**The Questions and Who is Asking of Social Engineering**

Alexander Cannell

CSIA 6200 - Hacking and Security Vulnerability Management

# 

# Abstract

This is a study of social engineering about the effectiveness of certain questions of gleaming information. What questions are better at gleaming information than others? What questions are people comfortable giving? How the relationship of questioner and the person answering the questions affects the answers. I used performed a survey to determine the results of this project. The participants were gagged on the comfortability of 77 questions.

*Keywords:* Security, Phishing Attacks, User Protection

# 

# 

The Questions and Who is Asking of Social Engineering

**Introduction**

In my undergrad Ethical Hacking class we learned about how the weakest point in any security system is going to be the human element. I have always been interested in the social engineering aspect of hacking especially the psychology behind it. If you can convince someone with the keys to open the safe door for you, why spend time trying to pick the lock. This is the major reason why social engineering is such a danger to system security.

Social Engineering is an attack that relies on human interaction; often, that human interaction involves tricking people into breaking security procedures. There are a lot of different types of social engineering attacks which includes Baiting, Phishing, Pretexting, and Scareware. Baiting is when a cracker or attacker with a malware infected physical device convinces someone to use the infected device. For example: the attacker leaves an infected flash drive laying around and the victim picks up the device and uses the device to download malware onto his computer. Pretexting is when someone lies to gain access to sensitive data. For example: an attacker pretends to be an authorized authority and requests personal and financial information to confirm the ID of an victim. Scareware is tricking a victim to believe that there is something wrong with their system and giving the attacker the opportunity to install malware. Phishing is the process of obtaining personal and/or financial information from a victim while the attacker fraudulently poses as a legitimate company. This process is most commonly used in email or social media. A specific or targeted attack to a certain company or individual is called spear phishing. (whatis, 2016)

This project idea started when I was playing a video game, Batman Arkham Knight. In the game you have the ability to mimic different character voices and give characters commands in those voices. Which made me think what effect different types of people have on our answering personal questions. Or in other words, how the relationship of the questioner and the person answering the questions affects the answers given. What questions are people comfortable giving to regular people, and which questions are on the more uncomfortable range? What questions are better at gleaming information than others? The purpose of understanding my queries into these questions can help bring an understanding to how to create a better defense against social engineering attacks when they present themselves in our personal life and our professional life. From an ethical hacking/penetration testing standpoint it is good to know how to be better at social engineering. Penetration testing is the process of testing a system to find vulnerabilities that someone with malicious intent would try to exploit.

# Method

## Participants

My participants who completed the survey included my pool of friends, family, and coworker. I created the social engineering survey using google forms, then posted the link on my Facebook wall; which was anonymous. I then asked people I knew or ran into to take the survey. It was really hard to persuade people to participate in my survey. I think they thought of me as Admiral Ackbar in Star Wars Trilogy fearing that my survey was a “TRAP!!!” (Star Wars, 1983) I was trying to glean personal information from them by assimilating someone attempting to hack my facebook account trying to obtain critical personal information from them. As a result, I got a total of 17 participants to take the survey, and I think I had a good amount of people participate.

## Assessments and Measures

I started my project by asking myself how could I address the proposed questions? The proposed questions being, “What questions are better at gleaming information than others?” “What questions are people comfortable giving?” “How the relationship of questioner and the person answering the questions affects the answers?” I decided in my planning that I would have to split each question up individually and have them answered in different sections of my survey. I followed that with research on different questions I would ask. It would surprise you how hard it was to come up with questions. It wasn't like coming up with questions on a date either because who asks on a date what your social security number is, or what is your credit score. I found myself coming up with questions like, “What is your favorite Ninja Turtle in TMNT(Teenage Mutant Ninja Turtles) and why?” Before you judge me on my dating questions, just know you can find out a lot about someone from their favorite ninja turtle; mine being Donatello. But dating questions were not very pertinent to this study, at least the dating questions I would typically ask someone on a date.

The next step I turned to researching different types of informational gathering, get to know you, personal, security, and financial questions. I complied everyone of these types of questions into a huge list. I then proceeded to eliminate the duplicate questions, silly questions, and off topic questions. I then took the questions these shorter list and mixed all the questions up out of topic to make the questions more random. I ended up with a list of 77 questions; Which is listed below:

What is your name?

What is your surname / last name?

What is your middle name?

Do you have a nickname?

Work & Occupation

What do you do?

Where do you work?

Do you like your job?

Why do you like your job?

Are you married / single?

Do you have a boyfriend / girlfriend?

What is your partner's name?

Are you a virgin?

Who was the first person you kissed?

Who is your best friend?

Have you cheated on someone before?

Do you have any children?

What are their names?

How many brothers and sister do you have?

How old are you?

When is your birthday?

Where were you born?

Where are you from?

What is your address?

What is your phone number?

What is your cell phone number?

What languages do you speak?

Who do you live with?

Do you smoke?

Do you live with your parents?

Do you live alone?

Who do you live with?

Do you live in a house or an apartment?

What is your e-mail address?

What is your social security number?

What was your childhood phone number?

What do you do in your free time?

What are your hobbies?

What type of music do you like?

Do you have a favorite singer or group?

What types of movies do you like?

Do you like to read?

What do you like to read?

Do you have any bad habits?

Do you snore?

Do you smoke?

What is your favorite food?

What medication are you on?

What is your mother’s maiden name?

Is there any food that you do not like?

What is your favorite color?

Why do you want to learn English?

How is your credit?

What languages do you speak?

Do you have any pets?

What pets do you have?

What were your pet names?

Which sports do you like?

Do you have a favorite team?

What is something you do well?

What is something you do not do well?

Are you romantic?

Have you ever been bankrupt?

What is your favorite numbers that you use the most?

Do you have any tattoos?

What is your passwords?

Describe yourself using only two words.

What makes you happy?

Are you a good cook/singer/driver?

What is your gross salary?

What is your favorite author?

What is your favorite book character?

What was your first car?

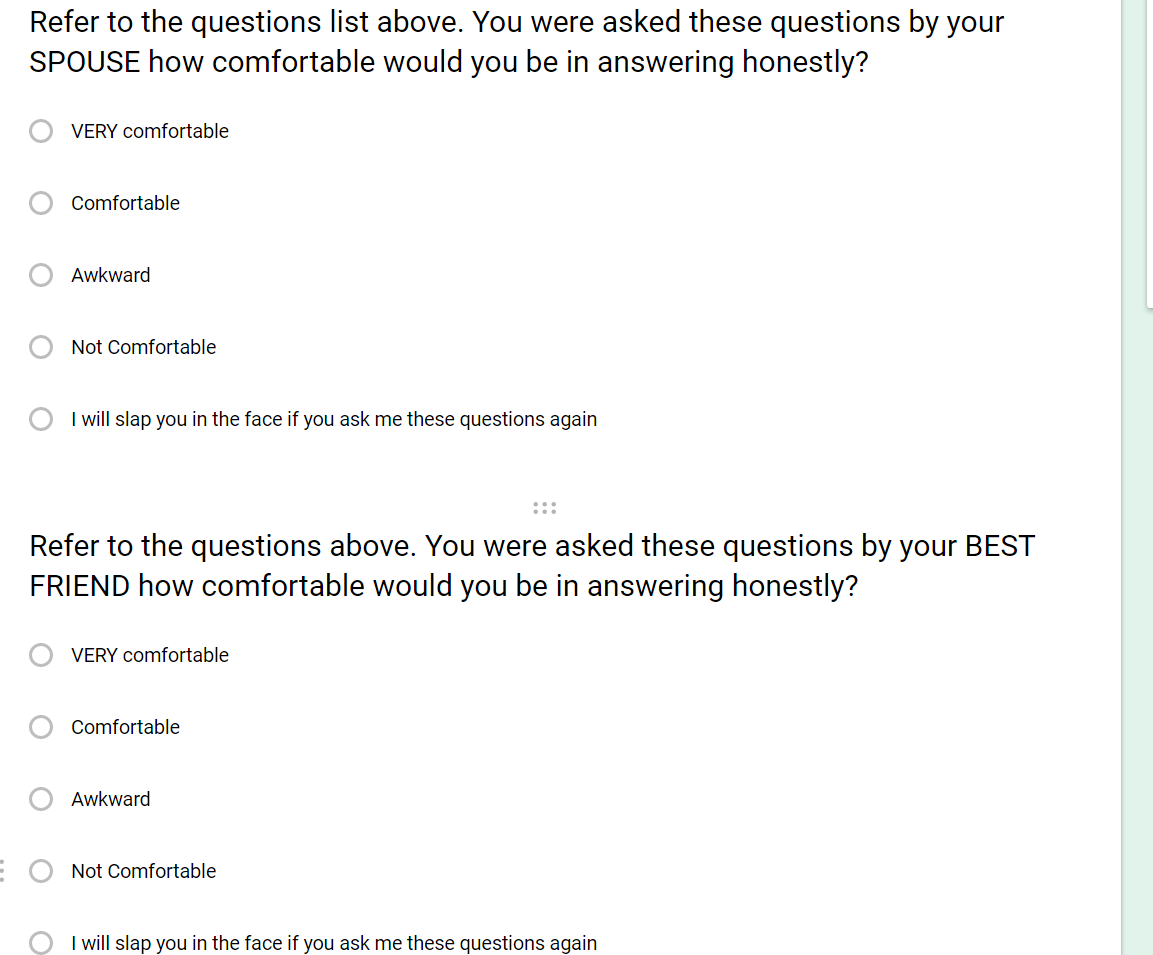
What was your first job?

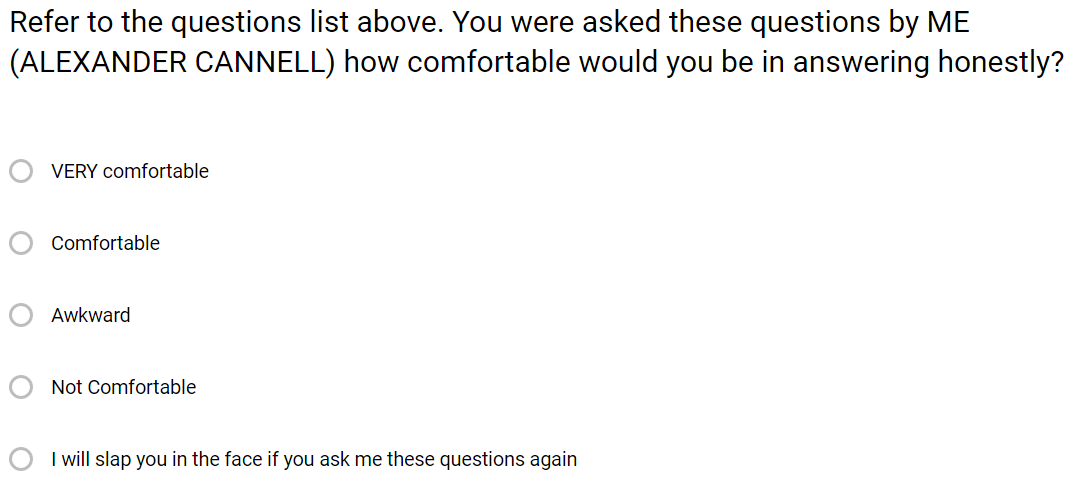
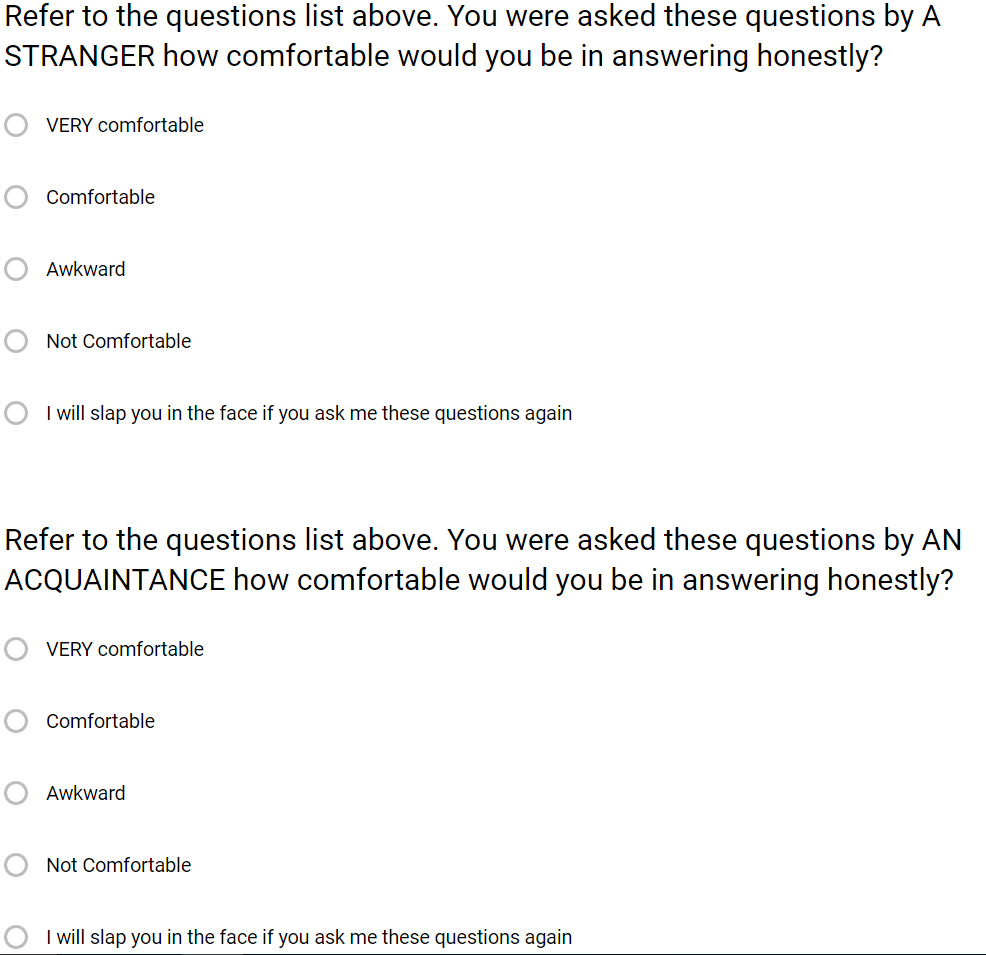
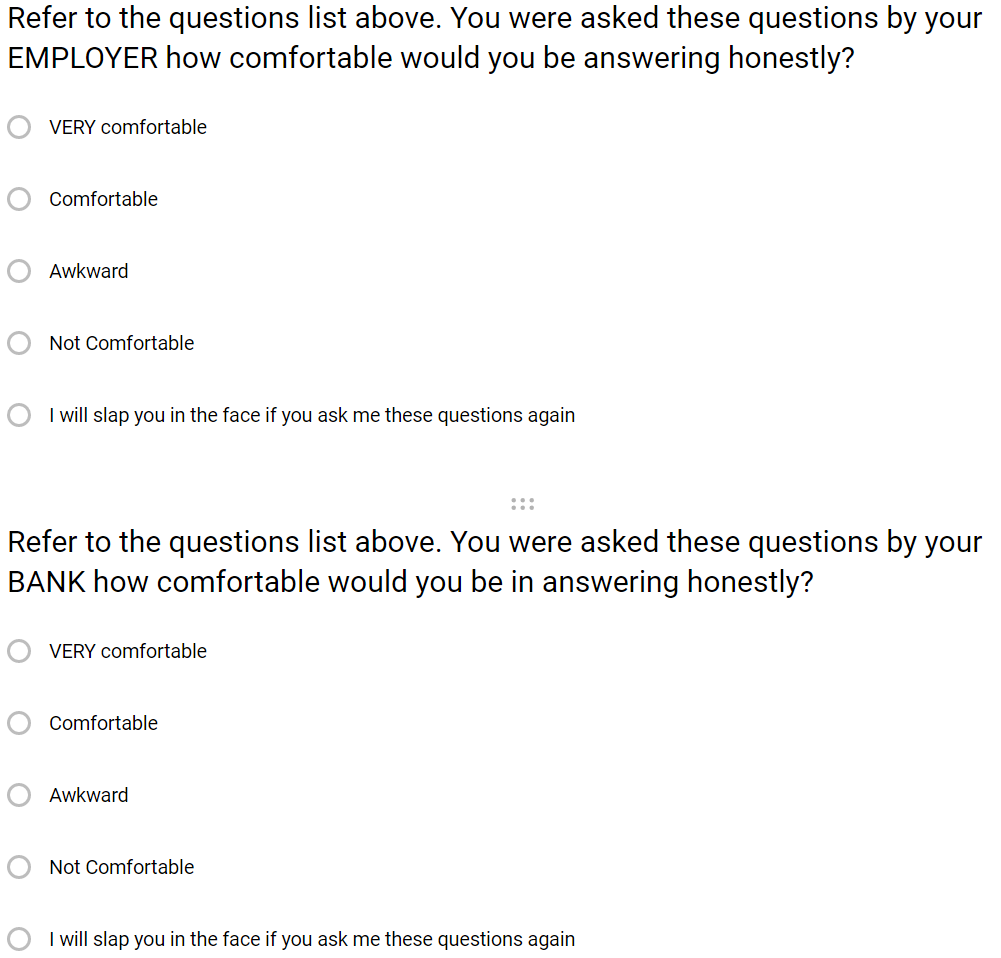
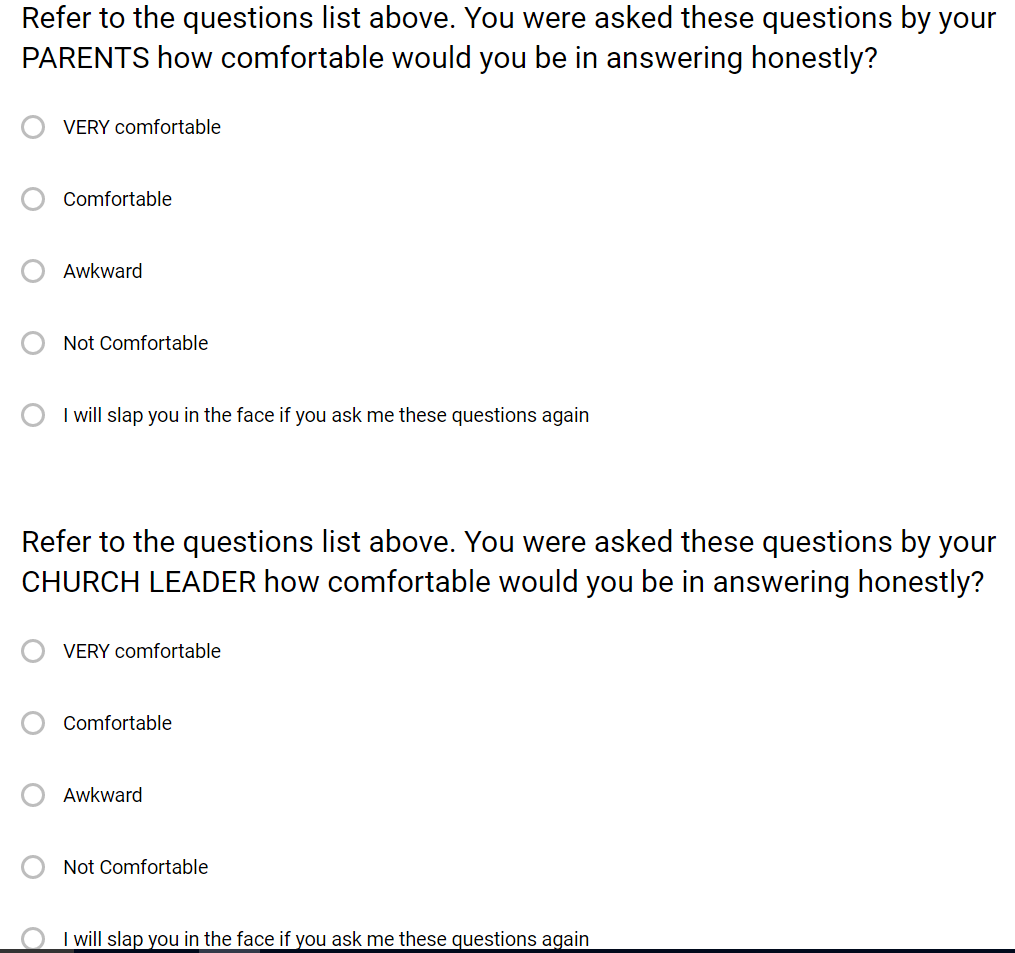
What was the name of \_\_\_\_\_ Grade teacher?

Your parents address?

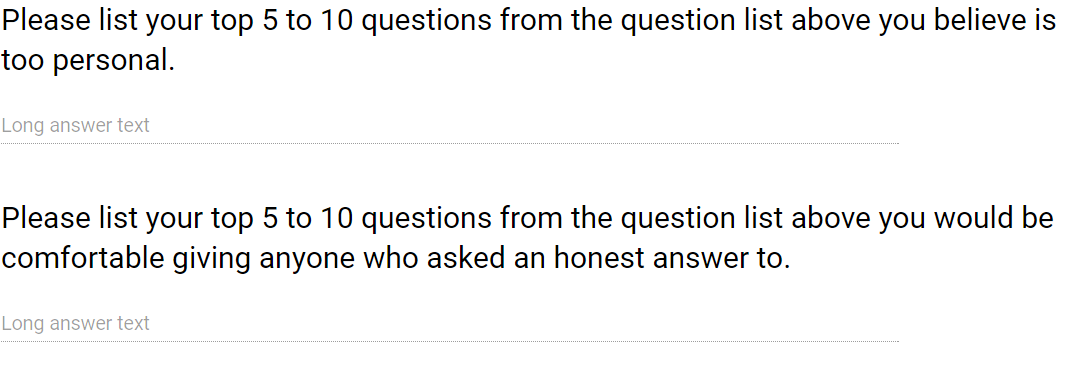
The list of 77 questions were used as a base of questions for the whole survey. Where everyone would refer back to the base questions to answer the questions proposed later. Each question had a level of uncomfortability ranging from Comfortable to Very Uncomfortable.

***How the relationship of questioner and the person answering the questions affects the answers?*** I found the best way to answer this question was to make a series of how “Comfortable” questions. With these comfortability questions I switched through various people that might be in different people's lives ranging from your spouse to a complete stranger. How the participate answered was by how comfortable they were to give an answer to these questions to that certain person. The selection of survey questions are below.

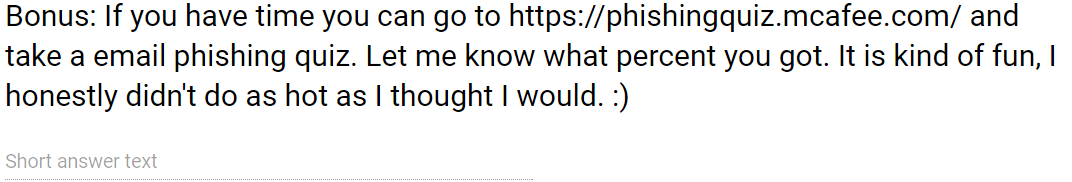




***What questions are better at gleaming information than others? what answers are people comfortable giving?*** The best way I found to answer these questions was to just ask the participate what questions they felt comfortable answering and what questions they felt uncomfortable answering. How I would determine which questions are better at gleaming information is from the questions they didn't list meaning that they didn't think about how awkward those questions were and the ones they actually didn't mind answering. Below are the two survey questions I ask participants.



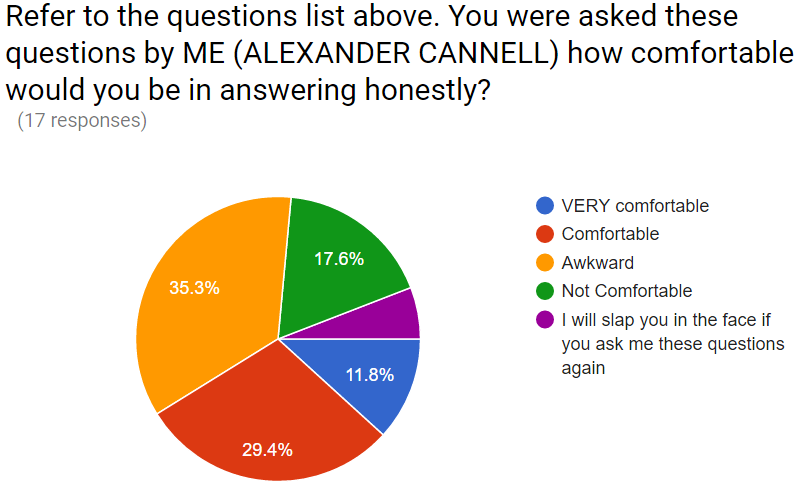
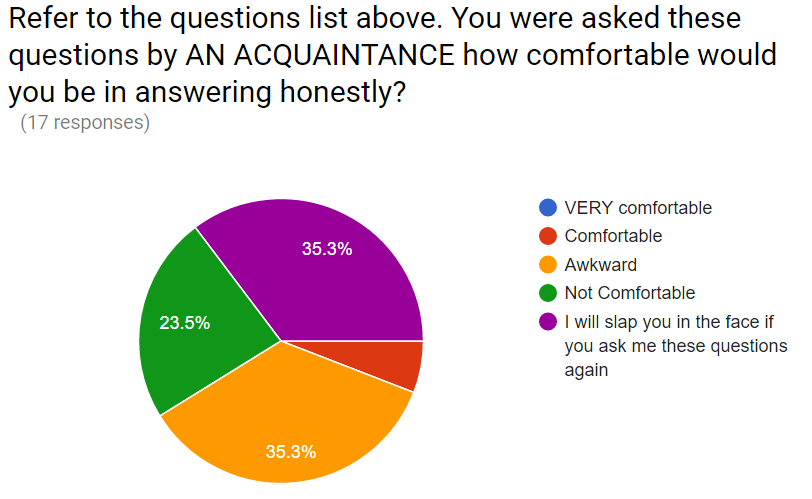
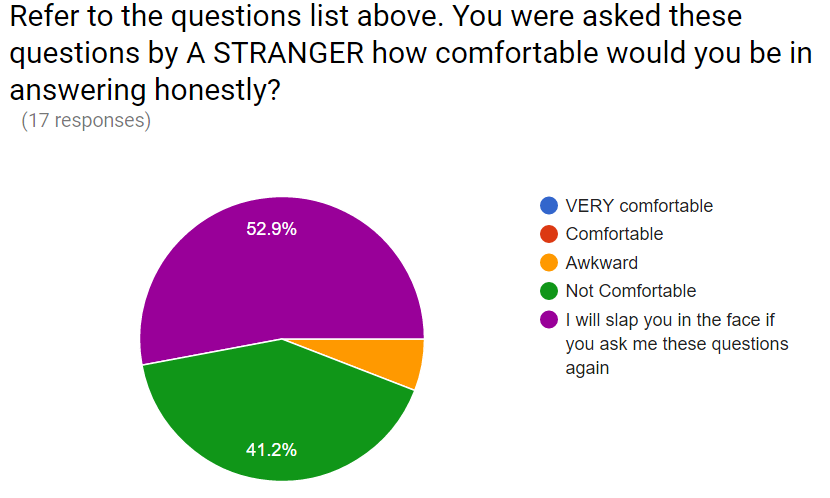
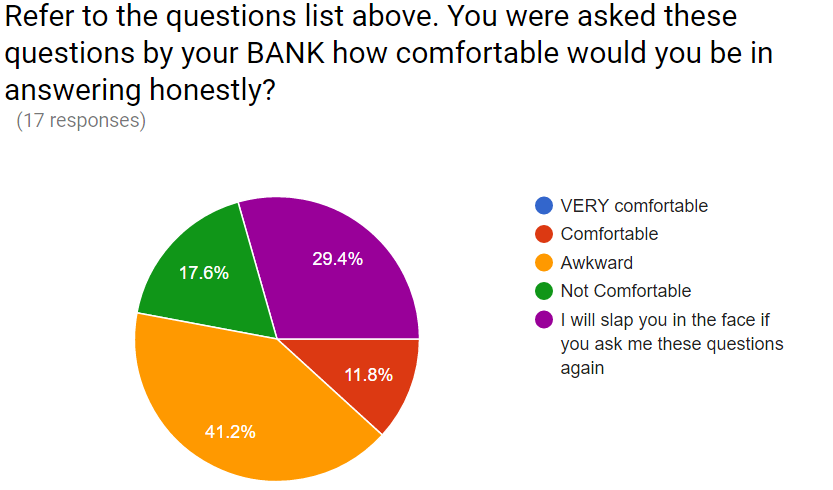
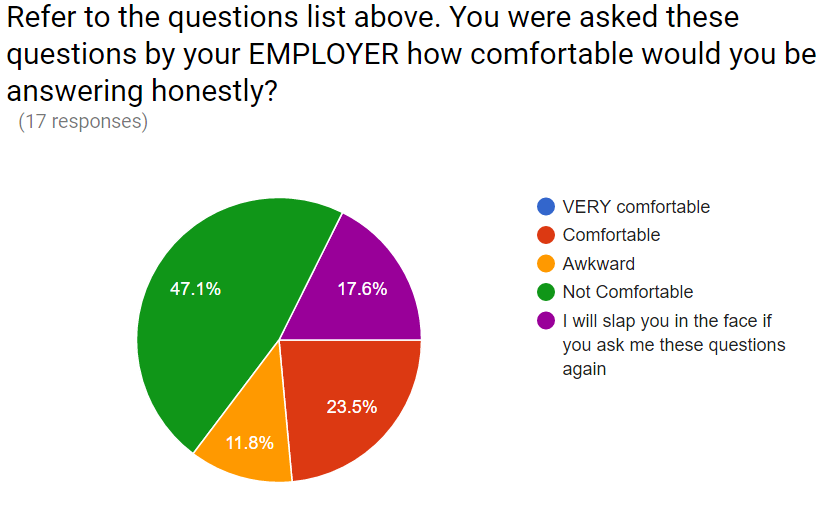
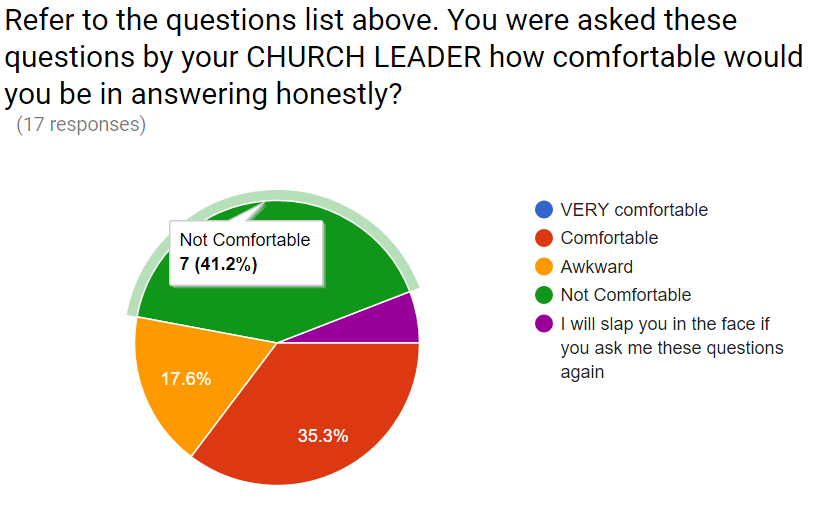
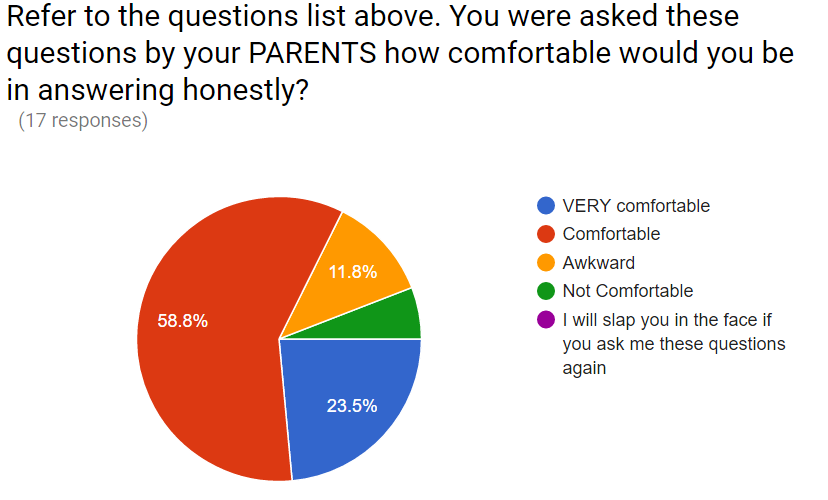
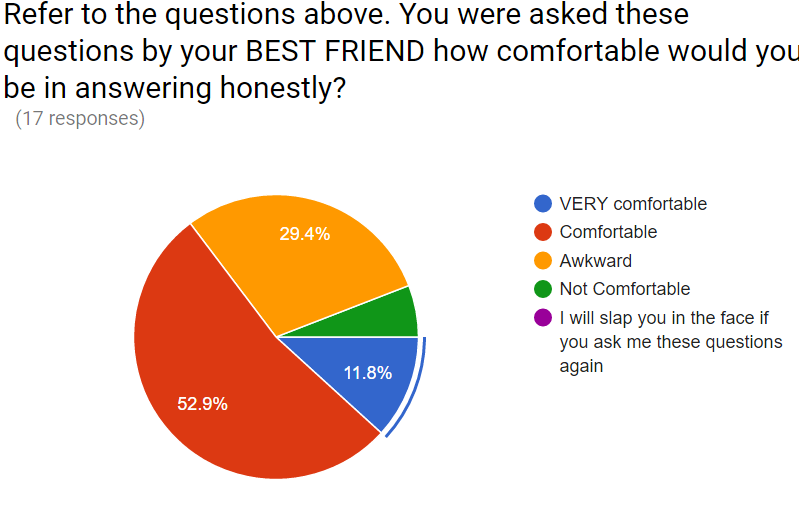
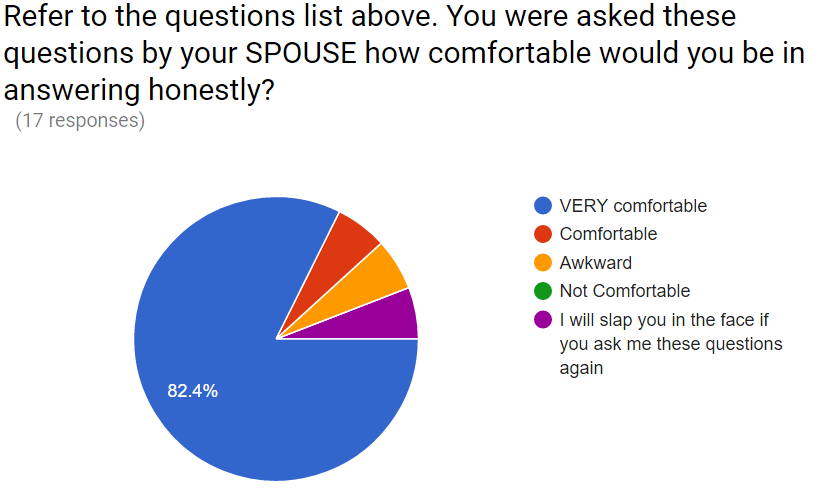
***Optional curiosity question.*** I found a Phishing quiz which was put together by the security company Mcafee. This phishing quiz tested the ability of people to recognize if an email is phishing email or not. I actually didn't do as well as I thought I would. The point being I thought it would be interesting to see if the participants could recognize a phishing mail or not. Then at the end of the quiz after it tells you how well you did, it teaches you how to better recognize malicious emails in the future.



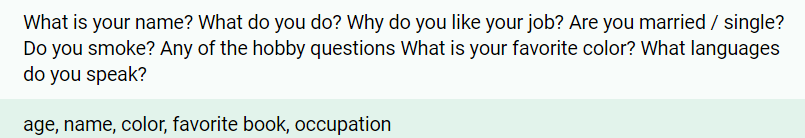
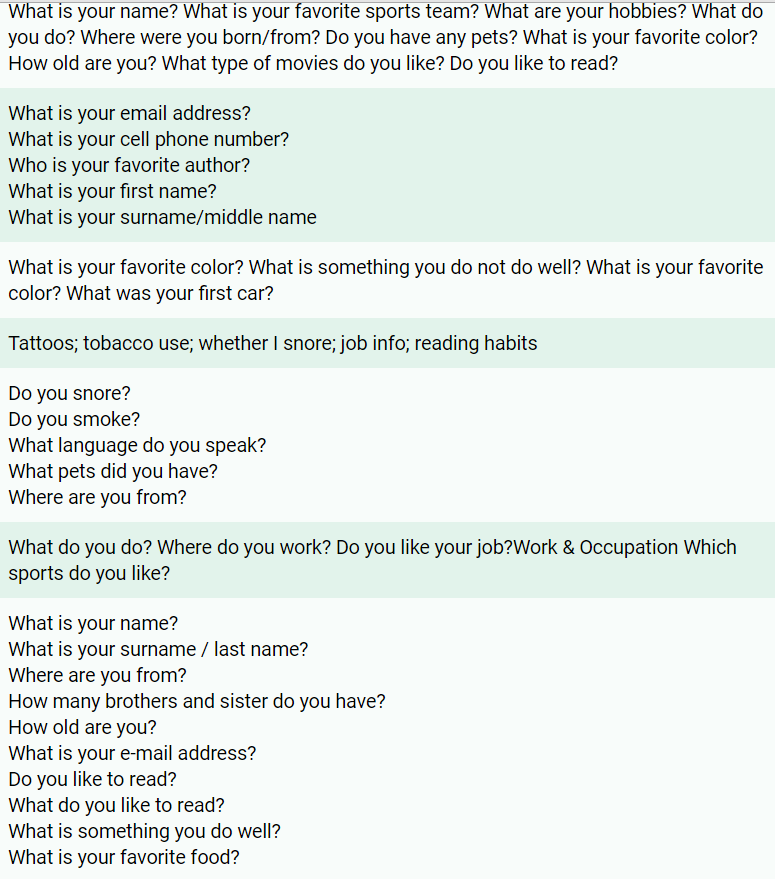
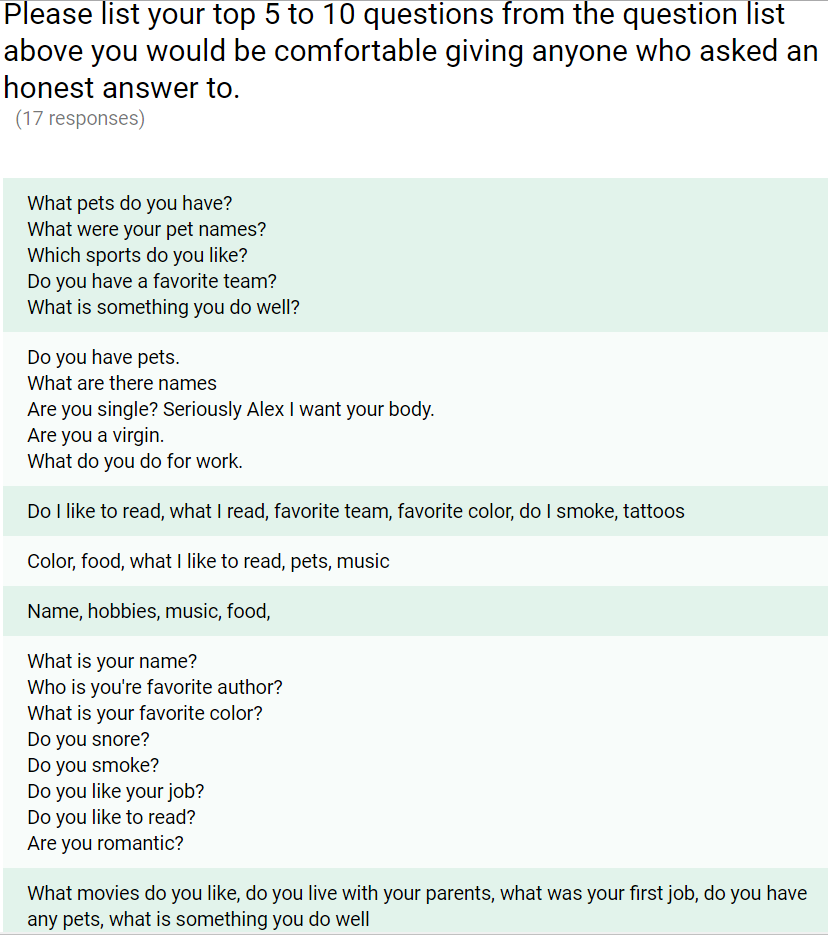
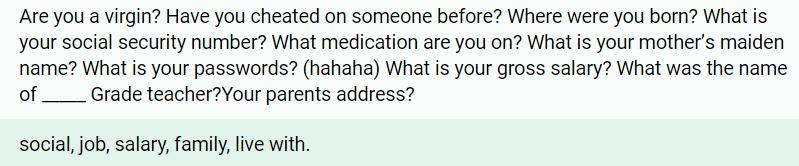
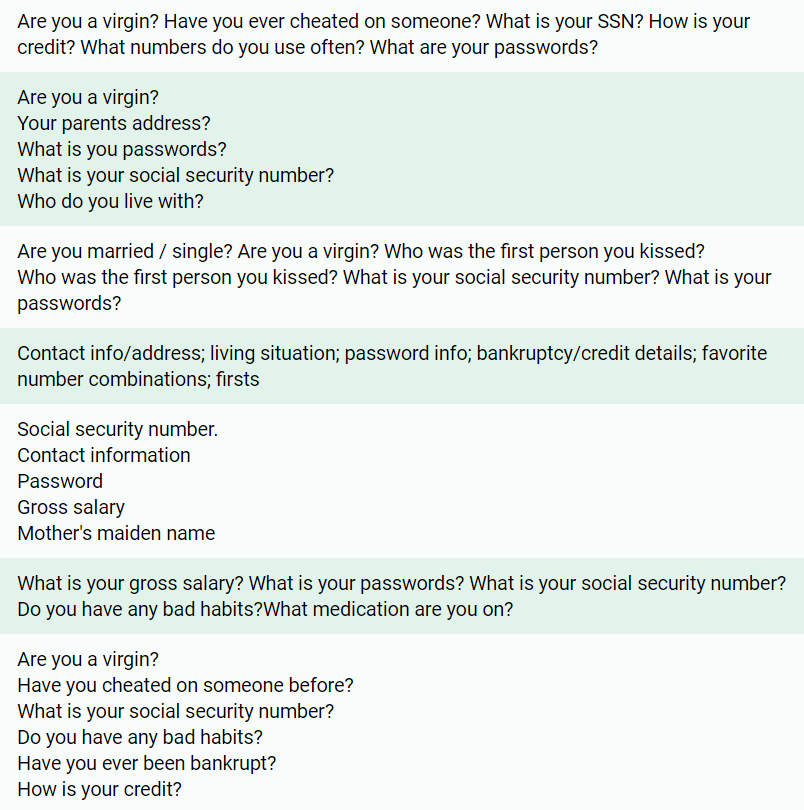
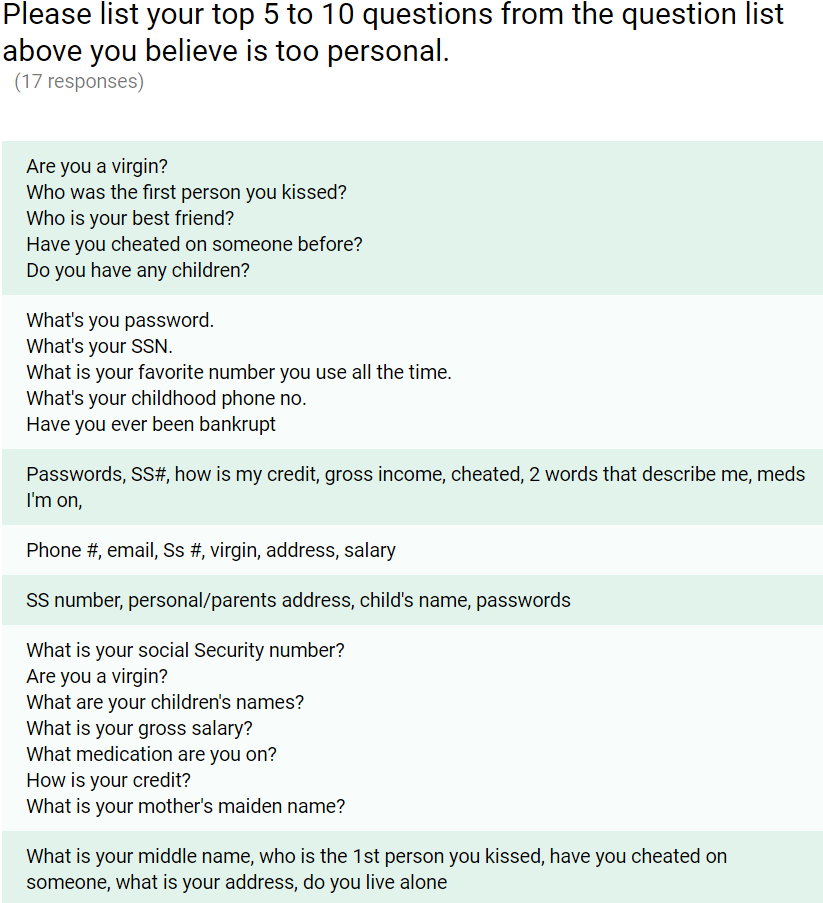
# Results

## Outcome from the first section

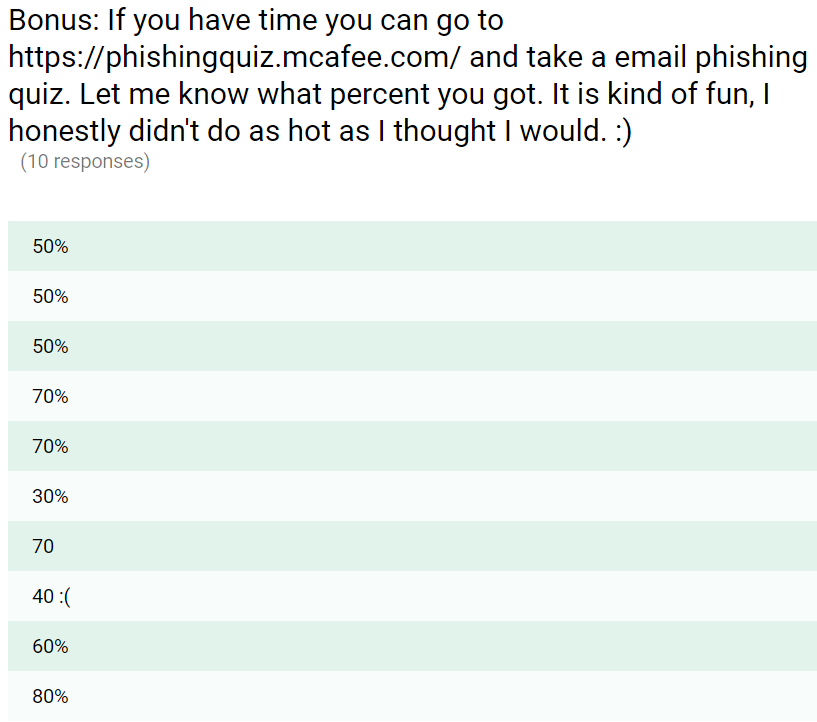
The results of the “How comfortable would you be” section was really interesting. As we go down the list you will notice that people become less comfortable. Participants are usually really comfortable about answering question honestly, which isn't a big surprise and should be this way. For the Best Friend participants, the results were half and half but mostly comfortable talking and answering questions from them. The parents question also got a majority of participants stating that they were comfortable talking with their parents. Now I realize that the next one might be skewed because I mostly took polls from people who are living in Utah or from Utah; as we know the majority of the population of Utah is religious. But I asked about Church leaders all the same, and the majority of the participants saying that they would find it awkward and not comfortable to be asked these questions, but that being said I found 35% of people would feel comfortable talking to their church leaders about these questions. The employer one was a gamble, I figured people wouldn't be comfortable answering some of these questions, as a employer I would feel awkward asking them; That said there was still 24% of participants comfortable with an employer asking these questions. No one felt comfortable about answering these questions with a Bank, Stranger, or acquaintance. For fun I asked about how participants would be answering questions from me, and I was actually really surprised at the results; 42% said that they would feel comfortable answering these questions honestly. Yes almost 50% would feel comfortable answering questions from me. These results made me very happy. Below are the percentages for each question.



## Outcome from the second section



## Outcome from the third optional section



# Conclusion

Social Engineering as defined from techtarget.com, “Social Engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.” (Techtarget, 2016) Social Engineering is a very dangerous tool that hackers use. This is so important to know how to recognize malicious activity not only in our company but in the interactions with people around us.

What I discovered from this research project is that Relationships to the questioner effects the answer given. The more you know someone the more forthcoming with their personal life someone will be.

I also discovered that participants were more uncomfortable with the very personal questions like gross income and are you a virgin? Also, the study shows that obvious probing questions like Social Security Number and Password, participants were uncomfortable. But when it came to security questions that banks or credit unions might ask someone applying for a credit card or a loan people were comfortable. Questions like favorite foods, books, or movies, the study showed that participants were very open about giving these answers. What I found interesting too was that people were comfortable giving out their cell number and email address. The study showed that people also didn't even list things like, “How old are you?:” “When is your birthday?” and “Where were you born?” Which also has sensitive information in it.

The phishing quiz results show us that 57% of people can pick out phishing in their emails. This is actually really good, but we could always do better. According to a study performed by Technical University of Vienna the best ways to protect ourselves against phishing and spear phishing emails is to protect use antivirus software with email protection, never click on links in emails from addresses you don't recognize, always type the URL in yourself, and never give out personal information. (UCSB, 2016)

Social Engineering continues to grow resulting in many vulnerabilities. In a study performed by Berkeley, it addressed the ways to prevent Social Engineering. Never provide confidential information to unknown or suspicious sources, avoid clicking immediately on links especially check where the URL is going, never use USB devices you don't know where they came from in order to reduce the risk of baiting, always….always use two factor authentication (requires two steps to log into a website) which is just an extra layer of security, and be educated on different attack. (Berkeley, 2006) Overall I was very impressed with the findings, people are a lot more cautious than I originally thought.

# 

# 

# References

What is social engineering? - Definition from WhatIs.com. (n.d.). Retrieved April 19, 2016, from http://searchsecurity.techtarget.com/definition/social-engineering

(n.d.). Retrieved April 19, 2016, from http://www.imdb.com/character/ch0000087/quotes

R. (n.d.). Why Phishing Works. Retrieved April 18, 2016, from http://www.eecs.berkeley.edu/~tygar/papers/Phishing/why\_phishing\_works.pdf

E. (n.d.). Protecting Users Against Phishing Attacks with AntiPhish. Retrieved April 18, 2016, from http://cs.ucsb.edu/~chris/research/doc/compsac05\_antiphish.pdf

(n.d.). Retrieved April 18, 2016, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Phishing: How many take the bait? (n.d.). Retrieved April 19, 2016, from http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx

Kaspersky Personal & Family Security Software. (n.d.). Retrieved April 19, 2016, from https://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.VxLLp\_krLmE

Spear-phishing statistics from 2014-2015 - InfoSec Resources. (2015). Retrieved April 19, 2016, from http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/