100% (A)

Building a Safe Cyber World

Luke Albert

CYSE 426

Professor Karahan

 As technology keeps rapidly advancing so do cyber attacks and cyber defenses. Every thirty-nine seconds there is a new cyber attack going on and there are about thirty thousand cyber attacks per day. The cost of cyber attacks this year in 2022 totals 7 trillion dollars in damage [1]. With new malware and malicious codes being created every day it is good to stay safe and practice safe cyber habits. There are a lot of different attacks and malware that are commonly used on the internet such as worms, botnets, phishing attacks, ransomware, spyware, viruses, and trojan horses. There are many ways to avoid being hacked and attacked by these types of malware. Besides attacks, many materials on the internet can damage and corrupt children’s brains and rewire the way they think. Almost everyone has a way to access the internet so simply not going on the internet is out of the question about how to be safe from the dangers in the cyber world. There are many ways to stay safe and avoid having critical personal and financial information stolen. There are also ways we can protect kids from seeing things that they should not see online.

 Before I talk about how we can be safer when exploring the internet I must go over the dangers and why it is a need to be safe and cautious when online. Trillions of dollars are lost every year due to cyber attacks and that number skyrockets even higher every single year. Cyber attacks are evolving and attackers are becoming smarter and smarter every day. Denial of service attacks are one of the most common attacks and it is an attack targeted at a website or network to shut it down making it inaccessible to the users. This attack isn’t necessarily damaging to the people trying to access the website but it can be extremely damaging to the company that owns the website or network being attacked. Another common attack is phishing attacks. These can be done through email, text messages, and even over a phone call. Phishing attacks are a type of social engineering attack where the attacker usually tries to get the victim’s passwords, personal information, and financial information. Phishing attacks are one of the biggest ways a ransomware attack is launched. Another common attack is an attack trying to obtain a victim’s password through a password-cracking tool such as John the Ripper. These types of attacks work well on users with weak passwords or the same password for multiple different accounts. Man in the Middle attacks is another common attack where the attacker will eavesdrop and hijack the victim’s connection to a host and is able to steal data. There are many different types of attacks that can be used, however, there are many ways to stay safe from these malicious attacks.

 Denial of service attacks can cause a lot of damage to the companies being attacked. These attacks will block out customers from being able to use the company’s website who is being attacked. This can cause the company to lose out on a lot of sales and even lose customers to other competitors. Attackers who use denial of service attacks typically use what is called a botnet to send many requests to a company’s server IP address causing it to slow down or stop working. These attacks on average cause services to go down for an hour thirty-three percent of the time, causes the services to be down for less than a day sixty percent of the time, and even can cause the services to be down for a month fifteen percent of the time [2]. Data breaches are uncommon in denial-of-service attacks typically the victim suffers a loss of business, loss of customers, and time and money trying to get the servers working again. These attacks don’t affect a single person, but they are typically targeted at businesses and companies. There are a few ways a business and company can prepare for and prevent a denial-of-service attack. One of these ways is to have a DDoS response plan. Having a DDoS response plan and having employees know what to do in case of an emergency can help mitigate damages from an attack. A higher level of network security is a way to prevent these attacks. Having firewalls and web security tools that can detect unusual amounts of traffic and able to shut down that traffic is useful to have in order to prevent an attack. Having multiple servers can also be useful because if one server goes down then the company can rely on the backup server while they try to get the first server back online. DDoS attacks are becoming more dangerous and common every year so preparing for these attacks and having the best security measures in place is a top priority for companies.

 One of the most damaging and dangerous yet common attacks is phishing attacks. There are many different types of phishing attacks that are used. One of the phishing attack methods is email phishing. These attacks are fake and malicious emails impersonating someone or impersonating a company. These phishing emails will prompt the victim to go to their website or open an attachment in the email and then install malware onto the victim’s computer or have them open a fake website and display their personal or financial information to be stolen. A way to avoid these is to be weary of malicious-looking emails and to never open a link or attachment through an email. Always type in the web browser into the URL to make sure it is the correct website and not a fake one set up by an attacker. These emails will look like it is sent from amazon or another company but in reality, it is sent from an email address that isn’t legit at all. Another type of phishing attack is a smishing attack. Smishing attacks happen over text messages or other chat messages. These attacks will provide urgency and may act like a company sending a link for the user to click on and enter personal information. Never open these links and never enter information into these links because they can be malicious and steal information. It is good to instantly block the sender and delete the text message. These smishing attacks can be on social media sites as well to lure people into clicking links to steal their account information. The third type of phishing attack is called vishing. These attacks occur on a phone call and the attacker is posing as a company or vendor asking for money with urgency. These attackers may also act like a bank calling their customers prompting for information such as name, address, credit card information, and even social security numbers. Never give out personal or financial information to a stranger on the phone. Always make sure the number is legit and if they are asking for personal information it is best to hang up and call the real company to see if it was a real call or a scammer. Phishing attacks can also lead to ransomware where the attacker will shut off a computer or network and ask for a certain sum of cash to unlock the systems. These attacks can happen if a victim clicks on a malicious link or attachment that has a virus or trojan horse attached to it. These viruses or trojan horses can then shut down the computer or grant remote access to the attacker and allow them to do what they please. It is best to stay safe and stay away from malicious callers, emails, and text messages and never open any links or attachments sent unless from a trusted source. Always enter the URL into the search bar for the best case of security.

 There are many password cracking tools on the internet such as John the Ripper and hashcat. These tools can help a hacker obtain a victim’s password. The best way to avoid these attacks is using a two factor authentication system to where the site prompts the user to verify their identification. The hacker then cannot get into the account without being able to verify, unless the two factor authentication is linked to the user’s email and the hacker has access to the user’s email account. One way the hacker would be able to get ahold of the victim’s email and password for the account trying to be hacked is by repeating passwords. Repeating passwords is one of the most unsafe cyber practices a person can have. Having different passwords for different accounts and websites make it harder to be hacked. This way if a hacker obtains one password they do not have all passwords. Another way to avoid having passwords stolen and hacked is to have very strong and unique passwords. Simple passwords such as “fox123” are terrible passwords because hacker tools can break into them very fast. Having a long password with a mix of uppercase and lowercase letters with numbers and symbols is the best way to have a strong password. Leave out personal information or dictionary words in passwords and make it complex and long to have a secure account. It can be hard to memorize different passwords for different sites and accounts so it can be good to have a list of passwords in a secure location. It wouldn’t be wise to have a piece of paper with all of the user’s passwords on the desk out in the open, but if the user has the paper and keeps it secure this can be a very safe password saving method. There are also password encryption apps that can store passwords however if this app gets hacked or breached then all of the passwords would be leaked and unusable.

 A mailman is delivering packages and sees a letter from the bank to a house on the route. The mailman then opens up the bank letter and sees the victims personal and financial banking information. The mailman then writes everything down and seals up the letter so it looks like no one messed with it and he then delivers the letter. This would be equivalent to a man in the middle attack. Man in the middle attacks is another dangerous attack that more people need to be aware of and cautious about. A man in the middle attack is an attack where the attacker will place himself in between a victim and the application the victim is trying to use. These attackers can create fake hotspots that look like free Wi-Fi spots for victims to connect to and have their information stolen. These attackers can also join in a public Wi-Fi spot that has no password and eavesdrop on others who are on the same Wi-Fi. Some of the best ways to avoid this kind of attack are to never use public Wi-Fi that doesn’t have a secure password, never access sensitive or confidential information through a website such as a banking app while using public Wi-Fi, log out of any applications not being used and lastly make sure the browser notifications are saying the websites are secure.

 Children can also be exposed to harmful things on the internet. Younger kids do not know the precautions to take while on the internet. Kids are more prone to being hacked because they aren’t yet aware of the risks online and are more gullible to click sketchy links when they pop up. Having an anti-virus installed on computers that can block malicious links and websites will help against cyber threats. Cyber attacks and hackers aren’t the only things that are dangerous to kids on the internet. There are many explicit, violent, and graphic images and videos online that can be harmful to those who watch, especially children. Setting control limits on kids’ computers is a way to block out these harmful websites and videos. A lot of systems have built-in kids’ settings that can be selected and will automatically block out eight-teen-plus websites. With anti-virus protection and kids’ settings, children will be safer from malicious and damaging websites and links.

 There are many dangers to watch out for while on the internet. There are hackers waiting to steal personal and financial information, shut down businesses, and steal money. There are many tactics these attackers use in order to gain information and data. One of these attacks is the denial-of-service attack. These attacks are targeted at businesses to shut down their network and business temporarily. These attacks can be prevented by having a good firewall and web security tools that can detect internet traffic. One of the more common and dangerous attacks is a phishing attack. These attacks are where the attacker acts as someone with authority to target people to steal their money and personal information and data. There are multiple different types of phishing attacks including email phishing, vishing, and smishing. These three attacks are through email, voice calls, and messenger. The attacker usually has urgency needing the task they ask for immediately, or the attacker may be acting as someone else such as amazon asking the victim to log in to steal the victim’s login and personal accounting information. These attacks can be avoided by never clicking links sent in emails or messages if the sender is unknown. These links are dangerous and can install malware such as worms and trojan horses to infect computers and networks. Attackers can gain sensitive and confidential information from these attacks. Don’t trust random callers asking for personal information always make sure that they are a known caller and be the one to call first. Always make sure to type the URL into a search bar to make sure it is the right website and not a fake one created by the attacker. Password cracking tools help hackers discover passwords created by users. A way to avoid these attacks is by having two factor authentication and strong long passwords. This way the hacker won’t be able to log into accounts without verifying their identity and the password cracking tools won’t be able to crack strong long passwords easily. Having different passwords for each account is also recommended because when one account gets breached then all accounts can be breached. Man in the Middle attacks is another attack to look out for. These attacks are where the attacker intercepts a connection between a user and their desired network. These can commonly happen over public Wi-Fi or if the user connects to a hotspot acting as free Wi-Fi access. These attacks can be avoided by not connecting to public Wi-Fi, using VPNs, not accessing critical and personal information while on public service. Protecting kids is also a priority when it comes to security so children are not exposed to harmful websites and graphic images that can affect their brain. Using child settings and having anti-virus for kids computers and accounts is a way to counter these graphic and damaging websites. These are all things to look out for and things to practice to stay safe online. By following these safe procedures users can be safe and their kids can also be protected. The internet is a great place however there are many risks and dangers while using it. it is best to be aware of the dangers and be protected to prevent an attack.

**References:**

B. Bhushan, G. Sahoo and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review," 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), 2017, pp. 1-6, doi: 10.1109/ICACCAF.2017.8344724.

Bulao, Jacquelyn. “How Many Cyber Attacks Happen per Day in 2022?” *Techjury*, 2022, https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref.

P. G. Kelley et al., "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," 2012 IEEE Symposium on Security and Privacy, 2012, pp. 523-537, doi: 10.1109/SP.2012.38.

Respicio, Annie, "SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD" (2019). Electronic Theses, Projects, and Dissertations. 944.
https://scholarworks.lib.csusb.edu/etd/944

S. Gupta, A. Singhal and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778.

Velimirovic, Andreja. “How to Prevent Ddos Attacks: 7 Tried-and-Tested Methods.” *PhoenixNAP Blog*, 15 Aug. 2022, https://phoenixnap.com/blog/prevent-ddos-attacks.

Hughes, Donna Rice, and Pamela T. Campbell. *Kids online: Protecting your children in cyberspace*. Grand Rapids, MI: Fleming H. Revell, 1998.