Human Factors In Cyber Security

Nathan Satterfield

Charleston Southern University

Abstract

This paper discusses the human elements of cyber security. Firstly, it discusses why it is so important and how humans are often the weakest link in security. It also goes into how attackers use nontraditional tactics to trick users into revealing sensitive data that would otherwise be difficult to obtain with other traditonal methods. These methods usually involve the attacker impersonating a boss or someone the victim trusts to trick them into disclosing private information that can be used for malicious purposes. It goes over why this is becoming more of an issue, due to the changing nature of the world of cyber security as an ever evolving field. It then breifly goes into the basics of how social engineering attacks, such as phishing, work and why they are so popular. Lastly, it provides information on how to recognize attacks, what to do if you encounter one, and suggestions on how to educate all users, as they are a higher risk factor.

Keywords: Cyber security, Social enginering

Human Factors In Cyber Security

When it comes to cyber security, no matter how much work is done to secure a machine or network, all it takes is one vunablity for an entire system to be compromised. One of the most common attack vectors is user error, not the computer itself. Human negligance has been attributed to 35% of data breaches from 2016 to 2017 (Walker, Witkowski, Benczik, & Jarrin, 2017). One reason for this is because of the limits on system security. Even with system security, vulnerabilities will always exist. However, there is the issue of usablity. If a network was secured with excessive policies, the computers would become very difficult to use. So there must be a balance between forcing security on users and training them to be aware of what they are doing. If we as individuals become more educated on how to prevent social engineering attacks, there would be a large decrease in successful cyber attacks. It is often falsely believed that "cybersecurity is the responsibility of IT; rather it is everyone's responsibility" (Walker, Witkowski, Benczik, & Jarrin, 2017). In reality, there is only so much the technology department can do. If the individuals in a company disregard polices or are uneducated on those policies, no amount of hardening will produce a secure enviroment. "The use of such technologies is negated in instances where employees fail to follow cybersecurity protocols or engage in activities that place themselves and the company at risk" (Hadlington, 2017). The main source of threats is the user: "threats to critical infrastructures and services come mostly from careless work behaviours and ignorance of basic cyber security practices" (Gyunka, Christiana 2017). All it takes is one wrong click by one person to compromise a company's entire network, and when there are hundreds or even thousands of employees in one company, it is just a matter of time until a breach occurs.

There are many different ways that users can unintentonally or unknowingly compromise a network. There are several different ways that users can cause breaches, but the root of most of those breaches is social engineering. Social engineering is a non-technial way to get users to breach polices and reveal information that would otherwise be unavailable to attackers. The attackers typically imitate a person of power in the victim’s life, whether this is a boss, a partner, or just someone the individual looks up to. Then, the “victims of these attack techniques are usually persuaded to willingly open wide their security door ways to unknown persons” (Gyunka, Christiana 2017). When you have someone willing to open the door for you, why waste time trying to break the door down? This is why social engineering attacks are so popular: all you need to do to perform a social engineering attack is to gain some basic information on the person you are trying to deceive and the system you are trying to compromise. Given how popular social media websites are, millions of people willingly give out information that can easily be used for an attack. Once the basic information on the victim is gathered, all that is needed is to use social engineering tactics and wait to be let in. Due to the nature of the attack, it is to succeed even if a few attempts fail. It is also very easy once you have enough information about an individual from a company and attempt to impersonate them, especially when coworkers have lack of education on social engineering. Most attacks are targeted at unknowing victims, but it is not uncommon for employees that are angry or unhappy with the company to intentionally allow attackers in. So not only must you educate users so that they know what not to do, you must also take precautions and set policies to prevent them from making mistakes. If users are allowed to do something harmful, it is not a question of if it will happen but how long until it happens.

In recent years, due to the rise in computer usage, this has become an even bigger issue. Almost every career path now will involve the use of a computer in some capacity, and "individuals who use information technology tools directly or indirectly should contribute to information security" (Durak, 2019). Thus, everyone needs to learn basic computer safety, and many individuals currently do not. This is why there are so many social engineering attacks. Many universities are beginning to require some technical courses, but "this needs to be improved, as it is essential to deal with the issues of cybersecurity in all bachelor's degrees, preferably during the first year, just because of the wide use of computers they will meet in their career in all professions" (Krasznay & Hamornik, 2019). Education is the key to prevention if you are unable to recognize an attack. It is almost impossible to avoid it, but even a surface level knowledge would be able to prevent a large amount of attacks.

The goal of every security professional should be to raise awareness of what attacks look like and what can be done to stop them. "Cybersecurity awareness is the consciousness of preventing third parties from getting, using, changing, disclosing, deleting, sharing, and/or damaging information without permission and unauthorized means" (Durak, 2019). Once a social enginering attack is recognized, it is incredibly easy to prevent it from succeeding. Once an attack of this nature is noticed, generally all that needs to be done to stop it in its tracks is not respond, as the goal is to trick the user into revealing private information. If no response is given, the attacker has gained nothing for their efforts.

One very popular attack method is phishing, which is a scam typically presented as a message sent over e-mail in order to trick users into revealing personal or confidential information. The scammer can use this information illicitly (Proctor & Chen, 2015). Phishing attacks "like most violations of information privacy and security, rely on deception. An interchange between a deceiver and a target receiver occurs, but the decisions made by the receiver ultimately determine whether the deception is successful” (Proctor & Chen, 2015). Once the message has been sent, what happens is up to the user. They must decide whether or not the email is legitimate, and if so, they should decide if giving the information to the individual asking is the best option.

The goal for a phishing attack is to make the request for information sound as legitimate and urgent as possible. The reason for this is that the more urgent the request sounds, the less time the user is going to waste checking to see if it is a legitimate request. The attacker also wants to make it look as official as possible to increase the likelihood of a response, revealing sensitive information. The personality of the users can also be used to estimate how likely they are to fall for such an attack: “measures of personality and impulsivity acted as significant predictors of detecting a phishing email. Individuals who scored higher on measures of extraversion and anxiousness performed significantly poorer on detecting phishing emails” (Hadlington, 2017). Attacks like this are so prevalent, because it is easy to make an email look genuine, and it is easy to reuse the same template. It is also easy to send large amounts of emails rapidly.

There is also the issue of decreased security as computer security tools become better and easier to use due to the fact that individuals have to put less effort into keeping their computers secure. As a result of this, “as automation reduces attack SP, the human operator becomes increasingly likely to fail in detecting and reporting attacks that remain” (Sawyer & Hancock, 2018). This has become increasingly problematic as many people now have automated security systems. Thus, the majority of users no longer know what to look for or what to do when they do find a vulnerability or attack. As we develop new tools to secure a system, the greater the risk the human element becomes. Humans are the weakest point of security, and the problem is only becoming worse. “The human is always the weakest point in defending against an attack and dealing with the consequences; therefore, reducing human-induced errors is most effective” (Linkov, Zámečník, Havlíčková, & Pai, 2019). So it is clear that educating users is the key to security. The most effective thing to educate users on is how to stop social enginering attacks. There are a few methods to detect and prevent such attacks. The first and most important method is to follow any and all guidelines set by the company the individual works for. The next thing is how to notice attacks of this nature. There are a few different ways to do this. An example is recognizing that communications with many typos or incorrect grammer are often a sign of an attack. Also, if an e-mail or other communication method has any attachments, they should only be opened if the user is expecting such a file. Lastly, users should take extreme caution when clicking on hyperlinks sent to them.

References

Durak, H. Y. (2019). Human Factors and Cybersecurity in Online Game Addiction: An Analysis of the Relationship Between High School Students' Online Game Addiction and the State of Providing Personal Cybersecurity and Representing Cyber Human Values in Online Games. *Social Science Quarterly, 100*(6), 1984-1998. doi:10.1111/ssqu.12693

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on HBGary. *Computing and Information Systems*, 21(2), 10+. https://link.gale.com/apps/doc/A491087352/AONE?u=chazsu_main&sid=AONE&xid=f54c9e2c

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). doi:10.1016/j.heliyon.2017.e00346

Krasznay, C., & Hamornik, B. (2019). Human Factors Approach to Cybersecurity Teamwork – The Military Perspective. *Advances in Military Technology, 14*(2). doi:10.3849/aimt.01296

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C. (2019). Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research. *Frontiers in Psychology, 10*. doi:10.3389/fpsyg.2019.00995

Proctor, R. W., & Chen, J. (2015). The Role of Human Factors/Ergonomics in the Science of Security. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 57*(5), 721-727. doi:10.1177/0018720815585906

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 60*(5), 597-609. doi:10.1177/0018720818780472

Walker, E., Witkowski, D., Benczik, S., & Jarrin, P. (2017). Cybersecurity – the Human Factor. Retrieved 2020, from https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf