# A taxonomy of attacks and a survey of defence mechanisms for semantic social engi...

# Abstract

Social engineering has increased the vulnerabilities in today's technological world. There are six types of social engineering attacks; baiting, phishing, email hacking and contact spamming, pretexting, quid pro quo and tailgating. Understanding how to avoid the attacks and what you can do to protect yourself is key to maintaining the integrity of your systems.


Social Engineering

Social engineering has been around since ancient times it has just morphed as technology and the way we receive information has changed. We have all heard the saying " knowledge is power," and this can be linked directly to social engineering. Social engineering has two different definitions. The first is associated with social sciences and is defined as the centralized planning to attempt social change. The definition we are discussing is the use of deception to manipulate individuals to divulge information used for fraudulent purposes. Although two separate definitions they are intertwined because they use the common threads to manage certain groups of people.

Social engineering is defined in many different ways, and if you research the definition, there are several versions. Information security social engineering (ITSE) is a relatively new term, and each definition classifies it differently. Some do not consider it a technical attack but disclosure, such as stolen passwords. Hacking Exposed, one of the most recognized consumer hacking books, identified social engineering as " a description of techniques using persuasion and deception to gain access to information systems," (Evans 12). Social engineering attacks may be implemented in several different

ways; however, they all have one thing in common “ In every social engineering attack, the attacker pretends to be another person or plays an inappropriate role.” (Smith, 2016)

“ Social engineering is an umbrella term for a broad array of computer exploitations that employ a variety of attack vectors and strategies to psychologically manipulate a user.” (Heartfield, Loukas 2016) To differentiate between nontechnical attacks researchers use the term semantic attack. A semantic attack refers to the manipulation with the purpose of breaching a computers security system through user deception. The user- computer interface provides the window of opportunity to implement an attack. Semantic attacks are grouped into specific attack families. These families may be grouped into several categories such as phishing, baiting, quid pro quo, pretexting and tailgating.

Phishing uses email to trick the user into divulging confidential information. An example would be an email from a banking institution directing the user to go to a website and log in. The site then collects the information to access the account. Another type of phishing attack is a drive-by-download. This type of attack can occur when a user visits a website, and the webpage attacks the computer. For a drive-by-download to be successful scripts must be embedded in the web pages. There is also spear phishing which targets a limited number of people, the language used in spear phishing is more tailored to each individual the email was sent to. Phishing attacks can be tracked through the resources they use such as spam mail, websites and the domain name. Since an ISP controls them, they can be traced back to the owner unless more sophisticated techniques such as botnets are used.

Phishing attempts grew by 65% in 2018, and the average cost for a mid-size company is $1. 6 million.

Baiting is another form of social engineering. It uses enticement by promising an item or goods such as free downloads. However, to receive an item, you must use login credentials. Physical media can be used in baiting attacks, an example of this would be employees are offered free USB drives with malicious code. This malicious code is downloaded onto the computers opening the door for hackers. Again, the common denominator is the human element.

Quid pro quo is a form of baiting but promises a service or benefit if you perform a specific action. The often impersonate someone such as someone from an IT department and tell the user there is a problem with their system that needs to be corrected. “ This allows the attacker to gain access and install malicious software or programs.” (Whiteman, 2017)

Pretexting goes a step further by grooming their targets to divulge sensitive information by first gaining their trust. They usually pose as an authority figure or even a coworker to build a rapport. Once trust is established questions are asked that pertain to the data they are gathering such as a person’s identity or security information related to the company or organization.

Tailgating or piggybacking refers to someone gaining access to a restricted area without proper authorization. The human element plays a significant role in this type of attack. They prey on weak security measures in this scenario by looking as if they belong in the area by dressing the same as

workers or even posing as a delivery person. Once they have gained access, they can maneuver around the facility to collect information.

Social engineering is tied to the user's behavior and how susceptible we are to the threats. Several areas play a role in how we react to attacks. Our personalities, environmental factors such as time constraints and physical disabilities. The attackers must gain the trust of the user and use these to their advantage. Users must be conscientious and follow the standards and procedures to maintain a high level of awareness to avoid these types of attacks. This is not always so easy due to the technological advances that have taken over industry and our personal lives.

Social engineering attacks can be carried out on any device or system we can connect to the internet or has email capabilities. Attackers can cause havoc using these techniques when targeting larger institutions such as government agencies, financial institutions, medical facilities, and social media websites such as Facebook, Twitter or Instagram.

Government institutions such as defense agencies, the Internal Revenue Service and the Office of Personnel Management (OPM). All systems have had their share of issues, but the one that stands out is the OPM breach discovered in March 2014. The attack was preventable, but due to lack of oversight and budgeting to appropriately manage their systems. " According to investigators, hackers likely gained access to OPM's local-area network on May 7, 2014, by stealing credentials and then planting malware and creating a backdoor for exfiltration. Actual exfiltration of data on background investigations did not begin until July 3, 2014, and it continued until August."

(“ Exclusive: The OPM breach details you haven’t seen — FCW,” 2015) Government agencies are dependent on our elected officials to pass a budget to allow for the agencies to install new technology to thwart attacks and to hire well-trained staff to oversee and implement security plans and protocols. For almost a decade the government agencies operated at funding level below what was needed to maintain an edge.

Financial institutions are a treasure trove for attackers. These attacks are disastrous to the company’s reputations and devastating to those who have their information stolen. Identity proofing was developed by the Silicon Valley analytic software firm to provide a solution to financial institutions to prevent fraud. “ Identity proofing covers circumstances ranging from new account applications to new device enrollment, and to successfully discern between fraudsters and legitimate customers, and financial institutions must be able to bring a wide range of capabilities to bear as part of their identity proofing workflows.” (FICO named a javelin 2017 identity proofing platform leader– 2017) Since online banking has become the norm, it is also essential for the user to be aware of phishing and other social engineering targets that the institution can’t stop. The human element plays a significant role in keeping your financial information safe at home.

Medical facilities are also at risk for social engineering attacks. The human element is the main threat in attackers being able to gain access. There are definite and definitive standards that healthcare professionals must comply with under the Health Insurance Portability and Accountability Act (HIPPA). Medical staff can access very private and sensitive information about a person’s health and personal and financial information stored as well. A

breach could be devastating to a medical facility and leave many patients at risk. During a study one of the most noted weakness were passwords. Not only were created passwords weak but employees were known to share passwords. Medical facilities are required to have security plans and protocols but to ensure personnel understands and use them properly needs in-house training. Training can alleviate some of the risks to their systems. The sharing of information outside of the work area combined with the weak passwords increased the risk. If you post where you work on Facebook or other social media websites and additional personal information has been used to create your password you have given the attackers a breadcrumb trail to follow.

Social media accounts are notorious for social engineering attacks. They seem innocent; in fact, a Pentagon attack occurred by an employee opening an ad for a vacation package that came through Twitter. Social media is a hacker's dream, billions of people sharing seemingly reliable information with family and friends it makes people an easy target. " Cybersecurity companies said spear phishing through social media was one of the fastest-growing methods of attack." (Frenkel, 2017) If you have noticed for example now on Facebook if you will see ads in your newsfeed for items you were recently searching. It makes it easy for attackers to know what you are interested in and use spear phishing techniques to tailor messages that contain malicious software. Being aware of how these attacks are conducted and how to manage privacy and security settings on social media sites are two ways you can protect yourself. These attacks will only continue to increase and evolve as technology continues to expand. " As information

technology and operational technology (IT/OT) continue to converge, enterprise applications and platforms will be at risk of manipulation and vulnerabilities, as stated in Trend Micro’s 2018 predictions report.” (PCA, 2017) In 2016 cyber-attacks cost the U. S Economy between $57 billion and $109 billion. This cost continues to increase because cyber threats are constantly evolving.  Companies must continue to invest in infrastructure, employee training and cybersecurity to ensure the continuing threats are maintained. “ In its 2018 Annual Cybersecurity Report, Cisco said malware is becoming more vicious and harder to combat. “ We now face everything from network-based ransomware worms to devastating wiper malware,” the report said. “ At the same time, adversaries are getting more adept at creating malware that can evade traditional sandboxing.” (McLane, 2018) Social engineering cyberattacks will not slow down in the future, and they will evolve to evade the new network landscape and continue to pose a threat worldwide.

Global cybersecurity is a growing crisis, as we have seen in the news there are ways information can be manipulated to sway opinions on political fronts as well as personal reputations.  “ Many states have acknowledged the contributions of the Internet to their economic and social development, and they are already accustomed to following mutually beneficial rules at the cyber operational level, most prominently, the network protocols.” (Yannakogeorgos, 2016) The significance of the of cybersecurity was recognized in January 2010 at the United Nations. The call addressed the fact that all states were responsible for combating cybersecurity attacks and risks and collaboration was key to for a successful outcome. However, Russia

and China are not completely in agreement with the current global policies proposed. They want to have control over issues that relate to their territories. This will allow them to control the cyberspace to control the data and prevent other states from being able to access their networks. " In contrast, the United States and its NATO allies tend in their pronouncements to view cyberspace as a central institution for a global economy, a means for worldwide scientific and cultural exchange, a common for political debate and development, and a social medium." (Yannakogeorgos, 2016) These are two very different outlooks. Differing perspectives will continue to be a challenge and have maintained global implications until the states can agree on how to handle the far-reaching effects of cybersecurity attacks. Cyber-attacks can disrupt our national defense, economy, societal norms. This will continue to be a global issue that states must confront not only to keep the peace but thwart criminal activities not only to gain monetary assets but to disrupt political movements in other states. We, however, can control what happens in our borders through regulatory laws.

The World Wide Web is like the wild west in the fact that in some instances it is still unchartered territory. What makes it even worse is that the forces behind what is happening are not always known. This is why regulatory laws are required to ensure those acting improperly can be held accountable. They also protect the consumers from companies violating such laws and causing them to be exploited. One such rule is the Federal Information Security Management Act (FISMA). FISMA is an ongoing collaborative effort to implement standards, and guidance agencies require to implement security strategies and programs to provide security in line with the risks

government agencies face protecting the organization from loss of confidentiality, integrity, and information availability. As government agencies, financial institutions are at high risk for cyber-attacks. The Gramm-Leach-Bliley Act also is known as the Financial Modernization Act of 1999 was enacted to protect personal private information. It is comprised of three parts. The Financial Privacy Act Rule which regulates the collection and disclosure of private financial information. Second is the Safeguards Rule; this mandates that the financial institutions must have security programs in place to protect data and prohibit pretexting. Pretexting is where information is accessed under false pretenses. The third part requires financial institutions to outline their information practices through privacy notices. This holds companies accountable to protect the information in their possession from fraud and improper use. More and more of our personal is data stored, and none is more important than our health data. Medical records have been mandated to move to electronic health records under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In 2000, The Standards for Privacy of Individually Identifiable Health Information set a national standard to protect certain health information. It identified protected health information and made them covered entities to protect the data. It also established guidelines to inform patients of their privacy rights. “ A major goal of the Privacy Rule is to assure that individuals’ health information is protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public’s health and well-being.” (“ Summary of the HIPAA Privacy Rule,” 2013) All of these laws have been put in place to force agencies to address security

issues to assess the risks and implement security plans and protocols to protect consumer and personal information.

Social engineering is the overarching term that includes several different types of cybersecurity attacks such as phishing, baiting, pretexting and tailgating. All of these have one element that assists the attackers, the human element. These attacks use the human weakness to infiltrate and attack the users. The implementation of the attacks is through mobile phones, websites, and networks connected to the internet. They target individuals, financial institutions government agencies for commercial gain, to collect sensitive information. Technology is forever changing at a fast pace and businesses and organizations must have fully engaged IT departments to mitigate the risks that are inherent to the ever-changing technological landscape. Many organizations and industries now are regulated by laws to ensure the protection and privacy of confidential information. Cyber-attacks under the social engineering umbrella will continue to have global impacts. How the global community reacts to these attacks will hinge on cooperation between states and the passage of international laws that can be agreed upon and implemented. The risks of social engineering attacks will never go away. The attackers will continue to find vulnerabilities to exploit. It is up to each industry, individual and our lawmakers to ensure we have sufficient security protocols in place to protect our information.

# References


- Smith, R. E. (2016). Elementary Information Security, 2nd Edition. [VitalSource]. Retrieved from https://bookshelf. vitalsource. com/#/books/9781284093070/
- HEARTFIELD, R., & LOUKAS, G. (2016). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys, 48(3), 37: 1-37: 39. https://doi-org. ezproxy2. apus. edu/10. 1145/2835375
- Katz, E. (2018, February 21). Phishing Statistics 2018: What Every Business Needs to Know. Retrieved from https://blog. dashlane. com/phishing-statistics/
- Social Engineering: What is baiting? | Mailfence Blog. (2018, June 30). Retrieved from https://blog. mailfence. com/what-is-baiting-in-social-engineering/
- Whiteman, Jack R., I., II. (2017). Social engineering: Humans are the prominent reason for the continuance of these types of attacks (Order No. 10684196). Available from ProQuest Dissertations & Theses Global. (2007620740). Retrieved from https://search-proquest-com. ezproxy1. apus. edu/docview/2007620740? accountid= 8289
- Exclusive: The OPM breach details you haven’t seen — FCW. (2015, August 21). Retrieved from https://fcw. com/articles/2015/08/21/opm-breach-timeline. aspx
- FICO named a javelin 2017 identity proofing platform leader. (2017). Dataquest, Retrieved from https://search-proquest-com. ezproxy2. apus. edu/docview/1949051260? accountid= 8289

- Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of U. S. hospitals to social engineering attacks: How many of your employees would share their password? International Journal of Information Security and Privacy, 2(3), 71-83. Retrieved from https://search-proquest-com. ezproxy2. apus. edu/docview/223742250? accountid= 8289
- Frenkel, S. (2017). Hackers hide cyberattacks in social media posts.
- PCQ. (2017, Dec 06). Cyberattacks will rely on vulnerabilities in 2018. PCQuest, Retrieved from https://search-proquest-com. ezproxy1. apus. edu/docview/1973437770? accountid= 8289
- McLANE, P. (2018). Cyberattacks Put Every Enterprise at Risk: Techniques diversify as corporate adversaries get smarter. Multichannel News, 39(15), 8–N. PAG. Retrieved from http://ezproxy. apus. edu/login? url= http://search. ebscohost. com/login. aspx? direct= true&AuthType= ip&db= bth&AN= 130449805&site= ehost-live&scope= site
- Knapp, K. J. (2009). Cyber-security and Global Information Assurance : Threat Analysis and Response Solutions. Hershey, Pa: IGI Global. Retrieved from http://ezproxy. apus. edu/login? url= http://search. ebscohost. com/login. aspx? direct= true&AuthType= ip&db= nlebk&AN= 253996&site= ehost-live&scope= site
- Yannakogeorgos, P. A., Lowther, A., & Books24x7, I. (2016; 2014; 2013;). Conflict and cooperation in cyberspace: The challenge to national security. Baton Rouge: CRC Press.

- Summary of the HIPAA Privacy Rule. (2013, July 26). Retrieved from https://www. hhs. gov/hipaa/for-professionals/privacy/laws-regulations/index. html