be more interested in using it and maintaining it.

One interesting belief about this software comes from the respondents who believe hackers only go after big fish. For these respondents, security software can serve as a speed-bump that discourages hackers from casually breaking into their computer. For these people, they don't care exactly how it works as long as it does something.

3.3 Email Security

Advice #5 is the only piece of advice about email on my list. It states that you shouldn't open attachments from people you don't recognize. Everyone in my sample was familiar with this advice and had taken it to heart. Everyone believed that viruses can be transmitted through email attachments, and therefore not clicking on unknown attachments can help prevent viruses.

		Virus Models				*Hacker Models*			
		Viruses are Bad	Buggy Software	Mischief	Support Crime	Graffiti	Burglar	Big Fish	Contractor
1.	Use anti-virus software	??	xx	??	!!		!!	xx	xx
2.	Keep anti-virus updated	xx	xx	??	!!				xx
3.	Regularly scan computer with anti-virus	xx	xx	??	!!				xx
4.	Use security software (firewall, etc.)	xx		??		??	??	??	xx
5.	Don't click on attachments	!!	!!	!!	!!	!!	!!		
6.	Be careful downloading from websites	??	!!	??	!!	??	??	xx	xx
7.	Be careful which websites you visit		xx	!!	??	!!	!!	??	!!
8.	Disable scripting in web and email								xx
9.	Use good passwords					??		??	xx
10.	Make regular backups		??	!!	xx	!!	xx	xx	xx
11.	Keep patches up to date		??	xx	!!	!!	!!	xx	xx
12.	Turn off computer when not in use		xx	xx	!!	??	!!	xx	xx

!!	Important	It is very important to follow this advice
??	Maybe	Following this advice might help, but it isn't all that important to do
xx	Not Necessary	It is not necessary to follow this advice
	Not Applicable	This model does not have anything to say about this advice, or there is insufficient data from the interviews to determine an opinion

Table 3: Summary of Expert Security Advice. Each folk model responds to this advice differently.

3.4 Web Browsing

Advice 6-9 all deal with security behaviors while browsing the web. Advice #6 states that users need to ensure that they only download and run programs from trustworthy sources. Many types of malware are spread through downloads. #7 states that users should only browse webpages from trustworthy sources. There are many types of malicious websites such as phishing websites, and some websites can spread malware simply by visiting the site and executing the javascript on the website. #8 states that users should disable scripting like Java and JavaScript in their web browsers. Often there are vulnerabilities in these scripts, and some malware uses these vulnerabilities to spread. And #9 suggests using good passwords so attackers cannot guess their way into your accounts.

Overall, many respondents would agree with most of this advice. However, no one seemed to understand the advice about web scripts; indeed, no one seemed to even understand what a web script was. Advice #8 was largely ignored because it wasn't understood.

Everyone understood the need for care in choosing what to download. Downloads were strongly associated with viruses in most respondents' minds. However, only users with well-developed models of viruses (the *Mischief* and *Support Crime* models) believed that viruses can be "caught" simply by browsing web pages. People who believed that viruses were buggy software didn't see browsing as dangerous because they weren't actively clicking on anything to run it.

While all of the respondents expressed some knowledge of the importance of passwords, few exerted extra effort to make good passwords. Everyone understood that, in general, passwords are important, but they couldn't explain why. Respondents with the *graffiti* hacker model would sometimes put extra effort into their passwords so that mischievous hackers couldn't mess up their accounts. And respondents who believed that hackers only target big fish thought that passwords could be an effective speed bump to prevent hackers from casually targeting them.

Respondents who believed in hackers as contractors to criminals uniformly believed that they were not targets of hackers and were therefore safe. However, they were careful in choosing which websites to do business with. Since these hackers targeted web businesses with lots of personal or financial information, it is important to only do business with websites that are trusted to be secure.

3.5 Computer Maintenance

Finally, Advice 10-12 concerns computer maintenance. Advice #10 suggests that users make regular backups in case some of their data is lost or corrupted. This is good advice for both security and non-security reasons. #11 states that it is important to keep the system patched with the latest updates to protect against known vulnerabilities that hackers and viruses can exploit. And #12 echoes the old maxim that the most secure machine is one that is turned off.

Different models had dramatically different suggestions as to which types of maintenance are important. For example, mischievous viruses and graffiti hackers can cause data loss, so users with those models feel that backups are very important. But users who believe in more criminal viruses and hackers don't feel that backups are necessary; hackers and viruses steal information but don't delete it.

Patching is an important piece of advice, since hackers and viruses need vulnerabilities to exploit. Most respondents only experience patches through the automatic updates feature in their operating system or applications. Respondents mostly associated the patching advice with hackers; respondents who felt that they would be a target of hackers also felt that patching was an import tool to stop hackers. Respondents who believed that viruses are buggy software feel that viruses also bring out more bugs in other software on the computer; patching the other software makes it more difficult for viruses to cause problems.

4. BOTNETS AND THE FOLK MODELS

This study was inspired by the recent rise of botnets as a strategy for malicious attackers. Understanding the folk models that home computer users employ in making security decisions sheds light on why botnets are so successful. Modern botnet software seems designed to take advantage of gaps and security weaknesses in multiple folk models.

I begin by listed a number of stylized facts about botnets. These facts are not true about all botnets and botnet software, but these facts are true about many of the recent and large botnets.

1. *Botnets attack third parties.* When botnet viruses compromise a machine, that machine only serves as a worker. That machine is not the end goal of the attacker. The owner of the botnet intends to use that machine (and many others) to cause problems for third parties.

2. *Botnets only want the Internet connection* The only thing the botnet wants on the victim computer is the Internet connection. Botnet software rarely takes up much space on the hard drive, rarely looks at existing data on the hard drive, rarely occupies much memory, and usually don't use much CPU. Nothing that makes the computer unique is important.

3. *Botnets don't directly harm the host computer.* Most botnet software, once installed, does not directly cause harm to the machine it is running on. It consumes resources, but often botnet software is configured to only use the resources at times they are otherwise unused (like running in the middle of the night). Some botnets even install patches and software updates so that other botnets cannot also use the computer.

4. *Botnets spread automatically through vulnerabilities.* Botnets often spread through automated compromises. They automatically scan the internet, compromise any vulnerable computers, and install copies of the botnet software on the compromised computers. No human intervention is required; neither the attacker nor the zombie owner nor the vulnerable computer owner need to be sitting at their computer at the time.

These stylized facts about botnets are not true for all botnets, but hold for many of the current, large, well-known, and well-studies botnets. I believe that botnet software effectively takes advantage of the limited and incomplete nature of the folk models of home computer users. Table 4 illustrates how each model does or does not incorporate the possibility of each of the stylized facts about botnets.

Botnets attack third parties.

None of the hacker models would predict that compromises would be used to attack third parties. Respondents who held both the *Big Fish* mental model and the *Contractor* mental model believe that, since hackers don't want anything on the computer, they would target other computers and leave the unwanted computer alone. Respondents with the *Burglar* model believe that they might be a target, but only because the hacker wants something that might be on their computer. They would believe that once the hacker either finds what they were looking for, or cannot find anything interesting, then the hacker would leave. Respondents with the *Graffiti* model believe that hacking and vandalizing the computer is the end goal; it would never cross their mind to then use that computer to attack third parties.

None of the respondents used their virus models to discuss potential third parties either. A couple of respondents with the *Viruses are Bad* model mentioned that once they got a virus, it might try to "spread." However, they had no idea how this spreading might happen. Spreading is a form of harm to third parties; however, it is not the coordinated and intentional harm that botnets cause. Respondents who employed the other three virus models never mentioned the possibility of spreading beyond their computers. They were mostly focused on what the virus would do to them, and not to how it might affect others. Also, since they had an idea of how viruses spread, those ideas only involved spreading through webpages and email. They don't run a webpage on their computer, and no one acknowledged that a virus could use their email to send copies out.

Botnets only want the Internet connection.

No one in this study could conceive of a hacker or virus that only wanted the Internet connection of their computer. The three crime-based hacker models (*Burglar*, *Big Fish*, and *Contractor*) all believe that hackers are actively looking for something stored on the computer. All the respondents with these three models believed that their computer had (or might have) some specific and unique information that hackers wanted. Respondents with the *Graffiti* model believed that computers are a sort of canvas for digital mischief. I would guess that they might believe that botnet owners would only want the Internet connection; they believe there is nothing unique about their computer that makes hackers want to do digitial graffiti on their computer.

None of the virus models would have anything to say about this fact. Respondents with the *Viruses are Bad* model and the *Buggy Software* models didn't attribute any intentionality to viruses. Respondents with the *Mischief* and *Support Crime* models believed viruses were created for a reason, but didn't seem to think about how using the computer to spread.

Botnets don't harm the host computer.

This is the one stylized fact on this list that any respondents explicitly mentioned. Respondents with the *Supports Crime* model believe that viruses might try to hide on the computer and not display any outward signs of their presence. Respondents who employ one of the other three virus models would find this strange; to them, viruses always create visible effects. To users with the *Mischief* model, these visible effects are the main point of the virus!

Additionally, the three folk models of hackers that relate to crime all include the idea that a 'break in' by hackers might not harm the computer. To these respondents, since hackers are just looking for information, they don't necessarily want to harm the computer. Respondents who use the *Graffiti* model would find compromises that don't harm the computer to be strange, as the main purpose of 'breaking into' computers is to vandalize them.

Botnets spread automatically.

The idea that botnets spread without human intervention would be strange to most of the respondents. Almost all of the respondents believed that hackers had to be sitting in

	Virus Models				*Hacker Models*			
	Viruses are Bad	Buggy Software	Mischief	Support Crime	Graffiti	Burglar	Big Fish	Contractor
Botnets attack third parties	?	–	–	–	–	–	–	–
Botnets only want the Internet connection	–	–	–	–	?	–	–	–
Botnets don't harm the host computer	–	–	–	+	–	+	+	+
Botnets spread automatically	?	–	–	–	–	–	–	–

+	Makes sense	It makes sense that malicious software / attackers would do this
?	Related	This statement is odd, but viruses or hackers might do something similar
–	Unusual	Malicious software / attackers that do this would be unusual

Table 4: How each folk model would probably react to the stylized facts about botnets

front of some computer somewhere when they were "breaking into" computers. Indeed, two of the respondents even asked the interviewer how it was possible to use a computer without being in front of it.

Most respondents belived that viruses generally also required some form of human intervention in order to spread. Viruses could be 'caught' by visiting webpages, by downloading software, or by clicking on emails. But all of those required someone to actively use the computer. Only one subject explicitly mentioned that viruses can "just happen" (Jack). Respondents with the *Viruses are Bad* model understood that viruses could spread, but didn't know how. These respondents might not be surprised to learn that viruses can spread without human intervention, but probably haven't thought about it enough for that fact to be salient.

Summary.

Botnets are extremely cleverly designed. They take advantage of home computer users by operating in a very different manor from the one conceived of by the respondents in this study. The only stylized fact listed above that a decent number of my respondents would recognize as a property of attacks is that botnets don't cause harm to the host computer. And not everyone in the study would believe this; some respondents had a mental model where not harming the computer wouldn't make sense.

This analysis illustrates why eliminating botnets is so difficult. Many home computer users probably have similar folk models to the ones possessed by the respondents in this study. If so, botnets look very different from the threats envisioned by many home computer users. Since home computer users do not see this as a potential threat, they do not take appropriate steps to protect themselves.

5. LIMITATIONS AND MOVING FORWARD

Home computer users conceptualize security threats in multiple ways; consequently, users make different decisions based on their conceptualization. In my interviews, I found four distinct ways of thinking about malicious software as a security threat: the 'viruses are bad,' 'buggy software,' 'viruses cause mischief,' and 'viruses support crime' models. I also found four more distinct ways of thinking about malicious computer users as a threat: thinking of malicious others as 'graffiti artists,' 'burglars,' 'internet criminals who target big fish,' and 'contractors to organized crime.'

I did not use a generalizable sampling method. I am able to describe a number of different folk models, but I cannot estimate how prevalent each model is in the population. Such estimates would be useful in understanding nationwide vulnerability, but I leave these estimates to future work. I also cannot say if my list of folk models is exhaustive — there may be more models than I describe — but it does represent the opinions of a variety of home computer users. Indeed, the snowball sampling method increases the chances that I will interview users with similar folk model despite the demographic heterogeneity of my sample.

Previous literature [12, 15] was able to describe some basic security beliefs held by non-technical users; I provide structure to these theories by understanding how home computer users group these into semi-coherent mental models in their mind. My primary contribution with this study is an understanding of why users strictly follow some security advice from computer security experts and ignore other advice.

This illustrates one major problem with security education efforts: they do not adequately explain the threats that home computer users face; rather they focus on practical, actionable advice. But without an *understanding of threats*, home computer users intentionally choose to ignore advice that they don't believe will help them. Security education efforts should focus not only on recommending what actions to take, but also emphasize why those actions are necessary.

Following the advice of Kempton [19], security experts should not evaluate these folk models on the basis of correctness, but rather on how well they meet the needs of the folk that possess them. Likewise, when designing new security technologies, we should not attempt to force users into a more 'correct' mental model; rather, we should design technologies that encourage users with limited folk models to be more secure. Effective security technologies need to protect the user from attacks, but also expose potential threats to the user in a way the user understands so that he or she is motivated to use the technology appropriately.

6. ACKNOWLEDGMENTS

I appreciate the many comments and help during the whole project from Jeff MacKie-Mason, Judy Olson, Mark Ackerman, and Brian Noble. Tiffany Vienot was also extremely helpful in helping me explain my methodology clearly. This material is based upon work supported by the National Science Foundation under Grant No. CNS 0716196

7. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, December 1999.

[2] R. Anderson. Why cryptosystems fail. In *CCS '93: Proceedings of the 1st ACM conference on Computer and communications security*, pages 215–227. ACM Press, 1993.

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

[4] P. Bacher, T. Holz, M. Kotter, and G. Wicherski. Know your enemy: Tracking botnets. from the Honeynet Project, March 2005.

[5] P. Barford and V. Yegneswaran. An inside look at botnets. In *Special Workshop on Malware Detection,*, Advances in Information Security. Springer-Verlag, 2006.

[6] J. L. Camp. Mental models of privacy and security. Available at `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735`, August 2006.

[7] L. J. Camp and C. Wolfram. Pricing security. In *Proceedings of the Information Survivability Workshop*, 2000.

[8] A. Collins and D. Gentner. How people construct mental models. In D. Holland and N. Quinn, editors, *Cultural Models in Language and Thought*. Cambridge University Press, 1987.

[9] R. Contu and M. Cheung. Market share: Security market, worldwide 2008. Gartner Report: `http://www.gartner.com/it/page.jsp?id=1031712`, June 2009.

[10] L. F. Cranor. A framework for reasoning about the human in the loop. In *Usability, Psychology, and Security Workshop*. USENIX, 2008.

[11] R. D'Andrade. *The Development of Cognitive Anthropology*. Cambridge University Press, 2005.

[12] P. Dourish, R. Grinter, J. D. 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, November 2004.

[13] D. M. Downs, I. Ademaj, and A. M. Schuck. Internet security: Who is leaving the 'virtual door' open and why? *First Monday*, 14(1-5), January 2009.

[14] R. E. Grinter, W. K. Edwards, M. W. Newman, and N. Ducheneaut. The work to make a home network work. In *Proceedings of the 9th European Conference on Computer Supported Cooperative Work (ECSCW '05)*, pages 469–488, September 2005.

[15] J. Gross and M. B. Rosson. Looking for trouble: Understanding end user security management. In *Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT)*, 2007.

[16] C. Herley. So long, and no thanks for all the externalities: The rational rejection of security advice by users. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, September 2009.

[17] P. Johnson-Laird, V. Girotto, , and P. Legrenzi. Mental models: a gentle guide for outsiders. Available at `http://www.si.umich.edu/ICOS/gentleintro.html`, 1998.

[18] P. N. Johnson-Laird. Mental models in cognitive science. *Cognitive Science: A Multidisciplinary Journal*, 4(1):71–115, 1980.

[19] W. Kempton. Two theories of home heat control. *Cognitive Science: A Multidisciplinary Journal*, 10(1):75–90, 1986.

[20] A. J. Kuzel. Sampling in qualitative inquiry. In B. Crabtree and W. L. Miller, editors, *Doing Qualitative Research*, chapter 2, pages 31–44. Sage Publications, Inc., 1992.

[21] J. Markoff. Attack of the zombie computers is a growing threat, experts say. *New York Times*, January 7 2007.

[22] D. Medin, N. Ross, S. Atran, D. Cox, J. Coley, J. Proffitt, and S. Blok. Folkbiology of freshwater fish. *Cognition*, 99(3):237–273, April 2006.

[23] M. B. Miles and M. Huberman. *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications, Inc., 2nd edition edition, 1994. MilesHuberman1994.

[24] A. J. Onwuegbuzie and N. L. Leech. Validity and qualitative research: An oxymoron? *Quality and Quantity*, 41:233–249, 2007.

[25] D. Russell, S. Card, P. Pirolli, and M. Stefik. The cost structure of sensemaking. In *Proceedings of the INTERACT '93 and CHI '93 conference on Human factors in computing system*, 1993.

[26] Trend Micro. Taxonomy of botnet threats. Whitepaper, November 2006.

APPENDIX

This appendix contains samples of data matrix displays that were developed during the data analysis phase of this project.

	Alice	*Bob*	*Carol*	*Deborah*	...
Virus Experience	Husband's laptop had one; caused it to freeze. Son's laptop; "ate" hard drive; got from download.	Grandmother got virus in email; rebooted into "safety" mode and displayed skull and crossbones	2 different viruses; had to format and resintall both times. ISP told her	No viruses	...
Worries about Hackers	Trust "computer companies" to deal with it	No problems, but "always in the back of my head"	"You have my music. Wahoo. If they really care that much, go ahead and look around"	I'm not important enough to be targetted. Still, doesn't put CC number in computer	...
Sources of Information	20/20 story about MySpace. Lots of stories from clients	Personal experience and stories from family members	ISP told her she had a virus. Learned some working collections for a large bank.	Her sons warn her about opening attachments. Feels confused. Got a crash course from job.	...
⋮	⋮	⋮	⋮	⋮	⋱

Table 5: A fragment of the data matrix from the initial analysis of Round 1. It includes a basic descriptions of each subject's statements for each of the major questions in the interview.

		Christine	*Dana*	*Erica*	*Floyd*	*Gail*	*Hayley*	*Irving*	*Jack*	*Kenneth*	*Lorna*
	Creator	No Creator	Teenager	No Creator	Teenager	Teenager	Criminal	Teenager + Crime	Teenager + Crime	Teenager	Teenager
	Effects	Errors	Annoying	Errors	Annoying	Annoying	Annoying + Spy	Spy	Annoying + Spy	Errors + Spy	Annoying
Viruses	*Only Visible?*	Y	Y	Y	N	N	Y	N	N	N	Y
	How to catch	Active	Active + Passive	Active	Active + Passive	Passive	Passive	Active	Happen + Active	Active	Active
	Sources	Email	Web + Email + Downloads	Web + Downloads	Web + Downloads	Webpages	Web + Email + Downloads	Email	Downloads + Email	Email	Email + Web
	Identity	Teenage	Teenager	Criminal	Anyone	Criminal	Teenager + Crime	Criminal	Teenager + Crime	Teenager	Teenager
Hackers	*Behavior*	Secrets	Break Stuff	Big Fish	Big Fish	ID Theft	ID Theft + Secrets	Big Fish	ID Theft + Break Stuff	Big Fish + Databases	Databases
	How to Prevent	No Info	Care on Internet	Care on Internet	Passwords + No Info	Care on Internet	Futility	Trust Software + Passwords	Care on Internet	Trust Software	Trust Institutions
Relationship	*Hacker & Virus*	Separate	As Tool	Separate	Separate	Separate	As Tool	Separate	As Tool	As Tool	Separate

Table 6: Intermediate data matrix developed for analysis. This matrix includes a number of facets of mental models vertically matched with each of the 10 Round 2 participants.

		Christine	*Dana*	*Erica*	*Floyd*	*Gail*	*Hayley*	*Irving*	*Jack*	*Kenneth*	*Lorna*
Viruses	**Viruses are Bad**										
	Buggy Software	x		x							
	Mischief		x		x	x					x
	Support Crime						x	x	x	x	
Hackers	**Graffiti**	x	x			x		x			
	Burglar					x	x		x		
	Big Fish			x	x			x			
	Contractor									x	x

Table 7: A sample data matrix from near the end of the analysis. This matrix shows which folk model was held by the Participants in Round 2. A similar table was developed for the participants in Round 1.