12-2021

PHISHING FOR ALL AGES

Rachana Vann

PHISHING FOR ALL AGES

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

---

by

Rachana Vann

December 2021

PHISHING FOR ALL AGES

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Rachana Vann

December 2021

Approved by:

Vincent Nestler PhD, Committee Chair,

Conrad Shayo PhD, Committee Member

Javad Varzandeh PhD, Committee Member, Information and Decision Sciences

Department Chair

ABSTRACT

Since the start of the pandemic in 2020 and the increase in teleworking, we have witnessed a subsequent increase in cyber-attacks. This project focused on the tools and techniques a teleworker should use to stay safe from online predators. An online predator or hacker is defined as someone who uses the internet to get access to proprietary information or seek a ransom. This project sought to introduce tools and techniques that would help people of all ages to stay safe online. The questions asked were: What techniques do online predators use to lure their unsuspecting victims? On the American Generation Timeline (AGT), which generations are impacted the most and why? What can be done to make the most affected generation(s) more secure? The project findings were: (1) Researching, Impersonating, Grooming, Taking Control, Intimidation, and Escape Plan are the five techniques that are used by online predators; (2) that Silent Generation and Generation Z are the most vulnerable; and (3) that using a combination of password protection, patching techniques, and anti-virus software installation would help minimize the number of cybercrime victims. Recommendations for further research include an extended investigation of why certain generational groups fall victim to certain predator attack types.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE :

INTRODUCTION

As a result of teleworking becoming the new “normal” due to the Covid-19 pandemic, we have witnessed an increase in cyber-attacks since Fall 2020. (Parker, Menasce Horowitz, & Minkin, 2020). As a result of this, cybercriminals have easier access to their prey due to more teleworking options becoming available (Sharma, 2020). Social Cognitive Theory (SCT) is also important to investigate on why the users become prey to cyber-attacks. Both The Economic Times and Aspen Institution have a different idea when it comes to finding out which generation is considered to be the “lowest hanging fruit”. The Economic Times’ research cites a Norton study that found out that millennials are the most commonly affected” (ET Online, 2017). Whereas the Aspen Institute found that “online scammers would most likely target the elderly” (Fahs,2020). With both of these studies we can point out that cybercriminals will most likely be looking for the lowest hanging fruits which turns out to be the younger generation and the elderly. Online predators are using digital tools, and techniques to lure their victims in. It is important for these users to understand the mindsets of online predators, so they will not become part of another statistic of an online attack.

Table 1 shows the American Generation Timeline (AGT) that will be used in this project and was developed by Visual Capitalist. The American Generation

Timeline is made possible by the Pew Research Center. The Pew Research Center has combined two of their research papers together to form the AGT onto their sister company's site (Ghosh, 2021). The goal when forming the AGT was "to make the world's information more accessible—simplifying an increasingly complex world through data-driven, visual storytelling" (Ghosh, 2021). This project uses the AGT to clearly identify the generation names and the birth years that are associated with them.

Table 1. American Generation Timeline

Generation	Age Range (years)	Birth Year Range
The Silent Generation	76 and over	1928-1945
Baby Boomers	57-75	1946-1964
Generation X	41-56	1965-1980
Millennials	25-40	1981-1996
Generation Z	9-24	1997-2012
Generation Alpha	0-8	2013-present

Source: Visual Capitalist 2021

It is important to keep in mind that people have extraordinary amounts of Personal Identifiable Information (PII). The Department of Homeland Security defines PII as “Social Security Numbers, driver’s license numbers, Alien Registration numbers, financial or medical records, biometrics, or a criminal history” (Department of Homeland Security, 2021). The goal of an online predator is to trick a person to reveal or give up some of their PII without knowing what is going on. To establish the best tools and techniques that a normal person can use to avoid to not fall as victim to these social engineering attacks we would need to answer these three questions:

1. What techniques does online predators use to lure their unsuspecting victims?
2. On the American Generation Timeline (AGT), which generations are impacted the most and why?
3. What should be done to make the most affected generation(s) more secure?

This project will go over the tools and techniques that an online predator would use to attract certain generations to become victims of a cyber-attack. This project will find out which generation(s) are more susceptible to fall for a social engineering attack. Various social engineering attacks will be referenced as the widely used tools of attack. Finally, recommendations for secure internet surfing will be given and suggestions for further research will be proposed.

Organization of the Project

This project is organized as follows: Chapter 2 will provide an examples from various researchers such as the Federal Trade Commission (FTC), Maggie Miller, and Kristine Solomon which all helped me organized the scammer's model that I have created to further explain the common tools, techniques, and procedures that an online predator would use to attract their victim. Chapter 3 will review research on what generation would fall for these social engineering attacks and the impact to them. Chapter 4 will provide reasons for answering phishing emails, Chapter 5 will provide the tools, and techniques for those certain generations to "stay safe" online. Finally, Chapter 6 will provide suggestions for further research.

.

CHAPTER TWO:

COMMON TOOLS AND TECHNIQUES OF AN ATTACKER

This chapter will be going over common tools and techniques of an attacker. This chapter will cover defining the attacker, Attacker's Methodology, Research, Impersonation, Grooming, Taking Control, and Intimidation and Escape Plan. Table 2 below lists all of the sources and articles that I have used throughout this chapter.

Table 2: External Information Database

Database Searched	Library Search Words	Number of Hits	Relevant Articles you used in the study	Authors
Duck Duck Go	Hacker, Attacker, Attacker Methodology, Attacker Research, Impersonating, Grooming, taking control, Intimidation, Escape plan	78	6	Federal Trade Commission, 2019; Federal Trade Commission, 2019; DuckDuck Go, 2020; Cohen, 2020; Solomon, 2021; Cisco. n.d; The NSPCC, 2019

Google Scholar	Hacker, Attacker, Attacker Methodology, Research, Impersonating, Grooming, taking control, Intimidation, Escape plan	8,660	1	Miller, 2020
OneSearch	Hacker, Attacker, Attacker Methodology, Research, Impersonating, Grooming, taking control, Intimidation, Escape plan	2,560,000	6	Federal Trade Commission, 2019; DuckDuckGo, 2020; Cohen, 2020; Solomon, 2021; Cisco. n.d; The NSPCC, 2019

After going through each database, I was able to document my findings, and the number of hits of each keyword that was able to help me find an article that was needed for this research. The most interesting thing is that DuckDuckGo declines to tell you the number of results because “we cannot easily determine the number of results for a particular search ahead of time” (DuckDuckGo, 2020). Within this chapter I have filtered out these results in order to find the common tools and techniques of an attacker.

An attacker can be determined by who is the bad actor and why you became their target. Attacker's Methodology can be things like identifying the steps and ways bad actors made you the target and their steps to ensure you fall as one of their victims

Research is part of an attacker's background check on you and finding information about their target to ensure you fall for the flag that planned to gain your trust. Impersonating is when the attacker after doing their research and gathering information from the target starts to impersonate someone that is similar to the target to gain their trust. When the attacker starts to take control of the victim, they will be giving the attacker private information that would allow the attacker to gain something from their target without them realizing it. After taking control, the attacker would start to intimidate the target by threatening to expose the information or delete something of value that the target needed if the victim did not follow the escape plan to not disclose the information to police or not following their instructions to pay the fees.

Defining the Attacker

An attacker can be defined in many ways (malicious user, attackers, and hacker). No matter the name, all these actors have one thing in common which is to destroy things. These attacks that these hackers would use are focused on manipulating the confidentiality, integrity, and the availability (CIA), of information and use it for malicious intent. An attack that harvests information from victims

would be an example of how an attack would tamper the confidentiality of data. An attack that focuses on manipulating data would be a prime example of tampering with the data's integrity. Finally, if an attack were designed to encrypt or delete all the information that the attacker finds would be an example of manipulating with the data's availability. This project will be focusing on how the attackers focus on manipulating the confidentiality with the data that has been captured via users. To gain the information that is needed these attackers would follow some sort of methodology.

Attacker's Methodology

In 2019 the Federal Trade Commission (FTC) published a video on their website called "*How to Protect Yourself from romance scams."* Throughout this video the FTC went into detail on how online attackers use six steps to successfully scam their victims. These six steps are: research, impersonation, grooming, taking control, intimidation, and escape plan. The FTC labels these six steps as a scammers model which can be found below in Figure 1. Throughout this project I will be going into detail on how online attackers use this Scammer's model to extract information from their victims. Now let us go into detail in the first step within the Scammer's Model.

Figure 1: Scammer's Model

Source: Federal Trade Commission 2019

Research

The first step that an online scammer would take is to research and find their target. Their “target” could be anyone. According to Maggie Miller a writer for the Hill points out that “it seems that Senior citizens are becoming the primary target for cyber-attacks” (Miller, 2020). Kristine Solomon from Yahoo points out that kids are more likely to fall victim to an online attack due to “interacting online a lot more than usual, especially through Zoom and social media. And that makes them more likely to click on the wrong link” (Solomon, 2021). No matter whom the target is, the attacker would need to do some serious research on whom they would like to attack. Once the attacker knows their target then they would need to impersonate someone.

Impersonating

One of the best things about the internet is that you can hide your identity behind a screen. With this sense of anonymity hackers can impersonate themselves towards other people and their victims. The hacker would try to impersonate themselves to be like someone else in front of their victims to abstract information from their victim. To achieve this goal of “likeness” the victim will try to be intimidating, familiar, or authoritative. To demonstrate these traits, they would need to craft some sort of message. These crafted messages are some sort of phishing techniques. Jason Cohen from PC MAG points out that “Phishing attempts have been on the rise since COVID” (Cohen, 2020). A simple phishing tactic would be a message that contains the four traits that were mentioned previously. The four traits are likeness, intimidating, familiar, and authoritative. Some more common phishing attacks during the 21st century would be used through the phones such as vishing (voice phishing) and smishing (SMS or Direct Message (DM) phishing). Once the attacker has gained the trust of their victims then they will provide them instructions to follow.

Grooming

Grooming is defined as establishing a belief or befriending someone to make them emotionally connected to you to gain the object (The NSPCC, 2019.). The object can gain trust, and belief that the attacker is real. Once the attacker gains the victim’s trust then there would be instructions that would be provided by the attacker. These instructions would be worded in a very kind way with the

proper mannerism. The reason for this is so that the attacker would maintain their relationship with their victim. Once the victim complies with the instructions then the attacker will take control.

Taking Control

Once the Attacker has accomplished their goal of obtaining the information of the victim then there will be significant consequences for the victim. The consequences of the information gained can range from low to very high. An example of a low consequence would be providing account credentials to an online gaming website to gain some “free” loot. Giving someone access to your social security number (SSN) would be a great example of a very high consequence. With an SSN a malicious user has essentially stolen your identity. Using some sort of intimidation tactic to hold your information for ransom, a malicious user could give you another chance by selling the information back to you for a fee whether it is money or cryptocurrency such as Bitcoin.

Intimidation and Escape Plan

Intimidation is usually expressed by an ultimatum. An example would be demanding payment for the information that was exposed. This payment would usually be in the form of cryptocurrency. Cisco defines this type of ultimatum as ransomware which “is a type of malicious software or malware. It encrypts a victim's data, after which the attacker demands a ransom. Once the ransom is

paid, the attacker sends a decryption key to restore access to the victim's data. The ransom can range from a few hundred dollars to millions of dollars. Typically, payment is demanded in the form of a cryptocurrency, such as bitcoins” (Cisco. n.d).If the victim does not comply then the attacker would form some sort of escape plan. The escape plan would contain destroying accounts and other assets that were used in the overall scam. Some of these assets may include burner email addresses, burner phones, fake accounts, fake aliases, and any devices that are associated with the attack.

CHAPTER THREE:

PHISHING STATISTICS

Overall Statistics

The FBI has stated that “phishing was the most common type of cybercrime in 2020” (FBI National Press Office, 2021). Now these phishing emails tend to lead their victims to fraudulent websites. In fact, Maddie Rosenthal, a researcher for Tessian, found that “96% of all phishing attempts arrive by email”. The report continues in saying that “75% of companies around the world experienced some kind of phishing attack in 2020” (Rosenthal, 2021). The same researcher also distinguished the top five subject lines that were contained in the email which can be found on figure 2.

Table 3: Top 5 Subject Line Keywords

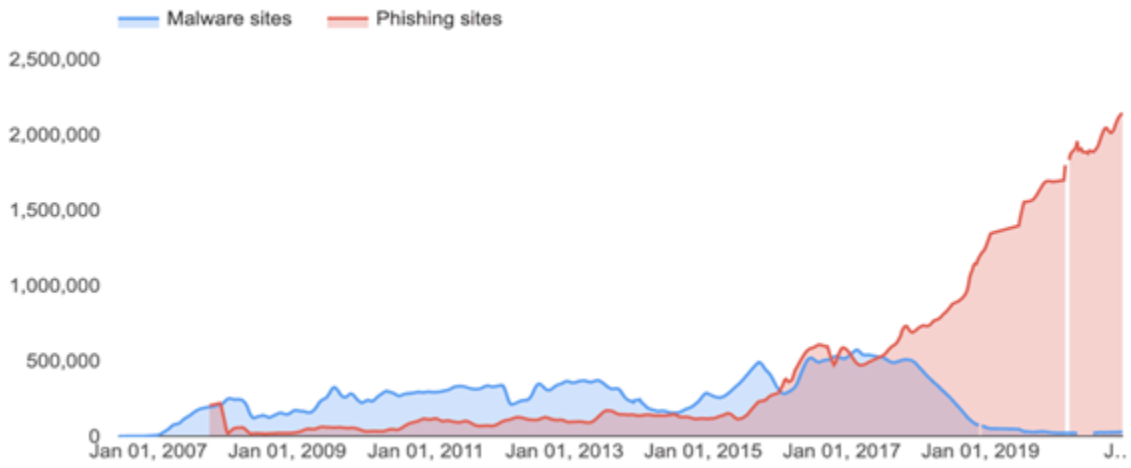
Ranking	Subject Line
1	Fw: Urgent Invoice
2	Payment is Urgent Do Not Ignore!
3	Important: Please Read
4	RE: Finance Request for CEO

5	Attention: Credentials needed for login to secure mainframe

Source: Rosenthal 2021

These subject lines are usually the first thing that an employee sees when receiving any email. When an employee sees this type of email from the scammer, this would mean that the scammer would be in phrase two which is impersonating the scammer's model. According to the report, if the end user interacts with the email, then it can cost the company "average of $150 per compromised record and if the scammer had breached the data successfully it would cost an average of $3.92 million in order for a company to bounce back". One of Google's Research and Development (R&D) sub company Safe Browsing took time to identify and detect malicious websites. According to Safe Browsing website "Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months)" (Google, 2021).

Figure 2: Malicious Website Count

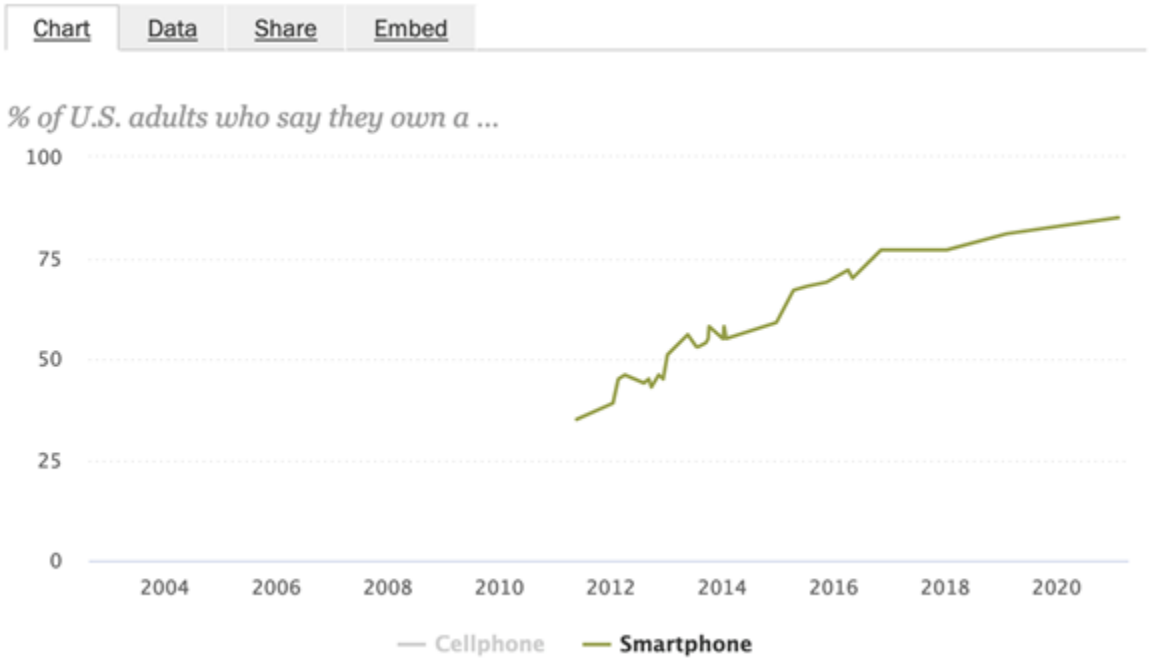


Source: Google 2020

The unfortunate truth about all is that LexisNexis published a report that found that “adults over 75 and young adults that are younger than 25 are the most vulnerable to fraud attacks” (Security Magazine, 2021). Now it would be a great time to dig deeper into these stats on why Silent Generation and Generation Z are the most vulnerable. Some of these websites that Safe Browsing found were related to COVID-19 Scams. According to (Rosenthal, 2021), “COVID -19 related scams reached their peak in the third and fourth weeks of April ''. The Pew Research company did an early survey in 2021 that was about mobile ownership overtime. Their research has shown that 85 percent of Americans own some sort of smartphone which was a significant jump from

their first survey that was conducted in 2011. The 2011 survey showed that only 35 percent of Americans own some sort of smartphone (Pew Research Center, 2021).

Figure 3: Percentage of U.S. Adults Who Say That They Own a Smartphone



Source: Pew Research Center 2021

With 85 percent of Americans who have smartphones there must be some sort of statistic that shows the rising numbers of mobile phishing attacks.

Smishing

Smishing is defined by Proofpoint as “a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone” (proofpoint, 2021). Figure 4 is a graph of a report that was published by Wandera in 2018. Figure 4 shows that smishing attacks is the most common type of mobile-based phishing.

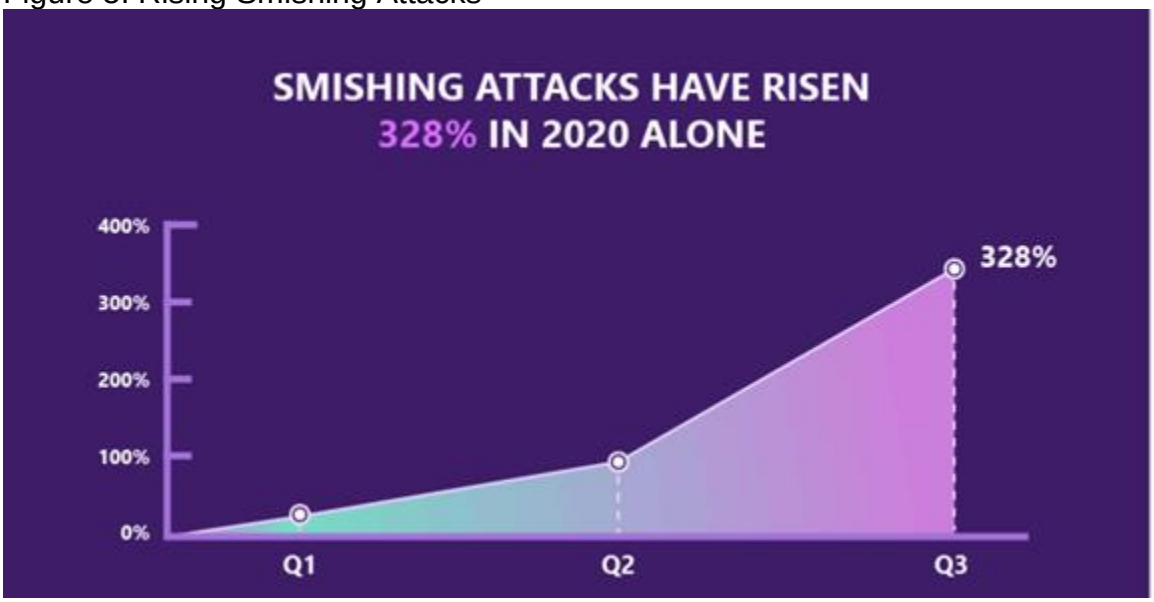
Figure 4: Smishing is the Most Common Mobile-Based Phishing

Source: Wanera 2018

This report from Wanera proves that there are numerous types of social engineering attacks that are targeted against users who own a smartphone. It is strange to see the number of phishing attempts on mobile devices have declined significantly since 2018. Since 2018 smishing attacks have grown significantly.

Proofpoint did research on smishing at the end of 2020 and found out that “mobile phishing increased more than 300 percent” (Laudon, 2020). The results of their report are represented in figure 3 below.

Figure 5: Rising Smishing Attacks



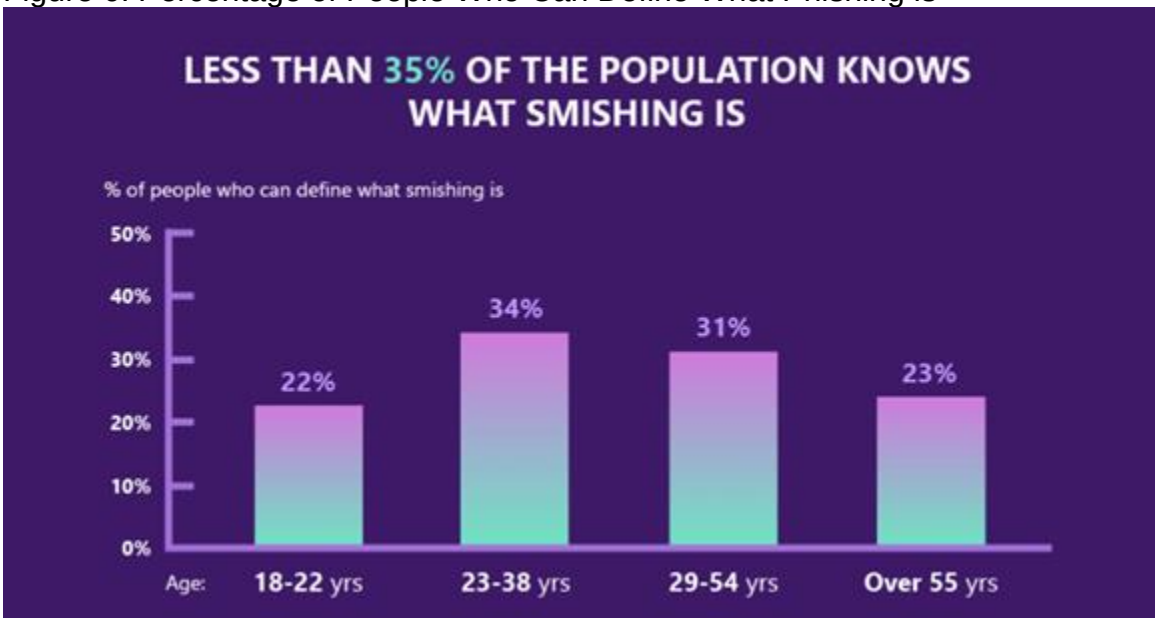
Source: Proofpoint 2020

With the rise of smishing attacks companies will cause companies to take a major financial loss which can cause up to millions of dollars.

Financial Loses.

The FBI's cybercrime complaint division has published a report in 2020 that "over 240,000 victims of phishing, smishing, vishing (phishing over the phone where a hacker makes a phone call or leaves a voice message), and pharming (when a hacker redirects users to a fake site in order to steal their sensitive info), costing over $54 million in losses (FBI National Press Office, 2021)". Surprisingly, figure 5 which is a visual representation of Proofpoint's published a paper that showed "only less than 35% of the population knows what smishing is" (Proofpoint, 2020).

Figure 6: Percentage of People Who Can Define What Phishing is



Source: Proofpoint 2020

This report from Proofpoint goes into detail about how Millennials, baby boomers and the silent generation are the three generations that will most likely fall for some sort of smishing attack. I would like to go into detail about the statistics behind the Silent Generation.

Silent Generation's Statistics

The US Department of Health and Human Services (DHSS) released a statement that "COVID-19 Scams are impacting the elderly". With DHHS contributing to Rosenth's research in claiming that the elderly is being the main target in these COVID -19 scams. It is important that we establish some backing in how these COVID-19 scams have affected these senior citizens. In early 2019 Maggie Fitzgerald published a story that claimed, "that nearly $3 billion disappears from the wallets and bank accounts of senior citizens annually" (Fitzgerald, 019). There are many reasons why these scammers are targeting the elderly.

The first reason is because the advisory knows that these types of people have some sort of steady income going through a variety of government substances or alternative means through family or savings. The second reason would be for urgency. The reason behind this is because these senior citizens would want to obtain their COVID-19 benefits as quickly as possible. This could

be since these senior citizens would want to obtain either the numerous COVID relief payments or the sign-up information to receive the COVID vaccination. We will be giving the background of the world wide web to have a better understanding of why this generation of people are falling for online phishing attempts.

Dawn of a New Era

The year of 1983 is known as the birth year of the world wide web. Now, in 1983 our youngest person who belongs in the silent generation would be thirty-eight years old whereas the oldest person would have been fifty-five years old. Between 1945 and 1983 the United States went through three wars. By the time the internet was invented these people would need to have a very steep learning curve. The resources are also scariest since only universities only have access to the internet. Now would be a great time to investigate how the hackers are taking advantage of the younger generation whose education system during the pandemic has taken a major turn towards remote learning.

Generation Z's Statistics

Since the pandemic, we are seeing the academic scene adapted from in person classes to Zoom classes. With zoom classes going on it is apparent that children are spending more time on the computer and clicking links that they do not know the origins of, as a result a total of "41% of school district cyber security

incidents and breaches were caused by phishing attacks" (Firch, 2021). The reports go on and say that there were a "total of 455 cybersecurity incidents in the educational sector in 2020" (Firch, 2021). Now outside of the education space these children have also fallen for other phishing attempts on different platforms.

Social Media

Social media can be Facebook, Instagram, Snapchat, Twitter, TikTok, YouTube, LinkedIn, etc. These are popular alternative platforms that we see young people interact with. The young generation rely on too many of these applications and it evolves as part of their daily life. Often, we see that it becomes a habit for one to grab their phone and check SMS messages or direct messages on social media. Furthermore, the younger generation often does not question the links that were sent to them from their group of friends or followers from either SMS message or direct message. Being popular, having more followers and likes are what the younger generation strive for. Having more likes equals more followers and more followers equals more sponsors more sponsors equal to more revenue and more revenue equal to more posts to being in public. In fact, the Pew Research Center did a survey at the end of 2020 to determine which age group uses social media the most and it turns out the young adults are the most active users. Figure 3 below are the results from the research.

Table 4: Percentage of U.S. Adults in Each Demographic Group Who Say They Ever Use

	Facebook	Instagram	LinkedIn
Total	69%	40%	28%
Men	61%	36%	31%
Women	77%	44%	26%
Ages 18-29	70%	71%	30%
30-49	77%	48%	36%
50-64	73%	38%	33%
65+	50%	13%	11%

Source: Pew Research Center 2020

Using common sense, we know that these young adults are humans and that all humans make mistakes. In fact, Internet Safety 101 points out that “nearly half of young people (47%) have received some sort of social engineering messages online (Cyberbullying Statistics, 2020). The reason for nearly half of these young people to fall for these types of scams is because they do not understand the phrase from the Better Business Bureau which is “If anything looks too good to

be true, it probably is” (Better Business Bureau, 1954). There are many research articles out there that explains why protecting any users from any sort of phishing attack is very important.

CHAPTER FOUR:

REASONS FOR TAKING THE BAIT

This chapter will be going over the reasons why the users are falling for social engineer attacks. There are five sections that this chapter will cover. Which are Underlying Truth, Home Users, Social Cognitive Theory, and Self- Regulation Theory. The underlying truth will contain the truth that social engineering attacks are targeted for everyone, not just the elderly and young people. This section will cover the disadvantages that a home user will have over a normal company when it comes to securing their home mobile devices. Social Cognitive Theory contains three things: personal factor, environmental factor and behavior. Inside of personal factors, it will contain the topic of underestimating the risk factor and emotional response to personal factors. Environmental factors will be covering some sort of external factor that is affected by personal factors. Behaviors and Habits are what one does on a daily basis. In the Self-Regulation Theory section it will contain ideas of how an individual controls their action and along with attribution theory. Now I would like to go over the first section which is the underlying truth.

Underlying Truth

Even though this report is proving that both the Silent Generation and Generation Z are the most impacted when it comes to phishing attacks, the truth is that social engineering attacks are targeted to everyone that has a device that

communicates over the internet, not just the Silent Generation and the Generation Z. Now it is time to dive deeper on why so many home users tend to fall for these scams time and time again.

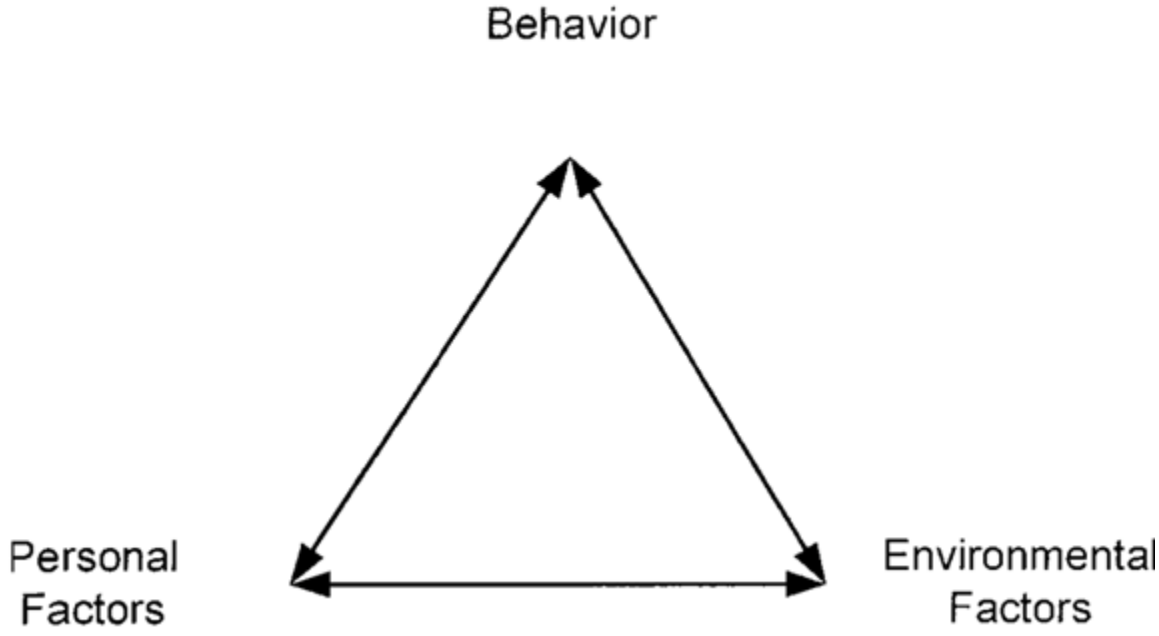
Home Users

Statista published a report in November 2020 that showed “that 47.1% of the world’s population have a household computer” (Statista, 2020). The great thing about having a household computer is that anyone that is a part of the household can use that computer for anything. However, the downside to having a household computer is that a single user will have to hold the responsibility of maintaining the upkeep and security maintenance of that machine. The sad truth is that a single individual would not have the finances or knowledge equivalent to a business in order to provide significant security to their home network. That is why the concept of Social Cognitive Theory (SCT) plays a major role in why many of these users fall prey to a cybersecurity attack.

Social Cognitive Theory

Social Cognitive Theory (SCT) is a theory “base used to explain the factors involved in individual decision making”. Social Cognitive Theory is built on three important factors which are: personal factors, environmental factors, and behavior. Figure 7 below shows how these three factors build upon one another.

Figure 7: Social Cognitive Theory Model



Source: Computer Security Behaviors of Home PCs 2020

Throughout the rest of this chapter, I will be going over each of these factors that play a major part in the Social Cognitive Theory. The First thing I would like to go over is the personal factors.

Personal Factors

Personal Factors include previous and direct experience, along with subjective norms. When it comes to computers it is important to relate both types of experiences to how much computer skill the user has. These computer skills can determine if the end-user is knowledgeable enough to navigate through any computer related problem. This could also be considered as computer Self-

efficacy. Computer self-efficiency " is the perception of an individual to use a computer to perform a particular function or task" (Computer Self-Efficacy, 1977). More often or not one's emotional response can have a negative impact which can affect the overall outcome.

Emotional Response

An email containing one or more of the keywords in a subject line in order to entice the user to copen it would be a good example of how a hacker would trigger a negative emotional response from the end-user. The physiological reason behind this suggests that "stress and anxiety can easily lead to poor or impulsive decisions online" (Tim Sadler, 2020). That is because "anxiety can disrupt neurons in the brain's prefrontal cortex that help us make smart decisions, while stress can cause people to weigh the potential reward of a decision over possible risks, to the point where they even ignore negative information" (Tim Sadler, 2020). However, the users themselves do not fully understand the risk in which they are taking by simply acknowledging and clicking on the phishing email.

Underestimating the Risk

People today think that they will never be hacked since the hackers are only targeting the big corporations. There are plenty of reasons why this thought process is illogical. While teleworking you might assume that your employer is handling all the cybersecurity for you. You might even still think in the popular

myth that “Apple computers can’t obtain viruses”. Unfortunately, both of those assumptions are wrong. For the end user, underestimating the risk of phishing attacks can be crucial since these types of attacks can do some serious damage to you and your network.

By clicking on the embedded link that is contained within the email then you are essentially giving the hacker your Personal Identifiable Information(PII). The hacker then takes your PII and starts impersonating you to your friends and family. The hacker would do this because the likelihood of people clicking on the link would be high since your name is familiar to them and that they would most likely trust your name. This sense of familiarity and trust would help the attackers to attract more victims. Sometimes the malicious email could contain some sort of virus and when opened could infect your machine. These infections can range from obtaining your passwords to encrypting your data with ransomware. No matter the situation it is very important that any user incorporates environmental factors in their daily routine to keep maintaining the upkeep and security maintenance of their machines. With the correct number of environmental factors in play it would definitely construct the subjective norm. The subject norm according to Dr. Ryan “represents the degree to which an individual is swayed by their perception of how people they respect believe they should act” (Ryna, 2010). Let’s go into detail on how the environmental factors can shape the subjective norm.

Environmental Factors

These environmental factors would most include some sort of communication. These types of communication would be very beneficial to the end-user because it would provide them knowledge with the most up to date information about the latest attacks and threats that are out there. Knowing these types of things would close the knowledge gap of the end-user so that their machines could be more secure. Family, friends, news, vendor, and work are the five most common places that an average user would establish their communication channel. There are advantages and disadvantages of each communication channel in which I would like to go over.

Family and Friends. Family and friends are an excellent communication channel since the average person according to Ben Renner “spends about 40 minutes a day talking to friends and family” (Renner, 2018). Both of your friends and family members will talk about the newest and greatest personal device out there which would pursue the end-user’s subject norm to obtain the latest and greatest device as it makes its debut. When the user obtains their new device then they would go and show it off at work.

Work. Showing off your new acquired device to your coworkers is a great way to establish communication between your coworkers that you are interested in technology. Now it would be very important to catch a conversation at the water cooler at work that has to do with news about the technology that you love.

News. There are many forms of news media that one person can follow to educate oneself about the technology that they process. The mainstream media would normally cover major releases about a product. Sometimes the news will cover major breaches that have happened throughout the technology industry. Normally, the vendor of the product will publish the latest news about releases and attacks that occur on their product.

Vendor. Traditionally, a user would travel to the vendor's site or newsfeed to find news about a certain product that they own or are interested in. In the 21st century these vendors have their own social media pages that people can interact with to obtain the news that they want at a moment's notice. In my opinion obtaining news from the vendor is the best way to go since it comes directly from the source. By bringing together both personal factors and environmental factors we can shape a positive behavior and habits in order to prepare for the next upcoming cyber-attack.

Behaviors and Habits

What is the behavior? One often asks what is the different behavior and habit? Why does one individual do things that should not have? Behavior is defined as the way one acts or conducts themselves. While a habit is defined as one's behavior in a routine to conduct or do something subconsciously. When behavior, environmental factors, and personal factors come together it is clear that a person can develop the proper approach to computer security and have a

better security plan than before implementing the Social Cognitive Theory. Behavior also plays apart in the Self-Regulation Theory.

Self-Regulation Theory

According to Positive Psychology “Self-Regulation Theory (SRT) simply outlines the process and components involved when we decide what to think, feel, say, and do” (Ackerman, 2021). SRT is the theory on how one controls themselves on a daily basis. For the purpose of this paper, we will be relating SRT to an individual who is confronted with a phishing attempt. Standards, motivation, monitoring, and willpower are the four contributing factors when it comes to SRT. The Standards part of SRT refers to the desirable behavior that an individual first comes up with in a given scenario. The motivation part of SRT are the contributing factors that are designed to motivate the individual to persuade one way. The monitoring factor is when the individual thinks about the current pros and cons of the situation in order to make the decisions. Finally, you have the willpower which is one’s internal strength to control one’s urge. SRT plays a big important part within cybersecurity. LTC Martin wrote that “Self-Regulation theory stems from the notions that cybersecurity of critical infrastructure is best executed when (1) private sector infrastructure owners voluntarily collaborate with the government cybersecurity efforts and that (2) the economic marketplace inherently drives owners toward Cybersecurity best practices” (Martin, 2016). Reducing the number of cyber-attacks is the motivation

behind the idea of “private sector infrastructure owners voluntarily collaborating with the government cybersecurity efforts ”(Marting, 2016). now if reducing the number of cyber-attacks is the motivation factor then it would need the willpower of the private sector owners to monitor the most up-to-date best practices for their company to follow within the cybersecurity industry. In order to understand why individuals, make those decisions we will need to take a look at the psychology behind self-regulation.

The Psychology Behind Self-Regulation. Professor Bandura a leading researcher in SRT states that “there are three parts to self-regulation which is a continuously active process in which we:

1. Monitor our own behavior, the influences on our behavior, and the consequences of our behavior.

2. Judge our behavior in relation to our own personal standards and broader, more contextual standards.

3. React to our own behavior (Ackerman,2021).

Within SRT comes another theory called Attribution Theory which deals with how people perceive the causes of everyday experience.

Attribution Theory:

Fritz Heider says that Attribution Theory is used to account for the way humans reconcile perceptions and observation in their quest for understanding" (Heider, 2015). Herbert Lin over at Stanford University wrote a paper on how Attribution Theory coexists within cyber-incidents. He simply says that "when it comes to Attribution Theory within cyber incidents the victim would like to know who is responsible" (Lin, 2016). Finding out who is responsible would be considered to be the quest for understanding. Attribution error is an unfortunate side of the coin when it comes to Attribution Theory. The unfortunate thing about Attribution error is that there are many internal and external factors that force individuals from understanding the whole picture.

Internal Factors

Each person is different in their own way. From beliefs, characteristics, and traits. Unfortunately, those things that make us different is what causes the individual to become blindsided from the truth from an internal factor. To overcome these internal factors from holding the individual back they must step out of their "comfort zone". When stepping out of the "Comfort zone" the individual must also expand on some external factors in order to see the whole picture.

External Factors

With 85 percent of Americans that own a smartphone it is common sense that they would follow some sort of news site to stay up to date. Usually, these news sources that the individual will follow would align with their beliefs. When these sources provide a likeminded individual with things that they like then they are responsible for keeping the whole picture away from that individual. One thing that external news sources would not cover are the constant attacks that keep on evolving over time.

Attacks Evolving Over Time

Attackers would start developing new attacks due to the response of their attacks being publicized. These attacks “will be designed to look more legitimate (Panda Security, 2021)”. These emails would target the user’s emotions and most importantly their wallets. The attackers are even broadening their horizon by crafting phishing messages for social media and SMS which is known as smishing. This is all to make their presence known and to achieve their goal in breaking the confidentiality, integrity, and availability of their target’s information.

With smishing attacks on the rise, it is important to understand the behavior and habit of these victims. The behavior and habit of the victims can play a crucial role in determining if the victims will be part of the statistic. Knowing that attacks are on the rise, it is best to educate the victims of this type of phishing scam to limit the behavior and habit that they often act on or

subconsciously. One of the best approaches to come up with is to have safety tools at a moment's notice.

CHAPTER FIVE:

TOOLS FOR STAYING SAFE

This chapter will be covering the tools for staying safe online. Designing these online safety tools will be introducing the “Cyber Hygiene Framework”. Within the Cyber Hygiene Framework, this chapter will be going over securing passwords, patching techniques, securing backups and user training which will contain its purpose, solution, and reference. Securing password will be covering password manager and it’s important. Patching techniques will cover security software and it's important. Security backups will cover backup solutions and why the user needs to have backups. Having user training will cover the idea that the user needs to have some sort of training to prevent themselves from falling into scams and keeping safe online.

Designing Online Safety Tools

Looking at the recent statistics of the silent and z generation, I came up with the online hygiene framework by adapting to several U.S. Government Framework. This framework is designed to help individuals to stay safe online and it is for all age groups. This framework is called “Cyber Hygiene Framework”. Figure four below will show three purposes and solutions to staying safe online. The first purpose is securing passwords and the solution would be to have a password manager. The second purpose is patch management, and the solution is to install the latest updates. The last purpose is keeping the machine clear of

virus and malware and the solution is by having security software such as antivirus or antimalware.

Table 5: Cyber Hygiene Framework

Purposes	**Solutions**	**Reference**
Securing Passwords	Password Manager	Consumer Reports
Patch Management	Installing Updates	Rapid 7
Keeping Machine clear of Virus and Malware	Security Software	Malwarebyte
Maintain information's availability	Backup solution	Norton
Overall Security Awareness	User Training	Federal Trade Commission

Securing Passwords

By taking a variety of sources and creating a guide for any generation to be safe online. Password security, Patching, and software installation are the three major recommendations that I would make to any user who would like to stay safe online. Password security is the use of having a combination password

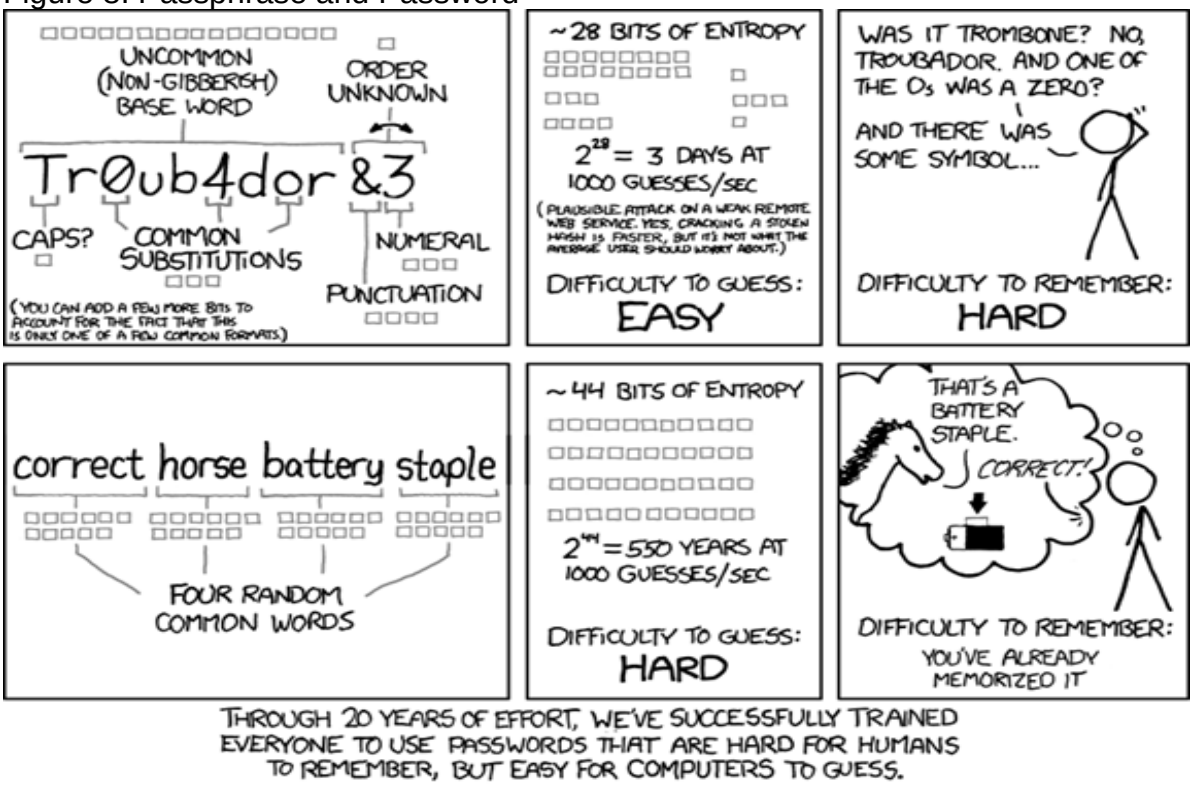
to limit the reuse of passwords. Patching machines would help to keep the machine updated from vulnerabilities and keep the machine on its latest version. Software installation will help to patch the vulnerabilities. Now I would like to go over why protecting passwords is important.

Jack Turner over at Tech Co published a study that NordPass conducted that reveals that “the average person has over 100 passwords to remember” (Turner, 2020). With 100 passwords to remember, there are bound to be password reuse and weak passwords. Password reuse is when you use one password for multiple accounts. When you (Tim Sadler, 2020) That is why I recommend that passwords are the first thing that any user should secure.

To secure your passwords I would recommend using a Password Manager. Andrew Chaikivsky over at Consumer Reports says that “a password manager will generate, retrieve, and keep track of super-long, crazy-random passwords across countless accounts for you, while also protecting all your vital online info—not only passwords but PINs, credit-card numbers and their three-digit CVV codes, answers to security questions, and more—with encryption so strong that it might take a hacker between decades and forever to crack” (Chaikivsky, 2017). There are even Password Managers out there that would generate a passphrase for you to use on any account. Both a passphrase and complex generated password will minimize the reuse of passwords and weak

passwords. Figure five below, will provide proof on passphrases and passwords used by a password manager.

Figure 8: Passphrase and Password



Source: xkcd 2019

Patching Techniques

Keeping the Operating System up to date with the latest patched would be the next recommendation that I would make to any user. According to Rapid7 If the user keeps their Operating System up to date with the latest patches “will

ensure that assets in your environment are not susceptible to exploitation “ (Rapid 7,2019). Finally, I would recommend for all users to install an anti-virus and an anti-malware software on their system. Malwarebytes sums up the function of these two products by stating “that both of these products refer to computer security software designed to detect, protect against, and remove malicious software” (MalwareBytes). Now I would like to go into detail about the most important thing that any user can do.

Securing Backups

Backing up personal information is critical for any user. In fact, Mr. Chivers over at Norton defines data backup as “a copy or archive of the important information stored on your devices such as a computer, phone, or tablet, and it’s used to restore that original information in the event of a data loss” (Chivers, 2021). A user can either backup their data locally or on the cloud. If the user chooses to do a local backup, then they would need to choose to do their backup on either removable media or an external hard drive. If the user decides to back up their information on a cloud, then they would choose from multiple cloud services such as Google Drive or Microsoft OneDrive. Finally, I would like to cover the most crucial thing when it comes to being aware of the ongoing security threats that are out there.

User Training

In the end, I truly believe that the biggest thing to do is to provide end user training. This user training will train the user on how to identify and respond to these types of social engineering attacks. The FTC published a list of six things that can help a user identify a phishing email. The six things are: “suspicious activity or log-in attempts, problems with your account or your payment information, confirming some personal information, includes a fake invoice, wants you to click on a link to make a payment, say you’re eligible to register for a government refund, or it might offer a coupon for free stuff” (Federal Trade Commission, 2019). Other things to consider would be to check the grammar and spelling of the email. This can be because the attacker might not be fluent in your language. This might present a problem because that crafted message might contain some common writing mistakes. If the user does come across a phishing message, then the appropriate action according to the FTC “would be to forward the message to either Anti-Phishing Working Group at reportphishing@apwg.org or to the FTC at ReportFraud.ftc.gov” (Federal Trade Commission, 2019).

CHAPTER SIX:

DISCUSSION AND FURTHER RESEARCH

This final chapter will be covering the results of the finding research questions, and further research. Based on the results of the finding, we know that the hackers around the world only want to manipulate the confidentiality, availability, and the integrity of information. This research goes into detail on the attacker's mindset when luring in their victims. AmTrust Financial points out that “the hacker’s job has become easier since teleworking has become the standard across various sectors” (AmTrust,n.d). Current routines of blindly clicking on links within meetings are no longer safe to either the silent generation or the generation Z users. Introducing a simple online hygiene framework along with persuading users to take cybersecurity seriously are two ways to solve this problem and add another line of defense in maintaining safety on the internet.

This project posed the following questions:

1. What techniques does online predators use to lure their unsuspecting victims?
2. On the American Generation Timeline (AGT), which generations are impacted the most and why?
3. What should be done to make the most affected generation(s) more secure?

Result 1:

Researching, Impersonating, Grooming, Taking Control, Intimidation, and Escape Plan are the five techniques that are used by malicious actors. Malicious actors will follow five techniques that form a model. This model helps the attackers scam their victims successfully and suggests that they can escape easily after exploiting the victim.

Result 2:

According to the discussion earlier on Silent Generation, the US Department of Health and Human Services (DHSS) released a statement that "COVID-19 Scams are impacting the elderly". With DHHS contributing to Rosenth's research in claiming that the elderly is being the main target in these COVID -19 scams. It is important that we establish some backing in how these COVID-19 scams have affected these senior citizens. In early 2019 Maggie Fitzgerald published a story that claimed, "that nearly $3 billion disappears from the wallets and bank accounts of senior citizens annually" (Fitzgerald, 019). There are many reasons why these scammers are targeting the elderly.

According to the discussion earlier on Generation Z, since the start of the pandemic we are seeing the academic scene adapted from in person classes to Zoom classes. With zoom classes going on it is apparent that children are spending more time on the computer and clicking links that they do not know the origins of, as a result a total of "41% of school district cyber security incidents and breaches were caused by phishing attacks" (Firch, 2021). The reports go on

and say that there were a “total of 455 cybersecurity incidents in the educational sector in 2020” (Firch, 2021). Now outside of the education space these children have also fallen for other phishing attempts on different platforms.

According to social cognitive theory, which is involved in individual decision making. A person’s personal factor, environmental factor and behavior plays a role in what made them become a victim. Based on Self-Regulation Theory which “outlines the process and components involved when we decide what to think, feel, say, and do” (Ackerman, 2021). If we monitor our behavior, the influence of our behavior and the consequences of our actions it will limit us from taking the bait. Which concludes that both the Silent Generation and Generation Z are the most vulnerable. Table 6 below outlines the sources to the generation which is most affected by.

Table 6. American Generation Timeline

Generation	Age Range (years)	Birth Year Range	Percentage of Cybercrime Attacks	Source of Percentage of Cyber Attacks
The Silent Generation	76 and over	1928-1945	50%	Aspen

Baby Boomers	57-75	1946-1964	9%	Phishing Tackle
Generation X	41-56	1965-1980	19%	Phishing Tackle
Millennials	25-40	1981-1996	11%	Phishing Tackle
Generation Z	9-24	1997-2012	12%	Phishing Tackle
Generation Alpha	0-8	2013-present	8%	comparitech.

Result 3:

Using a combination of password protection, patching techniques, and software installation would help minimize the number of victims that would be affected. Using a combination of password protection such a password manager can help to minimize weak password and password reuse. Using a password manager would help to organize the accounts and passwords without having to write it down. Patching and installing the latest update can help to prevent zero-

day vulnerabilities and can keep the machine clean from malware and viruses. Having a security software will help to clear the computer of a malware and virus.

With the evolving world of information technology and the bad actors who wish to manipulate it for their own use, there are many more steps that a user can take to strengthen their security. Further research is needed since the future of the unknown of the tools and techniques that a malicious actor would use.

Limitations

The limitations of this research project would be not having enough latest databases to cover phishing attacks on Silent Generation and Generation Z. Furthermore, other limitations can include not having enough individuals to volunteer to conduct survey data to back the research. Not having enough knowledge on psychological cognitive studies to conduct further backup on the mindset of Silent Generation and Generation Z. Lastly, due to the limitation of searches using English language terms and could not conduct more findings.

Suggested Future Research Topics

A great way to extend this study I would suggest six topics that would go well with this topic. The first topic is the psychological study of why people in both the Silent Generation and Generation Z are more prone to phishing attacks. The second topic would be a study of the impact of cyber-attacks on the victims. The third topic is to outline the best practices for social media since the majority of Generation Z victims use some sort of social media in their daily lives. In

addition, another area for further research to consider is how can you automate the protections provided in this study and what can you do to prevent these victims from becoming another one of the statistics. In addition, I would suggest considering looking into why these victims accept the risk knowing these phishing links are not safe. Moreover, another future research area is to investigate the prevalence of phishing scams through direct messages that lead to cyber bullying for Generation Z.

REFERENCES

Federal Trade Commission. (2019, May). *How To Recognize and Avoid Phishing Scams.* Retrieved from Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Federal Trade Commission Federal Trade Commission Consumer Information. (2019, June). *What You Need To Know About Romance Scams.* Retrieved from Federal Trade Commission Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams

Firch, J. (2021, April 29). *2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends.* Retrieved from purplesec.us: https://purplesec.us/resources/cyber-security-statistics/

Fitzgerald, M. (019, Feb 13). *Scams cheat older Americans out of almost $3 billion a year. Here's what to watch for.* Retrieved from CNBC: https://www.cnbc.com/2019/02/13/older-americans-lose-almost-3-billion-a-year-to-scams.html

Ghosh, I. (2021, May 7). *Timeline: Key Events in U.S. History that Defined Generations. Retrieved from Visual Capitalist:*

https://www.visualcapitalist.com/timeline-of-us-events-that-defined-generations/

Google. (2021). *Google Safe Browsing.* Retrieved from Google Transparency Report: https://transparencyreport.google.com/safe-browsing/overview?hl=en

Inspector, U. D. (2021, March 25). *Fraud Alert: COVID-19 Scams*. Retrieved from hhs.gov: https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/

Kratikal . (2020, December 7). *Staggering Phishing Statistics in 2020.* Retrieved from Kratikal : https://www.kratikal.com/blog/staggering-phishing-statistics-in-2020/

Laudon, M. (2020, November 02). *Mobile Phishing Increases More Than 300% as 2020 Chaos Continues.* Retrieved from proofpoint: https://www.proofpoint.com/us/blog/threat-protection/mobile-phishing-increases-more-300-2020-chaos-continues

Miller, M. (2020, December 2). *Scammers step up efforts to target older Americans during pandemic.* Retrieved from The Hill: https://thehill.com/policy/cybersecurity/528259-scammers-step-up-efforts-to-target-older-americans-during-pandemic.

Panda Security. (2021, 25 January). *Why do people still fall for online scams?* Retrieved from pandasecurity: https://www.pandasecurity.com/en/mediacenter/mobile-news/funeral-directors/

Parker, K., Menasce Horowitz, J., & Minkin, R. (2020, December 9). *How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work.* Retrieved from Pew Reearch Center: https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/

Posted By HIPAA Journal. (2018, December 17). *Study Highlights Seriousness of Phishing Threat and Importance of Security Awareness Training*. Retrieved from HIPPA Journel : https://www.hipaajournal.com/study-phishing-security-awareness-training-employees/

proofpoint. (2o21). *What is Smishing?* Retrieved from ProofPoint: https://www.proofpoint.com/us/threat-reference/smishing

Rosenthal, M. (2021, May 17). *Must-Know Phishing Statistics: Updated 2021.* Retrieved from Tessian: https://www.tessian.com/blog/phishing-statistics-2020/

Security Magazine. (2021, February 25). *Cybercrime report finds young adults and adults over 75 most vulnerable to fraud attacks.* Retrieved from

SecurityMagazine: https://www.securitymagazine.com/articles/94684-cybercrime-report-finds-young-adults-and-adults-over-75-most-vulnerable-to-fraud-attacks

Sharma, R. (2020, 11). *Cybercriminals Take Advantage of Increased Use of RDP During COVID-19 Telework.* Retrieved from TechCrack: https://www.techcrackblog.com/2020/11/cybercriminals-take-advantage-of-rdp.html

Solomon, K. (2021, March 16). *Are your kids remote learning? They could be the target of identity theft.* Retrieved from Yahoo: https://www.yahoo.com/lifestyle/child-identity-theft-norton-security-online-210701863.html