Mario Getaw

Professor Ben-Azzouz

COMP-305

3/30/2023

What is Social Engineering?

In today's day and age, the importance of online security has slowly become a household topic for most of the world. Using things like a VPN, firewalls, and malware scanners on our devices is not a foreign concept to most people anymore. One of the generally overlooked things in the cybersecurity world is social engineering. Social engineering is a broad term to describe the methods of manipulating, influencing, and tricking a target in order to gain access to a system, network, or information. A few of the main methods of social engineering are shoulder surfing, eavesdropping, tailgating, spam, hoaxes, and phishing. Some of the principles these methods take advantage of are things such as fear, curiosity, moral obligation, innate human trust, and ignorance. The main emphasis of this research is going to focus on phishing and how threat actors utilize these principles to gain access to sensitive information.

Phishing attacks: what are they? Phishing attacks are described as, "The practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email" (Cisco). This definition by Cisco Systems Inc. gives the perfect description of phishing as a broad topic. The goal of phishing is to steal sensitive data such as banking information or login credentials. Phishing attacks can also install viruses and/or malicious data onto the victim's system. Phishing attacks can be for quick and easy financial gain and large-scale attacks on big companies. Victims are lured in by messages that look like they are from a trusted sender. When fooled, the victim gives up some sort of personal or confidential data, and malware is often downloaded onto their machine. Phishers can do this by taking advantage of target’s emotions like fear, curiosity, moral obligation, innate human trust, and ignorance. Phishing attacks will often play the role of an authoritative figure in a company to provoke or capitalize on these feelings. One person in a company can compromise anything for the rest of the company, so it is important to be aware of phishing attacks.

Phishing attacks are not limited to small companies. In fact, according to CNBC, Facebook and Google lost around $100 million from phishing attacks between 2013-2015 (Huddleston Jr.). Evaldas Rimasauskas led an attack that posed as a Taiwan based company – Quanta Computer, a business partner with Facebook and Google. This is just one example. Even here at Wittenberg University, there was a phishing attack done through one of the football coaches, who accidentally clicked on a link and then lost control of his office 365 account. Emails were then sent out to the entire Wittenberg network making false opportunities of earning insane amounts of cash for crypto currency surveys. This is an attack that anyone on campus could have fallen victim to.

The most important part when it comes to topics in cyber security is prevention. How can one protect themselves from phishing attacks? The first thing to do is to become aware of the danger and educate oneself on what it is how it works. The next thing to do is to monitor all accounts regularly, change passwords often, keep an updated operating system, and never give out personal information via email. In order to detect phishing, examining hyperlinks in emails is one of the best ways to detect phishing. Just hover over the attached links and look for consistency in the message and the pop-up window that comes up. Make sure the URL is trustworthy as well – it will look like an official message. If possible, also verify with the alleged sender that it is a real message that they sent. If you receive a suspicious message, do not open it, and report it to your organization’s IT department or simply delete it. Phishing attacks are the most common cyber-attacks, so it is important to spread awareness about them.

Works Cited:

Salahdine, Fatima, and Naima Kaabouch. “Social Engineering Attacks: A Survey.” *Future Internet*, vol. 11, no. 4, Apr. 2019, p. 89. *Crossref*, https://doi.org/10.3390/fi11040089.

“What is Phishing?” Cisco.com, https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html