Cybersecurity: Identifying Civilian Threats and How to Protect Against Them

Kiara A. Richardson

kar15@rice.edu

Department of Computational Applied Mathematics and Operations Research

William Marsh Rice University

ENGI 501 - Workplace Communication for Professional Master's Students in Engineering

Professor Anne-Marie Womack

November 1, 2022

Executive Summary

Cybersecurity can be summarized as the style of protecting data, networks, devices, computers, and servers from unsanctioned access or malicious use. It is the practice of multiple methods that ensure the safety of information pertaining to individuals, organizations, businesses, and nations. Many forms of cyberthreats exist in this technically advanced society, however, spam/phishing, malware/ransomware, and identity theft are the most common cases that everyday civilians are threatened with.

Malware/ransomware can infect any device by encrypting servers and holding data hostage. The best way to avoid this issue is by having trustworthy antivirus software installed on devices and to regularly back up data and store it on platforms that have unlimited amounts of space. Instances of malware/ransomware should be reported to the Cybersecurity government agencies as per listed in the section.

Spam/phishing is seen all throughout the web in its multiple forms, email phishing being the most common. The best way to defend against it, besides the aforementioned ones, can be implementing multi-factor identification. This forces the user to provide multiple forms if ID before logging into their accounts. Instances of spam/phishing should be reported to the Cybersecurity government agencies as per listed in the section.

Identity Theft, one of the most heinous of crimes any cybercriminal can make, is something online users should be made aware of and know how to defend against. This threat falls under Cybersecurity because criminals can use a culmination of cybercrimes to get identifying information from a person. This can lead to unwanted credit charges, stolen social security numbers, and even unsanctioned loans taken out in the user's name. As mentioned already, instances of identity theft should be reported to the Cybersecurity government agencies as per listed in the section.

Table of Contents

Introduction

I. Cybersecurity and its Components

On a grand scale, countries around the world use information technology to conduct day to day business. This includes keeping up with national records like getting ID's and birth certificates. Because of this sensitive information, cyberattacks and data breaches are becoming more common. To combat this issue nations practice Cybersecurity methods. On a smaller scale, average citizens are also susceptible to data breaches. This comes in the form of getting their personal computer hacked, having their social media passwords stolen, or even having their credit cards and social security numbers violated. Obviously, cybercrimes like these are very dangerous to a civilian and can take months to rectify and get fixed. In this century, information is the most sought-after commodity, making it even more valuable to criminals. Cybersecurity is important because it can be used as a counter protective measure when encountering cybercriminals.

Cybersecurity, also known as Computer Security, is a broad term used to categorize a multitude of cyber analytics. It can be summarized as the "techniques and methods used to protect computers, networks, data, and servers from unauthorized access aimed at malicious exploitation" (Nadikattu, 2020). Cybersecurity can be used on drastically different scales. From protecting individual civilians, to safeguarding a corporation's data, to fortifying user data on different online platforms or media outlets, to defending a nations' secrets; having at least a minimal education in Cybersecurity can be the difference from losing or gaining anything in this digitized world. There are many components of Cybersecurity, but Application Security, Information Security, and Network Security are three areas of importance when learning about this topic.

Application Security is "putting in place measures or countermeasures geared towards protecting applications" (Nadikattu, 2020). The development team in charge presets safeguards that can eliminate security issues that may arrive. This is to ensure the safety and management of the application and its user. Information Security is "concerned with ensuring the integrity, security, and confidentiality information is maintained" (Nadikattu, 2020). The goal of this is to safeguard any information from unwanted or unwarranted access that can lead to exploitation. Many companies in America use techniques of Information Security to keep proprietary information safe. Lastly, Network Security is "concerned with devising measures that ensure the

usability, integrity, functionality, and security if a user network is maintained at all times" (Nadikattu, 2020). Displaying Network Security measures can be as easy as downloading anti-virus software on a personal computer or using a Virtual Private Network (VPN) when browsing the internet. These three facets of Cybersecurity are crucial when it comes to protecting oneself against cyberbullies.

II. Cyberthreats Defined

Cyberthreats can take many aliases when it comes to civilian targeted procedures. There are plenty of less common, but still equally terrible, forms of cyberattack like: Distributed Denial of Service attacks (DDoS), Corporate Account Takeover (CATO), and Automated Teller Machine (ATM) Cash Out (Know the Types of Cyber Threats, 2022). However, the most common forms that average civilians suffer from on a day-to-day basis are Malware and Ransomware, Spam and Phishing, and Identity Theft.

Malware is any type of code or software made with malicious attempt. The Massachusetts state government defines malware as "a program inserted into a system to compromise the confidentiality, integrity, or availability of data" (2022). In every case, malware is always installed without the host knowing and can significantly damage an operating system. Similarly, ransomware can prevent a host from even accessing their system via malware (Know the Types of Cyber Threats, 2022). Ransomware holds system data hostage and demands a form of payment from the user. This is usually in the form of a credit card or, what has been becoming increasingly popular, cryptocurrency. Majority of the time, once a payment is issued there is no guarantee that a user will gain back control of their operating system or personal data. Cyberattackers have full control and can choose what to do with that valuable information. In some instances, user data just gets sold on the dark web and that leads to even more problems for the user.

Spam is "unwanted, unsolicited, or undesirable messages and emails" while Phishing is a "form of social engineering, including attempts to get sensitive information" (Know the Types of Cyber Threats, 2022). Most forms of spam and phishing come in emails, be that sent to personal, work, or school emails. Cybercriminals trick users by sending fraudulent emails that use familiar

logos and names to entice the user into clicking on links. Any information input into these links go straight to the criminals.

Identity Theft, as defined by the United States government, happens when criminals steal personal information from a different person to commit fraud; the information can then be used to apply for credit, file taxes, or get medical services (2022). At first glance, Identity Theft does not seem like something Cybersecurity tactics can prevent, however, most cases of Identity Theft in America happen when Cybercriminals steal information and data from online users using tactics previously mentioned.

Detection and Prevention

I. Malware and Ransomware

Malware and Ransomware infect servers and encrypt files. This can be installed when a user clicks on malicious links, clicks on suspicious ads, or visits websites that do not have a common domain name. Websites with '.com', '.org', '.net', and '.gov' domains are safer and more common to use than websites that, for example, deal with illegal streaming's of videos, comics, and other forms of entertainment. Domains like that usually end in '.to' or '.dad'. Malware and ransomware can be easily found on websites whose domain sounds unfamiliar to the everyday user. In cases of ransomware and malware issues, the United States FBI department urges people to report these attacks to the Internet Crime Complaint Center www.IC3.gov ; if applicable, users should input the following information when visiting their website (Gonzales, et al., 2019)

1. Date of Infection
2. Ransomware Variant (identified on the ransom page or by the encrypted file extension)
3. Victim Company Information (industry type, business size, etc.)
4. How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
5. Requested Ransom Amount
6. Actor's Bitcoin Wallet Address (may be listed on the ransom page)
7. Ransom Amount Paid (if any)

8. Overall Losses Associated with a Ransomware Infection (including the ransom amount)
9. Victim Impact Statement

Protecting against attacks like these are not overly difficult and require minimal effort. The main thing someone can do is learn to surf the internet carefully by not clicking on suspicious links, ads, or emails. Other technical preventions that can lessen the risk of attack can be seen as doing the following (Gonzales, et al., 2019)

- Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; backups may be the best way to recover critical data.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.
- Only download software—especially free software—from trusted sites. When possible, verify the integrity of the software through a digital signature prior to execution.
- Ensure application patches for the operating system, software, and firmware are up to date.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Disable macro scripts from files transmitted via e-mail.
- Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

An amazing software to have on computers for protection is an application called ESET Security (it is currently installed on the laptop this paper was written on). ESET Security is an antivirus and antimalware internet security application that can be downloaded on personal and

work computers with a subscription. Not only does it protect against malware and ransomware, but it also notifies the owner when Wi-Fi connections are not secure; this leaves computers vulnerable. There are hundreds of other applications that can be installed on computers to protect them from attacks, but ESET is a highly recommended one in the technical community.

II. Spam and Phishing

Everyone with an active email account has faced the issue of spam emails, so much so that email engines have a button in the options menu titled 'spam mail' so that the interface can automatically detect the sender and send it straight to that folder. Spam also comes in the form of over-advertising. Recognize those websites that have ads blocking most of their webpage, to the point where the information is barely readable due to the minimal space? That's a form of spam too. Phishing and spam go hand in hand because oftentimes a spam email will be a phishing attempt (remember the malicious hyperlink example). This is known as email phishing, and it is the most common form. Other lesser-known forms of are (What is Phishing: Microsoft Security, 2022)

- Malware phishing - This type of attack involves planting malware disguised as a trustworthy attachment in an email. In some cases, opening a malware attachment can paralyze entire IT systems.
- Spear phishing - Spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity.
- Whaling - These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information.
- Smishing - A combination of the words "SMS" and "phishing," smishing involves sending text messages disguised as trustworthy communications from businesses. People are particularly vulnerable to SMS scams, as text messages are delivered in plain text and come across as more personal.

- Vishing - In vishing campaigns, attackers in fraudulent call centers attempt to trick people into providing sensitive information over the phone. In many cases, these scams use social engineering to dupe victims into installing malware onto their devices in the form of an app.

Phishing attempts are easy to fall for because scammers make them look believable. As stated before, they'll even use company logos in their messages to trick users. Spam folders in emails can successfully block most phishing attempts. However, criminals have learned to adapt along with technology, so here are other ways to protect against phishing (A. Hebert, et al., 2022)

1. Use security software to protect computers. Set the software to update automatically so it will deal with any new security threats.
2. Have settings software update automatically for phones. These updates could give critical protection against security threats.
3. Protect accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. Duo Mobile is great for phones and computers (many scholastic institutions use this). Multi-factor authentication makes it harder for scammers to log in to personal accounts if they do get usernames and passwords.
4. Protect data by backing it up. Back up the data on computers to an external hard drive or in the cloud/drive.

Just being informed about this type of cyberattack can help users gain an advantage to these criminals. Checking for typos and spelling/grammar errors is a way to detect phishing attempts while having strong alphanumeric passwords can also help with securing accounts and protecting data. Alphanumeric passwords are harder to hack because they are not as easily guessable by scammers. Also, having different passwords for different logins can ensure that personal data is protected. Though it may be hard to keep track of, it is worth it in the long run.

Like with malware and ransomware, the United States government urgers online users to report these acts in the hopes of stopping these incidents from happening again (A. Hebert, et al., 2022)

- For phishing emails, forward them to the Anti-Phishing Working Group at reportphishing@apwg.org.
- For smishing texts, forward them to the number 7726 and text SPAM.
- For any phishing attempt, report them to the Federal Trade Commission at ReportFraud.ftc.gov.

III. Identity Theft

Identity Theft is the most nefarious crime on this list. It encompasses many forms of cyberattacks, meaning, criminals can get personal account information from phishing/spam attempts and malware/ransomware attempts. There are some ways an outsider can help decrease the spread of Identity Theft. For instance, when personal information has been stolen but not used yet, a retailer, distributor, or wholesaler can properly check "whether a signature on a credit card receipt matches the one on the card" (K. Anderson, et al., 2008). This is a surefire way to catch a criminal in the act and help someone who is actively dealing with Identity Theft. In other cases, the United States government urges users to protect themselves by (Identity Theft, 2022)

- Keeping Social Security numbers secure. Do not carry a Social Security card in a wallet.
- Do not share personal information (birthdate, Social Security number, or bank account number) because someone asks for it.
- Place a hold on mail when away from home for several days.
- Pay attention to billing cycles. If bills or financial statements are late, contact the sender.
- Use the security features on mobile phones.
- Update sharing and firewall settings when using public wi-fi networks. Use a virtual private network (VPN) when on public Wi-Fi.
- Review credit card and bank account statements. Compare receipts with account statements. Watch for unauthorized transactions.

- Shred receipts, credit offers, account statements, and expired credit cards. This can prevent "dumpster divers" from getting personal information.
- Review credit reports once a year. Order it for free from Annualcreditreport.com.
- Freeze credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for a credit account under someone else's name.
    - The Experian App can be downloaded on mobile devices for easy access to credit reporting ratings. Fraud/scam attempts, freezes, and public criminal history of neighbors (if applicable) can be accessed through the app.

Other safeguards include creating strong alphanumeric passwords to accounts and installing protection software. Almost all these prevention tactics listed are interchangeable with other cyberattacks. Knowing this makes it easy for users because installing protection software can eradicate most of the problems they may face against cybercriminals, while being informed can protect against everything else.

As in the previous sections of this document, the United States government would like all Identity Theft cases reported to the Federal Trade Commission by one of two ways:

- online at IdentityTheft.gov
- by phone at 1-877-438-4338

With identity theft being one of the most damaging crimes a criminal can accomplish in the long run, depending on the severity of the theft, it can take weeks or months to resolve. Obviously, this can be very bothersome. That is why taking preventative measures ensures the safety of personal data and information in the long run. Like the saying goes, it is better to know the information and not need it, than to need it and not have it.

Conclusion

Cybersecurity is an essential toolset to have in this modernly digitized world. Knowing different Cybersecurity methods and prevention is very crucial. Currently, every person has an online profile/footprint. Protecting this profile is just as important as protecting a home. Cybersecurity is a way for the user to get that protection. All instances of malware/ransomware, spam/phishing, and identity theft can be reported to the United States government in hopes to put an end to these cyberattacks. Just being knowledgeable in these subjects can help prevent more attacks in the future. The defense suggestions made in this paper require minimal effort to maintain, yet it can be a pivotal moment of awareness if issues like the ones mentioned do happen. The more people who recognize these scams and act against them, the safer this online world can be.

References

About the contributors. (2019). In I. Gonzales, K. Joaquin Jay, & Roger L. (Eds.), Cybersecurity: current writings on threats and protection. McFarland. Credo Reference: http://ezproxy.rice.edu/login?url=https://search.credoreference.com/content/entry/mcfccwotap/about_the_contributors/0?institutionId=4655

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. Journal of Economic Perspectives, 22(2), 171-192.

Hebert, A., Hernandez, A., Perkins, R., & Puig, A. (2022, October 25). How to Recognize and Avoid Phishing Scams. Consumer Advice. Retrieved October 30, 2022, from https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Identity Theft. USA Gov. (n.d.). Retrieved October 30, 2022, from https://www.usa.gov/identity-theft#item-206115

Know the Types of Cyber Threats. Mass.gov. (n.d.). Retrieved October 30, 2022, from https://www.mass.gov/service-details/know-the-types-of-cyber-threats

Nadikattu, R. R. (2020). New Ways of Implementing Cyber Security to Help in Protecting America. Journal of Xidian University, 14(5), 6004-6015.

What is Phishing: Microsoft Security. What is Phishing? | Microsoft Security. (n.d.). Retrieved October 30, 2022, from https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing?ef_id=872a01eddd581596103662b33c66ca67%3AG%3As&OCID=AIDcmmdamuj0pc_SEM_872a01eddd581596103662b33c66ca67%3AG%3As&msclkid=872a01eddd581596103662b33c66ca67