End-User: Security or Convenience

By

Anthony Joshua Spisak
Criminal Justice
Ferris State University. 2017

Advisor:
Dr. Greg Gogolin
Full Professor
Accounting, Finance, and Information Systems Department

Fall, 2017
Ferris State University
Big Rapids MI

ACKNOWLEDGEMENTS

I would like to thank my beautiful fiancé for all her support and encouragement throughout my education. I would also like to thank my committee members Professor Cooper, Professor Emrick, and Dr. Gogolin for their guidance and support.

Table of Contents

List of Tables

Page

List of Figures

Page

Abstract

The research will show the likelihood of end-users keeping employer or personal data safe. This research is shown in a flash drive drop experiment where 20 USB flash drives are dropped in high trafficked public areas to see if end-users would, first, pick up the flash drives, and plug them into their computers and open the files inside. The results of the experiment prove end-users are susceptible to a social engineering tactic as simple as picking up corrupted flash drives. With 45% of the flash drives dropped in the experiment plugged into a computer, end-users are more than likely to leave data at risk.

Chapter 1

In the 21st century, technology is used in almost all aspects of our lives. Technology is relied on daily and has begun to impact simple human tasks. For example, technology is used to track our movements, record our sleep patterns, alert us when our laundry is done, or even tell us when our fridge is out of milk. We use devices such as Amazon's Alexa to see what the weather conditions are, or to play music. On top of all that, we use technology to store data. The data stored can range from tracking how many steps a person walks a day all the way to a criminal database holding all information on past and present criminals. The convenience of technology comes with the inconvenience of security. According to Harris (2013), end-users have been known to accidentally forfeit information over to a third party. This accidental disclosure of information can be done in several ways, such as exploiting the end-user using social engineering techniques.

Introduction to the problem

According to Zadelhoff (2016), the biggest threat to a business or organization is the employees. In today's world, businesses and organizations thrive on using technology. Technology in a business setting is used for all aspects of business: databases for filing information, communication, design, surveillance, transactions, and reporting. With the use of technology comes security. It is virtually impossible to protect all aspects of technology used. Unfortunately, the biggest security vulnerability is employees being unaware victims to social engineering attacks (Harris, 2013).

The problem at hand is making sure end-users, or employees, do not leave their employers vulnerable to an attack. According to Grimes (2017), social engineering is on the rise

with attackers exploiting employees to steal information from employers. These social engineered exploits come in various forms. Phishing scams sent as an email are a popular exploit used to spread virus onto the victim's computer. Another exploit that is gaining popularity is having victims picking up found hardware, such as USB flash drives. The USB flash drives can be riddled with malicious code just waiting for an end-user to plug the device into a device. Once the victim connects the hardware to a computer the malicious code begins to infect the victim's computer without their knowledge.

Background of the Study

Unfortunately, attackers today have many methods when it comes to exploiting a system. According to Harris (2013), businesses have to be security conscious of networks, software, and environmental aspects of the company. In addition to these factors, and all the components attached, businesses need to also worry about their employees, or end-users.

According to "United States: Find a Flash Drive" (2015), 1 out of 5 Americans is likely to pick up a found flash drive and insert the drive into their computer. This type of behavior can leave the person, or company, at risk to an attack without any knowledge that the flash drive was malicious. What makes a USB flash drive the perfect Trojan horse is the compact size of the device along with the amount of storage the device can hold. In addition to this, USB flash drives are cheap and everyone owns at least one. According to Berkman (2012), over 3 billion USB devices are sold annually. Flash drives make up a large number of these sales.

USB flash drives are given away at events for free with company logos on them. End-users use the flash drives for storing and transporting information. This makes them the perfect target for exploiting a system. The study will deduce whether or not end-users are likely to click

on files found on an unknown USB flash drive. Similar studies have found end-users are likely to pick up the USB flash drive, but also plug the device into their computers.

The Purpose of the Study

The purpose of the study is to see how secure end-users are with personal and corporate information. Cyber attacks can come in all shapes and sizes, but this study focuses on the likelihood of an end-user plugging a USB flash drive into a computer and clicking on the files. If an end-user picks up the unknown USB flash drive, plugs the drive into his or her computer, and opens the files inside, the end-user will demonstrate whether the end-user can keep data secure or not.

Rationale

The rationale of the study is to determine if end-users are more or less susceptible to social engineering techniques and how secure they are with personal and corporate information. In this study, I will deploy unknown USB flash drives. The goal of the study is to help educate end-users with security awareness. This will be done by using the data collected from the USB flash drive drop experiment, along with a survey, to see if end-users fall for social engineering tactics. The end game is to help end-users keep information secure by being aware of tactics they may or may not be aware of.

Problem Statement

How secure are end-users with data? This question will be measured in two ways. The first way is by doing a USB flash drive drop experiment to see the likelihood of end-users plugging an "unknown flash drive" into their computer and opening the files. The second way of measurement will be done through a basic end-user security survey.

Significance of the Study

The significance of the study is to help educate end-users from being exploited by attackers. The outcome of the experiment and survey will measure how far end-users are willing to dismantle their security?. The study can help professionals educate staff members on new tactics that can leave employees exposed.

Definitions of Terms

USB- Universal Series Bus

Trojan Horse- Hiding a virus in something you would not expect a virus to be in.

HTML- Hypertext Markup Language

Malware- Software intended to harm a computer.

Virus- malware that modifies computer code.

Ransomware- Holding information hostage until a sum of money is paid to access the decipher key.

Key Logger- Program that records all keystrokes on a computer.

GB/MB- Gigabyte/megabyte.

CIA Triad- confidentiality, integrity, and availability. Standards for cyber security.

Social Engineering- Using and manipulating people to gain private information.

Worm- type of malware that duplicates and infects all available computers

Assumptions and Limitations

There are several assumptions for the USB flash drive drop experiment. The first assumption is that all 20 USB flash drives work accordingly. All USB flash drives were tested before being placed in the field. Second assumption is that subjects who picked up the unknown USB flash drives had a computer with Internet access. The final assumption and ultimate assumption, is that someone would pick up the USB flash drive at the very least.

There are several limitations for the USB flash drive drop experiment. The first being the autorun script only working on the windows operating system with Google chrome or Mozilla Firefox downloaded on the computer. The second limitation in the USB flash drive experiment is the weather. Since the flash drives were left outside the weather could play a role in why the devices were not used. In addition to the weather, vehicles are also seen as a limitation. Because the USB flash drives were left in crowded parking lots, there is the possibility vehicles could have damaged or destroyed the devices. The last limitation to the USB flash drive experiment would be that no individuals picked up the USB flash drive.

The assumption that all individuals surveyed can read and write in English at or above a 5th grade reading level with the ability to comprehend what he or she is being asked.

The limitation for the survey portion is narrowed down to 31 people. The individuals surveyed are anonymous.

Chapter 2

With technology being so prevalent in our lives, information security professionals have a harder time securing information. With technology being such a big part of our lives, employees are bringing their own devices to work such as computers, tablets, and phones. These

devices all have the capability of connecting to the company network, which can cause harm to a business or organization. All of these devices connected to the network leave "more risk and a higher probability of an attacker causing mayhem from within an organization than from outside it" (Harris, 2013, p. 268).

CIA Triad

An information security professional has three major goals: confidentiality, integrity, and availability (CIA triad). These three goals are critical in protecting assets (Harris, 2013). The more prevalent technology becomes in our daily lives, and the more we depend on technology for daily functions, the more security conscious users need to become. With attackers finding more creative ways to target victims, information security professionals need to be on high alert. All of the countermeasures in the world will not help if employees are not educated on cyber security measures.

Social Engineering

Social engineering has always been a way for attackers to get information out of victims. According to Ciampa (2013) social engineering can stem from shoulder surfing, looking over shoulders for passwords, all the way to creating and implementing complex plans to steal employee credentials. Either way attackers prey on victims to get information they need.

A popular social engineering tactic is phishing. According to Hong (2012), phishing is when an attacker lures an individual into giving up information. This can be done by spoofing an email address to confuse the victim of who they are talking to or by embedding malware into an email that infects the victim's computer. Regardless, the victim gives the attacker the information he or she needs. This type of attack is a popular tactic for targeting a large-scale

population. According to Harris (2013), phishing attacks spiked in the early 2000's but have been around since the early 90's. In the past, users would fall victim to these attacks by thinking the links and emails they were receiving were from creditable sources and not from criminals.

Another social engineering tactic is shoulder surfing. Shoulder surfing is looking over an unsuspected person's shoulder to gain login information including usernames and passwords (Ciampa, 2013). This type of social engineering is a basic attack, but can be catastrophic to the victim and their information.

Social engineering tactics work because the victim falls prey to trust. According to Krombholz, Hobel, Huber, and Weippl (2015), social engineering attacks work best when the attacker, through trust, has compromised the victim. The victim does what the attacker wants because he or she trusts the attacker and does not think what they are doing is harmful in any way. In this case, no matter what social engineering tactics are used, the attacker has infiltrated the targeted company. This then leaves the company vulnerable to criminal exploitation.

Logon Spoofing

Logon spoofing tricks the victim into thinking that the logon screen they see is legitimate. Once the victim records his or her credentials into the spoofed logon, the information is recorded and given to the attacker. Then, the attacker is able to gain access into the system (Harris, 2013). This form of attack leaves the victim unsuspected and clueless to the attack until after the attacker has done his or her business.

This type of attack also leaves the end-user, or victim, subject to divulging information without their knowledge. The end-user believes he or she just typed their username in password in wrong and that no harm was done. However, they just gave the attacker the same privileges

and authority they have access to.

Dictionary Attack/ Brute Force Attack

Dictionary attacks use a list of words that are compared with a systems password file. Matched values indicate a password. To stop dictionary attacks, passwords need to be hashed, not sent in clear text, encrypted, complex, and changed often (Harris, 2013). These simple recommendations can help keep passwords secured from attackers leaving the victims more secure.

Brute force attacks are long drawn out attacks. Brute forcing a password consists of "trying every possible combination until the correct one is identified" (Harris, 2013, p. 270). This type of attack allows the attacker to gain access to passwords. Brute force and dictionary attacks are used together to help speed the process along. Both attacks are used when the attacker has access to the victim's credentials.

USB Flash Drives

USB flash drives are lightweight portable devices that can hold large amounts of data. USB flash drives are commonly used because they are easy to use and can transfer data back in forth between computers. USB flash drives are an easy way to copy and transfer information According to Yang (2004), USB flash drives are housing units that connect flash memory to a circuit board that can connect to commonly found USB's in computers. USB flash drives have the capability of holding small or large amounts of data depending on how large the device is. For example, USB flash drives can come in small memory sizes such as 128 MB or can be as large as 64 GB. Depending on the data size of files you want to copy or store, will depend on the size USB flash drive needed to store all the information.

This easy to use device makes it a perfect carrier of a new social engineering attack. USB flash drives can be loaded with any type of malicious code to attack victims. Placing malicious software on the device and having an unsuspected victim plug the device into a computer can cause catastrophic damage without the victim knowing. In this instance, the end-user may or may not know the damage that can be caused by plugging in an unknown USB flash drive. The end-user may believe the USB flash drive is harmless rather than dangerous. In any case, an attacker with malicious intent can compromise an end-user and the authority they have on a system by getting the end-user to plug a malicious USB device into their computer.

Additional Flash Drive Experiments

A similar experiment was conducted on a larger scale. According to Tischer et al. (2016), 297 USB flash drives were dropped on the University of Illinois campus. The USB flash drives were loaded with an HTML image that would track if the USB flash drives had been opened and would prompt users to an optional survey. This allowed for the team to see if the USB flash drive was opened, how long it took for the USB flash drive to be opened, and to gather feedback on why the USB flash drive was opened. The experiment found the average flash drive was opened at a median time of just under 7 hours.

Tischer et al. (2016), explains the optional survey found 68% of end-users plugged the USB flash drive into a computer to find its owner. The purpose of plugging the USB flash drive into the computer was not for personal gain but to return the property. Tischer et al. (2016), also explains USB flash drives were dropped with and without a set of keys on them. The experiment found USB flash drives with keys were more likely to be returned to the researchers than USB flash drives without keys. In any case, the end-users still plugged the USB flash drives into a

computer and executed the HTML files on them.

Tischer et al (2016) explains how the experiment was a success by explaining how a high number of flash drives were plugged into computers. The researchers concluded that USB flash drives would be a successful means of deploying a social engineering attack on an unsuspected victim.

USB Flash Drive Drop

An effective way for attackers to exploit the human element, or end-user, in a company is through USB flash drives. Two examples of this can be found through the Stuxnet worm and an experiment of flash drives dropped in a company parking lot. Both examples exploit the human element of end-users.

The first example of using a USB flash drive in a successful malicious manner can date back to 2010 when the Stuxnet worm infected an Iran nuclear plant. According to Eitel (2011), the Stuxnet worm was launched on Iran computers through a USB flash drive. The worm made a piece of equipment malfunction in the nuclear plant ultimately destroying the plant.

According to Johansson (2008), a test was done to see the effectiveness of installing a Trojan horse on a USB flash drive and dropping these devices throughout a company's parking lot. The test was done with the owner's permission to see how vulnerable end-users were to the company. The outcome of the experiment showed that the employees, or end-users, picked up the USB flash drives and plugged them into their work computers. This allowed the Trojan horse to be uploaded to the system leaving a backdoor, or vulnerability, into the system.

This experiment was done on a small scale focusing on a single company. The outcome of the experiment yielded a high percentage of employees picking up the dropped flash drives

and plugging them into their computers. This experiment was done almost a decade ago; however, the outcome of the experiment should yield similar results today.

End-user Survey

According to Moyle and Kelley (2012), in their recent survey, found that hacktivists and cybercriminals are among the most sever threats towards Information Technology (IT) professionals. The survey included over 100 IT professionals and found IT professionals are least likely to stop leaks coming from social media; however, the IT professionals feel they are making good progress in combating the situation.

Moyle and Kelley (2012) found that out of the 24 agencies surveyed only 7 of them complied with an above average rating in risk management and access management. With less than half the agencies not being able to score above average markings draws the questions of how secure employees are with the information they are being entrusted with. This brings us back to how secure employees are with data.

The results from Moyle and Kelley survey opens the door into training employees and the younger generation. If the next generation is made aware of cyber threats from an early age, they will be more inclined to combat the situation. Surveying a younger population may yield better results than what Moyle and Kelley found with IT professionals.

Summary

The human element has always been a popular target for attackers. Whether the attacker is sending out phishing emails, spoofing logons, or coming up with complex plans to steal data like the Stuxnet worm, end-users are always a good target. While information security professionals work to secure the technology side of things, attackers look to exploit other areas.

This is where end-users become victims to the attackers plans.

Research Question

With social engineering on the rise, attackers look to exploit end-users. This can be done multiple ways, however for the sake of this experiment I focus mainly on the security consciousness of the end-user. The basic question being asked is, 'how likely are end-users to open files on an unknown USB flash drive?' The experiment focuses on the human element of the end-users and whether or not they would be susceptible to leaving their employers and themselves at risk. Opening the files would demonstrate the end-users are susceptible to being exploited for information and data.

In addition to the previous questions, the experiment will show how secure end-users are with data in a survey portion. The survey will focus on how security conscious end-users are with the technology they have at their disposal. The survey will give insight on how educated end-users are and whether they are sacrificing security for convenience.

Chapter 3

The purpose of the experiment is to conclude the likelihood of end-users leaving employer or personal data at risk. Determining how vulnerable end-users are towards social engineering tactics, such as picking up and plugging in unknown USB flash drives into their devices, can help combat the threat towards data being corrupted or stolen. Eitel (2011) explains the Stuxnet worm was introduced to the Iran Nuclear facility through a USB flash drive. If end-users are susceptible to social engineering tactics, like picking up unknown USB flash drives, then the thought of a criminal dropping malware infested USB flash drives in a parking lot as a means to commit a crime are likely to occur.

The experiment demonstrates, in a non-intrusive, ethical, and moral way, the likelihood of end-users plugging unknown USB flash drives into their computers. The USB flash drives are to simulate a criminal's intention of using the USB flash drive for unethical reasons. This can come in the form of a malware attack, ransomware, virus, or even to download a key logger without the user's knowledge. The purpose of these attacks are to steal, corrupt, or hold information hostage for criminal gains in the form of money.

The experiment uses an autorun command file that, once clicked on, opens up a generic website associated with the USB flash drive. Once the file has been opened the website counts the number of people who have viewed the website tracking whether the flash drive was plugged into a computer or not. The autorun command cannot harm the computer in anyway and can simply be deleted making the flash drive brand new again.

2.0 Swivel Flash Drive

The start of the flash drive experiment begins with purchasing 20 USB Flash Drives. The flash drives selected for the experiment are FEBNISCTE 2.0 USB swivel 128MB black flash drives, as shown in Figure 1: USB Flash Drives. All USB flash drives used for this experiment were of the same brand, color, and storage capacity. The flash drives come in packs of 10. Two

Figure 1: USB Flash Drives

packs of the flash drives were ordered for a total of 20 USB 2.0 Flash Drives. Flash drives are then removed from the package and numbered, 1-20 with sticky notes.

Email Setup

After each of the 20 flash drives are numbered, an email address needed to be created. For the purposes of this experiment a Gmail account was created, Flash01Drive@gmail.com. The Gmail account is created to help keep track of each flash drive through its own website. The Gmail is needed to create 20 different accounts with WordPress, which creates a unique website. The websites are used to document if the flash drives were opened or not.

WordPress Setup

Using Flash01Drive@gmail.com as a base email address, 20 other emails are than used to create a free website on WordPress. Using the plus sign and adding the next corresponding number to the base email address does this. For example, flash drive 2 has the corresponding email address, Flash01Drive+1@gmail.com. This allows for the creation of a new website with a different username and password on WordPress; however, it still allows for all the verification emails to go through the base email, Flash01Drive@gmail.com. In return, 20 different websites can be created and monitored for each specific flash drive. As shown in Table 1: WordPress and Gmail Account.

Table 1:

WordPress and Gmail Account

Flash Drive Number	Website	Email (@gmail.com)
1	Flash01Drive.wordpress.com	Flash01drive@
2	Flash02drive.wordpress.com	Flash01drive+1@

3	flashdrive03.wordpress.com	Flash01drive+5@
4	04flashdrive.wordpress.com	Flash01drive+6@
5	5flashdrive.wordpress.com	Flash01drive+7@
6	006flashdrive.wordpress.com	Flash01drive+8@
7	070flashdrive.wordpress.com	Flash01drive+9@
8	8flashdrive.wordpress.com	Flash01drive+10@
9	09flashdrive.wordpress.com	Flash01drive+11@
10	10flashdrive.wordpress.com	Flash01drive+12@
11	flashdrive11.wordpress.com	Flash01drive+13@
12	12flashdrive.wordpress.com	Flash01drive+14@
13	13flashdrive.wordpress.com	Flash01drive+15@
14	14flashdrive.wordpress.com	Flash01drive+16@
15	15flashdrive.wordpress.com	Flash01drive+18@
16	16flashdrive.wordpress.com	Flash01drive+19@
17	17flashdrive.wordpress.com	Flash01drive+20@
18	18flashdrive.wordpress.com	Flash01drive+21@
19	19flashdrive.wordpress.com	Flash01drive+22@
20	20flashdrive.wordpress.com	Flash01drive+23@

Once the 20 WordPress accounts are created, the creation of a generic website can be made. The idea of the website is to track if the website has been viewed or not. If the website has been viewed, then a conclusion can be drawn that someone opened the contents of the flash drive. If the website has not been viewed then the contents of the flash drive were not opened. Having 20 separate websites associated with a specific flash drive allows for this to happen. The WordPress website should be generic so attention is not drawn.

Flash Drive Setup

Each flash drive consists of an autorun and batch file placed on the root of the flash drive.

The autorun file is then hidden on each flash drive with the batch file being the only displayed item. The batch file names either suggested the files were resumes or bank statements. The flash drives are divided in half. Half the flash drives were resumes (1-10) and the other half are bank statements (11-20). Each file would be named with a common name underscore resume, or bank statement, .bat. Example resume file would be, Jim_resume.bat. Example bank statement file would be, Shannon_bankstatement.bat. These files would trigger the autorun file to open the correct website pertaining to that specific flash drive. Once the autorun command opens the website, the WordPress website logs the view letting me know the contents of the flash drive were viewed on a computer.

The autorun file consists of a text document saved as Autorun.inf. The contents of the file are shown in Figure 2: Autorun.inf File. This document is then saved on the root of the USB flash drive and then hidden so users do not accidently click on it.

```
[Autorun]
Open=Robert_Resume.bat
Action=Start
```

Figure 2: Autorun.inf File

The batch file consists of a text document saved as, in this case, Robert_Resume.bat. This allows the autorun script to open the batch file when clicked upon. The contents of the batch file is shown in Figure 3: Robert_Resume.bat File. The corresponding website is changed for each flash drive.

```
@echo
start firefox "Flash02drive.wordpress.com"

@echo
start chrome "Flash02drive.wordpress.com"
```

Figure 3: Robert_Resume.bat File

These two files allow for the autorun script to open the corresponding website automatically when the user clicks on the batch file. If the user has Google Chrome or Mozilla Firefox installed on their computer, the script will open the corresponding website.

Flash Drive Locations

The locations for the flash drives to be dropped are in high trafficked parking lots. The idea behind high trafficked parking lots is to increase the possibility of an end-user picking up the flash drive and plugging the device into their computer. For this experiment, I selected local shopping centers and restaurants (Howell and Brighton, Michigan area). Shopping centers and restaurants have high traffic volumes making them perfect places to increase my chances of flash drives being picked up. The method used is to drop the flash drives off in the parking lots started mid-morning, around 10 am and 2 pm, so that the flash drives were present in the parking lots when people would be getting off of work to visit the shopping centers or restaurants. This increases the probability of USB flash drives being picked up.

Flash Drive Drop

Flash drives are dropped in parking spaces close to the shopping center or restaurant. The idea of the drop is to make it look like the flash drive fell out of the car on accident. Each flash drive is dropped either on, or close to the parking lot yellow line. Pulling your vehicle into a parking spot closer to the establishment allows for a better chance for someone to see the USB flash drive. Once the spot has been picked, I inconspicuously opened the vehicle door and dropped a USB flash drive close to the yellow parking line.

Internet Security Survey Overview

The Internet security survey consists of anonymously surveying 18 to 24 year olds. The purpose of the survey is to gain an insight into the younger generations knowledge of cyber security. The survey is conducted in an open environment with the individuals simply agreeing or disagreeing with each question. The individuals will have the opportunity to agree or disagree with each question being asked. They will then be allowed to comment on the question to pull further insight into how security conscious they are towards cyber security.

After each questions is asked documentation will take place. For example, question one found 24 out 27 individuals agreed with the response. The survey will be used as a tool to draw a comparison between the younger generation and the older generations cyber security consciousness. As Zadelhoff (2016) explained, employees are the biggest threat to an organization. Depending on the response of the students, an argument can be made whether or not future employees will be as big of a threat as they are now.

Conducting the Survey

The survey will be conducted within a 5-10 minute time interval. The individuals will be asked a series of questions and their response will be to agree or disagree. A few questions will ask for the individuals to comment on. These responses will be recorded. See Figure 4: Survey.

Question

1. What I do on my computer could affect other people?
2. I use the same password for everything?
3. Do you walk away from your computer while it is still logged in?
4. Do you open unknown links while on the Internet?

5. Do you share your username and password with anyone?
6. Do you change your passwords frequently?
7. Would you plug an unknown USB flash drive into your computer?
8. What do you do with an unknown USB flash drive?
9. How many people have a smartphone, tablet, laptop, iPod, or iPad?
10. How many people have a Xbox, PlayStation, or Nintendo?
11. Do you connect your device to public Wi-Fi?
12. Do you use Snapchat?
13. Do you share your location on Snapchat?
14. What applications do you use on your devices?

Figure 4: Survey

Valid Method

I believe this method is valid because it is a non-intrusive method. I want the experiment, along with the survey, to be done in the most morally and ethical way without bringing any harm to anyone's devices. I feel having the USB flash drives being tracked through an autorun script that opens a generic website that I made accomplishes my goals. The end-users suffer no ramifications from opening the file except for the inconvenience of having to close the web browser. This method allows me to see if the website had been viewed and how many times the website was viewed. This method allows me to draw the conclusion to whether or not the file on the flash drive was opened or not.

My method for conducting my survey is also valid because it allows me to gather anonymous data from a younger generation. Many researchers have established that older

generations in the current work force are not as cyber security conscious, as they should be. Surveying a younger generation will give insight on educational methods that can be used to make them more aware.

Chapter 4

Results

The results from the USB Flash Drive drop experiment is staggering. It was perceived that the experiment would yield results similar to what "United States: Find a Flash Drive" (2015) had concluded with 20 percent of Americans picking up an unknown USB flash drive and using it. My experiment, on a small scale level, yield results of 40 percent of the USB flash drives being picked up and used multiple times. The goal of the experiment was to conclude the likelihood of end-users putting information at risk by plugging an unknown device into his or her computer.

Table 2:

USB Flash Drive Locations, Time and Date

Flash Drive Number	Type of Parking Lot	Date/Time
1	Strip Mall	11-06 10:14am
2	Strip Mall	11-06 11:23am
3	Strip Mall	11-06 1:07pm
4	Shopping Center	11-06 1:02pm
5	Super Market	11-06 1:13pm
6	Restaurant	11-06 1:10pm
7	Super Market	11-06 1:17pm
8	Shopping Center	11-06 1:20pm

9	Gas Station	11-06	1:27pm
10	Restaurant	11-06	1:36pm
11	Shopping Center	11-06	1:39pm
12	Strip Mall	11-06	1:44pm
13	Super Market	11-06	1:50pm
14	Shopping Center	11-06	2:53pm
15	Hockey Rink	11-06	2:40pm
16	Shopping Center	11-06	3:06pm
17	Shopping Center	11-06	3:17pm
18	Strip Mall	11-06	2:58pm
19	Shopping Center	11-06	2:56pm
20	Restaurant	11-06	3:03pm

Each one of the 20 USB flash drives were dropped in the parking lot to simulate the drive falling out of a car by accident. The drives were dropped between mid morning and early afternoon with the idea that people would see the drives while visiting the parking lots after work.

Success Rate

The experiment showed that 2 out of 5 people are willing to plug an unknown USB flash drive into their computer. The data shows that out of the devices that where opened, 50 percent were opened more than once. 12 percent of the devices were opened four times whereas 38 percent of the devices opened, were only opened once.

Table 3*:*

USB Flash Drive Opened

Flash Drive Number	Type of Parking Lot	Opened Amount and Date

1	Strip Mall	Once	11-06
5	Shopping Center	Twice	11-16
6	Restaurant	Once	11-06
11	Shopping Center	Once	11-06
13	Super Market	Four	11-06
17	Shopping Center	Twice	11-06
18	Strip Mall	Twice	11-06
20	Restaurant	Once	11-16

The table above illustrates which locations had the greatest success rate. The USB flash drives dropped at shopping centers seemed to target a large audience. This allowed for multiple openings of the flash drive. The table also demonstrates when the device was viewed. Most of the devices viewed were viewed on the same day they were dropped; however, two of the devices were viewed 10 days later. *Figure 5*: USB Flash Drive Opened Dates, shows when on which day the devices were opened.

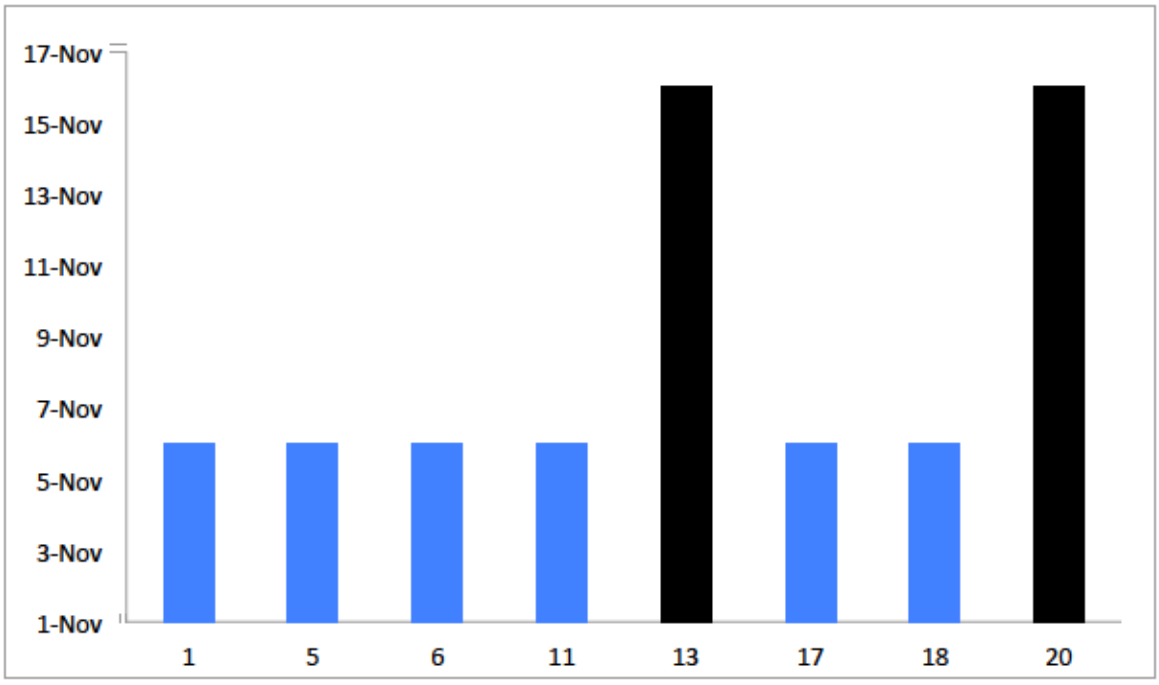

Figure 5: USB Flash Drive Opened Dates

Missing or Destroyed USB Flash Drives

The following day, November 7, 2017, USB flash drive drop locations were revisited to see if the drives had been picked up. Out of the 20 USB flash drives dropped only one USB flash drive had not been picked up. The USB flash drive was found in a gas station parking lot. The USB flash drive had been ran over by a vehicle. All the other USB flash drives were not found in the same location as they had been dropped in the previous day. A conclusion was drawn that individuals in the parking lots picked up the USB flash drives within the 24-hour span.

Table 4:

Flash Drive Retrieval

Found USB Flash Drives	Not Found USB Flash Drives	Opened USB Flash Drives
1	19	8

Secondary Research

The USB flash drive drop experiment showed a second portion of experimental research. Each USB flash drive had a file within the device to automatically launch a website to keep track of the device had been plugged into a computer or not. The first 10 USB flash drives files (1-10) contained file names such as Jim_Resume.bat. The other 10 USB flash drives (11-20) contained file names such as Shannon_bankstatement.bat. The idea was to see if the USB flash drives dropped in similar locations with different file names would yield the same results. *Table 5*: Resume.bat v. Bankstatment.bat, shows out of the USB flash drive files opened, the bankstatement.bat files were opened more than the resume.bat files

Table 5:

Resume.bat v. Bankstatment.bat

USB Flash Drive	File Name	Percentage Opened
1-10	Name_Resume.bat	38%
11-20	Name_Bankstatement.bat	62%

Multiple Openings

Having more of the Bankstatment.bat files opened on the USB flash drive drop experiment was not the only secondary data collected. Each bankstatement.bat file was opened more than once in 80 percent of the USB flash drives. When compared to the resume.bat files only 33 percent of the time were these files opened more than once. Two explanations can be given for the multiple openings. The first explanation would be that the individual who plugged the USB flash drive into his or her computer had both Google Chrome and Mozilla Firefox. The autorun script looked for both of these programs on the computer once the file was clicked on. If both programs existed on the computer then the website would have been opened twice. This would have allowed for multiple views showing the drive had been opened multiple times. The second explanation is that the bankstatment.bat files peaked the individual's interest more than the resume.bat file did. This would account for the individuals clicking on the files multiple times giving more than two views on the website associated with the corresponding USB flash drive.

Summary of USB Flash Drive Drop

The idea of the experiment was to demonstrate whether end-users keep information they have secured. Simulating a social engineering tactic to log whether or not files from the USB flash drive had been opened by a stranger. The results to the experiment show that the social engineering tactic would work and that if the USB flash drives had been filled with malicious code for malicious intent, 40 percent of people are likely to fall for the attack.

The experiment also proves the higher the individual's curiosity, the more likely they were to click on the file. Since the experiment was successful, it is fair to say that USB flash drives loaded with malicious code that automatically download when connected to a computer, without the user's knowledge, will leave the end-user exposed. This demonstrates that nearly half of the end-users in this experiment are susceptible to leaving information exposed and being a security risk.

Anonymous Survey

The second part of my experiment deals with an anonymous survey of 18 to 24 year olds. The 18-24 year olds were survived anonymously and were asked general questions about their cyber security habits. Each response by the 18-24 year olds gave an additional insight into end-user security moving forward.

Each question was broken down for simple understanding. The survey indicates that the 18 to 24 years olds who were surveyed interact with technology daily. With this interaction, I wanted to see how security conscious they were. *Figure 6*: Computer Decisions, shows that over 80 percent of the 18-24 year olds surveyed believed their actions online have consequences.

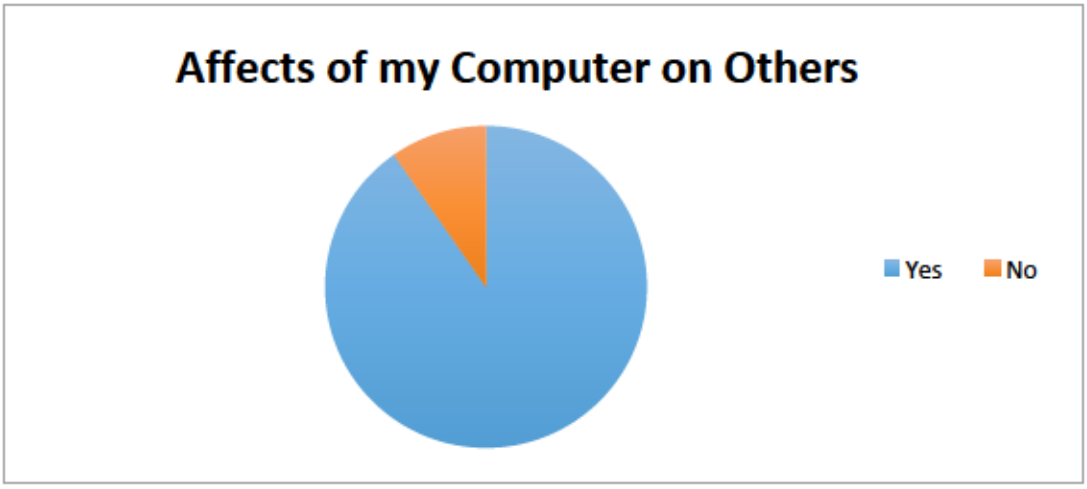

Figure 6: Computer Decisions

Security

The 18-24 year olds surveyed did not think changing their passwords was relevant unless asked to do so. In fact, 77 percent of the 18-24 year olds surveyed used the same password for multiple accounts. The 18-24 year olds surveyed, explained that their passwords would be different only if the password asked for a variety of characteristics. In addition, the 18-24 year olds surveyed, believed sharing username and password credentials was sometimes a good idea depending on the situation. 58 percent shared login information with others. One reason would be to share Netflix account information so multiple accounts did not have to be purchased.

Furthermore, the 18-24 year olds surveyed saw no harm in getting up and walking away from their computer while it was still logged in. Not a single 18-24-year-old who was surveyed thought leaving their computer unattended was a bad idea. Many of the 18-24 year olds surveyed explained that the computers are never left in public places unattended and that as long as they were with a friend it would be safe. The thought process was if a trusted person was near their computer nothing could go wrong.

The 18-24 year olds surveyed also had a unique approach towards opening unknown links. Every 18-24 year olds surveyed agreed they have at one point in time opened unknown links. Some of the 18-24 year olds surveyed argued that all links are unknown and that they cannot be known unless they are opened. Others said they click on pop-ups if they look like games or advertisements for deals on Amazon. The 18-24 year olds surveyed agreed that at some point in their life they had clicked on an unknown link that infected their computer and or destroyed it.

The 18-24 year olds surveyed all agreed they use open Wi-Fi networks. This was another case where all the18-24 year olds surveyed agreed they have connected to free Wi-Fi before. Some argued they had connected to Xfinity Wi-Fi, which they pay for in their own Internet package. None of the 18-24 year olds surveyed saw the harm in using the free Internet. They believed the free Wi-Fi was for anyone to use and did not see any consequence in using public Wi-Fi.

Upon further questioning, more than half the 18-24 year olds surveyed agreed they had looked at personal information on their devices connected to public Wi-Fi. This information included things like bank statements, purchasing items on Amazon, or even logging into financial aid information.

18-24 Year Olds and USB Flash Drives

When it came to finding USB flash drives, the 18-24 year olds surveyed had a unique approach. At first, when asked what they would do with finding a USB flash drive that was not theirs, many of the 18-24 year olds surveyed hesitated. After thinking about it, many of the 18-24 year olds surveyed agreed they would leave the USB flash drive alone. The follow up question,

was figuring out what the 18-24 year olds surveyed would do if they found a USB flash drive and did not leave it alone. 83 percent of the 18-24 year olds surveyed agreed they would plug the device into a computer to see if someone had a document with their name on it within the device. If they did they might be able to give it back to the correct owner. If it did not, then they would more than likely keep it for themselves.

Snapchat

Each 18-24 year olds surveyed owns or has access to some type of Internet accessible device. *Figure 7*: Student Devices, shows the number of students with Internet accessed devices. These devices are categorized by how many 18-24 year olds surveyed own the device. Each of the 18-24 year olds surveyed have at least one of the devices. Many have multiple.

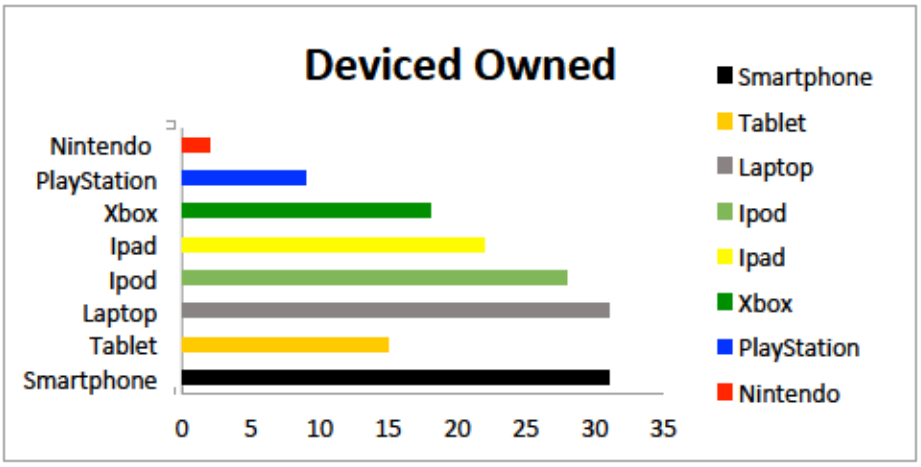

Figure 7: 18-24 Year Old Devices

Snapchat is a popular app amongst the 18-24 year old population. All 18-24 year olds surveyed had the application installed on some type of device mentioned above, minus the Xbox, PlayStation, and Nintendo. Each student had agreed they use the application Snapchat to

communicate with their friends, and in some case family. When asked if the application was sharing their locations, the 18-24 year olds all agreed the application was. 18-24 year olds surveyed agreed without the application sharing their location, certain filters would not be able to be present.

Xbox-PlayStation Live

Figure 7: 18-24-Year-Old Devices, shows a small percentage of 18-24 year olds had gaming consoles. Of the 18-24 year olds who had these gaming consoles, 93 percent had access to play with strangers via the Internet. This allows for the 18-24 year olds to play with their friends along with strangers.

Applications Used

Applications can range from a variety of things: cooking, fashion, war, or even flow charts. Depending on age, applications have a target audience. For 18-24 year olds, applications mainly involve connecting with people. Some of the applications involve games. The most downloaded application by 18-24 year olds was Snapchat, followed by communication applications: Facebook, Twitter, Instagram, Whatsapp, Tinder, and LinkedIn. Some of the 18-24 year olds applications included gaming: Clash of Clans, Xbox, and Clash Royale. Entertainment applications were also a big download for 18-24 year olds: Netflix, Hulu, Google Home, Twitch, StreamTV, and YouTube.

Survey Summary

The idea of the anonymous survey was to gain an understanding of the younger generations view on cyber security. The purpose was to see if the younger generation was a more secure end-user then the prior generations. Unfortunately, it seems that the younger generation is

just as vulnerable as the older generations.

The conclusion can be made that cyber security is not getting any better. All the 18-24 year olds surveyed saw no harm in violating basic cyber security protocols, such as leaving a computer logged in and unattended. The survey helps support that at any age, end-users are a serious threat towards information security.

Chapter 5

Summary of Findings: USB

My findings from my USB flash drive drop experiment showed that 2 out of 5 people are vulnerable to a social engineering attack using USB flash drives. This information concludes that end-users are susceptible to falling victim to social engineering tactics that leave their information vulnerable.

Furthermore, the USB flash drive experiment showed that files containing the words, bank statement, were more likely to be opened then files containing the word, resume. This information concludes that end-users with a peaked interest can fall victim to becoming vulnerable towards exposing their information.

If end-users are willing to plug an unknown USB flash drive into their computer, that was found at a super market, then end-users are more than likely to do the same if the unknown USB flash drive was found in their work parking lot. This demonstrates how end-users can leave a company exposed to an attack. The USB flash drive experiment was a non-intrusive experiment. The end-user had to pick up the unknown USB flash drive, plug the USB flash drive into his or her computer, open the contents of the USB flash drive, and click on the document in the USB flash drive. Once all of that had been done, the contents of the USB flash drive would simply

open a website and do nothing more. The website could be closed and the contents of the USB flash drive could be deleted. The experiment validates, if an end-user is willing to go through all those steps to see what contents are on the USB flash drive, then the same end-user is willing to plug an unknown USB flash drive into his or her computer that downloads malicious code without the knowledge of the end-user. The end-user would then be the cause of the new threat to either the company's information or their own personal information.

The USB flash drive drop experiment also demonstrates how the social engineering tactic can play towards a long con. For example, while conducting the experiment 75 percent of the people who plugged the own unknown USB flash drive into their computer did so the same day the USB flash drives were dropped. This leaves 25 percent being opened several days later. This data indicates that the individual picked up the USB flash drive and took it home and forgot about it. More than likely the USB flash drive device was either found at home days later or was found when it was needed. Either way the USB flash drive was plugged into the computer. The user may or may not have realized the USB flash drive was the unknown one they had found. This opens the argument that even though the USB flash drive device was not opened the day it was found it could have been confused with a device that belonged to the owner and was used in place of the actually owned device. This means if someone where to put malicious code on the unknown device and the individual who found the unknown device took it home and forgot about it, the malicious code would have a greater chance of making it on a computer days later. The individual would mistake the unknown USB flash drive as one of his or her own. This would lead to that individual either exposing their own personal data or possibly taking the infected device to work, because they think it is one of their own, and plugging it into a work computer. Either way the end-user is bringing in the threat.

Summary of Findings: Survey

My findings for the survey portion include the younger generation is not anymore secure then the older generation. While conducting the survey on 18-24 year olds, I found that simple cyber security rules were being violated. For example, all the 18-24 year olds had agreed they have used public Wi-Fi to check personal information. This personal information can stem from financial aid to bank statements to purchasing items on websites. Regardless, all 18 to 24 year olds agreed they had done it at some point in time. This could leave them vulnerable to attacks on their device depending on secure the transactions are.

I also found that 77 percent of the 18-24 year olds who were surveyed used the same password for multiple accounts. The only time these individuals would change their passwords was if they were asked to do so, otherwise the password stayed the same. Included in that percentage is the amount of people who used the same password for multiple accounts. The logic behind the same password was it was easy to remember. The downfall to this logic is that this leaves the user vulnerable to getting every account they have created hacked into. Keeping the same password for each account leaves that end-user vulnerable.

In addition to using the same password on multiple accounts, 58 percent of the 18-24 year olds surveyed admitted to sharing username and password information with multiple people. The argument was sharing the login credentials with others allows for only one subscription of something to be bought. For example, many of the 18-24 year olds shared Netflix or Hulu accounts with their friends. The downfall to sharing accounts with others is it leaves the primary account holder's information available to anyone who has access to the account. Billing and credit card information can then be stolen.

Out of all the 18-24 year olds who were surveyed, 83 percent agreed they would plug an unknown USB flash drive into their computers. Many did not see how the USB flash drive could harm them in anyway and figured the USB flash drive was now theirs. Not a single person surveyed thought about the negative consequences the USB flash drive could have on their computer. When it came to USB flash drive security, the consensus was that USB flash drives can only hold information and if there were information on the device that was harmful the computer would catch it before it could disperse on the computer.

When it came to using applications, the 18-24 year olds surveyed all agreed they use applications like Snapchat with location sharing capability. None of the surveyed population saw any harm in sharing locations with friends. In fact, many believed the location sharing capability was a positive rather than a negative because it allowed for family members and friends to be tracked.

The USB flash drive experiment and 18-24-year-old survey both show the lack of end-user security. A conclusion can be made that end-users will always sacrifice security for convenience. In terms of the USB flash drive drop experiment; individuals who picked up the drives were doing so for either the purpose of a free USB flash drive or in terms to find its owner. Regardless of their decision, the individuals who picked up and plugged the USB flash drives into their computers threw security out the window.

In terms of the 18-24 year olds who were surveyed, all of them were sacrificing security for convenience in some way. Somewhere sharing login information to share accounts, others were sharing locations, and many were using similar passwords, which never changed, for multiple accounts. Either way, the study shows in terms of security, end-users are more likely to

give up security to keep things simple.

Further Study

The USB Flash drive drop experiment was done in a high trafficked public setting. The idea was to see how vulnerable end-users are with personal information. If an end-user was to pick up the USB flash drive and plug it into their computer and open the corresponding documents than the conclusion can be drawn they would be susceptible to the same tactic with a USB flash drive holding malicious data. An additional study would be to get permission from a corporation or large business and do the same experiment with the employees of the company. If the general end-user is vulnerable to the social engineering tactic it would be a reasonable assumption that some of the employees of the company would also be vulnerable.

It would also be interesting to conduct the experiment in different countries. Similar studies have been conducted in America, but I did not run across any studies in other countries. It would be interesting to find out if end-users in other countries are as relaxed on security as end-users are in America.

In addition, further study of the survey could also be geared towards older and younger people. It would be interesting to see whether older or younger end-users also trade security for convenience.

References

Berkman, F. (2012, October 8). Did you Know 3 Billion USB Products are Shipped Every Year? *Mashable*.

Ciampa, M. (2014). *Security Awareness: Applying Practical Security in your World* (4th ed.). Boston, MA: Course Technology, Cengage Learning.

Eitel, E. (2011, March 1). The Ultimate Cyberweapon: USB Flash Drives? *Motion System Design*. Retrieved from Business Insights: Global.

Grimes, R. A. (2017, March 21). Vastly Improve your IT Security in 2 Easy Steps. *InfoWorld*.

Harris, S. (2013). *All in One CISSP* (6th ed.). New York, NY: McGraw Hill Education.

Hong, J. (2012, January 26). The State of Phishing Attacks. *55*(1), 74-81. Retrieved from ACM Digital Library.

Johansson, J. M. (2008). Security Watch Island Hopping: The Infectious Allure of Vendor Swag. *TechNet*.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015, June). Advanced Social Engineering Attacks. *Information Security and Applications*, *22*, 113-122. Retrieved from ScienceDirect.

Moyle, E., & Kelley, D. (2012, April 1). Threats Vs. Readiness. *InformationWeek*. Retrieved from Business Insights: Global

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., and Bailey, M.

(2016). Users really do plug in USB drives they find. In IEEE Symposium on Security and Privacy , pages 306–319. IEEE Computer Society.

United States: Find a Flash Drive, Pict it Up: Experiment Shows How Lack of Cybersecurity Knowledge Can Impact Organizations. (2015, October 26). *Mena Report*. Retrieved from Academic OneFile.

Yang, F. (2004), *U.S. Patent No. US6733329 B2*. Washington, DC: U.S. Patent and Trademark Office.

Zadelhoff, M. V. (2016, September 19). The Biggest Cybersecurity Threats are Inside your Company. *Harvard Business Review*.

Appendix

18-24 Year Old Survey

Question

1. What I do on my computer could affect other people?
    a. Yes: 25
    b. No: 6
2. I use the same password for everything?
    a. Yes: 24
    b. No: 7
3. Do you walk away from your computer while it is still logged in?
    a. Yes: 31
    b. No: 0
4. Do you open unknown links while on the Internet?
    a. Yes: 31
    b. No: 0
5. Do you share your username and password with anyone?
    a. Yes: 18
    b. No: 13
6. Do you change your passwords frequently?
    a. Yes: 3
    b. No: 28
7. Would you plug an unknown USB flash drive into your computer?

   a. Yes: 26

   b. No: 5

8. How many people have a smartphone, tablet, laptop, iPod, or iPad?

   a. Smartphone: 31

   b. Tablet: 15

   c. Laptop: 31

   d. iPod: 28

   e. iPad: 22

9. How many people have a Xbox, PlayStation, or Nintendo?

   a. Xbox: 18

   b. PlayStation: 9

   c. Nintendo: 2

10. Do you connect your device to public Wi-Fi?

   a. Yes: 31

   b. No: 0

11. Do you use Snapchat?

   a. Yes: 31

   b. No: 0

12. Do you share your location on Snapchat?

   a. Yes: 31

   b. No: 0

13. What applications do you use on your devices?

   a. Entertainment: Netflix, Hulu, YouTube, Google Home, Clash of Clans, Clash

Royale, Pintrest, Twitch, and SteamTV

b. Social: Snapchat, Twitter, Facebook, Instgram, WhatsApp, Tinder, LinkedIn, Slack, and Uber,

c. Music: Spotify and Pandora