Hacking the Human

David McDaniel

mcdanielda15@students.ecu.edu

November 2018

East Carolina University

Abstract

Information security professionals must plan for, identify, and mitigate threats originating from a myriad of sources. While these individuals and teams are required to implement numerous technological controls and protections such as firewalls, intrusion detection systems, strong password usage, and even encryption, it is often a threat from an inside vector that is overlooked. These insider threats are frequently in the form of social engineering attacks from external actors on the organization's employees. In this paper, the author begins by providing an introduction to social engineering, briefly explaining its history in regard to information security. Next, the author seeks to explain several types and vectors of social engineering attacks. The third segment of this paper focuses on recent high-profile social engineering attacks. In the fourth and final part of this paper, the author seeks to explain several strategies for mitigation and defense of social engineering attacks.

INTRODUCTION

Information security, in a broad definition of the term, is ensuring the proper confidentiality, integrity, and availability of information assets of an organization (Anderson, 2003). Indeed, nearly every textbook, study, or expert presentation regarding information security includes the discussion of at least one of these three facets. However, as information assets are hardened by increased security controls, encryptions, and more, often, the weakest link is the human (Heartfield & Loukas, 2016). The *Oxford English Dictionary* offers two definitions of social engineering, only one of which is applicable to the information provided in this paper: "[t]he use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes" (Social Engineering, n.d.). In today's cyber environment, social engineering, as well as the definition provided above, is generally recognized as an attempt to fraudulently gain access to an information asset in an effort to exploit the asset for any number of reasons, including financial gain, political reasons, ideology, fame, and more (Hayes, 2017).

HISTORY OF SOCIAL ENGINEERING

There exists a well-known tale in ancient Greek mythology of the Trojan Horse where Greeks built a large wooden horse to infiltrate the city of Troy (Serban & Serban, 2014). While it is debated how much of this story is true (White, 2014), what is known is that the construct of human deception has been prevalent for centuries, if not millennia. In these early instances, the deception was largely performed for personal or political gain.

In 1946, following the Manhattan Project, an influx of government defense funding advanced technology and ushered in the phone "phreaking" movement within the 1970s (Jatfield, 2018). Phone phreaking, or illegally making phone calls on a telephone network without being charged (Gold, 2011), is often considered one of the beginnings of the modern-day hacking culture (Jatfield, 2018). Jatfield (2018) further explains that this was also one of the first instances of using deceptive tactics for their own gain, the very definition of social engineering. Through the next several decades, as technology improvements were made in the forms of more advanced technical protection methods, the use of social engineering tactics begin to rise (Thompson, 2006).

TYPES AND VECTORS

Technology assets can become targets of social engineering attacks through seemingly countless vectors. These methods can include the use of carefully crafted email messages, phone calls, in-person verbal encounters, or even through the use of faking a gift in the form of a Trojan Horse just to infiltrate the enemy's city. Depending on the target, a malicious actor could choose any one or combination of these vectors to execute their attack. Some of the most popular types of social engineering attacks include:

Phishing

As described by Martin, Dubé, and Coovert (2018), phishing attacks and their respective responses by victims account for a majority of the cybersecurity breaches. Phishing is defined as "a fraudulent form of email that solicits personal or financial information from the recipient, such as a password, username, or social security or bank account number" (Resnik & Finn, 2018). Often, the email messages received from these attackers are formatted and designed to be nearly indecipherable from messages from legitimate sources (e.g., the recipient's financial institution or employer).

Spear Phishing

A subset of phishing attacks, spear phishing targets specific individuals of an organization. Typically, the selected targets are of chosen based upon the target's value or perceived susceptibility of success. Spear phishing emails require significantly more effort on behalf of the attacker, but this effort is more likely to prove fruitful as personalized phishing messages have a higher success rate than those of generic messages (Tiwari, 2018).

Pretexting

Pretexting is defined as an attack which relies on the attacker creating a false good pretext with a victim in order to gain access to information or a facility. An example of such an attack is for an attacker to impersonate a maintenance worker in order to gain access to the physical premises of the organization (Bisson, 2015). Once on-site, attacks upon the physical or technical infrastructure of the facility would be much easier to accomplish.

Baiting

Baiting is a social engineering attack in which the victim is promised something in order to gain their cooperation. Steve Stasiukonis, vice president and founder of Secure Network Technologies, Inc. (2006) documented a baiting experiment where his organization planted a Trojan on several USB thumb drives and scattered them throughout the employee parking area of a credit union's facility. What was found is that out of the 20 USB drives planted, 15 of those were found and inserted into a company system, executing the payload and initiating keylogger software.

Quid Pro Quo

Latin for “something for something” (Quid pro quo, n.d.). Recently, a surge of quid pro quo attacks has emerged where an attacker makes a telephone call to the victim and imitates a technology vendor (e.g., Microsoft) offering the victim a good or service, such as virus and malware removal. In this example, once the attacker gains access to the victim’s system, will install malware of their own in order to gain access to the victim’s system and/or data.

Tailgating

Typically, organizations require authorization to access a facility’s premises via access controls such as key cards, physical keys, or numeric keypads. Tailgating attacks occur when these controls are subverted by an unauthorized individual following an authorized individual into the building or area (Ritchey, 2015). This can allow malicious individuals to gain access to the facility in order to cause harm to either the organization’s property or the employees (Ritchey, 2015).

RECENT HIGH-PROFILE ATTACKS

In the past several years, it seems that it has become routine to see the announcement of a company’s network being breached or a suspected state-sponsored act of cyber terrorism has been carried out. Many of these attacks were carried out by exploiting vulnerabilities in the technical infrastructure of the organizations. For example, over 143 million Americans had their personal information accessed during the Equifax breach of 2017, which was enabled by exploiting a vulnerability in the Apache Struts database system (Luszcz, 2018). However, many breaches occur because of non-technical reasons, such as social engineering.

2011 RSA SecurID Phishing Attack

On March 17, 2011, RSA, the maker of secure authentication tokens was targeted in a social engineering attack. Two hacker groups, allegedly conspiring with a foreign government, sent phishing emails to several RSA employees, impersonating familiar people (Armerding, 2017). These phishing emails were flagged by the company's email spam filter, but at least one recipient opened the attached malicious Microsoft Excel document, allowing the attackers into the network (Rashid, 2011). The successful phishing attack allowed the malicious actors to exploit a zero-day Adobe vulnerability and access sensitive information regarding RSA's SecurID system, resulting in the company replacing millions of SecurID tokens (Krombholz, Hobel, Huber, & Weippl, 2015).

Sony Pictures Entertainment

In November of 2014, a hacker group called The Guardians Of Peace (or GOP) hacked into Sony Pictures Entertainment and stole hundreds of gigabytes worth of proprietary and private employee information, posting the information online for public access (A Breakdown and Analysis of the December, 2014 Sony Hack, 2014). While there is much discrepancy and secrecy about how the attack occurred, several researchers, such as Stuart McClure of Cylance has determined that the attack was initiated via a "pattern of phishing attempts" (Bisson, Sony Hackers Used Phishing Emails to Breach Company Networks, 2015). After successfully phishing several critical staff members' Apple ID accounts, the attackers proceeded to research their victim's on LinkedIn, finding information regarding co-workers who may have elevated network privileges for additional social engineering attacks (Keizer, 2015). Keizer (2015) continues to explain that these social engineering attacks proved fruitful in gaining credentials that were subsequently hard-coded into customized malware tools targeted at the organization.

Associated Press Twitter Account

On April 23, 2013, the Twitter account for the Associated Press posted a message stating "Breaking: Two Explosions in the White House and Barack Obama is injured" (Santiago, 2017). While it was quickly determined that the post was erroneous, during the three minutes of confusion, the stock market lost a value of $136 billion (Fisher, 2013). The Associated Press reports that the post, reportedly made by a group calling themselves the Syrian Electronic Army, was preceded by a phishing attack containing malicious links and attachments (Perlroth & Shear, 2013).

MITIGATION AND DEFENSE

Regardless of the threat that an organization takes, it must utilize proper protocol. Using the proper methods of risk identification, assessment, and management, an administrator or organization can help alleviate the potential for a successful attack or, in the case of a successful attack, minimize the potential impacts of the attack (McDaniel, 2018). This is important whether the risk is of a technical nature (e.g., malware) or a non-technical nature (e.g., phishing and social engineering). Below, multiple methods of social engineering mitigation techniques are explained. However, it should be noted that as each organization and situation is unique, the selection and execution of these methods in any given situation should only occur once a full risk assessment has been completed, and the specific technique confirmed to be applicable.

Education

When performing any research for recommended security practices to mitigate social engineering threats, it is inevitable that the top recommendation is user education. As explained by Lou, Brody, Seazzu, & Burd (2011) security education, training, and awareness (SETA) programs are implemented by many companies to serve several purposes: (1) improve employee behavior; (2) inform employees on where to report policy violations; and (3) enforce the accountability of employees for their actions.

Often, if organizations offer a phishing and social engineering training session, it is during the hiring and onboarding process for a new employee. However, during an interview with Business Insider's Natasha Bertrand (2015), Joe Loomis, CEO of CyberSponse, explains that after 90 days of training, if an employee is not re-trained on phishing scams, they will begin to click on malicious links again. Luckily, due in part to security awareness training at organizations, phishing attacks are becoming less efficient (Goldscmidt, 2018). In an article for CSO, Steve Ragan (Ragan, 2018) explains that despite advances in technology, organizations cannot secure their information systems in spite of the human element. Ragan (2018) continues to explain that continuous training, no matter the stigma given to it by the organization's staff, is important in fostering a culture where security is a part of the user's core focus.

The United States Computer Emergency Readiness Team publishes a guide on how to best identify and avoid becoming a victim to social engineering attacks, specifically phishing attacks. Many successful training programs implement most or all of the points put forth in their publication. Of particular interest for educational and training programs is to "[b]e suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information" and "if you are unsure whether an email request is legitimate, try to verify it by contacting the company directly" (US-CERT, 2009). Identifying a message as illegitimate is the first step against phishing email. Without this identification, any additional user education proves to be useless in the mitigation process.

Policy

Closely related to user education is the proper development and application of policy for an organization. Policy dictates the acceptable use and procedures within a company. Particular policies on acceptable Internet and telecommunications usage can minimize the chance of encountering social engineering attacks. Other policies can also provide non-technical protection from these attacks. For example, an organization implementing a strict “clear desk” policy minimizes the risk for unauthorized individuals from gaining access to information left in plain sight (Chizari, Zulkurnain, Hamidy, & Husain, 2015). In addition to developing the policy and implementing it across an organization, it is important for the organization to enforce the policy uniformly. Improper application and enforcement of policy within an organization can cause both confusion among the users and prove damaging for an organization as litigation can be brought against companies enforcing policy for some staff members and not others (Tanner & Guin, LLC, n.d.).

Software Updating Patching

It should be understood that social engineering is generally “a precursor to, or simultaneous to, technology-based attacks” (Harrington, n.d.). As part of these technology-based attacks is reconnaissance activities to determine if a user and/or organization is utilizing unpatched, vulnerable software in their organization. (Olavsrud, 2010). Keeping all software packages updated throughout an organization is important both for the threats social engineering present as well as threats occurring via other vectors (e.g., vulnerability scans from external actors).

Although modern operating systems from Microsoft, Apple, and others provide administrators and users plenty of notification and visibility to available operating system patches, some software packages do not provide these notifications. Users and administrators must be vigilant to ensure that software security patches are attained and applied in a timely manner to minimize risk. With the rise of the Internet of Things (IoT) devices, this issue is sure to grow in importance (Yaqoob, et al., 2017). Many IoT devices do not contain an easily-accessible user interface in order to apply patches. For example, IoT-enabled light-bulbs do not provide an interface that is easily accessed by a user for patch application. Combined with the longevity of light emitting diode (LED) technology, these bulbs could be in place for years, if not decades. During this extended time period, almost certainly vulnerabilities will be identified in the bulb's code. While not a direct social engineering mitigation method, patching software provides less incentive and opportunity for malicious actors attempting to gain access to an organization's systems.

Multi-Factor Authentication

A primary target of social engineering attackers is the login credentials for a user's account, whether an email account, an enterprise login account, or an account to a sensitive application such as a health information system or financial information system. Single-factor authentication methods implement one of three possible factors: (1) something you know (e.g., a password); (2) something you have (e.g., a one-time password generator); or (3) something you are (e.g. biometric data such as a fingerprint) (What is MFA?, n.d.). Social engineering attackers attempt to gain access to systems that offer single-factor authentication solutions, generally accessed with a username/password combination (something you know). In order to combat the risk associated with the breach of these credentials, organizations can opt to implement a multi-factor authentication (MFA) solution. When an MFA solution in place, an organization is still protected, even if a user's username and/or password are compromised, as the attacker would not be able to authenticate without also having access to the second or even third method of authentication.

However, there is a downside of using MFA. Specifically, three major disadvantages can be encountered: (1) factors can get lost; (2) false security; and (3) it can be turned against users (Korzun, 2017). While the specifics of these disadvantages are beyond the scope of this paper, organizations should assess both the risks and advantages that MFA offers and choose whether MFA is right for their environment and, if so, which method of MFA (e.g., SMS codes, USB security keys, etc.) would best service their needs.

Anti-Virus

Similar to the importance of patching all software packages on systems, anti-virus software applications should be implemented and kept updated to combat potential attacks. Many modern antivirus software packages also include features to mitigate spam emails, identify phishing emails, and prevent the unwanted download of files (Social Engineering, n.d.). Keeping these utilities updated ensures that the systems can identify and block the latest known phishing sites and emails.

Web Browsers

Vendors of modern web browsers understand the need for user security. Accordingly, all major vendors such as Microsoft, Google, Mozilla, Apple, and Opera have implemented technical controls into their web browsers to detect when a user access a malicious website (Mohsin, n.d.). This protection can be included natively, within the web browser, or it could be added (or expanded) through the use of optional plug-ins by anti-malware vendors.

Some vendors, such as Citrix and some anti-virus vendors, offer a sandboxing method that is used to access potentially risky websites without risking the organization's network. The Citrix sandboxing method launches a web browser running in their Cloud environment which contains zero connectivity to the corporate network (Protect your network, n.d.). The isolation of the browsing activity ensures that any malicious downloads or scripts located on the web page will be completed in the sandboxed environment and be unable to harm other systems. Upon closure, the sandboxed environment is destroyed, eliminating any threat.

Multi-Layered Security

Each of the aforementioned mitigation methods is important in their own right. However, a true mitigation strategy for social engineering (and other) risks involves a concept termed multi-layered security. Called "defense in depth" by some, a multi-layered approach ensures that if one layer of the organization's security were to be breached, another layer(s) would still provide protection to the information assets (Gragg, 2001). For instance, if an attacker were to successfully convince a worker to give up their login credentials to their corporate email account, a second control of having multi-factor authentication enabled would prevent the attacker from utilizing those credentials to gain access. Additionally, if the attacker somehow bypassed MFA, a robust antivirus solution could detect the intrusion and either stop the attack or alert the necessary administrator so that action can be taken.

CONCLUSION

In this paper, the author has attempted to provide the reader with a high-level taxonomy of social engineering attacks including phishing, spear phishing, pretexting, baiting, quid pro quo, and tailgating. While all of these attack types are of concern to organizations of all sizes, the prevalence and continued success of phishing attacks make clearly the most widespread of all social engineering attacks. Organizations of all sizes and individuals must be proactive in utilizing user training programs to inform users of possible social engineering attacks. These training programs should be implemented in a continuous manner to keep information security and social engineering at the forefront of users' minds. In addition, other mitigation techniques should be implemented such as multi-factor authentication and anti-virus solutions. Keeping anti-virus solutions and all other software packages patched with the latest security updates from the vendors also assists in the mitigation of the risks associated with social engineering and other threats to information security. The combination of all of these countermeasures into a multi-layered security approach is imperative to enhancing the security as it provides secondary lines of defense in case the primary defensive layer gets breached.

REFERENCES

A Breakdown and Analysis of the December, 2014 Sony Hack. (2014, December 5). Retrieved from RiskBased Security: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

Anderson, J. M. (2003, May). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Armerding, T. (2017, October). The 16 biggest data breaches of the 21st century. *Computerworld Hong Kong*.

Bertrand, N. (2015, August 10). *'It Only takes one email': 3 reasons why China reading Obama administration private emails is even worse than it seems*. Retrieved from Business Insider: https://www.businessinsider.com/china-reading-obama-administration-email-2015-8

Bisson, D. (2015, March 23). *5 Social Engineering Attacks to Watch Out For*. Retrieved from Tripwire: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Bisson, D. (2015, April 22). *Sony Hackers Used Phishing Emails to Breach Company Networks*. Retrieved from Trip Wire: https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

Chizari, H., Zulkurnain, A. U., Hamidy, A. K., & Husain, A. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science, 1*(4), 188-198.

Fisher, M. (2013, April 23). *Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?* Retrieved from The Washington Post:

https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.602d2aef307e

Gold, S. (2011). Understanding the hacker psyche. *Network Security, 2011*(12).

Goldscmidt, C. (2018, March 2). *Modern Phishing Campaigns and Effective Prevention*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2018/03/02/modern-phishing-campaigns-and-effective-prevention/#b4c4bc5649db

Gragg, D. (2001, December). A Multi-Level Defense Against Social Engineering. *SANS Institute InfoSec Reading Room*.

Harrington, T. (n.d.). *Training, Awareness Keys to Battling Social Engineering*. Retrieved from ISACA: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=647&utm_referrer=direct%2Fnot%20provided

Hayes, J. (2017, March 13). *The human behind the hack: identifying individual hackers*. Retrieved from The Institution of Engineering and Technology: https://eandt.theiet.org/content/articles/2017/03/the-human-behind-the-hack-identifying-individual-hackers/

Heartfield, R., & Loukas, G. (2016, February). A Taxonomy of Attacks and Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys, 48*(3).

Jatfield, J. M. (2018, March). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102-113.

Keizer, G. (2015, April 23). *Sony hackers target employees with fake Apple ID emails*. Retrieved from Computerworld: https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html

Korzun, J. (2017, October 25). *Disadvantages of two-factor authentication*. Retrieved from Electronic Products: https://www.electronicproducts.com/Programming/Software/3_disadvantages_of_two_factor_authentication.aspx

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015, June). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011, July-September). Social engineering: the neglected human factor for information security management. *Information Resources Management Journal, 24*(3).

Luszcz, J. (2018, January). Apache Struts 2: how technical and development gaps caused the Equifax Breach. *Network Security, 2018*(1), 5-8.

Martin, J., Dubé, C., & Coovert, M. D. (2018, December). Signal Detection Theory (SDT) Is Effective for Modeling User Behavior Toward Phishing and Spear-Phishing Attacks. *Human Factors: The Journal of Human Factors and Ergonomics Society, 60*(8).

McDaniel, D. W. (2018). *Identification, Assessment, and Management of Risks in InfoSec.*

Mohsin, T. (n.d.). *Anti-Phishing: Browser Security Features*. Retrieved from InfoSec Institute: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-browser-security-features/#gref

Olavsrud, T. (2010, October 9 9). *Best Defenses Against Social Engineering Attacks*. Retrieved from eSecurity Planet: https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

Perlroth, N., & Shear, M. D. (2013, April 23). *In Hacking, A.P. Twitter Feed Sends False Report of Explosions*. Retrieved from The New York Times: https://thecaucus.blogs.nytimes.com/2013/04/23/hacked-a-p-twitter-feed-sends-erroneous-message-about-explosions-at-white-house/

Protect your network from browser-based attacks by isolating web browsing activities. (n.d.). Retrieved from Citrix: https://www.citrix.com/digital-workspace/secure-browser.html

Quid pro quo. (n.d.). Retrieved from Legal Information Institute: https://www.law.cornell.edu/wex/quid_pro_quo

Ragan, S. (2018, April 9). *Social engineering: It's time to patch the human*. Retrieved from CSO: https://www.csoonline.com/article/3268225/security/social-engineering-its-time-to-patch-the-human.html

Rashid, F. Y. (2011, April 4). *RSAs SecurID Breach Started with Phishing Email*. Retrieved from eWeek: http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email

Resnik, D. B., & Finn, P. R. (2018, August). Ethics and Phishing Experiments. *Science and Engineering Ethics, 24*(4), 1241-1252.

Ritchey, D. (2015, January 7). *Tailgating: A Common Courtesy and a Common Risk*. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/86026-tailgating-a-common-courtesy-and-a-common-risk

Santiago, S. (2017, March 28). *The Most Famous Cases of Social Engineering*. Retrieved from Open Data Security: https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/

Serban, V. G., & Serban, O. (2014, June). Social Engineering A General Approach. *Information Economica, 18*(2), 5-14.

Social Engineering. (n.d.). Retrieved November 14, 2018, from Oxford Dictionaries: http://www.oed.com.jproxy.lib.ecu.edu/view/Entry/272695#eid134551514

Social Engineering. (n.d.). Retrieved from Avast: https://www.avast.com/c-social-engineering

Stasiukonis, S. (2006, June 7). *Social Engineering, the USB Way*. Retrieved from DarkReading: https://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081

Tanner & Guin, LLC. (n.d.). *Employers Must Enforce Policies Uniformly*. Retrieved from FindLaw: https://corporate.findlaw.com/human-resources/employers-must-enforce-policies-uniformly.html

Thompson, S. T. (2006, December). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries, 25*(4).

Tiwari, A. (2018, May 30). *What is Social Engineering? What are Different Types of Social Engineering Attacks?* Retrieved from Fossbytes: https://fossbytes.com/what-is-social-engineering-types-techniques/

US-CERT. (2009, October 22). *Security Tip (ST04-014)*. Retrieved from United States Computer Emergency Readiness Team: https://www.us-cert.gov/ncas/tips/ST04-014

What is Multi-Factor Authentication (MFA). (n.d.). Retrieved from Centrify: https://www.centrify.com/solutions/why-multi-factor-authentication/

White, F. (2014, July 9). *Was the Trojan horse real?* Retrieved from History Answers: https://www.historyanswers.co.uk/ancient/was-the-trojan-horse-real/

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I., Al-garadi, M. A., Imran, M., & Guizani, M. (2017, December 24). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks, 129*(2), 444-458.