CYBERSECURITY

HOW DOES IT AFFECT ME AND HOW CAN I KEEP MYSELF SAFE?

WHAT IS CYBERSECURITY?

"Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."[1]

Cybersecurity is becoming an ever-increasing need in today's society. With the increase in use of technology it is important to make sure our personal information isn't stolen.

This Photo by Unknown Author is licensed under CC BY-SA-NC

WHAT DOES IT HAVE TO DO WITH ME?

Cybersecurity is a broad field that covers every aspect of life, from work to home. Keeping ourselves and our families safe from cyber criminals should be a top priority. Cyber criminals could manipulate people into giving up credit card or bank account information, sensitive information about their company, and much, much more. The effects of this information being obtained by cyber criminals can range from loss of money to identity theft. With technology becoming more and more a part of our everyday lives, it is important to stay vigilant and informed on how to avoid becoming a victim to cyber crimes.

CYBER THREATS – PHISHING

"The term phishing defines attempts by outside parties to gain access to private information about users."[2] This includes login credentials, credit card numbers, bank information, etc. The hacker can use emails, text messages, and phone calls to accomplish this task.

Have you ever gotten or heard of someone getting an email from an African prince whose money was tied up and he needed to borrow some of your money to free up his money then he'd pay you back? This is an example of a phishing attack. They would get you to send them money or bank information. Another form is an email from 'your bank' telling you of a problem that needs instant action on your part. They might have you click a link from the email to a website that looks like but isn't your bank's website. Then you'd enter you bank account information, and the hackers would be able to access your bank account and withdraw money, make transactions, etc.

CYBER THREATS – TYPES OF PHISHING

STANDARD PHISHING

Phishing tends to be mass produced methods to get at a lot of people all at once. The victims are usually random individuals not targeted specifically. For example: an email from a certain, big bank (not actually from the bank) could be sent out to several thousand randomly selected emails. Even if only a small percentage of the people fall victim, the hacker(s) could still reap a large sum of money.

SPEAR PHISHING

Spear phishing is a type of phishing that targets individual people or organizations. The goal of these phishing attacks is for more specific information such as trade secrets, financial gain, or military intelligence. Often these emails look like they are from someone the person knows. This can cause the victim to drop their guard and fall for the trap.

WHALE PHISHING

Whale phishing targets high-profile employees, such as the CFO or the CEO. The intent of these attacks is to obtain highly sensitive and/or vital information. The hacker could also manipulate the victim into making a high-worth wire transfer to himself.

CYBER THREATS – MALWARE

"Malware is also known as malicious code or malicious software. Malware is a program inserted into a system to compromise the confidentiality, integrity, or availability of data. It is done secretly and can affect your data, applications, or operating system."[3]

Malware compromises the integrity of the system it infects. The data can then potentially be stolen, deleted, or held for ransom.

CYBER THREATS – TYPES OF MALWARE

RANSOMWARE

Ransomware is a type of malware that prevents access to a user's data, sometimes threatening to delete the data if the ransom is not paid. The hacker will encrypt the data and request the ransom to give you the key to unencrypt it (though there is no guarantee they will give you the key when the payment is received).

DRIVE-BY ATTACK

A drive-by attack is another way of distributing malware. A hacker will look for an insecure website and put malicious script into the website's code. This can cause malware to infect anyone's computer that opens this website or redirect the victim to a website controlled by the hacker.

TROJAN HORSE

A Trojan is a malicious program that masquerades itself as useful software. They persuade people to install the program by making itself seem like routine software. Once installed, it infects the computer with the malware. Often Trojans are designed to steal financial information.

CYBER THREATS – OTHER

PASSWORD ATTACKS

A password attack is simply an attempt to crack or obtain a person's password with illegal intentions. There are a couple different methods to do this, including brute-force and dictionary attacks. These attacks repeatedly guess a person's credentials for a website or service until they guess correctly. The hacker's program can guess between 100 and 1000 times each second. After hours or days the hacker can have your account information.

EAVESDROPPING

"An Eavesdropping breach, also known as snooping or sniffing, is a **network security attack** where an individual tries to steal the information that smartphones, computers and other digital devices send or receive[.] This hack capitalizes on unsecured network transmissions to access the data being transmitted. Eavesdropping is difficult to detect since it doesn't cause abnormal data transmissions."[4] For instance, if you do banking transactions over an unsecure network (like at a coffee shop), an eavesdropping attack could send the information you send to the bank (your account information) to the hacker. Now the hacker has access to your bank account.

HOW DO I KEEP MYSELF SAFE?

All cyber threats range from easy-to-spot to hard-to-detect. For example, phishing emails tend to have a lot of traits that differ from the type of email they are trying to imitate. This makes most phishing attacks easier to identify. Keeping passwords complicated, not sending or receiving sensitive data on an unsecure network, and not clicking links in emails: these are some of the many ways to protect yourself and your data.

HOW TO KEEP YOURSELF SAFE

- If you receive an email that looks off, check to see if it is a phishing scam. Here are some of the traits most phishing emails and attacks have:
  - Poor spelling and grammar (If an email is from someone important [like a bank] they will have correct spelling and grammar.)
  - Requests for personal information (If anyone emails you asking for sensitive information, ignore the email and call the person/company. This also determines whether the email was or wasn't a phishing attack.)
  - An offer is too good to be true
  - You're asked to send money to cover expenses
  - Unrealistic threats
  - It appears to be from a government agency (They will typically use mail to contact the public.)
  - The tone of the email appears to be urgent
- Always keep your antivirus software up to date.
- Regularly back-up your data.

HOW TO KEEP YOURSELF SAFE (continued)

- Never open links from an email. If you want to visit the website, type the URL in your browser directly. Links to websites in phishing emails can lead you to a website manned by a hacker.
- "Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Don't share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor."[5]
- Never do sensitive browsing (such as banking and shopping) on a network that is not secure (like free WIFIs).
- Monitor your accounts for suspicious activity. If you see anything unfamiliar, it could mean your account has been compromised.

HOW TO KEEP YOURSELF SAFE (continued)

Keep in mind that the field of cybersecurity is always expanding and changing. As the technical world advances, new methods are created to combat the adapting cyber criminals. This makes it very important to remain informed on new ways to keep you and your personal information safe in this all-the-more tech savvy culture.

[1] Lord, Nate. "What is Cyber Security? Definition, Best Practices & More." *Digital Guardian*, 15 July 2019, digitalguardian.com/blog/what-cyber-security. Accessed October 2019.

[2] Dobran, Bojana. "Preventing a Phishing Attack: How to Identify Types of Phishing." *PhoenixNAP*, 11 Jan. 2019, phoenixnap.com/blog/what-phishing-attack-how-to-identify-protect. Accessed October 2019.

[3] "Types of cyber threats." *Mass.gov*, www.mass.gov/info-details/types-of-cyber-threats. Accessed October 2019.

[4] Dobran, Bojana. "17 Types of Cyber Attacks To Secure Your Company From in 2019." *PhoenixNAP*, 21 Feb. 2019, phoenixnap.com/blog/cyber-security-attack-types. Accessed October 2019.

[5] Drapala, Kara. "Top Ten: The Most Important Cyber Security Tips for Your Users." *Cisco*, 8 Oct. 2013, umbrella.cisco.com/blog/2013/10/08/top-ten-important-cyber-security-tips-users/. Accessed October 2019.

Cucu, Paul. "How 4 Types of Cyber Threats Break Your Online Security." *Heimdal Security*, 10 May 2017, heimdalsecurity.com/blog/cyber-security-threats-types/. Accessed October 2019.