Fighting Phishing with Training

Bernard Ayuyao

Old Dominion University

CYSE 600 36666 Cybersecurity Principles

June 02, 2021

Fighting Phishing with Training

Have you ever been a victim of phishing or know someone that had been a victim of phishing? Do you know what a phishing email is when you see one? Do you understand how phishing works and have received training at your job to be more aware about phishing? There have been many victims from phishing and there are many ways that employees fall into becoming victims from phishing every day. We try to understand phishing and gather data of victims, understand techniques attackers use for phishing, and apply training to make ourselves less vulnerable to phishing. Once we learn more about phishing and apply what we learned to our every day lives when we use our computers at work or at home, we will educate ourselves and make us more knowledgeable so that we can avoid phishing scams.

First, we try to define what phishing is. From the journal article titled "A Real World Study on Employees' Susceptibility to Phishing Attacks", De Bona defines susceptibility to phishing as "providing credentials to the phishing site. In contrast the majority of phishing studies conducted within a company defined susceptibility as clicking on the link in the email." (De Bona & Paci, 2020, p. 8). This gives us a good understanding what phishing is when we see it. Once you understand phishing and how it works, you can make yourself more aware by educating yourself and receiving training. De bona continues writing "41% of organizations have been victim at least daily of phishing attacks, while 77% experienced attacks at least every month in the last year. This same report highlighted that 30% of phishing emails are opened by the target victims and 15% of victims are usually targeted at least one more time within the year." (De Bona & Paci, 2020, p. 1). This data shows that phishing is very common in the workplace and employees can be exposed daily. Imagine having an organization with a thousand

employees. That gives the attacker a thousand chances to get an employee to successfully click a phishing email and we want to prevent that from happening.

Next, we want to understand the techniques attackers use to create successful phishing emails. There are several techniques out there and they are psychological techniques called taxonomy. According to De Bona, “The taxonomy consists of six principles of persuasion: authority, scarcity, commitment, liking, reciprocation and social proof. The principle of authority states that humans tend to comply with requests made by figures of authority, such as law enforcement personnel or inline manager.” (De Bona & Paci, 2020, p. 2). With the most powerful psychological influences being authority, De Bona continues writing “Similarly, the impact of persuasion principles in making employees vulnerable to phishing attacks is yet to be investigated in the workplace settings. Previous research highlighted that users are more susceptible to phishing attacks when authority and urgency persuasion techniques are exploited. These same persuasion techniques are likely to increase the likelihood that employees respond to a phishing email given that workplaces have a hierarchical organization and usually require employees to work under time pressure.” (De Bona & Paci, 2020, p. 1). This is relatable, especially in the Navy because it is a very demanding job. There is a hierarchical organization over the whole crew of a ship and deadlines must be met which causes a lot of time pressure. Commanding Officers want to get ships out at sea because of higher authority. All that pressure trickles down to the crew. Fortunately, phishing has not been an issue that is overlooked because of pressure from higher authority. A false sense of urgency should be avoided.

Finally, in order to combat phishing, we must train our people because knowledge is power. There are two types of training we can give in our workplace. The first is traditional facts-and-advice and stories from people who have been victims of phishing attacks. De Bona

writes, “They found that facts-and-advice training is more effective when delivered by a security expert, while stories are more effective when provided by people with whom they have something in common.” (De Bona & Paci, 2020, p. 3). This is true and powerful just like the stories and experiences I am sharing as examples on this paper. In the Navy, we would have our Communications Officer brief and give training on these topics to prevent any attacks in our system. The last thing you want out of your career is to be the story of the one who clicked a phishing email. It will be a lesson you will always remember. The second type of training is embedded training. De Bona writes, “Other studies have examined the effectiveness of embedded training, which consists in delivering training when users click in the link present in a phishing email.” (De Bona & Paci, 2020, p. 3). This type of training is very effective because it gives employees hands on training and experience on what phishing emails look like and what to do when they see one. In the Navy, we would do annual online module trainings on this topic where we walk through scenarios and a few of them would be phishing.

All in all, phishing is a cheap way of attacking a business because the attacker can send a mass amount of phishing emails and it takes just one employee to become a victim of phishing. We now know what phishing is and the statistics of the victims, the most powerful techniques used, and most importantly that training is the best way to combat phishing scams. We must be smart when we see phishing emails and make sure you are not acting on a false sense of urgency because majority of phishing emails come with authority and urgency. It is important to keep our minds sharp and do refresher trainings so that we won’t be too relaxed or complacent. No one wants to be made an example of in the next training topic or story of phishing.

References

De Bona, M., & Paci, F. (2020). A Real World Study on Employees' Susceptibility to Phishing Attacks. 10. Retrieved from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/3407023.3409179