Company Risk

Sam Roethemeyer

University of Advancing Technology

NTS201 – Security Essentials

Current Company Risk

Our company faces many types of potential intrusions and/or attacks constantly. One of these intrusions can happen to anybody anywhere not just in this company. Phishing emails are one of the major risks that you can't block with automated devices like firewalls or Intrusion Protection Detection Systems. Our company will begin training our employees on better identifying these emails, and other policies in place to make sure that our employees are always on the lookout for these emails.

In the next few months, we will train our employees about how to identify malicious emails. To begin, we will go through various emails that we have received from vendors and customers with any sensitive data redacted and show them how they should look and what to look for to know they are real. After that, we will show some carefully crafted emails without telling them that they are malicious, to ask them what about these emails prove they are from credible people.

The malicious emails that we show will be crafted out of techniques that are used by attackers today. We will also show some of the emails that we have received that have been caught and saved for learning such as the training we are now doing. In this training, we will show how emails can be made to look very similar, along with other parts of the email that make it seem legit. These can range from using the same phone numbers, addresses, and images that other companies use to mimic their emails. Here is an example of an email address that is made to look similar but is different. JaneDoe@apple.com would be the legit email, but JaneDoe@appIe.com looks similar, but the lowercase L is switch to an uppercase I, and in certain fonts they look identical. This is a simple example, but that can look similar and will fool anybody with an untrained eye.

Another way they can trick is by using an email that is meant to be urgent and grabs your attention quick without a second thought and almost brings you to a panic. This is achieved by claiming that a certain account has been accessed or changed without your approval. If you had an account somewhere that deals with important information, such as insurance, get suspended out of nowhere, you're going to investigate it. If you have an unexpected charge from your amazon account or other e-commerce site, you're going to panic a bit and try to figure out what's going on. That's where they get you, because they include phone numbers and links to places that are not legit businesspeople that work for these companies, but rather the attackers and the sites they create to steal any information they can get. Nowadays, people give out so much information for these companies, that they don't bat an eye when it asks for sensitive information. This leads to a trust that people give these companies, but don't realize that where they are putting this information in, is not the company they trust.

In order to help combat the problem of employees that don't know when an email is malicious or not, we will send out "practice" emails sporadically as to test the employees' knowledge of what to do. If the employee sees the email and reports it or does nothing, then they pass. If they don't, but instead click on links that are in the email, they fail and will receive further training. It won't be on a schedule, as the employees could predict the emails and won't be fooled. It will happen several times a year and within a two-week period for new hires. With everything we are doing regarding training and practice emails, this should help our employees keep their guard up enough to prevent any attacker from going after them.

References

Lance Spitzner. Cyber Security Training. (2021, October 7). Retrieved November 12, 2021, from https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/.

NortonOnline. (n.d.). *Phishing email examples to help you identify phishing scams*. Norton. Retrieved November 12, 2021, from https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html.