Journal of Global Awareness

Volume 4 | Number 2 Article 8

December 2023

Social Engineering Cyber Threats

Young B. Choi
Regent University, Virginia Beach, USA

Recommended Citation
Choi, Young B. (2023) "Social Engineering Cyber Threats," *Journal of Global Awareness*: Vol. 4: No. 2, Article 8.
DOI: https://doi.org/10.24073/jga/4/02/08
Available at: https://scholar.stjohns.edu/jga/vol4/iss2/8

Abstract

The article explores the pervasive threat of social engineering in cybersecurity, emphasizing its success in infiltrating information systems by manipulating individuals rather than employing traditional hacking methods. The author underscores the vulnerability arising from human trust, as individuals, especially those lacking technology education, tend to be targets. While cryptography offers partial security, social engineering complicates overall system security. Mitigation strategies include educating employees on threats, risks, and security policies, coupled with enforcing penalties for noncompliance. Additionally, employing two-factor authentication and physical token-based access adds layers of protection. The article delves into semantic attacks, classifying various exploitation methods and emphasizing the critical role of user awareness. It addresses prevalent scams such as phishing, vishing, impersonation, and smishing, noting their impact on individuals and organizations. The study extends its focus globally, highlighting a unique advance fee fraud targeting vulnerable populations. Social engineering remains a significant challenge despite technological advancements, necessitating a multifaceted approach combining technical defenses, education, and public awareness.

Keywords: social engineering, cyber threat, cybersecurity, cyberattack, attack

Introduction

Social engineering is “a technique used by hackers or other attackers to gain access to information technology systems by getting the needed information from a person rather than breaking into the system through electronic or algorithmic hacking methods. According to a 2004 Information Technology Education Conference (CITC5 '04), “These attacks can be physical and psychological” (Orgill, Romney, Bailey, & Orgill, 2004, p. 177). The reason that social engineering is so successful and so dangerous to organizations is that “trusted people can fail to be trustworthy when it comes to protecting their aperture of access to secure computer systems due to inadequate education, negligence, and various social pressures” (Orgill et al., 2004, p. 177).

Discussion

People naturally trust technology until they are scammed and become very paranoid about it. CITC5 '04 stated the problem this way: "Social Engineering is an ever-present threat to the security of computer systems due to the illogical, social nature of human beings. The social engineer attempts to exploit the natural desire of humans to trust others; to assist in other labors, and to gain favor in their eyes" (Orgill et al., 2004, p. 177). Individuals who are not very experienced with technology or have not been exposed to education about the risks involved are very trusting by nature and therefore more susceptible to falling for a scam.

Cryptography is only a part of computer security and does not provide complete security by itself. Social engineering adds to the complexity of computer system security. The best methods for mitigating a social engineering attack include employee education on threats, risks, and organizational security policies with penalties for noncompliance (Orgill et al., 2004, p. 181). Education is the key to securing against uninformed computer users who easily fall for common social engineering attacks. Another wonderful way to protect against these attacks is by requiring physical token-based access or two-factor authentication mechanisms, which require more than one piece of information to authenticate. Physical token-based authentication is not easily transferrable knowledge that an attacker can learn and exploit. Biometrics are a good example of this.

The term “social engineering” is often used as a category of attacks that includes a wide variety of exploitations used to attack various targets with different strategies for psychologically manipulating an individual into doing something or revealing some information. The intention is for this to result in unauthorized access for the attacker or to unwanted activities on behalf of the attacker. A semantic attack is a particular variation of social engineering attack that “bypass technical defenses by actively manipulating object characteristics, such as platform or system applications, to deceive rather than directly attack the user” (Heartfield & Loukas, 2016, p. 37:1). It breaches a system’s security by deceiving the user.

The biggest weakness in a network or system is the end user. Hardware manufacturers and application programmers attempt to build security into their products while leaving room for custom configuration modification by administrators to meet the needs of their organization best. Built-in security cannot

always provide protection if the user of these products is not aware of what information should remain confidential and when it is appropriate to reveal confidential information. Security cannot prevent an end user from performing an unwanted activity that leads to a successful attack. “Even the strongest technical protection systems can be bypassed if an attacker successfully manipulates the user into divulging a password, opening a malicious email attachment or visiting a compromised website” (Heartfield & Loukas, 2016, p. 37:1). Examples of a semantic attack exploits include phishing, file masquerading, application masquerading, web pop-ups, advertisements, social networking, removable media, and wireless exploits.

Phishing is typically performed through mediums like email, webpages, URL links, instant messaging, or forums. File masquerading can be used in various file types like Office document files, application files, or system files. Application masquerading can be used in scareware, ransomware, or rogueware-type applications. A web pop-up semantic attack exploit could be a media plugin, error messages, or a bogus questionnaire. Malvertisement exploits might be an infected ad, a one-click fraud, or a download button. A social networking exploit could be a friend injection, fake video links shared around social networking, or game requests. Removable media exploits are often seen with USB sources, flash drives, memory cards, or other types of removable media. Wireless exploits might be a rogue access point or a rogue RFID chip (Heartfield & Loukas, 2016, p. 37:1).

An effective way to classify, analyze, compare, and secure against semantic social engineering attacks is by grouping exploits into related attack families based on relationships between application behavior and response so that the characteristics are universally applicable. According to Heartfield & Loukas (2016), the aim is “to help researchers and engineers develop technical defense approaches for both current and future semantic attacks by addressing core semantic attack characteristics rather than particular implementations” (p. 37:2). This helps researchers to evaluate the requirements for a solution to the attack based on current and future threats. There are also various stages and characteristics throughout an attack. The UK government’s National Technical Authority for Information Assurance (CESG) has defined three control stages of orchestration, exploitation, and execution for cataloguing the distinctive characteristics of an exploit.

Orchestration is the first control stage defined by CESG. This stage includes characteristics like how the target is chosen, how the attack reaches the target, and whether the attack is automated or manual. Researching how a target is chosen helps to identify "the conditions for exposure to an attack" (Heartfield & Loukas, 2016, p. 37:4). This is going to be classified with a target description, whether the target is an individual or a group selected at random or selected based on their identity. This includes whether it was explicit targeting based on identity or promiscuous targeting based on random selection.

How the attack reaches the target can help identify platforms that are used. This includes a method of distribution used to reach a target. Methods of distribution can include software distribution exploiting system flaws, local distribution from within a system, or remote distribution originating from an outside host web server or application (Heartfield & Loukas, 2016, p. 37:6). Method of distribution can also include hardware distribution with an attack being distributed without the target's operating system. Knowing if the attack is automatic or manual helps to identify what information can be discovered about the attacker's behaviors. The mode of automation classifies exploits based on the level of involvement by the attacker in the attack's activation and administration. A manual attack requires intervention from the attacker, while an automatic attack is delivered without the attacker's intervention.

The second control stage defined by CESG is exploitation. This stage includes characteristic classifications based on how the user is deceived. CESG uses what is called a deception vector to “define the mechanism by which the user is deceived into facilitating a security breach and can be categorized as cosmetic, behavior-based, or a combination of the two” (Heartfield & Loukas, 2016, p. 37:8). A cosmetic exploit type uses a manipulated GUI to exploit the trust that exists between a GUI designer and the user. The GUI designer trusts that the application be used correctly. The user trusts that the GUI will work as designed. A behavior-based cosmetic exploit achieves deception by offering what looks to be the intended behavior of a legitimate system rather than deceiving by looks. Interface manipulation is another characteristic classification for the exploitation stage.

The execution control stage defined by CESG focuses on whether the attack completes deception in one step or if the deception persists. If researchers can find one step that can be thwarted in an attack deception, then the exploit could be

stopped more easily. If the deception persists, then the exploit deception will continue to attempt to deceive the user until successful. The exploit might use a one-off approach where the user triggers the attack with some action. The exploit might instead use a continual approach where the deception attempts continue even after an attack is triggered. The exploit might consist of one or several steps. A single-step exploit requires that a target user carries only a single action to trigger the attack. A multi-step exploit requires a target user to be deceived multiple times to trigger the attack (Heartfield & Loukas, 2016, p. 37:10).

With all these classification groupings, researchers can organize exploits based on these behavior and response relationships to find current and future attack solutions. In doing it this way, which platform is used does not matter as much since the attack characteristics are not tied to platforms. For example, a phishing website looks legitimate but is used to distribute malware or steal user information and/or user money. A phishing website is classified as an automatic attack without the intervention of the attacker. It is classified as promiscuous targeting because its targets are selected at random rather than by the target's identity. The target is whoever visits the spoofed website. A phishing website's orchestration is classified as a remote distribution method since it originated outside the target's system from a remote host. A phishing website's exploitation is classified as using a hybrid type deception vector since it employs both cosmetic and behavior-based deception. It is classified as programmatic exploitation. A phishing website's execution is classified as a one-off single-step attack. It requires only one action to trigger, and only one step for deception is needed to get a user to conduct that action.

Social engineering is quite common nowadays. It is used in more than two-thirds of all hackings, according to Laura Shinn of Forbes.com (2017). Laura writes about the findings of Social-Engineer.org in a report identifying the four main ways in which social engineering is occurring: phishing, vishing, impersonation, and smishing. Phishing is when a hacker uses a platform like email to deceive someone into revealing access information to obtain unauthorized access to some system. Vishing is when the attacker uses a voice platform like a phone call to do the same thing. Impersonation is done in person. An attacker may attempt to exploit someone by loaning physical access information like an ID card or trick security personnel into granting access based on false pretenses. Smishing occurs through text messaging (Shin, 2017).

According to SocialEngineer.org (2014), phishing accounts for 77% of all socially based attacks. Businesses targeted by phishing attacks lost $43,000 per account. On average, individuals targeted through impersonation attacks lost $4,200 (Social-Engineer.org, 2014). Shin continues by identifying the current top social engineering scams to be aware of. The IRS scam is when hackers call the target with a spoofed phone number showing that they are calling from Washington, DC, and claiming to be calling from the Internal Revenue Service. The hacker already knows basic information about the target and uses threats to deceive the target into sending an overdue payment through a nontraceable money transfer to the attacker. Another current top scam is ransomware, which is when hackers deceive targets into installing malicious software that encrypts all data within access of the target's system. The target is then presented with a message demanding payment for the decryption key to unlock the data. Often, the attacker will take payment and not unlock the data for the target, so paying the ransom is an ineffective solution and makes the problem worse. A Business Email Compromise scam (BEC) is when a hacker attempts to gain access to an email account to find confidential financial data or login information. This is often done through malware-infected file attachments or password reset links (Shin, 2017).

Every year, the FTC, the IRS, and other sources put out warnings stating that the IRS will never call to demand immediate payment over the phone, demand that you pay taxes without having the option to appeal, require you to use specific payment methods, ask for credit card information over the phone, or threaten to bring in local police if you fail to pay. Still, the IRS phone scam is one of the most successful attacks nowadays, mostly targeting the elderly, who are easy prey for an attacker. The attackers claim to be employees of the IRS, demanding immediate payment with the threat of arrest or property seizure if the victim fails to meet the attacker's demands. "They use fake names and bogus IRS identification badge numbers, and they sound very convincing. In many cases the caller becomes hostile or insulting" (*Important information regarding IRS scam phone calls*, 2015). It is easy to see why the elderly and other victims might fall for this type of attack.

A 2017 report from the 26 International World Wide Web Conference 2017 (WWW17) held in Australia investigated a unique advanced fee fraud scam targeting Nigerians, among other global scams. In this report, WWW17 indicates that "criminals exploit the socio-political and economic problems prevalent in the country to craft various fraud schemes to defraud vulnerable groups such as

secondary school students and unemployed graduates" (Mba, Onaolapo, Stringhini, & Cavallaro, 2017, p. 1301). Truly little is known about social engineering scams targeting the continent of Africa, creating an impression that they are immune to cyberattacks, while Western nation cyberattacks have been professionally researched and documented. The research investigated a form of 419 advance fee fraud scam unknown to the West. An advance-fee fraud, also called an up-front fee fraud, is a scam that promises to send you money, products, or services in exchange for a fee, offers a special deal, or asks for help relocating funds out of a country. If the target falls for it, they pay the fee to the attacker, expecting to receive some appealing amount of money, products, or services in return.

A unique type of 419 scam is targeting economically weak and vulnerable Nigerians. In one example, the attacker convinces Nigerians to purchase mobile phone prepaid credit for the attacker in exchange for manipulating school grades. The attacker simply converts the prepaid credit into money and doesn't provide what is promised (Mba et al., 2017, p. 1302). This shows that social engineering is a global problem, and just because people may not have advanced technology like Western countries, they are still a potential target for social engineering attacks.

A generic form of social engineering attack is known as fake tech support call scams. This is where an attacker tricks a target into believing that their computer has a problem, such as a virus or slow system, and offers to fix the problem for a fee. The attacker typically does this by calling the target directly or with an advertisement made to look like a system notification pop-up from Microsoft or Apple. The pop-up tells the target that their computers are infected and offers support via telephone. If the target calls the provided number, the attacker claims to be from Microsoft or Apple (Kobie, 2017). Often, the attacker will ask the target to pay hundreds of dollars for support for a problem that does not exist. The FTC is working with local and international authorities to combat these scams.

When attackers impersonate tech support and initiate contact with a target, it is not very sophisticated hacking, according to Brian Kelly, Quinnipiac's chief information security officer. Kelly says, "If you don't initiate that conversation, you probably don't want to have it" (Grahn, 2017). Recently, senior Lezlie McEachern was contacted by a tech support employee claiming her computer was infected with a virus. McEachern fell for it and ended up paying $250 to the attacker. She ended up getting her money refunded and was incredibly lucky to have gotten the refund.

McEachern advises this: "Just look up the company that sent you the message, and if somebody sends you a message, do not call them. You should be reaching out to people to help with your computer, somebody should not be reaching out to you" (Grahn, 2017).

Seniors are often the targets of social engineering attacks and other scams. In 2016, the US Senate released a publication of the top 10 frauds targeting seniors. The first is IRS impersonation scams. The second is Sweepstakes scams. Third is robocalls or unwanted phone calls. Fourth is computer tech support scams. Fifth is identity theft. Sixth is grandparent scams. Seventh is elder financial abuse. Eighth is grant scams. Ninth is romance scams. Finally, the tenth is home improvement scams (*Senate Aging Committee Announces Top 10 Frauds Targeting Our Nation's Seniors*, 2016). The Senate Aging Committee has placed an extremely high priority on stopping these scams on our nation's seniors.

The committee maintains a Fraud Hotline (1-855-303-9470) with investigators taking fraud reports and providing help and guidance to victims of these scams, often directing seniors to appropriate authorities. These attackers target seniors in numerous ways. They sometimes "inspire fear by impersonating a law enforcement official and threatening adverse actions if a senior refuses to send them money, or they may pretend to befriend a lonely senior online and convince the victim to send them money" (*Senate Aging Committee Announces Top 10 Frauds Targeting Our Nation's Seniors*, 2016). The committee views raising awareness of these scams as critical in stopping them.

Another sophisticated type of social engineering attack is performed through a web browser where the attacker can produce a website that appears to the target to have the same URL as a legitimate website with a legitimate security padlock and HTTPS certificate from a valid certificate authority when it is using a fake web server, a fake certificate authority, and a fake certificate. This can easily deceive a target into revealing private financial or login information without recognizing the deception. This attack relies on web users' trust in web browser security indicators. The reason the attack is not easy to detect is due to the fact this complies with security measures and appears legitimate to web browsers (Benítez-Mejía, Zacatenco-Santos, Toscano-Medina, & Sánchez-Pérez, 2017, p. 24).

In this type of HTTPS phishing attack, the phishing is invisible to the web user. HTTP over TLS was designed to protect confidential information sent over the web. Once a secure connection is established, a web browser typically indicates this with a padlock symbol, and the address changes from standard HTTP to HTTPS. These are the primary indicators that web users regularly notice before they expect that the information being transmitted is encrypted and secure from unauthorized disclosure. Not many web users delve into the advanced details of certificates to look for irregularities to be able to detect this type of phishing attack.

The attacker prepares for this attack by creating a fake certificate authority and a fake web server. The attacker must somehow modify the victim's host file, "adding the IP address of the fake web server" (Benítez-Mejía et al., 2017, p. 25). This can be done in three separate ways. The attacker can physically access the victim's computer and modify the host file himself; the attacker can achieve remote access to the victim's computer through deception to modify the host file remotely, or the attacker can convince the victim to modify the host file for them. Once this is completed, the phishing attack can begin.

First, the victim types the URL in the web browser, requesting a connection to the legitimate web server. Then, the fake web server listed in the victim's host file shows its certificate to the web browser. The web browser tries to confirm that the certificate is valid. A fake certificate authority then confirms that the certificate is valid when it is not. The web browser is tricked into thinking it is valid, and the connection is established to the fake web server. The fake web server then can capture login information from the victim. Then, the fake web server redirects the victim to the legitimate web server, having already captured the login information for the attacker, which can be used for unauthorized access (Benítez-Mejía et al.-Pérez, 2017, p. 25).

The Oxford Academic *Journal of Cybersecurity* article "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack" (2015) by Jon R. Lindsay explores the effectiveness of cyberattack deterrence through denial and punishment. Specifically, the article examines whether either option is feasible or if there is little that can be done to deter attacks. "Scholars and policy analysts are generally pessimistic about cyber deterrence" (Lindsay, 2015).

This article offers insight into the attempts to deter cyberattacks like social engineering attacks. One interesting aspect that is analyzed in the article is that of deterrent effectiveness for low-value attacks compared to high-value attacks. Interestingly, deterrent for high-value attacks is typically more effective and deterrent for low-value attacks are always ineffective. In other words, "Deterrence works where it is needed most, yet is usually fails everywhere else" (Lindsay, 2015). This is why many experts view the denial deterrent as feasible and the punishment deterrent as less than feasible.

Phishing attacks are the most used social engineering attacks. Combating phishing attacks is extremely important for all of us. Because of this, phishing has been the focus of academic and industry research. According to a report from the 26 International World Wide Web Conference 2017 (WWW17), "From October 2013 to February 2016, phishing scams caused at least $2.3 billion in damages, involving 17,642 businesses in more than 79 countries" (Cui, Jourdan, Bochmann, Couturier, & Onut, 2017, p. 667). Phishing is a serious global concern.

A few approaches have been researched for improving the detection of phishing sites. One approach is to look for the phishing site and the legitimate site that it mimics by comparing similarities between the two sites. A second approach is to compare the characteristics of phishing sites. Similar characteristics that can reveal phishing might be found in web forms or URL structures. A few methods have been offered for finding similarities between sites. A hash-based method has been used where the HTML of the phishing page is hashed using SHA1.

Because it has been found by those who have evaluated this method that a significant percentage of phishing sites are replicas of those in their database, measuring the hash values can help find phishing sites. Another method is to compare the structure of the DOMs by computing a "tag vector" of the phishing page (Cui et al., 2017, p. 668). The WWW17 report shows that attackers like to create phishing sites based on past phishing sites, so there are generally a lot of consistent similarities to already discovered phishing sites. This helps with detection mechanisms by looking for these commonalities.

A 2017 Data Breach Investigations report from Verizon shows the growing impacts on business from phishing and another social engineering threat called pretexting. The report shows that forty-three percent of data breaches used phishing. However,

pretexting is another tactic on the rise. This attack is primarily used to attack financial employees (Verizon releases results of its 2017 data breach investigations report, 2017). Pretexting is when an attacker impersonates someone else to use that person's identity to obtain information.

Conclusion

Social engineering is a profitable attack for attackers, so it will continue to advance in technology, and the effectiveness of social engineering attacks will continue to change as deterrent and denial mechanisms are developed. Everyone, no matter how secure and prepared, is susceptible to a social engineering attack to some degree. Everyone is a target, although some targets are more exposed than others, and some targets are more valuable. Researchers tend to agree that security technology alone is not enough to combat these attacks. Education and awareness are critical to overcome the human component that can be exploited.

References

Benítez-Mejía, D. G., Zacatenco-Santos, A., Toscano-Medina, L. K., & Sánchez-Pérez, G. (2017). HTTPS: A phishing attack in a network. *ICICM 2017*, 24-27. https://doi.org/

Cui, Q., Jourdan, G., Bochmann, G. V., Couturier, R., & Onut, I. (2017). Tracking phishing attacks over time. *WWW2017*, 667-676. https://doi.org/

Grahn, M. (2017, Mar 01). Information security warns about fake tech support. *University Wire.*

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48, 1-39. https://doi.org/

Important information regarding IRS scam phone calls. (2015). Washington: Federal Information & News Dispatch, Inc.

Kobie, N. (2017, May 15). FTC cracks down on tech support scams. *IT Pro*, Retrieved from https://www.itpro.com/

Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattacks. *Journal of Cybersecurity*, *1*(1), 53-67. https://doi.org/

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. WWW17 Companion: Proceedings of the 26th International Conference on World Wide Web Companion, 1301- 1310. https://doi.org/

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The Urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. CITC5 '04 Proceedings of the 5 Conference on Information Technology Education. 177-181. https://doi.org/

Senate aging committee announces top 10 frauds targeting our nation's seniors. (2016). Washington: Federal Information & News Dispatch, Inc. Retrieved from https://www.aging.senate.gov/

Shin, L. (2017, January 04). Be prepared: The top 'social engineering' scams of 2017. *Forbes*. Retrieved December 07, 2017, from https://www.forbes.com/

Social-Engineer.org. (2014, April 28). The social engineering infographic. Retrieved December 6, 2017, from https://www.social-engineer.org/

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behavior & Information Technology*, *32*(10), 1014-1023. https://doi.org/

Verizon releases results of its 2017 data breach investigations report. (2017). *Wireless News*. https://www.ictsecuritymagazine.com/