The Importance of Social Engineering

Jalaya Allen
Norfolk State University

The Importance of Social Engineering

COVA CCI Cybersecurity Undergraduate Research

Norfolk State University

By: Jalaya Allen

Date: 11/24/22

Email: j.m.allen107415@spartans.nsu.edu

Introduction:

Most people are afraid of being attacked when walking to their car, relaxing at home, or doing normal things like shopping. Though the unlikeliest of attacks have become one of the most dangerous. Just imagine someone having the ability to watch your every move online and virtually. They can find your credit card information, passwords, social security number and so much more. Then with that information, they can steal your identity and sell it on the black market as well as threaten you for money. Attacks like these use something called Social Engineering to trick the user into giving up their information without even realizing. Though you may be asking, what is Social Engineering? Well Social Engineering are manipulation tactics that are aimed at getting people to give up their confidential information. These manipulation tactics play on our desires as well as our sense of urgency. Have you ever gotten a text or call saying that you have a package you didn't order being shipped to your house and the only way to cancel the order was through clicking a link or calling the number listed? Or got an offer in your email saying that you were selected for a special prize, and you only have a certain time frame to claim it? These are common types of social engineering tactics that can play on your emotions. The best ways to avoid scams is to first understand what they are and why it is important. Next, you need to be able to recognize the different types of attacks and how to avoid them. Then, we will talk about what is ethical hacking and why is it important. Lastly, we will talk about how to avoid scams.

Importance:

Social engineering is important because it plays on our emotions and connections to one another. While hacking is an option, it is easier to give a group the same scam and wait for at least one person to fall for it. If this type of scam was executed in a company environment, getting at least one person's credentials is enough to take over the company system. For this tactic, you do not need to be tech savvy. Some of the more recognizable scams are robocalls or phishing emails [1]. Due to human mistakes, we are more of a danger to ourselves than any type of software or hardware vulnerability. Cybercriminals, which are people who engage in criminal activities via computer or internet, also stalk their prey by doing reconnaissance as well as search for vulnerable security measures. It can take up to a few weeks or months before they call or confront you with a story. When they do this, they are trying to gain your trust by making you believe that they are on your side or just another associate of yours. Once they have gained your trust, they will try to convince you to do tasks that will compromise your security [2]. Consequences of getting scammed is getting your sensitive information like social security number, drivers license, important files and more taken or held over your head for black mail.

Different Types:

Some types of social engineering are Phishing, Scareware, Dumpster Diving and Tailgating. Phishing being the outrageous number of scam emails that fill your spam and inbox. These appear to be from reputable organizations like banks or companies to give you a sense of safety. Then they will request your account information under false pretenses like sending you money or that your account has been hacked and you need to type in your information to verify yourself. Scareware is a type of deception software that will send pop-ups to your devices telling

you that you need to buy or download some type of software that you really don't need. With scareware, you are bombarded with threats of the many things that could happen to your device to pressure you into getting the software that is being displayed to you [2]. Dumpster diving is one of the easiest and most preventable ways to get information. When dumping sensitive information or documents into the trash intact, you are putting yourself at risk. Any type of confidential information that can be found in the trash can be used against you. Statistics also show that more than 4 million of the spam emails that we get on a regular basis is more than 88% because of dumpster diving [3]. Then, tailgating is when someone physically gains access to a building or area because either someone held the door for them, or they followed behind them without their knowledge. Though once they have access, they can then take devices or gain access to confidential information. Tailgating can also include giving unauthorized access to a device and allowing them to install malware [4]. These are only a few of the many types of social engineering attacks.

Ethical Hacking and its Importance:

Ethical hacking is hacking that is geared toward improving systems as well as security measures. Typically, these hackers are called hat hackers or penetration testers. Their job is to hack into systems to exploit unknown weaknesses and create firewalls, which are network security monitors that manage what goes in and out the network. Since this is a heavy task, there are two dedicated groups called, blue team and red team. Blue team oversees evaluating the organizations security and defending it from attacks [5], while red team simulates cyberattacks using social engineering techniques as well as utilizing malware [6]. These teams work together to create real world scenarios and develop solutions to the issues that arise. This is important because if a cybercriminal gets into your network, they can gain access to important files like

customer information, tax returns, social security numbers, as well as autosaved passwords that are associated with your online account [7]. Though, because of ethical hacking, on each device that a person has, there are continuous updates that are advised that you download to minimize the risks of a weakened system. The techniques learned can also be found to teach anyone who is willing to learn online for free or through courses that go into even greater detail.

How to prevent Social Engineering:

To protect yourself from Social Engineering attacks, make sure that you download anti-virus and anti-malware software onto your devices. Anti-Virus software disinfects your device if it detects a virus, blocks malicious and potentially harmful code as well as monitors your network [8]. Anti-Malware protects your devices from any malicious software that was made to do you harm like damage your device or network and spy on you [9]. Shredding documents with confidential information will keep people from finding important information in the trash. Having different passwords for different sites and devices will lessen the chances of someone getting access to all your information if there is a data breech or hacking to your system. Make sure to check the senders of emails and phone numbers to make sure it is someone you know or trust. If you don't know who it is, do not click on any links because this could cause malware to be downloaded to your device. Setting up two step authenticators can help if someone finds out your password because they would need a verification code to fully access the site or device. This will also give you a heads up if you need to change your password because someone has tried to log into your account. Even after all these methods, the most important is keeping yourself informed. To fight something, you must know what you're going against.

Conclusion:

Your security is the most important thing in this digital world. Without online security, you are vulnerable to cyberattacks that can result in identity theft, ransom attacks, and your information being sold to the black market. Though even with efficient online security, you need to be aware of social engineering attacks. Attacks like phishing, scareware, dumpster diving, and tailgating. To combat some of these issues, we have ethical hackers who do penetration test to find vulnerabilities in your network and systems. The teams who execute ethical hacking techniques are blue team and red team, blue team defending while red team attacks. Though these two teams do the most they can to find and minimize vulnerabilities, the best way to decrease cyberattacks is to also become educated in how to keep your information safe. Things like using anti-virus software, shredding important documents, using different passwords, checking senders, and setting up two set-authenticators minimize your individual risk. Everyday technology is evolving, and everyday new methods of attacks are invented, so are we going to allow people to steal our identities or are we going to stay informed so that we can effectively protect ourselves?

Sources:

4. *10 types of social engineering attacks: CrowdStrike*. crowdstrike.com. (2022, October 5). Retrieved November 25, 2022, from https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/

8. Allen, J. (2020, August 20). *What does antivirus software really do?* Windows Central. Retrieved December 7, 2022, from https://www.windowscentral.com/what-does-antivirus-software-really-do

1. Caldwell, N. (2021, May 17). *What is social engineering and how can you stop it?* Arctic Wolf. Retrieved October 27, 2022

3. EasyDmarc. (2022, November 14). *What is dumpster diving in cybersecurity?* EasyDMARC. Retrieved November 25, 2022

2. Raghavan, R. (2020, June 25). *Different types of social engineering & how to prevent them?* Web Solutions Blog. Retrieved October 27, 2022

7. Kevin.montalvo@motiva.net. (2021, April 14). *The top 3 tricks of Cybercriminals Againts Your computer network: Long Island, NY: Motiva*. Motiva Networks. Retrieved December 7, 2022, from https://motiva.net/top-3-tricks-of-cybercriminals-to-attack-your-computer-network/#:~:text

6. Schulz, S. (2022, November 24). *What is a red team in cyber security?* GoGet Secure. Retrieved December 7, 2022, from https://gogetsecure.com/red-team-cyber-security/#What_Does_a_Red_Team_Do_Exactly

5. *What is a blue team?* XM Cyber. (2022, June 13). Retrieved December 7, 2022, from https://www.xmcyber.com/glossary/what-is-a-blue-team/#:~:text=What%20is%20a%20Blue%20Team%3F%201%20BLUE%20TEAM,3%20THE%20VALUE%20OF%20BLUE%20TEAM%20TESTING%20

9. *What is Anti-Malware & How Does It Work?* ConnectWise. (n.d.). Retrieved December 7, 2022, from https://www.connectwise.com/cybersecurity-center/glossary/anti-malware