Haekka

Lesson 12 | What to do when Something Goes Wrong

Updated 2020-09-14

You should have a very low bar for suspicion about digital security. And you should have a similarly low bar when it comes to reaching out to appropriate people at your company if you suspect, detect, or otherwise feel uneasy about anything related to your digital security. Waiting to ask will never benefit you or your company.

It is safe to assume that you are under attack at all times. There are many groups initiating attacks, those attacks are using software to scale, and that software is easy and cheap to acquire. The key is staying ahead of the attackers and the key to staying ahead of the attackers is to be proactive when you see or sense something that doesn't feel right.

If you suspect any of the following, even just slightly, reach out to your manager and / or IT group that is responsible for security.

- You open an attachment in an email.
- You get an email that has a mismatch of the sender name and email address.
- You get an email with grammatical errors asking you to click a link.
- You get an email about a personal service, like Netflix, on your business email address.
- You learn that a computer user you share a computer with, say a spouse or child, has had one of their accounts compromised.
- You lose your phone or computer.
- You learn that a public data breach impacted your username and password and you use the same password at work.
- You find a service running on your computer or phone and you don't know what it is.

Employees represent the perimeter of company defense. And they are taking on more responsibility in that defense when they work remotely.

Be suspicious and proactive about the security of all of your devices and accounts.