1.1 Folk Models of Home Computer Security

Rick Wash and Emilee Rader

Abstract Home computer systems are insecure not just because they are administered by untrained users, but also because those users make intentional choices that lead to poor security. We describe 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. These models are frequently used to justify ignoring expert security advice. One reason why botnets are so difficult to eliminate is that they cleverly take advantage of gaps in these models so that many home computer users do not take steps to protect against them.

1.1.1 The Relationship Between Folk Models and Security

Home users are installing paid and free home security software at an increasing rate. 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. Compromised computers often go undetected, and are used as tools in cybercrime enterprises.

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, below are identified eight *mental models* [6, 4] 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 [5].

These mental models are *folk models* for home computer users. Folk models are ideas about how the world works that are not necessarily accurate in the real world, thus leading to erroneous decision making, but are shared among similar members of a culture [4]. 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 what leads them to make the decisions they do. 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 of folk models, Kempton [7] 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 people possessed one of two different 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 concluded 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.

Examples from Real People. Understanding folk models in the abstract is great. But to really understand how people think, it helps to see it in their own words. Therefore, the discussion below uses numerous quotations from a series of interviews with home computer users to concretely illustrate these mental models [11]. Everyone quoted here has been given a pseudonym (such as Nicole or Irving) for anonymity, but each name corresponds to a real person who is a non-expert computer user with at least one computer in his or her home.

1.1.1.1 Common Elements of All Folk Models

Folk models of home computer security threats can be divided into two broad categories: 1) models about viruses, spyware, adware, and other forms of malware, which everyone refers 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. Everyone seemed to possess at least one model from each of the two categories. For example, the subject we refer to as Nicole believed that viruses were mischievous, and hackers are criminals who target big fish. These models are not necessarily mutually exclusive. For example, a few people talked about different types of hackers and described more than one folk model of hackers.

By listing and describing these folk models, we do not intend to imply that these models are incorrect or bad in any way. They are all certainly incomplete, and do not exactly correspond to the way malicious software or malicious computer users behave. 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 no “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 outside the context of security, Medin et al. [8] 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. [2] found strong differences between expert and novice computer users in their mental models of security.

Most people who were interviewed made a distinction between ‘viruses’ and ‘hackers.’ 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. For example, Irving tried to explain the distinction by saying “The hacker is an individual [who is] hacking, while the virus is a program infecting.” After some thought, he clarified 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 interviewees thought 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 decided that "I guess if they hack into your system and get a virus on there, its gonna be the same thing." She had never realized that they were distinct in her mind, but it made sense to her that they might be related. She then went on to ask the interviewer, if she got hacked, could she forward it on to other people?

This also illustrates another common feature of mental models. When exposed to new information, most people 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 [9]. Many details of these folk models were probably formed in this way.

1.1.2 Folk Models of Viruses and other Malware

Almost everyone who was interviewed had heard of computer viruses and possessed some mental model of their effects and transmission. Most focused primarily on the effects of viruses and the possible methods of transmission. The term 'virus' was used as a catch-all term for malicious software. Everyone seemed to recognize that viruses are computer programs. Many different types of malicious software were classified under this term: computer viruses, worms, trojans, adware, spyware, and keyloggers were all called 'viruses.'

Thanks to the term 'virus,' many people 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.' People who had a Mac believed that Macs are 'immune' to virus and hacking problems (but were usually worried anyway).

	Folk Model			
	Bad Things	*Buggy Software*	*Mischief*	*Support Crime*
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 1.1 Summary of interviewee's folk models about viruses, organized by model features

Overall, we found four distinct folk models of ‘viruses’ through our interviews. 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.’ Interviewees 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. People with these models could use them to extrapolate many different situations and use them to make many security-related decisions on their computer. Table 1.1 summarizes the major differences between the four models.

1.1.2.1 Virus Model #1: Viruses are Generically ‘Bad’

A few people had an under-developed model of viruses. These people knew that viruses cause problems, but could not really describe what problems. They just knew that they were generically ‘bad’ to get and should be avoided.

People with this model knew of a number of different ways that viruses are transmitted. These transmission methods were things that the person had heard about somewhere, but the person did not attempt to understand or organize them into a more coherent model. Zoe believed that viruses can come from strange emails, or from “searching random things” on the Internet. She said 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.”

People with this model were uniformly unconcerned with getting viruses: “I guess just my lack of really doing much on the Internet makes me feel like I’m safer.” (Zoe) A couple of people with this model used Macintosh computers, which they believed to be “immune” to computer viruses. Since they are immune, it seems that they had not bothered to form a more complete model of viruses.

Because these users were not concerned with viruses, they did not take any precautions against being infected. These users believed that their current behavior doesn’t really make them vulnerable, so they don’t need to go to any extra effort. These respondents seemed to recognize that anti-virus software might help, but were rarely concerned enough to purchase or install it.

1.1.2.2 Virus Model #2: Viruses are Buggy Software

One group of people saw computer viruses as an exceptionally bug-ridden form of regular computer software. In many ways, these people believed that viruses behave much like most of the other software that home users experience. But to be a virus, it had 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 believed 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.

Interviewees with this model did not feel that they needed to exert much effort to protect themselves from viruses. Mostly, these users tried not to download and execute programs that they didn’t trust. Sarah intentionally “limited herself” by not downloading any programs from the Internet so she didn’t get a virus. Since viruses must be actively executed, anti-virus programs 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 ran anti-virus software just in case a virus was accidentally put on the computer.

Overall, this is a somewhat underdeveloped folk model of viruses. People who possess this model had never really thought about how viruses are created, or why. When asked, they talked about how they hadn’t thought about it, and then made guesses about how ‘bad people’ might be the ones who create them. These interviewees hadn’t put too much thought into their understanding of how viruses work; all of the effects they discussed were either effects they had personally seen or more extreme versions of bugs they saw in other software. Christine said, “I guess I would know [if I had a virus], wouldn’t I?” presuming that any effects a virus might have would be evident in the behavior of the computer. No connection was made between hackers and viruses; they are distinct and separate entities in the interviewees’ minds.

1.1.2.3 Virus Model #3: Viruses Cause Mischief

A good number of people 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 people believed that viruses are created to be annoying, they rarely had a well-developed idea of who created them. They did not naturally mention a creator for the viruses, just a reason why they are created. When pushed, these interviewees talked about how viruses 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.

People with this model always believed that viruses can be “caught” by actively clicking on them and executing them. However, most also believed 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 believed that care in clicking on attachments or performing downloads is important, these interviewees also tried to be careful about where they go on the Internet. One respondent (Floyd) tried 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 people 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 had not thought about how sites go bad or who causes them to go bad. She was just concerned with the outcome.)

1.1.2.4 Virus Model #4: Viruses Support Crime

Finally, some people believed that viruses are created to support criminal activities. Almost uniformly, these people believed 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, people with this model worried 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, interviewees who had this model believed 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 believed 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, people 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 even turned her computer off when it was not in use to avoid potential problems with viruses.

1.1.2.5 Multiple Types of Viruses

Some people believed that there are multiple types of viruses on the Internet. These interviewees frequently believed that some viruses are mischievous and cause annoying problems, while other viruses support crime and are difficult to detect. People that talked about more than one type of virus usually included 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.

When people have multiple mental models, they generally 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.

1.1.3 Folk 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 everyone seemed to have some concept of who these people are and what they do. The term "hacker" is applied to describe anyone who does bad things on the Internet, no matter who they are or how they work.

People who were interviewed generally described the main threat that hackers pose as "breaking in" to computers. Different people gave different reasons for why a hacker would want to "break in" to a computer, and to which computers they would target for their break-ins, but usually agreed on the terminology for this basic action. "Breaking in to a computer" meant (to most people) 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 people did not understand how this works, but still believed it is possible.

Below are described four distinct folk models of hackers. These models differed mainly in who the interviewees believed these hackers were, what they believed motivated these people, and how they chose which computers to break in to. Table 1.2 summarizes the four folk models of hackers.

1.1.3.1 Hacker Model #1: Hackers are Digital Graffiti Artists

Some people believed that "hackers" are technically skilled people who cause a technological version of mischief. Often these hackers were envisioned as "college-age computer types" (Kenneth). They saw 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 people 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 provided the motivation; hackers do it ”for sheer sport” (Lorna) or to demonstrate technical prowess (Hayley). Some people envisioned a competition between hackers, where more sophisticated

	Folk Model			
	Graffiti	*Burglar*	*Big Fish*	*Contractor*
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 1.2 Summary of interviewee's folk models about hackers, organized by model features

viruses or hacks "prove you're a better hacker" (Kenneth); others saw 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 were sometimes described as maladjusted individuals who "want to hurt others for no reason." (Dana) These hackers were often described as "miserable" people. Interviewees felt that hackers do what they do for no good reason, or at least no reason they can understand. Hackers were believed to be lone individuals; while they may have hacker friends, they are not part of any organization.

People with this model often focused on the identity of the hacker. This identity—a young computer geek with poor morals—was much more developed in their mind than the resulting behavior of the hacker. As such, people with this model usually gave clear examples of who hackers are, but seemed less confident in information about the resulting break-ins that happen.

These hackers like to break stuff on the computer to create havoc. They intentionally upload viruses to computers to cause mayhem. Many interviewees believed that hackers intentionally cause computers harm; for example Dana believed that hackers will "fry your hard drive." 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 targeting 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 they 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)

1.1.3.2 Hacker Model #2: Hackers are Opportunistic Burglars

Another set of people believed 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 "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; interviewees talked in detail about what the hackers were looking for but spoke very little about the identity of the hacker.

Almost exclusively, the criminal activity they described was some form of identity theft. For example, some interviewees believed that if a hacker obtained their credit card number, then that hacker can make fraudulent charges with it. But others 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, people envisioned the hacker himself using this financial information (as opposed to selling the information to others).

Since hackers target information, people with this folk model believed 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," (Erica) possibly install monitoring software, and leave. The computer continues to work as it did before. The main concern of interviewees was how the hacker might use the information that they steal.

These hackers were believed to 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, people who believed this folk model don't have a good model of how hackers choose, and believed that there is a decent chance that they will be a victim someday. Gail talked about how hackers are opportunistic, saying "next time I go to their site they'll nab me." Hayley believed that they just choose computers to attack without knowing much about who owns them.

Respondents with this belief were willing to take steps to protect themselves from hackers to avoid becoming a victim. Gail tried to avoid going to websites she was not familiar with to prevent hackers from discovering her. Jack was careful to always sign out of accounts and websites when he was finished. Hayley shut off her computer when she wasn't using it so hackers cannot break into it.

1.1.3.3 Hacker Model #3: Hackers are Criminals who Target Big Fish

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

Most tellingly, this group believed that hackers only target the "big fish." Hackers primarily break into computers of important and rich people in order to maximize their gains. Almost every person who held this model believed 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 believed that “I’m small potatoes and no one is going to bother me.” Interviewees with this model often talked about how other people are more likely targets: “Maybe if I had a lot of money” (Floyd) or “if I were a bank executive” (Erica).

For these people, protecting against hackers wasn’t a high priority. Mostly they found 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 trusted their passwords to protect them. Their actions indicated that they believed 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.

1.1.3.4 Hacker Model #4: Hackers are Contractors Who Support Criminals

Finally, there is a sort of hybrid model of hackers. In this view, hackers 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.

Interviewees with this model showed evidence of more effort in thinking through their mental model and integrating the various sources of information they had. 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 believed you have to be in front of the computer to do that. This indicates that these people 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, interviewees with this folk model believed that these hackers are not likely to be identity thieves. They believed that the hackers are more likely to sell this identity information for others to use. Since the hackers just want to sell information, the reasoning goes, they are more likely to target large databases of identity information such as banks or retailers like Amazon.com.

People 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, people’s own personal computers aren’t in danger. Therefore, no effort is needed to secure their personal computers.

However, all respondents with this model expressed a strong concern for who they do business with online. These people 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 are highly sensitive to third parties possessing their data.

1.1.3.5 Multiple Types of Hackers

Some interviewees understood that there are multiple types of hackers. Most of the time, these people believed 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). People with this belief then tried to make the effort to protect themselves from both types of hacker threats as necessary.

Some amount of cognitive dissonance occurred when interviewees had heard about both mischievous hackers and criminal hackers. There are two ways that respondents resolved this: The simplest way was to believe that some hackers are mischievous and other hackers are criminals, and consequently keep the models separate. A more complicated way was to try to integrate the two models into one coherent belief about hackers. The ‘contractor’ model of hackers is the result of this integration of the two types of hackers.

1.1.4 Following Security Advice

Computer security experts have devoted much time and effort to simplifying security advice so home computer users can easily understand and follow it. There are many websites and other online resources available to non-specialist users, including support forums where home computer users can ask security-related questions. However, many home computer users still do not follow available advice.

There is a disagreement among security experts as to why computer security advice directed at “regular” users isn’t followed. Some experts believe that home computer users do not understand the security advice, and therefore more education is needed. Others believe that these users are simply incapable of consistently making good security decisions [3, 10].

However, none of these explanations account for the fact that certain types of security advice tend to be followed by home computer users, while other advice is not. The folk models described above begin to provide an explanation of what expert advice users choose to follow, and what advice is ignored. By better understanding why people choose to ignore certain pieces of advice, we can better craft advice and technologies to have greater security.

Table 1.3 lists 12 common pieces of security advice for home computer users. This advice was collected from the Microsoft Security at Home website[1], the CERT Home Computer Security website[2], and the US-CERT Cyber-Security Tips website[3], and much of this advice is duplicated across websites. The content of the table represents the distilled wisdom of many computer security experts. It then summarizes, for each folk model, whether that advice is “important to follow”, “helpful but not essential”, or “not necessary to follow”. The table illustrates how home computer users apply their folk models to determine for themselves whether to follow a given piece of advice.

The most notable rows in the table are labeled “xx”, and indicate when users believe that a piece of security advice is not necessary to follow. In addition, rows labeled “??” denote instances where users having a given folk model believe that advice will help with security, but do not see the advice as so important that it must always be followed. Often, users will

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

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

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

decide that following advice labeled with '??' is too costly in terms of effort or money, and ignore it. Finally, advice labeled '!!' is extremely important, and users feel that it should never be ignored, even if following it is inconvenient, costly, or difficult.

	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

Table 1.3 Summary of Expert Security Advice. Rows contain common security advice. Each column represents a different folk model. Each folk model responds to this advice differently:

!!	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

Anti-Virus Use Security advice for home computer users often includes the recommendation to run anti-virus software and make sure it is updated regularly (rows 1-3 in Table 1.3). People mostly use their folk models of viruses to make decisions about anti-virus use, for obvious reasons. A belief that viruses are just buggy software is likely to lead to the idea that it is possible to keep viruses off of a home computer by tightly controlling what software is installed on it. This tight control combined with the belief that viruses need to be executed manually to infect a computer (and if a virus is never executed a computer can't be infected) means anti-virus is unnecessary.

Users 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 make an effort to follow the best practices around anti-virus software.

In contrast to people with other models, the burglar folk model leads to a belief that one group of people believes that anti-virus software can help detect and 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.

Other Security Software. There are other types of security software in addition to anti-virus, and home computer users are commonly advised to do things like run a firewall or other more comprehensive Internet security software suites (row 4 in Table 1.3). Most folk models incorporate an unsophisticated concept of what security software other than anti-virus does: it provides general "security". Because the purpose of software such as firewalls is vague and unspecified by these models, people do not treat security software as an important part of protecting their computers. People who hold the graffiti-hacker or burglar-hacker models believe 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.

Another interesting belief about this software comes from the big fish model of hackers. People with this model believe that hackers only go after big fish, and that security software can serve as a speed bump that discourages hackers from casually breaking into their computer, making them a more unattractive target. In this way, it is not necessary for the model to be correct or for people to understand how security software protects, for value to be placed upon using it.

Email Security. Nearly all of the folk models incorporate the idea that bad things can happen if you open email attachments from people you don't recognize (row 5 in Table 1.3). All of the virus models support the belief that viruses can be transmitted through email attachments, and therefore not clicking on unknown attachments can help prevent viruses. People with the big fish and contractor folk models don't believe that they would be targeted, and therefore aren't worried about receiving bad email from hackers.

Web Browsing. Browsing the web involves the potential for encountering many security risks, and much advice is provided to home computer users about how to avoid situations where one's computer might be compromised (rows 6-9 in Table 1.3). Overall, most folk models are consistent with this expert advice; however, the models also do not incorporate a clear cause-and-effect relationship between the advice and better security. In particular, the idea of a "web script" is not explicitly part of any folk model, and therefore is largely ignored because it is not understood.

Because downloads are strongly associated with viruses in most of the virus-related folk models, it naturally follows that the advice about careful downloading would make sense in the context of these models. However, only users with well-developed models of viruses (the *Mischief* and *Support Crime* models) believe that viruses can be "caught" simply by browsing web pages. People who believe that viruses are buggy software don't see browsing as dangerous because they aren't actively clicking on anything to run it.

In addition, all of the folk models are consistent with the idea that passwords are important, but like the advice about browsing the web, the association between passwords and better security is only vaguely defined in several of the models. For example, people with the *graffiti* hacker model sometimes put extra effort into their passwords so that mischievous hackers can't mess up their accounts. And people who believe that hackers only target big fish think that passwords could be an effective speed bump to prevent hackers from casually targeting them. But most folk models do not support a belief that it is important to make good, strong passwords.

Finally, the contractor folk model, in which hackers are believed to work for criminals, supports the idea that people who are not logically the target for criminals are therefore safe from hackers. Web browsing is relevant to security in this view of the world in that one's choices about websites to do business with might make one more or less of a target. For example, a belief that hackers target web businesses with lots of personal or financial information is consistent with advice to be careful which websites you visit, because it is important to only do business with websites that are trusted to be secure.

Computer Maintenance. Finally, security experts often give advice to home computer users concerning computer maintenance (rows 10-12 in Table 1.3). Different folk models vary dramatically in terms of how consistent they are with this type of computer security advice. 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.

Keeping patches up-to-date is a very important behavior for maintaining a secure computer; however, most of these folk models are not directly consistent with this advice. Most people only experience patches through the automatic updates feature in their operating system or applications, and therefore cannot form an idea of what these patches are for. The hacker folk models are more consistent with the advice about patching: If a person feels that they would be a target of hackers, then he or she also feel that patching was an import tool to stop hackers. Also, people who believe that viruses are buggy software folk model associate viruses with the appearance of more bugs in other software on the computer; therefore patching the other software makes it more difficult for viruses to cause problems.

1.1.5 Lessons Learned

Across all the models, everyone worries about how hackers and viruses would affect them. People primarily see the danger to themselves, and don't really consider how malicious people can use them to attack third parties. This self-focus leads people to take precautions only when they feel they are directly at risk. Clever attackers have exploited this feature to form large-scale botnets, and as long as people continue to focus solely on personal risk, botnets will continue to be a problem.

These folk models also illustrate one major problem with many 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.

Finally, following the advice of Kempton [7], 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.

References

1. ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (December 1999), 40–46.
2. ASGHARPOUR, F., LIU, D., AND CAMP, L. J. Mental models of computer security risks. In *Workshop on the Economics of Information Security (WEIS)* (2007).
3. CRANOR, L. F. A framework for reasoning about the human in the loop. In *Usability, Psychology, and Security Workshop* (2008), USENIX.
4. D'ANDRADE, R. *The Development of Cognitive Anthropology*. Cambridge University Press, 2005.
5. JOHNSON-LAIRD, P., GIROTTO, V., , AND LEGRENZI, P. Mental models: a gentle guide for outsiders. Available at http://www.si.umich.edu/ICOS/gentleintro.html, 1998.
6. JOHNSON-LAIRD, P. N. Mental models in cognitive science. *Cognitive Science: A Multidisciplinary Journal 4*, 1 (1980), 71–115.
7. KEMPTON, W. Two theories of home heat control. *Cognitive Science: A Multidisciplinary Journal 10*, 1 (1986), 75–90.
8. MEDIN, D., ROSS, N., ATRAN, S., COX, D., COLEY, J., PROFFITT, J., AND BLOK, S. Folkbiology of freshwater fish. *Cognition 99*, 3 (April 2006), 237–273.
9. RUSSELL, D., CARD, S., PIROLLI, P., AND STEFIK, M. The cost structure of sensemaking. In *Proceedings of the INTERACT '93 and CHI '93 conference on Human factors in computing system* (1993).
10. SRIKWAN, S., AND JAKOBSSON, M. Using cartoons to teach security. *Cryptologia 32*, 2 (2008).
11. WASH, R. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)* (2010).

(Preliminary title) **The Death of The Internet – and What Can be Done to Stop It**

John Wiley & Sons (Asia) Pte Ltd

高等教育出版社
HIGHER EDUCATION PRESS