Lesson 9 | Preventing Phishing

Updated 2020-09-14

In the last lesson, we covered what phishing is and reasons to be suspicious of certain kinds of email. This lesson is about preventing phishing attacks and what to do 1) if you are suspicious of email and 2) what to do if you think you are a victim of a phishing attack.

Phishing is the most common form of attack that you, as an employee, will see. It is worth extra time and thought to understand what to do if you suspect a phishing attack.

People sometimes assume phishing attacks are easy to detect, like the Web 1.0 Internet scams involving Nigerian princes and bank wires. Modern phishing attacks aren't like that. They are sophisticated. Like the rest of the web, phishing attacks have incremented to Web 2.0 and 3.0 level sophistication. And the software that runs phishing attacks is only getting better.

And, even if these fake email messages contain signs of being a phishing attack, those signs can be subtle. And you might receive the phishing email at a time when you're rushing for some reason, like at the very end of the day, or when you're tired and not paying 100% attention. In those times, you are not vigilant about your email. Trust us, this happens a lot. And the scale of phishing attacks means you will get them in your inbox.

What do you do if you get an email and you suspect it's a phishing attack?

First, you should have an extremely low bar of suspicion for all emails you receive. Email volume, especially within modern technology companies, is on the decline as more and more communications and workflows are integrated into tools like Slack and Microsoft Teams. Sometimes it is just a sense when you read an email and not an obvious "there's no way this is a real email".

Second, do not click on any links or open any attachments in the email. It's best to not open the email at all or to close the email if you've already opened it.

Third, if you have any suspicion about an email you receive, you should immediately contact the sender but not by replying to the suspicious email or through email at all. If it is a phishing email, there is a chance that the sender's account has been compromised and they do not even know it. If that is the case, replying to the email will only connect you with the attackers. Contact the sender via another channel - phone, chat, or in person.

Fourth, unless you get an immediate confirmation from the email sender that the message is legitimate, reach out to your security team. If you don't have a security team, reach out to your manager or whoever might be in charge of email. At smaller companies, roles are often overlapping. Again, do not use email here. While it is unlikely that your entire email system has been compromised, it's better to use another form of communication. The reason to do this is that there is a chance that others at your company got the same message and you want to proactively prevent them from being victims.

Ideally, your company has a process for dealing with suspected phishing attacks and compromised email accounts. If they don't, and many smaller companies don't, that's fine. As long as the email is quarantined and investigated.

The thing to remember about phishing, and email in general, is that you should be suspicious of all emails you receive. Phishing attacks are often not obvious. And we sometimes chance upon opening them when we aren't paying close attention.