**How to Prevent Social Engineering Attacks**

95/100 95% (A)

Luke Albert

CYSE 280: Windows System Management and Security

Professor Malik Gladden

November 29th, 2022

Two men enter a bank in the middle of the day in Jamaica with printed badges two clipboards and button-up shirts with the bank company’s name on them. These two men do not work for the bank. They are human hackers, Chris and Ryan, trying to breach and steal data from the bank. Inside the clipboards are USB keys, lockpicks, and a camera to videotape information inside the bank. As the two men walk into the bank one man acts as if he is talking to someone inside the bank already. The two men walk right past the bank security guards and walk right upstairs. They find a confidential ATM testing center room and enter it as the bank workers believe they are there for an audit and let them walk right in. Shortly after taking pictures of everything valuable in that room, they walk out and find another room where they find a lady leaving the room. The two men hold the door open after she opened it as a kind gesture and got their entry to the call center. This Call center has rows and rows of desks and computers. Chris and Ryan ask someone to log onto one of the computers for them and the person logged in with no questions asked. While Chris is videotaping her username and password. Now Chris and Ryan can plug in their USB keys and get to work. They are now able to gain access to valuable information and the bank’s network. This is a case of Social Engineering. Social Engineering is using deception and posing as someone else to gain access to confidential and personal information to use for typically fraudulent purposes. Chris and Ryan posed as workers for the Bank giving them an audit. This allowed them to bypass security and gain workers’ trust to get into classified information (Rhysider 2020). There are a lot of trusting people that can be manipulated and taken advantage of. That is why we need to bring more attention to social engineering and educate our peers and coworkers on how to prevent it. Thousands of companies every year lose millions of dollars to social engineering attacks. There are many different types of social engineering attacks. There are three main types of attacks, and they include phishing emails, physical breaches, and pretext calling.

Phishing emails are one of the most common cases of social engineering. Phishing emails consist of an attacker sending fraudulent or malicious emails to try and deceive victims. These attackers will pose as companies such as Amazon or Facebook explaining there is a problem with the victim’s account. Typically, these emails will have malicious links where the victim will click on the link and have to enter confidential and personal information into a fake website login, and have their information stolen (Fatima 2019). The victim believes the link is to the actual website of Amazon or whichever website the attacker is impersonating. Instead of the link going to the real website, it will bring the victim to a fake website where the hacker then will have access to any information the user inputs. Attackers will even attach malicious malware to links and attachments in emails where a victim will click on a link or attachment and instantly download dangerous malware, trojan horses, and worms.

There are many ways to avoid phishing emails and it isn’t too hard to do so. One of the easiest ways to avoid phishing emails is to never click on any suspicious links or any links at all. It is best to just type the URL into the search bar instead of clicking on a link in the email (Steinzmetz 2022). This way if an attacker posing as amazon sends an email with a link to amazon the victim would then just type amazon.com into their search bar instead of clicking the link and be sent to the real website. They then can enter their information safely and realize there was no issue at all and the sketchy email was just a hacker trying to obtain personal information. Another way to avoid phishing emails is to have the browser updated to the newest update and protect computers with security software. A little protection goes a long way, the security software will protect the user from malicious websites and links. Protecting personal accounts with two-factor authentication is also a good way to protect personal information. Two-factor authentication will prompt whoever is trying to sign into the account to verify their identity with another means, usually by a text message code or email code.

There are a few different types of phishing emails which include spear phishing and smishing as well. Spear phishing is phishing emails targeting a specific person or group. This type of phishing email will be more targeted towards the person’s company or things they like. These emails are sent from someone impersonating a known or trusted sender. Smishing includes phishing through SMS messages. These text messages will act like banking institutions or other companies and leave a link for the user to click and enter their bank details or other accounts. It is best to ignore random text messages from unknown numbers.

If someone were to be exposed to a phishing link and clicked on the link there are some things needed to do immediately to reduce loss. This person should change their username and password for whichever site they had their personal information compromised. If the victim uses the same password for everything, then they must change every single account password. It is not a safe practice to use the same password for multiple accounts. If banking information was compromised, then the victim should call their bank immediately and either freeze their bank or let them know of possible fraudulent purchases. If the scammer had gotten ahold of the victim’s social security number or credit card then they should visit IdentityTheft.gov and follow the steps on the website for whatever information was stolen.

Physical breaches are where an unauthorized person gains access to crucial and confidential information and areas through the use of social engineering tactics. Chris and Ryan walking into the Jamaican bank acting as auditors to gain access to confidential areas is a great example of a physical breach attack. Typically, before a physical breach attack, there is some research done on the company being attacked before the breach is started. Some homework for the attacker includes open-source intelligence-gathering or OSINT (Hwang 2022). OSINT includes going online to websites such as LinkedIn, Twitter, Instagram, and Facebook and looking for employees of the targeted company. By going to the company’s LinkedIn profile the attacker can find out a list of employees that work for the company. The attacker can then see employees posting information to LinkedIn such as an upcoming audit and this adds a tool for the attacker to use. The attacker could also go further and search for different employees’ social media accounts to see if they are posting any valuable information about the company that the attacker can use to gain trust or access to the building. After doing a lot of research on many different websites and accounts of various employees there is typically one employee posting something they shouldn’t be which allows the attacker to gain any valuable information useful to their attack. After obtaining information from OSINT the attacker can then plan their breach. Physical breach social engineers can be referred to as human hackers because they themselves are breaching into the company at this point. These human hackers will try to enter the building acting as if they belong there as Chris and Ryan did with the Jamaican bank. With the knowledge from OSINT attackers are able to gain the trust of employees by knowing things that shouldn’t typically be known to outsiders of the company. Once the attackers can get in they can steal all the data and hack the computers they want and leave.

There are many ways to stop a physical breach and social engineering attack from happening. It is good to have meetings with employees so they can be aware of the dangers and threats they may encounter while working. Tailgating is one of the easiest ways an attacker can get into a classified building. Tailgating is when an attacker follows an authorized individual into a building or room where one would typically need to verify their identity to enter. A simple way to counter this is to tell employees to never let anyone in behind them and not hold doors for anyone. This way they don’t let anyone without authorized access into confidential rooms or buildings. Another way to help stop physical breaching is to have employees check other employees’ credentials and verify they should be there, especially if the person does not look familiar. Chris and Ryan were able to successfully tailgate into two confidential rooms of the bank by following someone into the room and holding the door open for someone leaving another room. This should not have happened, and the workers should have closed the doors and not willingly let someone walk into any rooms that require authorized access. Companies need to hold meetings explaining to their employees the dangers of social engineering and how to keep an eye out to prevent it. Carelessness can cost a lot of money, so it is best to be careful and not display any confidential information online.

The last type of social engineering is pretext calling. This type of attack occurs over a phone call and the attacker will pose as someone with importance or authority to try and get the victim’s name, date of birth, social security number, bank details, and whatever other information they can gather from the victim (Stenberg 2020). My grandmother will get calls from people posing as her grandchild that is in a lot of danger and in need of immediate cash. This is an example of pretext calling and it is sickening to me that attackers will go for the elderly who may not have the clearest mind. Typically, these pretext callers will first try to gain the victim’s trust and then try to obtain their personal information. There’s no way to assure that a victim won’t get pretext calls however there are ways to avoid being scammed by these callers.

One way to avoid these scam callers is to never provide any personal, confidential, or financial information to anyone over the phone who initiated the contact. Always say “sorry I can’t give out this type of information without initiating contact with the company first.” This way we can be sure that we know whom we are speaking to and who is legitimate. Never give a random number any personal information. Always make sure the number is trustworthy and real. Pretext calling is illegal and dangerous but if everyone follows these steps then there will be a lot fewer pretext-calling victims in the world.

Social engineering is dangerous and can cause a lot of damage to companies and a lot of lost money. However, there are ways to counter social engineering and stop it from claiming another victim. It is good to always suspect a random call or email may be malicious and to proceed with caution. Never open links or attachments in emails to avoid the risk of being attacked by a phishing email. Always type the URL of the website of interest instead of being trigger-happy with the links. Always have computer browsers and windows updates updated to the newest update for the best and most updated security. Physical breach hackers can be easily stopped with safe work practices such as always closing the door behind one person to assure no one tailgates into the building or room, and always making sure employees or people inside the building have the correct credentials to be allowed in the building. Never be too kind to strangers to let them take advantage of the situation. Social engineers live off people’s kindness. Don’t be mean to people just don’t let them off the hook and make sure they are allowed to be in classified areas. Never post classified information about a company online especially publicly because a social engineer could be watching and taking notes. Lastly, pretext calling can also be easily prevented by remembering to never give out personal, financial, or confidential information over the phone to a stranger. Always make sure that the number being called is correct and the correct company, and if a number is claiming to be a number simply hang up and call the company and verify if what the first person was saying is true. Social engineering can cause a lot of damage and issues, but it is easily preventable by following these safe practices.

References:

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. Old Dominion University Libraries. Retrieved November 29, 2022, from https://web-s-ebscohost-com.proxy.lib.odu.edu/ehost/pdfviewer/pdfviewer?vid=0&sid=dcd7ebad-eb03-4fd3-afbc-fda8ca23a5f4%40redis

Hadnagy, C. (2022, February 28). The official social engineering hub. Retrieved November 29, 2022, from <https://www.social-engineer.org/>

Hwang, Y., Lee, I., Kim, H., Lee, H., & Kim, D. (2022, February 18). Current status and security trend of OSINT. Retrieved November 29, 2022, from https://www.hindawi.com/journals/wcmc/2022/1290129/

Rhysider, J., & Hadnagy, C. (2020, July 7). Human hacker – darknet diaries. Retrieved November 29, 2022, from https://darknetdiaries.com/transcript/69/

Steinmetz, K. F., & Holt, T. J. (2022, August 5). Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations. Old Dominion University Libraries. Retrieved November 29, 2022, from <https://journals-sagepub-com.proxy.lib.odu.edu/doi/full/10.1177/08944393221117501>

Stenberg, M., Rocco, P., & Farole, S. (2020). Calling in “Sick”: COVID-19, Opportunism, Pretext, and Subnational Autocratization. Retrieved November 29, 2022, from https://watermark.silverchair.com/ksac017.pdf?token=AQECAHi208BE49Ooan9kkhW\_Ercy7Dm3ZL\_9Cf3qfKAc485ysgAAAswwggLIBgkqhkiG9w0BBwagggK5MIICtQIBADCCAq4GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMYGr5ekylyQjEIRYTAgEQgIICf7uMueLpXomsHIrennnubT2jmSy7ge-XlCCmeGFsEEQl8QP3Z-uEIBoiR4AEeUQkAieOf28BXpGtu6bgVGlxzZIv4Mt3Wqd1l3\_YldP4EV\_gJQLrOwKtX06WOcY1onyRpbMafFBZG8nIxRWtIaVbnvLDONy8Q8JCtO1acAMWxnGn8ZQQ87D3ps2roATcqDvzkB3GS8gHS5ofqqg2GdQ4F9OqomnZvKBwc1m1Ya06VdNxA5ni51VYTL6aNjhORwe2NKVrTtBk3AtJDXqR\_Q7S2VT831txeHCcRDU-XkSpuRWo74-QN7RlTZKt1L-gkVH-gLqEtsSOmTZ1ZPgLvWEmFEk8OEG0Qk--PfXJmlUHJkkkAMb2aK2T5Cj3g-gNudXINQ\_mutCW5J3ljctAJPOJYOg-UzSntsGTTe-7MaXdv-czHIKJK0r8UUcx0l8XYVotSetWH9vlJ\_4zVhA7daOcpU1RFDSl8LOlTtIRlOX-lMyu8ALNy9L03n6XKN-g53xdjGWkI6IWqLPzs6MMR4Uaxf6gZAGWRjWcWQODytetZWgrT4FO-YolqOCb9E7n1Jm1nLxfYJbzRp1ix2hdYrRhQqgwDixcxbKyh75a4VEo62gz5oo6OZaNXqW8rhRrUmqFvYe-Pc8DBu4wUq4bL-FcTeyCV7p0pq-KXqMwUibRXWxZuG4Lpsvtf6I\_PnTH4YZ7NjNPAJCUXHkLKMpSpw3r\_h-h83jMqVXS21oTy56XRNIApawNMp6B9cLG3FKg4ORjGgBLghDZXn7daFgMEDdeHJsZhkCF3JZh3x\_xdetqEBTRJhTjWVkgMj1sKOzIroRRP4-yQlnhhZz7hVqB3n5lvw