Michael Burns

CSC301-01

Professor Ola Ajaj

Cybersecurity Speech

Identity theft is the fastest growing cybercrime in the United States and affects million of innocent users each year. In fact, according to the Federal Trade Commission, identity theft incidents have reached 9.9 million cases per year. This cybercrime is one of the worst because an attacker can steal all of your information and legitimately acts as you. They can commit crimes as you, open bank accounts and credit cards as you. How do you prove it’s not you? How do you prove who’s who? Unfortunately, hackers are getting better day after day and finding the flaws behind new securities and exploiting them for their own good.

Resolving an identity theft attack is quite difficult, complex, lengthy and costly. For every incident of identity theft, it takes about $500 and 30 hours to resolve the attack. There are almost 10 million identity theft attacks every year, each on average taking about 30 hours and $500 to resolve. That’s a lot of time and money each year dedicated to resolving these attacks. This money and time can be put elsewhere to prevent these attacks from happening in the first place. Most of these attacks come down to user error, however, identity theft attacks can still occur if a cybercriminal was to hack an organization that has your information. They would break into the database and can access all the information the organization has about you. Anything from your name or email address all the way to social security and credit card numbers (if not using end-to-end encryption).

I have been a victim of identity theft on a few occasions. Most of the time I find out about my information being leaked is from my iPhone. In the Keychain (or password manager), if my password has been compromised in a data breach, Apple notifies you immediately and encourages you strongly to change it. This unfortunately has happened many times to me, however, Apple is trying to put an end to the theft. They want you to try to change your password as soon as possible so the hacker’s cannot sell your information or use it to their advantage. Apple cannot force you or deactivate your account if they know you password for a website has been breached, but these are steps in the right decision.

My first incident with identity theft happened in the fall 2018. I had ordered some new computer parts from an online computer retailer called Newegg. They are a popular tech company known mainly for selling computer parts and other electronics. About a month after I made my purchase, I had a notification from my bank, saying my account was frozen until I called the bank and spoke with them about a suspicious charge. I thought this was phishing at first, but I received a letter in the mail the next day stating that notification. When I called the bank, they asked me if I made a transaction at a foreign travel agency for over a thousand dollars. Obviously, I did not make this transaction, and the bank canceled my debit card, sent me a new one and reversed the transaction. A few days after I received my new debit card, I had a letter from Newegg notifying all it’s customers that there was a data breach. The letter also strongly recommended that you change your password on the website, as well as to check credit card statements from a few months back to make sure there is no suspicious activity.

Thankfully, this issue was caught and resolved quickly, and didn’t evolve into anything more severe. It is still alarming to think how much of your information is just out there on the dark web, and has been stolen by hackers. I always use PayPal whenever I make online purchases to make sure that my transaction is as secure as possible. Everyone always has to look out for their online purchases, stay proactive at checking credit card and bank account statements for any suspicious activity. Check your password manager often to make sure your passwords have not been compromised or leaked in a data breach, as well as do not reuse the same password ever.

One cyberattack that leads to identity theft is phishing. Phishing is a cyberattack where a threat actor sends an email that looks legitimate, but is used to steal your information. The attacker uses deception to trick people into clicking on an official looking email. For example, the email might say that there was an issue with your Facebook account and to click a link to fix it. The link will redirect you to a website that has a very similar domain name to Facebook, but the spelling will be off by a letter or two. That is called the second-level domain (“facebook” in [www.facebook.com](http://www.facebook.com)). Another hint that gives away it is a fake website is the top-level domain will be different. The top-level domain is after the second-level domain, examples are “.com”, “.gov”, “.org”, etc. The website might say “facebook.org” instead of “facebook.com”. Many people do not look out for this, or the misspelling in the top-level domain.

Unfortunately, phishing attacks are most likely the cyberattack that, almost nowadays, everyone is taught to avoid. Yet, most cyberattacks, more than eighty percent, are phishing. Hackers have gotten clever when it comes to making these emails look legitimate. Unless you are technologically advanced and know what to spot, a good phishing email will trick most people.

I believe that every person with an email address has experienced phishing attacks almost once a week, if not more. Most of them get caught in the spam mail folder of your email, but the ones that make it through can look pretty deceiving. I would get some that would be tagged as “important”, and since they’re an “important” email, I get a notification on my phone. That always makes me believe the email is legitimate, however, when I read through the email I discover its flawed.

I noticed that the most phishing emails were going around during the COVID-19 pandemic. It is sad to think that in such a trying time, people would manipulate the situation for their own good. When school, work and every aspect of our lives went remote, many people had to adapt to technology they were unfamiliar with. My math professors at the time at community college never used the school’s online web portal unless it was for class roster or inputting grades. All the homework, notes and reference sheets were a physical copy. Not to go off on a tangent, but this is the way math should still be taught, and trying to do math on a laptop is a battle in itself.

These phishing emails were based upon so many issues going around during the pandemic. From unemployment monies to masks and fake vaccine waitlists, there was just about a phishing email that tricked people throughout the pandemic. There was so much panic and fear, and majority of society was not trained at the time to look out for phishing attacks. My parents would come up to me almost every day saying that received an email to be put on a waitlist for the vaccine or to sign up for the stimulus money. I told them every time to not click on the email, and to come to me whenever they see something suspicious like that.

West Chester does a good job of notifying it’s students of a phishing email. Whenever we receive one, usually within the hour, the IT department sends out a notification about a fake email and to delete it. Deleting it is the best way to avoid any repercussions because there is still the chance you can click on it accidentally on your smartphone. When I attended community college before I transferred to West Chester, I would get many phishing emails. However, the IT department was not as quick at notifying students of the email. One time, back in the fall semester, the IT department emailed all faculty and students about a phishing email a week after it was sent. Most students check their email inbox daily, so this is way too late to try to prevent any misconception.

My dad works for a larger natural gas company based out of New Jersey. There is a fairly large corporate authority above him. He works as a natural gas technician, but there is so much technology he deals with. All employees have company issued laptops, smartphones and cellular data in all their service vehicles. All the material ordering, manuals for meter sets and paperwork is fully online. Even the monitors on the meter sets can now be checked on an application via Bluetooth when in close enough to it.

The IT department at his company is large with respect to the size of the entire company. Every week, there is a training on some form of technology – whether that be a new trick in Microsoft Office or updates of a new cybersecurity attack. The IT department will actually make phishing emails, and send them to all employees and staff in the company to see who clicks on it. Those who click on it are noted and are required to take an hour long course on phishing attacks, as well as a quiz before they are able to return to work.

Evolution of Malware

The evolution of technology has come a long way since the first electronic, fully programable, digital computer was invited in 1943 by Alan Turing (Bricsys). Computers have improved drastically over the past 50 years, and the most improvement has been made within the past twenty years. However, the idea of the computer has been around since the ancient Greek ages. It was not an electronic computer, however, it was a hand-powered mechanical device that archaeologists believe was used to calculate astronomical events, like eclipses. It was called the Antikythera mechanism and was developed around the years 200 BC – 70 BC (Bricsys).

There were other computers invented before Turing’s, however, what makes Turing still relevant to today’s computers is that his was the first fully electronic, programmable and digital (Bricsys). The most important being the programmable part. The reason this is the most important aspect of the computer is because everything we do on a modern-day computer is programmed by a software developer. Starting with the operating system the computer uses, to the network devices used to communicate from one side of the world to the other, and everything application used on the computer- it’s all programmed.

Another reason the programable aspect of the computer is crucial is due to the newest form of crime- cyberattacks. Just how a computer is programmed to do some of the most helpful factors of society, like calling help during an emergency or being able to attend school and talk to loved ones during a pandemic, there is a malicious side to programming. Malware is software that is designed to cause disruption and/or harm to a computer or network of computers to gain unauthorized access or leak private data (Cisco).

Malware attacks started getting more complex and severe starting in the early 2000s. One notorious attack was called the SQL Slammer. The attack occurred in 2003, and the type of malware was a worm. A worm spreads by itself to perform malicious actions on other computers, and unlike other types of malwares, does not need to be embedded in a computer program (Shareef). SQL is a type of programming language that is designed for relational database management system, or basically to store data in a database.

The SQL Slammer exploited a vulnerability in Microsoft SQL Sever 2000 software. It manipulated an unpatched issue in the buffer overflow, which deals with writing data to memory locations. The hacker was able to use the buffer overflow vulnerability to infect SQL servers and systems that were running the unpatched version of Microsoft SQL Server 2000 (Shareef). This was one of the fast spreading attacks, bringing the Internet to a standstill for a few hours. Some devices affected by this denial-of-service attack were Bank of America’s thirteen thousand ATM machines, and knocking out cell phone coverage for an estimated twenty-seven million people (Shareef).

This attack occurred in 2003, and affected a lot of people at the time. Fast forward nearly twenty years later to the present, and we can see the correlation between the improvement in technology as well as the severity of cyberattacks. One of the most recent cyberattacks was during the 2022 Russian-Ukrainian war. This is an issue the cybersecurity community is currently facing. Both countries are focusing their efforts heavily on cyberwarfare, to the extent that both these countries are trying to hack into each other’s power grid to cause wide-spread blackouts. As far at the media knows, both countries have hired third-party organizations to hack the other countries’ infrastructure. It is shocking to see how the evolution of and progression of technology is now a main component of warfare.

There is a plentiful amount of issues the cybersecurity industry is facing today, and everyday. It almost seems that there is a new cyberattack everyday, and cybersecurity professionals work around the clock to resolve the threat. An cyberattack that exploits a vulnerability that has not been patched, nor is there a solution to resolve the issue, is called a zero-day attack (Check Point Software). Zero-day attacks are arguably the most severe type of attack because the attack is so new that cybersecurity professionals are not quite sure how to go about resolving it (Check Point Software). This gives the hackers the upper hand, and makes them more powerful in their malicious acts.

Another issue the cybersecurity community faces is ransomware. While this attack is nothing new, it is very costly to resolve. Data is now so valuable, whether it is personal or belongs to a company. A hacker can charge any amount they want to turn the data back to its respective owner. According to an independent study conducted with five-thousand information technology managers across twenty-eight different countries, the average cost to resolve a ransomware attack was $622,596.18 (Cyber Security News Daily). Yes, over half a million dollars, on average, to resolve an incident of ransomware.

Malware authors, those who write the code to make malware, are increasing drastically. While there is no actual statistic to how many malware authors exist, we can estimate the rising number by the amount of new malware produced. One of the main goals of a malware author is to make the code for the malware so discrete that it cannot be traced back to them, or another party that uses it. They precisely craft their code in a way that avoids reverse engineering it, or being detected (Malware Author).

While this statistic is somewhat outdated, it does give insight to the vast amount of new malware being developed. According to McAfee, one of the largest anti-virus companies, the number of unique malware binaries during November 2007 was under four million. A little over a year later, in December 2008, the number of unique malware binaries rose to an astounding sixteen million (Malware Author). In the span of that year, the amount of malware quadrupled. As stated earlier, there are currently no statistics to the amount of malware authors, but to quadruple the amount of malware in a year, there has to be a lot of new developers.

One reason that we do not know the exact number of malware developers is due to importance of their role. The first priority of a malware author is to develop malicious code for another party to purchase, and use for whichever activities they would like. The second priority is to make sure that their code is untraceable, and their identity is hidden (Malware Author). Since developing and selling malware is very illegal, getting caught ruins the entire operation.

Malware authors are overall motivated by one thing, the same reason most people conduct business, legal or illegal, and that is more money. Coding is a lucrative career, it is one of the fastest growing legitimate careers with so much potential for growth. The salary, benefits and overall job satisfaction are some of the highest within the software development field. Being able to use the code for illegal activities definitely adds some value to coding. Especially, in a day and age where someone is willing to good money to use the malware however they choose to.

Referring back to ransomware attacks, it costs on average over half a million dollars to resolve a case of ransomware. If the malware developer writes the code for the ransomware attack, they can charge the victim as much as they want for them to recover their data. If one ransomware attack earns a hacker over half a million dollars, that is more than the average software developer will make in three years. Money is a motivator, and it is also the root of all evil.

New and emerging technology is exciting. It is always intriguing to see what’s new and the advances technology makes increase our life satisfaction. However, the newer the technology is, the more likely there are unpatched portions of the software, and the more likely there will be a zero day attack. This is one thing hackers look out for because a company has to meet a deadline to push out a new product for its customers, and usually has to cram everything in. Employees get very stressed and burned out, and it is easy for them to miss a vulnerability that a hacker can notice quite easily.

Works Cited

Barfield, Rose. “Who Invented Computers?” *Bricsys CAD Blog*, 14 Apr. 2021, blog.bricsys.com/who-invented-computers.

“Biggest Cyber Security Challenges in 2021.” *Check Point Software*, 31 Mar. 2022, www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2021/#:%7E:text=The%20leading%20cyber%20security%20challenges,like%20the%20COVID%2D19%20pandemic.

“Just a Moment...” *Malware Author*, [www.sciencedirect.com/topics/computer-science/malware-author. Accessed 21 Apr. 2022](http://www.sciencedirect.com/topics/computer-science/malware-author.%20Accessed%2021%20Apr.%202022).

Shareef, Tashreef. “The 8 Most Notorious Malware Attacks of All Time.” *MUO*, 16 Sept. 2021, [www.makeuseof.com/most-notorious-malware-attacks-ever](http://www.makeuseof.com/most-notorious-malware-attacks-ever).

“What Happens in a Ransomware Attack?” *Cyber Security News Daily*, 27 Nov. 2021, cybersecuritynewsdaily.com/what-happens-in-a-ransomware-attack.

“What Is Malware? - Definition and Examples.” *Cisco*, Cisco, 1 Apr. 2022, https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html. (what is malware)