“Making Security More Usable”

Qualitative Data Analysis in Usable Security

CS4690, Empirical methods in HCI

Sunyoung Kim & Sarah Williams
902266533  902269945
1. Introduction

Today, we are living in the digital world. We read electronic newspapers, we do online banking, we buy things on line, and we communicate with each other via on-line communities, e-mails or instant messaging. Such dependence upon transmission of bytes used in the virtual world based on a computer platform yielded a great amount of digitized data that we now have to deal with as well as a pipeline between ourselves and the outside world we have to watch over, in other words “a network”. As the amount of data grows, so does the amount of valuable data to protect. As the width of the pipeline increases, so does its vulnerability. For example, CERT/CC (Computer Emergency Response Team Coordination Center, a federally funded research center for internet security vulnerabilities) reported that the total number of security vulnerabilities in 2006 was 8,064, while it was only 171 in 1995. Therefore, we cannot help but protect our computers from a variety of security threats such as viruses, Phishing scams, worms, and Spyware. However, most end-users confront difficulty in securing their computers from those threats. Even though a great number of security solutions have been provided, it does not seem that end-users are able to effectively utilize them to secure their computers.

In this project, we aimed to generate ideas about how we could improve security systems so that they are more usable by end-users. For this, we conducted 2 interview sessions, and analyzed 18 transcripts in total. During the interview sessions, we followed the interview guide which starts with a question of what security means, covering the current usage of three main computer security factors, firewall, password and Phishing/Spyware/Malware.

2. Analysis Process

![Diagram of Analysis Process](image-url)
In order to address the research aims discussed above, we analyzed the data both inductively and deductively (See Figure 1). Our first approach was inductive. We both read over all interviews with no explicit preset framing questions. This process challenged us to see the data outside of any biases or favored outcomes that we may have harbored in our minds. We made excessive use of memos (in the form of post-it notes each with the interviewee’s unique code as the header) so that we could easily remember what themes were dominant within each interviews. Figure 2 shows what the interviews looked like after the inductive pass. As you can see, the number and types of themes which emerged varied greatly from participant to participant.

After a discussion of the emergent themes (which served as a way of keeping each other accountable), we then approached the data deductively where we asked two main questions: “What difficulties were users having with their security systems?” and “What are some ways that we can make security systems more usable?” Here we pulled out direct quotes that answered these questions, grouped them together and analyzed for trends among responses. In addition, to be thorough, we repeated this process for responses to each individual interview question group in hopes of being thorough. Finally we employed the process of grounded theory (labeling, grouping and categorizing) to find dominant themes in the dataset. More details about this are in the Data analysis section.

But although our data was gathered through interviews, a lot of rich quantitative data surfaced. Apart from the obvious numbers that could be pulled out (for example the range of number of passwords
kept by the interviewees), we used framing questions that address type, frequencies, magnitudes, causes, structures, processes, consequences and agency to help us group participants into categories of responses and give context to the rest of our results. This process yielded the results in Section 3 below.
3. Data Analysis

1) What is Security?

57% of interviewees mentioned that Computer Security is “Protecting their computers from outside intrusions” such as viruses or hacking. On the same trajectory, 20% said that they felt secured when nobody else but them can access their computer. While the prior notion of computer security is about keeping a computer from others virtually, the later notion is keeping it from physical access. Either virtually or physically, people regarded Computer Security as accessing and using their computers by nobody else but themselves. As minor opinions, 2 interviewees described that their own activities of using the internet such as not visiting sketchy websites influence their computer security. And, one interviewee mentioned that keeping his personal information in his computer is what computer security is for him.

To protect computers, 38.5% of interviewees were using the anti-virus software, and 25.6% mentioned that they were turning the firewall on. MacAfee (4 persons) and Norton (3 persons) were mentioned as the specific anti-virus software currently using, and SpyBot was mentioned once. One interesting finding was that all the interviewees who were using the firewall were also using the anti-virus software. But it was not the vice versa. Not all the interviewees who were using the anti-virus software were using the firewall. Here, we found out that using the anti-virus software is the most common activity for computer security, while using the firewall is accompanied by utilizing the anti-virus software. Apart from the firewall and the anti-virus software, interviewees mentioned variety of methods they are doing for computer security. 3 interviewees mentioned that they take care of passwords for security, while 2 interviewees used special browsers like Firefox or Maxthon for security reason. Interestingly, 2 interviewees mentioned that they lock the door to prevent their computers stolen. As other minor responses, 2 interviewees told us that they disconnect the network when they are not using it, because the status of connecting on the network increases the possibility of unexpected intrusion, and other 2 interviewees said that not visiting websites which are sketchy is what they do for computer security. One
mentioned that he is careful when downloading files not to get any virus.

As an answer of “things you should but don’t do”, one interviewee mentioned that he saved his password in his browser and the windows which he should not. Because if someone takes the computer, they will be able to access all the data he has. Majority of responses about this question was that they were doing fine, saying they take enough care of their computer security.

2) Firewall
The majority of interviewees know almost exactly what the firewall does but only in general terms. Most mentioned that the firewall takes a role of preventing access into one's computer from outside via network. One interesting thing is that 4 among the interviewees mentioned that the firewall deals with data, like “allowing certain data to be able to flow into a computer”, “scanning incoming/outgoing data” or “monitoring data comes in and out” as long as they know, meanwhile most of others said that the firewall blocks people from coming into a computer somehow. Only 2 persons did not answer the question about what the firewall is. (For more description of definitions, see the appendix.)

Most people replied that they rarely configure their firewalls, just turning on with a default set. 2 persons answered that they turn it off when it bothers as the answer of configuration. They seem to regard turning on and off as configuration, too. One mentioned that he configure port forwarding in the firewall to allow outside computers to access internal ones directly, while another said that he set which to block and which not to block.

As an answer of “what do you wish to know about the firewall”, 57% mentioned that they want to know what the firewall does and how it works, for example what it blocks and what it allows or how to decide whether to block or not etc. About this, some mentioned that they want visualized information or simple sentences of explanation. 2 persons said that they want to get a feedback from the firewall. The feedback can include whether it is turned on or off or it blocks something or not. Only one person said that he is doing well and does not need to know any more about the firewall.

3) Password
44% of people used 4 to 6 passwords. The number of 2 to 3 passwords was followed as next majority by 4 interviewees. 3 persons were using 3 passwords, while one was using 2 passwords. Only one interviewee mentioned
that he is using over 10 passwords. Actually he did not remember how many passwords he is using, mentioning like “I don’t know. Maybe 10, 15, or 20?”

As an answer of “how do you remember your passwords?” most interviewees said that they do not have any specific strategy for memorizing those. “Just memorizing because I use it everyday, that’s all” was the majority of responses. Meanwhile, there were a couple of unique methods for memorizing passwords. One person mentioned that all his passwords are same except the last one character which is a digit. That’s why he easily remembers all the passwords he is using.

Among 18 interviewees, only two of them replied that they write down their passwords somewhere either on a piece of paper or on a electronic file, because it is too long, about 25 characters. Except these two, everyone mentioned that they never write their passwords down somewhere.

The period of changing passwords was almost same throughout majority of interviewees; they rarely change their passwords unless it is required. Therefore, some mentioned that it is quite bothering to change GT passwords every three months or so. Only 3 interviewees mentioned that they voluntarily change their passwords every 4 to 6 months based on the importance of websites or on-line services.

A majority responded using upper and lower cases with symbols and numbers as a method to make passwords strong. We also found out four unique methods to make passwords strong. One person used an applet that gives him random characters that include upper and lower cases to make a password. A couple of interviewees used some tricks based on a keyboard’s characteristic, like “I try to spell stuff out and then switch numbers into it or I pick an area of the keyboard like a corner and try do something cool there” or “I type Korean words on the English keyboard, so it doesn’t make sense in English but I know what it means.”

4) Phishing, Spyware, Malware
Almost all the interviewees tried to explain what Phishing, Spyware and Malware are based on their own knowledge. “Phishing” was the term people know its meaning the least. Meanwhile, a lot of people seemed to confuse between Spyware and Malware. 3 persons explained Spyware as Malware, and Malware as Spyware. Whatever they explained about these three terms, or whether they explained those correctly or not, every interviewee without exception had an idea of what kind of threatening exist. (For full explanation of definitions, see appendix.)

To protect oneself from Phishing, “not opening suspicious e-mails” was the major response (63%). A couple of responses were about careful actions, such as “preventing actions like not giving out my information” or “I check carefully…”

To protect oneself from Spyware and Malware, two activities took 73%; either using the anti-virus software (40%) or using the internet service carefully based on self judgment (33%). Here, we found one very interesting point that : these one of two main
activities for protecting one from Spyware and Malware is to lean on technology, while the other is to trust one’s own knowledge. A popup block was used for security reason by 2 persons. As other activities, interviewees mentioned checking currently running software by clicking ctrl-alt-del or downloading files only from credible websites as a protection activity.

It seemed that many people experience of Phishing, Spyware or Malware. All interviewees except one, said that either they or their friends had that sort of experience except only one interviewee. The most common experience was to get viruses whether Spyware or Malware, followed by Phishing. 3 persons mentioned that the virus had crashed either their or their friends’ computer. As long as all the definitions about Phishing, Spyware and Malware were wrong or confused, however, here we cannot say how many “actual” Spyware or Malware they experienced. Because during the interview sessions they said things like “I got Spyware before.” But the definition he explained about Spyware was wrong. Apart from mentioning Spyware or Malware, a couple said that their computers got slowed down.

5) Threatening

As an answer of “when people feel their computer security is threatened”, 50% mentioned that either they think their computers are somewhat safe, or they do not see themselves as a prime target. A couple of interviewees were threatened by pop-ups, while a couple mentioned that they felt that visiting sketchy websites threatened computer security. Interestingly, one interviewee said that her computer security is always threatened when she is connected to the internet.

As for places that threaten computer security, people mentioned public places whether using the wireless service or using public computers as the most threatening place (50%). Among other 50% of responses, 1/3 didn’t have any particular threatening place, while the other 1/3 threatened when they purchase things via on-line. Minor opinions are using Facebook or using laptops at home only etc.

Downloading files from the internet was ranked as the most threatening activity; 7 out of 10 mentioned when they download files they would be vulnerable. As for other opinions, using on-line banking or kicking one’s door to physically access one’s computer were mentioned. One person said “I am weary of certain websites and how they secure things especially when I purchase something.”

6) Consequences from a lack of security
A little bit less than 50% of people said that they were concerned about losing their valuables either physical or not; 47% of interviewees were concerned about someone stealing their money and identity by consequence from a lack of security. A little bit over than 50% of people did not mention any stealing or loss of physical possessions; they were concerned about loss of computer performance or crashing of computers. One person described in detail about a consequence of a lack of security, saying “It’s like eating stale food. Literally corrupting my hard drive and mess it up totally. I could go bankrupt in a second.”

7) Coding: Themes
The coding process was conducted as follows. A few themes emerged from the inductive pass over the data: The role of family and friends, the physical versus the virtual, thoughts versus actions, personas (paranoid, “I’m fine” or neutral, apathetic), Responsibility for security, emotion, suggestions for improvements, becoming more secure, and becoming less secure. Instead of doing full coding to find new themes, we coded the interviews for these analytical categories. We felt that this approach would be more time efficient and also much yield a much more focused analysis.
We show these categories with their associated properties below. (Participant Code is in parens)

Open Coding Results :
The role of family and friends
- Friends/ Family with bad experiences regarding security but not them (JP1,s1000) ,(Armsgsgdg) (fmpx2)
- “I have a father…and a boyfriend…and I’m sure both have done things to my computer, but what I do not know” (ARG)
- “… My boyfriend was close to me and he looked at the website and said “What are you trying to do!” He yelled at me! And then I was like Phew Wow” –KIS01
- Changes password on GT account because Dad has access to it. (ARG)
- Changes password if noticed that someone else changed it (ARG)
- Feels safe at people’s houses (ARG)
- Friends played practical joke; changed facebook when computer was left unattended (ARG)
- Banking information on the parents computer which is more secure(ARG)
• Security is having Dad fix the software; obeys father when he says keep a certain software on (0091369)
• Used to crash dad’s computer, blame it on sisters, father would become angry at sisters but be responsible for fixing the computer(0091369)
• Lots of friends who suffered from identity fraud (KIS01)
• Friends are freaked out by passwords (KIS01)
• Set up Dad’s system securely because he works for the airforce (9817a)
• Inherited a malware infested computer from parents and had to fix it up for his personal use (9817a)
• Trusts the antivirus advice of friends (SKY01)
• Heard about many people experiencing problems with popups so thought that this was normal (SKY01)

The physical versus the virtual
• Password is like a treasure map, don’t write it down (S) (Armsgsdg)
• Password is like a fingerprint
• Will not leave computer on when owner is not around (S)
• Computer is secure when no one has control over it except owner. (P1)
• Stealing/ Burlary
  o Stealing computer = stealing data (P1)
  o Someone could kick down the door and have access to the computer then all is lost (JP1)
• Locks door (P1), (JP1) (Armsgsdg)
• Locks computer to bed (0091369)
• Ignoring computer security is like walking in Piedmont Park “holding thousands of dollars in my hands” – this behavior is stupid  (P1)
• Must be protected when connected to an external device like a USB flash drive (P2)
• Lack of security is like eating stale food, getting sick and dying (P2)
• If the physical security battle is lost, the virtual battle is lost (JP1)
• Recognizes need for virtual security but only acts aggressively to physically secure the computer (JP1)
• Will protect premises more with guard dogs (JP1)
• Computer is like your home – people can burglarize it no matter how hard you try (JFTHETA)
• Internet is a wider entry point (irKnJC1)
• Has a physical password list somewhere that is lost (0091369)
• Distracts people near them by talking to them while typing the password (0091369)
• Analogy: Won’t keep wallet in back pocket (Armsgsdg)
• “strenuous .. configuration” (9817a)
• Writes passwords on desk first before throwing them away (9817a)
Thoughts versus actions
- Does not make credit cards passwords more secure even though ebay account got hacked and they made other passwords are stronger (S)
- Turns the computer off when leaving the house but not worried about roommates being able to access the computer while he/she is in the house (S)
- Recognises need for virtual security but only acts aggressively to physically secure the computer (JP1)
- Knows the right way to come up with strong passwords but doesn’t do it RAG ZERO ZERO ALEPH)
- Guilt about not protecting homework files like they should (irKnJC1)
- Thinks that they should have a firewall but doesn’t have it ; Laziness prevents action(ARG)
- Very knowledgeable about security but still feel for phishing (KIS01)
- Knows that portforwarding is not secure but does it anyway because it makes life easier (9817a)

Personas
- (paranoid,
  - “I am paranoid” - KIS01
- “I’m fine” or neutral,
  - I’m alright because I have no major issues right now (Silver Surfer)
  - Not needing to know more about firewalls (JP1)
  - Due to trust in software (s1000)
  - Experiences with computers have been relatively happy (0416449)
- apathetic),
  - About passwords when using a placeholder email address (P1)
  - Because does not feel that risks are great (Silver Surfer)
  - Does not feel the need for security (s1000)
  - Doesn’t really care, just turned on defaults (s1000)
  - Doesn’t seem to care that physical password list is lost (0091369)
  - Believes in their luck/ is optimistic (SKY01)

Responsibility for security,
- Owner of computer (most participants)
- Dad and/or boyfriend (ARG)
- Dad alone (0091369)
- Child (interviewee) responsible for father’s computer security (9817a)
- Responsibility for security is hers but also a social responsibility like a murder or public assault (SKY01)

Emotion
- Distrust
  - Distrust when antivirus software is asking for more money (S)
o Distrust anything they get in email - restricts himself to reputable well-known sites (JP1)

• Trust
  o Trust in the security of the banking website (S)
    ▪ Bank Of America website feels secure because of the picture and the numbers and 5 minute logout window (ARG)
  o Trusts the default configurations (P1, P2, s1000, fmpx2)
  o Trusts their common sense (P1, RAG ZERO ZERO ALEPH) (Armsgsdg) (fmpx2)
    ▪ Trusts in own judgment about recognizing sketchy sites etc (P2)
  o Trust in security software (s1000)
  o Trust that some people are not smart enough to be more secure so they are not the easiest target (Armsgsdg)
  o Does not question security of his machine when in the library (Silver Surfer)
  o Does not understand why someone would want to put a virus on their machine (JFTHETA)
  o Trusts/ guarantees that Dad’s computer is completely secure. Trusts in Dad’s ability to make their computer secure (ARG)
  o In Georgia tech’s ability to recognize a good password: If Georgia Tech website accepts password, it is strong (ARG)

• Feels safe
  o when seeing a McAfee popup during startup (P2)
  o Feels protected when firewall is turned on (s1000)
  o At people’s houses (ARG)
  o When members of the network can be traced eg the Georgia Tech network (KIS01)

• Hope/Guessing/ Uncertainty
  o that computer is safe since nothing bad has happened (P2)
  o That they are doing enough to protect computer (JFTHETA)
  o Hopes/Thinks antivirus takes care of threats they haven’t heard about as well as threats that they know about (s1000) (0091369)
  o Uncertainty about what firewalls do (0416449)
  o Never know what will happen when popups occur (0091369)
  o Hoping that he is protected against phishing (Armsgsdg)
  o Unsure of whether expired firewall/ antivirus is protecting computer (9817a)
  o About whether firewall is working in general – several participants
  o Not sure if efforts to fix computer worked even if symptoms are gone (9817a)
  o Unsure whether spyware is the threat or the software against the threat (SKY01)
  o Hopes antivirus works (fmpx2)
• Resignation/Apathy
  o Resigned to the fact that people can hack into their machine. Must pay attention to physical security.
  o “If someone really wanted to get into my stuff, they could. I’m not all that smart about protecting myself.” (JFTHETA)
  o Does not seem themselves as a prime target (JFTHETA)
  o “I’m not much of a target” (9817a)
  o Not much of a target (SKY01)
  o Her data is not desirable (SKY01)
  o Doubt that there is any way to tell for sure whether a site is legitimate (fmpx2)
• Annoyance
  o With Norton Antivirus security popups (JFTHETA)
  o Firewalls are annoying, because of popups (0091369)
  o By MacAfee popups (9817a)
  o Security is cumbersome (SKY01)
• Obligation/ Guilt
  o Obligation To keep the MS firewall up (JFTHETA)
  o Obligation To change passwords after a while (JFTHETA)
  o Guilt about not protecting homework files like they should (irKnJC1)
  o Guilt : Thinks that they should have a firewall but doesn’t have it (ARG)
  o Guilt at not scanning IP ports, not doing as much as she can (KIS01)
  o Guilt and shame at not remembering the word spam: (KIS01)
• Eager to encourage interviewer to be more secure (KIS01)
• Relief
  o After getting proof that current antivirus solution worked (KIS01)
  o That she is not the easiest victim (KIS01)
• Worry
  o After reading security articles and seeing how computers can be hacked (KIS01)
  o Worried about malware not phishing and spyware

Suggestions for Improved Experience
  • Preventative Measures
    o Be notified about danger to computer before harm is done to it, ie preventative for example hotmail lets you read an attachment before you open it. (S)
    o Programs are first screened by McAfee before files are accessed (P2)
- "preventative action such as not giving out that information [personal]" (irKnJC1)
- Wants to see first warning signs before harm is done (9817a)
  - Password is secret, it shouldn’t be recorded (S)
  - More knowledge could help
    - Does not know what step to take to prevent damage to computer except turning it off (P1)
    - Know the technology behind everything (P1)
    - More than just “general titles” about what the firewall is doing (Silver Surfer)
    - In order to know when you’re at risk, you need to understand “where the files are coming from and whether it’s a trusted source of not” (Silver Surfer)
    - More indepth knowledge
      - about firewalls (s1000)
      - About firewalls and how to set it up (ARG)
    - Doesn’t know what to do besides antivirus plus firewalls (0091369)
    - A firewall tutorial would be nice (0091369)
    - An explanation of what the pros and cons are of turning a security feature on or off. (fmpx2)
  - Run an OS offering better security than the often targeted Microsoft products for example Linux (P1, KIS01)
  - Ability to report suspicions or check up on things/confirm things in the real world helps prevent problems
    - Called paypal when phishing was suspected (P2); Calls back site to verify (KIS01)
    - Called friend to confirm that email was indeed from them (P2, ARG)
    - Would report suspicious emails (Silver Surfer)
    - Logs into site to see if information is missing (0091369)
  - Checking with the Task Manager helps prevent problems
    - Ctrl-Alt Del (P2) (KIS01) (9817a)
  - Integration with default settings
    - Software should work with not against the Windows Firewall (Silver Surfer)
  - Backing up Data (JP1) (fmpx2)
  - No hand holding
    - No excessive help guides or hand holding during installation
  - Software being free (s1000)

**Becoming more secure ...**
- Because of a bad security related incident
Because eBay got hacked into (S). Now S is very careful to make sure that the write address is in the address box (S).

- After CIH virus (KIS01)
  - Because interviewer pointed out a phishing technique they did not know about (S)
  - Changing passwords when account becomes compromised (P1)
  - Feels like s/he’s more secure because less and less viruses are detected (Silver Surfer)
  - More or less secure depending on which computer is used (Silver Surfer)
  - More secure passwords depending on importance of data being secured (JFTHETA)
  - By cutting out experimental habits (s1000)
  - By not having anything valuable on machine at all ie no data perceived as valuable to another person (s1000) (fmpx2)
  - Would change password if problems occur for example, password hacked/compromised (ARG) (0416449)
  - After a website told him to be more secure with passwords (Armsgsdg)
  - After clicking a bad popup (SKY01)

**Becoming less secure**
- Used to change passwords often in the past but not now. (P2)
- Less secure to avoid the hassle (JP1)
- When computer slows down or websites blocks, firewall and antivirus are the first to go (SKY01)

Axial Coding Results:

![Trust and Personas](image-url)

**Figure 2 Trust and Personas**
As figure 2 shows, the emotion Trust seems to be the basis of how users behave. Paranoid individuals trust no one and no software explicitly, Those who are apathetic trust everyone, their security advice and trust in the fact that no one really wants to attack them and steal their data. Those in between trust their own common sense, their own judgment and the default settings on antivirus software. We also initially thought that persons could be placed in buckets of paranoid, I’m fine and apathetic. However, upon closer examination it is clear that very few can be categorized this way. In fact, each participant seems to exhibit bits and pieces of each trait: they may be paranoid about some things but lax about others. The notion of thought versus action comes into play here but more importantly, their behavior is determined by how much they value the data in question.

Figure 3 Becoming more Secure is influenced by social, mental and technical mechanisms

As figure 3 shows, persons can be influenced to become more secure through social, mental and technical means, not just technical. The data clearly shows that often times if the user is not employing secure practices themselves, their family members and friends jump in with advice or in actually running and configuring things themselves. Family and friends have unique opportunities to be in the right place at the right time and intercept bad behavior for example KIS01’s boyfriend preventing her for falling for phishing. Users also use their mental models of security to drive their security practices. Drawing analogies with real life helps them be more secure for example, thinking about your data like money and not walking
in the park with your money on your sleeve (JP1). Finally, when users made suggestions about being more secure, they were always technical. Why not social and mental? Perhaps users feel obligated to do technical things when we may be able to influence them better through social and mental means.

**Becoming Less Secure**

Thoughts Versus Actions
- Wanting to be more secure but not doing so
- Because of laziness

Because of annoyance

**Figure 4** Becoming less secure and its relationship to the dichotomy between Thought and Action

As figure 4 shows, people become less secure because of annoyances in being secure and because of the differences between their thoughts and actions. People want to be more secure but obstacles of usability and annoyances, and perhaps laziness and apathy get in the way.

The various emotions found in open coding seem to form the basis of all other coding categories.

Selective Coding

In Selective coding, one needs to pick a central category and build a story around it. That category for us is “Becoming more secure” in Figure 3. People approach security, like many other things, in social, mental and technical ways, not just technical. The story we have built is the following. Everyone values their physical security but have trouble transferring that concern to their virtual security. The reason for this is that a person’s whole body is valuable to them, however, a person’s data is not always important. Some of it is more important than others. The importance of the data drives action. To a lesser extent, past annoyances with attempts at security also influence action however people seem to be content with being a bit uncertain about whether their security software is working. They will not change their behavior or actions they have taken in the past unless something bad happens. In general, persons approach security from social, mental and technical means – this implies that targeting people and getting them to be more secure involves strategies along all these three lines.

**Discussion/ Suggestions**
So coming back to the research questions of what is difficult for people as they use their software and what ideas can we generate to make systems more usable, we have come up with three main suggestions:

- The first suggestion we have regards the root of the problem. People don’t realize the desirability of their data. Even if they regard it as useless to another person, they don’t realize that it is sought after by hackers and needs to be protected. This implies that programs need to remind users of the importance of their data perhaps through examples of why and how hackers can use their data even the simplest piece of data to harm the individual.

- Based on the target individuals, software and programs need to employ social, mental and technical strategies. For example, for people that are mostly apathetic towards security, strategies like comic strips or an online social network might be the best approaches for them. These entertainment media can be used to get them to involve their family and friends in their security practices and could try to bridge the gap between physical and virtual security in a fun way. Comic strips could easily exploit the physical analogies that already exist within a user’s brain.

- Of course security software usability needs to be improved. Our suggestion here can be summed up as Overview first, Details on Demand – a common principle in information visualization. People are annoyed with security pop-ups, security software slowing down the computer, the pains of configuration. This may be solved by causing security notices to be more discrete and general to begin with but giving the user the chance to click on a discrete notice (perhaps in one corner of the screen) and be given an in depth explanation of why and how the security software operates the way it does. So when viruses get on a machine, they are usually installed and then flagged by the antivirus program. Participants seem to want to be notified before any harm is done.

4. Easy/hard/surprising

Firstly, recruiting participants was quite easy. Friends and even acquaintances could easily find a spare 30 minute space in their schedule to accommodate us. In addition, the interviews themselves were quite enjoyable. Not only did it give us a chance to apply the interviewing techniques skills we’ve learned in class, we both learned much more about security and where we could be much more cautious about our digital data. The process of analysis, though time consuming was also something we both looked forward to and enjoyed. Extracting themes and answering research questions seemed very much like the role of a detective as s/he hunts for clues to solving a mystery. We enjoyed the

But this process did not come without some obstacles. Analysis is time consuming – all parts of it require serious time commitments. Transcription was our first taste of this as we spent a combined twelve hours in transcribing our interviews. Analyzing data is also time intensive, first in reading over interviews and second returning to them for quotes and identification of themes. In some cases, it took about one hour to read one interview! One thing that was particularly frustrating was the fact that extracting quotes from the paper involved manually typing them into the paper instead of copying and pasting them from a transcript.

During the interview itself, there were some difficulties. It was hard to stick to the interview guide for two reasons: we ourselves were learning a lot about security and each interviewee was quite unique (one paranoid about security while the other apathetic). Both reasons caused us to follow up on interesting topics
that arose which uncovered interesting data but also might have been a bit indulgent on our parts. The balance between following up on interesting events surrounding the participant and following up on any and everything interesting to us (the interviewers) was a bit hard. In addition to all of this, explaining security terms to our interviewees was challenging because English was a second language. Finally, one of our initial participants decided not to show up our interview! This was both frustrating and surprising. Even to this day, the person has not contacted us to apologize for missing the interview even though on the day of the interview we sent a reminder email. That said, it was a valuable lesson learned about allotting adequate time for scheduling and conducting interviews.

Finally, we found that users’ strategies for remembering passwords were surprisingly creative! Almost every strategy we’d read was new to us. Password remembrance strategies can be deemed on the one hand as private but when asked most participants freely shared what they did. If more people knew about engaging strategies, we feel that people may realize that creating a strong password does not always have to be boring and may be motivated to make their passwords stronger. Finally, we were blown away by how much we learned about security. We ourselves thought that we were living secure lives but can clearly see now that we can be much more cautious with a little more effort.

5. What we would do differently

First of all, as we mentioned at the paragraph above, we ourselves learned a lot about computer security by interviewing and analyzing transcripts. However, our interviews would be more effective if we had studied the terms in regard of security ie the statistics of how many/what kind of problems are caused by viruses, Spyware and Phishing scams, and the current security systems’ functions, interfaces and shortcomings. We had a question which asks meaning of the terms. And when we asked interviewees about meaning of the terms, one interviewee asked back about it to us, mentioning that she does not know what those are, and thus wants us to explain those. Thankfully, our first interviewee whose major was “information security” explained all the terms quite clearly during that interview session, which enabled us to repeat what the previous interviewee described to the second interviewee. Were it not for her explanation, we would have gone through the whole second interview based on our speculations about definitions of the terms which could be wrong. Moreover, we recognized that getting armed with correct information about computer security beforehand would prevent us as an interviewer from accepting wrong information from interviewees. We found out that some people misunderstood certain terms, or underestimated the current security systems’ functions provided. If we had not been equipped with correct information about those, wrong information gathered from some interviewees could have lead us to the wrong conclusion.

Secondly, we would make and use a piece of sheet with tables on which we can write down the numbers (quantitative data) interviewees responded during the interviews. We had an interview guide of questions, which enabled us to anticipate what kinds of quantitative data we could get. To organize quantitative data from transcripts, we kept turning pages back and forth looking for interviewees’ comments about quantitative factors. As long as one interviewer leads the interview and another takes a role of note-taking, the note-taking interviewer would be able to mark the numbers (for example, the number of passwords people are using, how often they change their passwords, etc.) on the piece of sheet (which could have been prepared even before the interviews based on quantitative data we expect to get), instead of digging through all the transcripts to find out quantitative data afterwards.
Lastly, we think it would be a lot more helpful if we had used the electronic version of transcripts. When we do this project again, we would definitely use the electronic files of transcripts. As we mentioned earlier, transcription was one really difficult part of this project. However, now we can say sorting all the raw data into organized categories was a lot harder than transcribing. We did have 18 transcripts, and had 17 questions in total. We had to sort out all the answers of questions, we had to match memos taken while either reading transcripts or conducting interviews, and we had to turn pages of transcripts numerous times to find out things I remember that I read before. For that, we even thought about cutting all the sheets of transcripts into pieces of answers and grouping those. However, we decided not to do so, because it would be a lot harder than rewriting the parts we needed from the transcripts.

6. Conclusion
In our introduction, we mentioned that even though a great number of security solutions have been provided, it does not seem that end-users are able to effectively utilize them to secure their computers. From the data, it seems to be due to people’s annoyances with security pop-ups, security software slowing down the computer, the pains of configuration and the doubt, uncertainty, guilt and shame associated with not really knowing what the security software is doing. We have made some suggestions in the coding section that not only address technical deficiencies but deficiencies in the way that software today is addressing the social resources currently around participants and mental models that already exists in users’ minds. We believe that making your computer more secure will be a much easier and more enjoyable experience if security software designers become more aware of both the technical and nontechnical factors that influence computer use.

[Appendix: Data Coding]

1. What does it mean to you to make your computer secure?

- Protecting my computer from possible malicious use which includes protecting it both from user actions that are accidental and could cause bad things to happen, from bad users from showing up and using the computer in unsafe ways, and outside users or programs coming in through other avenues besides that keyboard and using it in unapproved ways.
- I feel like my computer is secure when no one can access anything that I don’t want them to. I guess that would include everything from credit card information to email passwords to my resume.
- I don’t explore internets that are not safe and be notified in a way that I can understand when it’s not.
- I have lots of personal information on my desktop, and keeping it secure is computer security.
- No hiding programs in my computer. I have to secure my email so nobody can access it.
- Securing information which is important personally.
- Protecting my computer from any harm while I’m connected to an external device.
- It means that no person except me has any measure of control over my computer
- Protecting it from viruses
- No virus, protecting programs.
- Protect the computer using a firewall.
- Protect a computer from outside intrusion. Nobody can access my computer on the internet.

1-1. what steps do you take to protect your computer, your data

- I turn on my firewall and use anti-virus program.
- Having a firewall and anti-virus protection.
- I should have firewall.
- I want to have firewalls up, use Firefox and anti-virus software.
- Protect the network connection using firewall in addition to a virus scanner and a firewall. I password protect important files, and lock the door to an apartment so nobody can come in and log onto my computer.
- I have Norton, and I’m pretty good at rotating passwords in and out. Special paying attention to passwords like the one for bank account.
- I make backup copies of data and ensure that my firewall is on at all the time.
- I have Norton Antivirus on, and update it often. I don’t visit sketchy websites.
- I use anti-virus software and firewall. I password my hard disk to lock it.
- I have MacAfee software.
- I disconnect from the internet.
- I have McAFee and firewall.
- Keep my door locked.
- I have a firewall and anti-virus software.
- I have a MacAfee. And I try to make sure websites I visit are secure.
- I don’t download any weird software. And I’m using Spybot.
- I have Norton and a firewall.
- Data backup and virus scanning.

1-2. Are there things you don’t do, why is that?
- I saved passwords in my web browser. If someone takes the computer and they will be able to crack it.

2. What do you think firewalls do?
- It filters incoming traffic to prevent unwanted visitors.
- It is just kind of disguising your IP address so that it helps prevent hackers from simply getting into your computer. Firewall hopefully prevents anybody trying to access your computer.
- It prevents people from getting in through ports.
- It blocks people from coming into your computer somehow.
- It blocks an external user to access the information on my computer.
- It is a barrier from the internet, between your computer and the internet. It monitors which data comes in and out and decide whether to allow going into my computer from the internet or out of my computer.
- It prevents people from accessing your information from outside.
- It limits the open ports that my system is putting out and any IPs that are trying to access my computer either to take information from it or send information to me, before it lets them give any of those transactions.
- It scans incoming data, preventing incoming things which look suspicious.
- It is designed to prevent people from getting access to your computer.
- It allows certain data to be able to flow into a computer and block unwanted stuff.

2-1. How/Do you configure your firewall?
- I just turn it on. This program asks me too many questions.
- I configure port forwarding in the firewall to allow outside computers to access internal ones directly.
- I turn it on or off.
- Use default.
- Block or unblock
- I set it as medium security level.

2-2. What do you wish that you knew about your firewall?
- I just want some knowledge in depth.
- I’m good.
- I wish to know what exactly it does. It might be good to show how it works or what it is catching.
- What the firewall is.
- I wish I could know better what they are doing visually, and I want to adjust level of security.
- Whether it’s working or not.
If there is a list of things which can make sure for my computer security that I could get by running the firewall, and another list of things which can cause a security problem when I turn it off.

- It can have a short explanation of what does virus protection, and e-mail protection with a couple of short sentences that says “this is what it is.”
- I want it tells me when it blocks something.
- A better explanation of how the program is working and how it protects me would help.
- I wish it would explain more in detail of what it does, and how it protects.
- I’d like to know more information about the incoming traffic like from other country.
- A visual feedback so I can recognize whether it is running.

3. What strategies do you have to help you remember and manage your passwords?

- I start it based on a word that does not make sense in English but in Japanese or Latin.
- I type Korean words on the English keyboard, so it doesn’t make sense in English but I know what it means.

3.1. How/Do you make your passwords strong?

- I include some set of letters and numbers.
- I downloaded an applet that gives me random characters that include upper and lower cases.
- I try to spell stuff out and then switch numbers into it or I pick an area of the keyboard like a corner and try do something cool there.
- I use some characters from the URL for the last some characters of passwords.
- I create passwords based on my address, my parents’ or grandparents’ addresses. Address includes some numbers and characters. I use them to make my passwords.

4. The terms Phishing, Spyware, and Malware. What do they mean to you?

- Phishing is like when people try and trick other people into giving up their credit card information. Malware is software that doesn’t do what you want it to. Spyware is something that tracks web habits.
- I don’t know what Phishing means exactly. Spyware is simply programs that get onto your computer that report back to advertisers what you’re using on your computer, monitoring your internet activity etc. Malware is anything that might hurt your computer, maybe not necessarily a virus but something that will slow your computer down.
- They are all bad and they mean viruses and spam.
- I don’t know what Phishing is. About Spyware and Malware, I know that you can get those from the internet by installing something on your computer.
- Phishing is when they put some hardware and software in the ATM machines, and then when you swipe your card, they can take your information, data and money. Spyware is a program that can show some other user things you type in the computer, like passwords. I have no idea about Malware, though.
- Phishing means someone faking their identity to get personal details from a person. Spyware tries to send information from my computer to someone else’s without notifying me. Malware is something like, say if I access some website and that website automatically downloads some application onto my computer.
- I have no idea what Phishing is. Spyware is something installed on my computer and monitors/records what I do/have. Malware is stuff that is destructive to your computer or data, like virus.
- Malware is something running on your computer without notifying you. Maybe it uses up CPU or does something wrong. Spyware is something that sends data to somebody else without your knowing. Phishing is searching through a lot of other people’s ports to find security breaches that can be exploited.
- Spyware would be the one that comes on your computer and try to collect information about you without your consent. Malware is still a program on your computer but they are there to mess up your programs.
- I don’t know what Phishing is. Spyware is one that marketers install something in your computer somehow or someway to follow everything that you do. Malware is malicious software.
Phishing is when a link is sent to a user in an unsolicited fashion that prompts them to take action. Spyware is software that gets loaded on a computer, generally surreptitiously that records the user actions. Malware is either viruses that damage data or take over the computer and harness its network connection.

4-1. How do you protect yourself from Phishing?

- Preventing action such as not giving out information.
- I never open e-mail from someone I don’t know.
- I just delete it.
- I use the firewall.
- I’m very careful with the e-bay, looking up the URL to make sure that’s the same.

4-2. How do you protect yourself from Spyware and Malware?

- I use anti-virus software.
- I am careful not to click suspicious links or websites.
- I check running software by clicking ctrl-alt-del.
- I use popup blocks.
- I only download from sites that have firewall up and choose carefully from which sites I download stuff off.

4-3. Have you ever had any bad experiences with these?

- I have experienced that there’s been a lot of Spyware on my computer.
- My computer got slowed down.
- I had problem with my computer last year, for some virus. I reinstalled my computer.
- A friend of mine had Spyware on his computer before.
- I clicked one e-mail and it automatically opened a lot of windows which had some sexual images. I tried to close all but I couldn’t. So I just restarted my computer.
- I had a computer with full of Malware.
- I got Phishing e-mails.
- Some e-bay situation.
- I have had data on friends’ computer got lost when a virus crashed the system.

5. When do you feel your computer’s security might be threatened?

- Porn site
- I don’t see myself as a prime target.
- I think my computer is somewhat safe.
- Pop-ups
- When I’m using the internet

5-1. Certain places where you use your computer?

- Using the internet at the public place like Starbucks, airport, dormitory or hotel
- I don’t take my laptop anywhere except home.
- No particular place
- Using public computers
- Facebook
- On-line purchasing

5-2. Certain types of activities that you use your computer for?
Someone could kick down my door, walk in my apartment and have physical access to my computer.

I am leery of certain websites and how they secure things especially when I purchase something.

When I download bunch of things from the internet, I'd be vulnerable.

On-line banking

6. Consequences from a lack of security

- Hacking
- Stealing through credit card or identity theft.
- My computer can get viruses.
- Loss of data and money
- Loss in computer performance
- It’s like eating stale food. Literally corrupting my hard drive and mess it up totally. I could go bankrupt in a second.
- My computer can get crashed.