# Final Paper: Effects of Social Engineering in Cyber Incidents

Diana Y. Solorzano

Department of Cybersecurity, Old Dominion University

CYSE 495: Human Factors and Policy in Cybersecurity

Dr. Saltuk B. Karahan

August 01, 2024

Every day we see a new article about another organization being breached or a new cyber-attack taking hundreds or even thousands of victims. With the advances in technology, almost every department within an organization is to some degree, dependent on technology to complete their work. Whether it's providing a secure and private network, hosting servers in a data center, or even using any software program. When we begin to incorporate technology into organizations, we are forced to look at how we can keep this information secure and safe. This doesn't just mean locking everything down and enforcing some type of secure entry point. Along with advances in technology, hackers are finding new vulnerabilities and creating new malware to exploit these vulnerabilities. For years we have been hearing the IT community refer to humans as the weakest link in any organization, which explains why social engineering attacks have been on the rise in the last couple of years.

What exactly is social engineering? IBM defines social engineering as "attacks that manipulate people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals, or making other mistakes that compromise their personal or organizational security" (IBM 2022). Social engineering attacks focus on using psychological manipulations and leverage a user's emotions in order to get them to take some type of malicious action. Many techniques create a setting where the users may begin to feel fearful, curious, or a sense of urgency which can be used as leverage by the attacker. Most of these attacks simply require the users to make one click, log in once, open one file, or provide some information. That one action results in their hardware, personal information, or organization's network being at risk. With users being the targets, organizations are forced to consider this evolving threat to protect themselves and their organizations.

Social engineer attacks were once known as master manipulators who would call a vulnerable older individual and get them to click on a link and log in, allowing the hacker to steal their life's savings. While these attacks still occur, they have most definitely evolved with time, branched out beyond calls, and have become increasingly more difficult to distinguish as real or fake. What does this mean for organizations when it comes to handling these types of cyber incidents?

As mentioned earlier, social engineering techniques are constantly changing but the concepts remain the same. Todd Jones lists 12 of the most common attacks in their article as; 1. Phishing Attacks, 2. Spear Phishing, 3. Whaling, 4. Smishing and Vishing, 5. Baiting, 6. Piggybacking/Tailgating, 7. Pretexting, 8. Business Email Compromise (BEC), 9. Quid Pro Quo, 10. Honeytraps, 11. Scareware, and finally 12. Watering Hole Attacks. Let's take a closer look at Phishing Attacks, Business Email Compromise (BEC), and Quid Pro Quo and how these specific attacks affect organizations when it comes to experiencing and handling cyber incidents (Jones, 2023).

Phishing attacks can usually be described as "an attacker trying to trick someone into providing sensitive account or other login information online" (Fortinet, 2023). Phishing attacks can be deployed in many different forms, but the end goal remains the same of having the users provide some type of information or credentials. Some of the most common phishing attacks used on organizations are whaling attacks, vishing, and spear phishing attacks. Whaling attacks are known as strategic attacks that are tailored for high-up individuals in an organization. These types of attacks are mainly delivered via emails and hope to get the credentials of users who have authority. These types of attacks are usually targeted toward chief executive officers and chief financial officers because of the access and authorizing power (Fortinet, 2023). Vishing attacks are voice phishing attacks that convince users that they are legitimate callers and use psychological manipulation to convince the user to provide some type of information. Spear phishing attacks are very similar to whaling attacks except that they require more reconnaissance since these attacks are targeted to specific groups or people. These attacks don't restrict their attacks to just high-up individuals within an organization but rather focus on targeting users who have access or authorization within a company. Phishing attacks can be used to target any user within an organization as long as they have some access or privilege deemed valuable.

Business Email Compromise (BEC) attacks can be described as "a type of social engineering attack that takes place over email. In a BEC attack, an attacker falsifies an email message to trick the victim into performing some action — most often, transferring money to an account or location the attacker controls" (CloudFlare, 2022). Organizations need to be aware of these types of attacks since organizations handle extreme amounts of money and assets. These attacks are similar to phishing attacks but they generally tend to not contain any malicious malware or links to click. This difference can make it difficult for organizations to filter out and restrict these emails, no malicious material makes it more difficult to spot them as they try to come through the network.

Finally, Quid Pro Quo attacks can be defined as attacks to manipulate user to once again give up information, credentials, and access. The difference with this attack is that the hackers will pretend to be their organization or another IT department needing to either repair something on their computer or account. This attack takes advantage of the of the trust user have in IT support (Thepsiri, 2024). Hackers tend to use technical terms to get the users to trust them and explain to them that they simply need to fix something “real quick” and then ask the user to log in, in order to gain access or privilege. Users are the weakest links in an organization due to the lack of knowledge and quantity. If hackers send out malicious social engineering attacks to hundreds of employees, they would only need a couple or even just one employee to fall victim to be successful.

One of the biggest organizations known today, fell victim to a well-planned social engineering attack. This was known as the 2020 Twitter Bitcoin Scam. Twitter is a global multi-million dollar company that invests time and money in keeping their organization secure, yet this attack almost took them out. It was reported that on July 15, 2020, an attacker had been sending out phishing emails trying to get employee credentials. While most employees knew better and tried to spread the information about the malicious attack about 6 employees fell for this attack, compromising the whole organization. The hackers had redirected the users “to a dummy site controlled by the hackers and entered their credentials in a way that served up their usernames and passwords as well as multifactor authentication codes” (Thompson, 2020). This attack led to fake tweets such as the infamous tweet from Binance stating that they would be giving back around $52 million in bitcoin and high-profile accounts such as Elon Musk and Kanye West dropping out of nowhere. The organization spent endless resources and time trying to get the hackers out of their network. As a result, every employee was forced to get on a video call to confirm that they had changed their passwords so the credentials the hacker got were no longer working. This was the result of a couple of users falling victim to a social engineering attack.

So, what can organizations do to prevent these specific types of cyber attacks? The 2 most effective ways for organizations to prevent these types of social engineering attacks from occurring, is through educating their users and implementing security policies. The Twitter attack demonstrated that it only takes a few users to not know what they are looking for, in order for a whole organization to get hacked. Security awareness training is an effective way for organizations to minimize their chance of falling victim to these attacks. If organizations properly train their user on the current social engineering attacks and techniques, they will become more aware of the information and material they are receiving. Properly training users on detecting these attacks also gives users the knowledge on how to handle these situations and how to better determine if an email, call, or text is legit. Many companies have begun implementing phishing emails tests in order to determine how aware and caution their user are and provide more training to those who fail. Implementing security policies can also help minimize the risk of an organization falling victim to these types of attacks. Policies can be applied to all aspects of an organization. They can range from user verification, password resets, and even social media usage relating to work. These types of policies make it more difficult for hackers to not only perform reconnaissance for their attacks but also makes it more difficult for them to gain initial access (Team, 2022). Social engineering attacks are not going anywhere any time soon, so organizations will need to consider the techniques and methods to best prevent these types of cyber incidents in order to keep not only themselves and their employees safe, but their organization as well.

## Reference Page

CloudFlare. (2022, November 3). What is business email compromise (BEC)? - cloudflare. https://www.cloudflare.com/learning/email-security/business-email-compromise-bec/#:~:text=Business email compromise (BEC) is,often bypass traditional email filters.

Fortinet. (2023, March 11). *19 types of phishing attacks with examples*. https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

IBM (2022, June 14). *What is social engineering?*. IBM. https://www.ibm.com/topics/social-engineering

Jones, T. (2023, December 8). *The 12 latest types of social engineering attacks (2024)*. Aura. https://www.aura.com/learn/types-of-social-engineering-attacks

Team, S. (2022, April 12). *8 ways organisations prevent social engineering attacks*. Australia's #1 Cybersecurity Services Company. https://www.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks

Thepsiri, T. (2024, June 5). *What is a quid pro quo attack & how to avoid becoming a victim*. IT Consulting & IT Solutions in Connecticut & Massachusetts. https://www.kelsercorp.com/blog/it-quid-pro-quo-social-engineering

Thompson, N., & Barret, B. (2020, September 24). *How twitter survived its biggest hack-and plans to stop the next one*. Wired. https://www.wired.com/story/inside-twitter-hack-election-plan/