Social Engineering

COM 450

Christine Potthast, Patrick Berry, and Hamad Al-Naimi

March 5, 2019

Abstract

With cybersecurity being an ever-so-challenging field, many institutions focus on firewalls, antiviruses, and other tools to combat any potential threat. An area of cybersecurity that is often overlooked is social engineering. Social engineering consists of tactics that take advantage of people giving others trust (Granger 2). Through clever manipulation and schemes, there are several ways hackers can easily gain access to information they are not authorized to access. For a hacker, social engineering is a much easier method in gaining information than a more technical attack. Instead of passing through several perimeters to access an institution's server to intercept data, it is much easier to manipulate people. By manipulating the people who have access, hackers can gain confidential information much more efficiently. In this paper, we will cover several forms of social engineering attacks, including phishing, quid pro quo, baiting, pretexting, tailgating, and shoulder surfing, as well as measures against them.

Phishing

Phishing is a form of social engineering wherein an attacker attempts to acquire sensitive information from a victim by impersonating a trustworthy third party. There are several different types of phishing, such as general phishing, spear-phishing, whaling, and vishing. In a general phishing attack, the attacker sends an email from a spoofed email address to as many people as they can, with the hope that some percentage will follow the link. They may attain the email addresses to which they send the malicious email by hacking into a company's email address store. In this attack, the address from which the email is sent is spoofed to appear to come from a trustworthy source. Banks, social websites, auction sites, online payment processors, or IT administrators are common purported identities. When users receive the email, there is an embedded link that the user must click to be redirected to the malicious site. This site is typically designed to look identical to the genuine site to avoid suspicion on the user's part. There will then be a prompt for the user to enter their username and password to "login" to the site, but the attacker instead steals the user's credentials. Once the user has completed the login process and the attacker has collected the information, the site may display an error message instructing the user to return later. This is another measure used by attackers to alleviate suspicion. Spear-phishing is similar to general phishing, but it is directed at a specific individual or company. Typically, in this form of phishing, the attacker will gather data on the victim to more gear the attack to a particular target. For example, an attacker targeting university students could gather data and determine which individuals are friends. They could then spoof the email address to make it appear that the email has come from a friend or teacher. Whaling is similar to spear-phishing; it is spear-phishing attack aimed at a senior executive or high-profile target. Vishing, voice phishing, is another form of phishing. This attack consists in a message from the attacker

telling a user to call a certain number, where they are then prompted for their credentials. Businesses can lose millions of dollars in attacks such as these, so preventative measures are essential.

An example of a phishing attack that occurred in 2018 involved attackers impersonating Airbnb. This attack took advantage of the confusion created by the European Union's General Data Protection Regulation (GDPR). The GDPR put forth new regulations regarding personal data protection and privacy for all members in the EU. This required some changes in terms and conditions, which was the basis of the attack (Bisson, 2018). Attackers sent emails that seemed to have originated from Airbnb and assumed that the user had an account. It then directed users to follow a link to accept the new terms and conditions to be able to continue to use the service. However, this link took them to a fake site where personal information entered was stolen.

Phishing is a very large problem, so prevention and countermeasures are imperative. These can take the form of user training, public awareness, login security measures, technical security measures, and legal repercussions. User training is probably the most impactful measure against phishing. Users should be trained to be aware of suspicious emails and not to click on any links unless they have confidence in its legitimacy. Attacks often take the form of "account verification" requests, so users should be extra weary of these. A good practice is to contact the company before acting. Additionally, legitimate corporations typically address users by their name or username, so a generic greeting should be another red flag for users. Even if the user has relative confidence in the legitimacy of the link and request, it is safer to directly type the URL of the company than to follow hyperlinks. After users have been trained, the company should test their awareness and vulnerabilities by simulating phishing campaigns. This helps the company identify users who need further training. Public awareness is another preventative technique

against phishing. There are websites, such as Safe Browsing, available that contain lists of known phishing sites. Other websites, such as FraudWatch International, provide specific details about exact phishing messages and attacks. Once phishing websites have been identified, companies such as PhishTank can be enlisted to disable them. Login security is another preventative measure against phishing. Some companies have a picture assigned to each user that is displayed on the legitimate website before login. Others display a dynamic grid of images that the user must choose from, and the user is assigned a theme by which they pick a grid picture. Another login security measure is two-step authentication with the user's cell phone. Technical security measures include spam filters on emails. These utilize machine learning and natural language processing approaches to classify phishing emails. There are also legal repercussions for phishing attackers who are caught. If attackers can be traced, they can be arrested and face consequences. The Fraud Act of 2006 gives jails time of up to ten years for fraud such as phishing, depending on the circumstances. Overall, this attack persists because it exploits human weakness, and the best technology or security measures cannot prevent a user from clicking on a link.

Quid Pro Quo

Quid Pro Quo is another form of social engineering that targets user information. The Quid Pro Quo attack promises a benefit, typically in the form of a service, in exchange for information from the user. This attack generally consists of three phases, which include sabotage, advertising, and assisting. (Ivaturi, and Janczewski, 2011) The first step consists of the attacker sabotage a company's network so that they cannot function or are hampered. This then leads to the second stage of the attack, advertising. The attacker advertises himself as someone who can fix the problem with some aid from the user. This brings the process to its final stage, assistance.

In this stage, the attacker fixes the problem and asks the user to log on to the system to ensure that it works, wherein the attacker steals the user's credentials. Alternatively, instead of stealing the user's credentials, the attacker could have the user download a software patch with embedded malware. The attacker may also skip the sabotage stage and simply call random numbers at a company looking for anyone with a problem, which they then address and exploit. During this process, the attacker may instruct the user to disable their antivirus software to avoid detection. At the end of the process, the problem of the company is fixed, and the user has little cause to be suspicious.

Like with phishing, the biggest preventative measure against such a quid pro quo attack is user training and awareness. User training should guide users to be suspicious if ever they are contacted by a company who claim solutions to their problems. If a user is called by an "IT department", they should be cautious, not simply lowering antivirus software or downloading whatever alleged fix is available. A good practice is to not act on any phone call right away, but to call the company back at the publicly listed phone number. Additionally, it is always wise for the user to update their password regularly.

Baiting

Baiting is a form of attack that takes advantage of people's trust in a medium that they somehow obtained. Usually, because the victim is curious, a malware-infected medium is connected to a server or workstation, jeopardizing the entire network. There are two ways the medium gets in the hands of the victim, by finding it or by distribution. In most cases, the medium is found by the victim and because they are curious, they connect it to the network. In other cases, the hacker could have the infected medium sent directly to the victim in some form, therefore, almost guaranteeing that it will connect with the network. The most common instance

of this form of attack is in the form of a hard drive (Arfuso, 2015). The hacker would physically leave a hard drive in an open location, visible to victims. To entice the victims, many times the hard drive could have a company logo on it or anything to make them believe that the medium is trustworthy. Since the victim is curious, they plug it into their workstation. Consequently, the hacker now has access to not only that device but the institution's network. The best method in defending against baiting attacks is through educating the entire team. An institution should host workshops and other educational events that educate employees to never connect an unidentified medium to the network. Since baiting is such an easy method for hackers, it is one of the most common attacks out there.

Pretexting

The practice of obtaining information under a false identity, often impersonating a trustworthy position, is known as pretexting. Pretexting is generally not as easy as telling a simple lie to obtain information; there is generally a thorough process that the hacker undertakes to acutely prepare for the attack. With the goal of reaching the trust of the victim, the hacker will do anything to make the victim believe in their false identity. During this social engineering engagement, the hacker needs to determine their new persona. The background story, clothes, attitude, and personality of the hacker will all determine if they can earn the trust of the victim (Hadnagy, 2011). This means that lengthy research is required for a successful attack to occur. It is also essential for the attacker to go in with a clean slate, truly embodying the persona they are trying to obtain, not showing anything personal about themselves. The attacker has to also focus on execution, trying to keep the entire process clean and not lengthy (Hadnagy, 2011). If the attacker asks for too much access and gets greedy, the entire attack can fail. It is better for an attacker to keep the entire engagement as simple as possible. The pretext should be smooth and

not very complicated to the point the attacker could forget a step. One of the most popular pretexting cases was the Hewlett-Packard scandal. When the company had a board member feeding information to outside sources, the company hired an outside service to investigate their board members. This was very controversial because to obtain the information the investigators needed, they used pretexting tactics, impersonating an identity in which they are not. Specifically, the hackers manipulated the board members to receive phone records, in an attempt to identify who was feeding information to outside sources (Ivaturi, 2011). This case inspired stronger privacy laws regarding pretexting for the future. To prevent this from occurring to an institution, employees need to be trained to be more cautious. There should be more set identification measures in place to ensure that information is not obtained by unauthorized hackers.

Tailgating

It is very important to understand the concept of tailgating. Tailgating is a type of social engineering attack that usually involves a lack of proper authentication, allowing an unauthorized individual to follow an employee into such a restricted area. The tailgating attack is very dangerous, because there are often unauthorized people present at access point that could exploit these vulnerabilities to gain access to sensitive areas or information.

It is apparent that using such a technique helps the attacker focus on the target and understand the best way to compromise the security of a building or a person. The user, or employee, should be aware of his surroundings and realize that not everyone is who they claim to be. Every individual must realize that they are a part of the security of the whole organization and ensure that they are the only person who enters the area on their own authentication. Even if the person trying to follow an employee into the restricted area claims to be another employee,

they should not be allowed to gain access. This pertains to areas where sensitive information is stores, as well as other areas, as attackers may have goals other than simply stealing information. Thus, employees should always be wary of unknown individuals, particularly if they try to access restricted resources.

Several measures can be employed against tailgating. One example is the distribution and use of badges or ID cards with different levels of security access, with access granted on a need-to-know basis. Thus, only employees with specifically assigned access to sensitive information would be allowed to access an area where such content is stored. Another check against tailgating is the implementation of security guards and cameras at access points. Security guards would be able to spot someone attempting to tailgate and stop them. If for some reason an attacker managed to bypass the security guards, them at the very least they would be recorded on camera and be able to be identified and tracked down as soon as the breach is discovered and the surveillance is analyzed. These are just a few steps that could be taken to significantly reduce the likelihood of tailgating,

Shoulder surfing

Another form pf social engineering is shoulder surfing. Shoulder surfing consists of an attacker looking over the shoulder of a user to gather information. It can be used for obtaining the personal information including the passwords, numbers, and other data that is confidential for an individual person or a company, simply by looking over the shoulder of the victim.

Often times, this kind of attack occurs when an individual is using an ATM or doing some transaction in an open place or in a reckless way. In such cases, any individuals out in public could be watching and be an attacker, particularly around an ATM. This type of attack

could also take place within the workplace. If an unauthorized or ill-intending individual can infiltrate a building, they could simply come in to gather user credentials to later use against the company. This can be done by blending in with those around and observing when employees log into their system.

There do exist measures against shoulder surfing, and many of them come down to common sense and caution. For example, when entering a pin at an ATM, the simple practice of covering the number pad while typing the pin is sufficient to prevent shoulder surfing. This is slightly more difficult in the workplace, as people are naturally more comfortable there than out in the public. However, the easy action of looking around and making sure there is no one explicitly watching greatly mitigates the chance of information being stolen via shoulder surfing. These practices are exceedingly easy to implement, so employee training on the topic would be fast and painless, while exponentially decreasing the chance of a data breech from this attack.

References

Arfuso, Greg & Patterson, Nigel. (2015). A Look into Social Engineering. Retrieved from https://commons.marymount.edu/pattersonportfolio/wp-content/uploads/sites/4250/2016/03/CorporateCyberSecurityGroupProject.pdf

Bisson, D. (2018, August). *5 of the Most Notable Phishing Attacks of 2018… So Far*. Retrieved from https://blog.barkly.com/phishing-attacks-campaigns-2018.

Granger, Sarah. Social Engineering Fundamentals, Part 1: Hacker Tactics. Retrieved from https://s3.amazonaws.com/academia.edu.documents/33172114/04SocialEngineeringWebQuest.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1551657297&Signature=XqiPE7FAeAXfpexoqN1HwqQDUcA%3D&response-content-disposition=inline%3B%20filename%3D04Social_Engineering_Web_Quest.pdf

Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. Wiley Publishing.

Ivaturi, K., & Janczewski, L. (2011). *A Taxonomy for Social Engineering Attacks*. In *CONF-IRM*. Retrieved From https://aisel.aisnet.org/confirm2011/15/?utm_source=aisel.aisnet.org/confirm2011/15&utm_medium=PDF&utm_campaign=PDFCoverPages

Krombholz, K. Advanced Social Engineering Attacks. Journal of Information Security and Applications, 22, 113-122. Retrieved from https://www.sciencedirect.com/science/article/pii/S2214212614001343