So you click a phishing link

Welcome to another installment of the weekly security topic! As we kick of the new year, it is time for a look at mitigating risk. As the advancement of AI generated phishing emails becomes more and more prevalent, falling for these is only going to increase. Of course, the first course of action is to increase user awareness and help couch others into identifying and catching these as they come in. Unfortunately, one is bound to get past even the sharpest of people. Studies have shown that almost half of all C-Level executives will fall victim to a phishing email. This just goes to show that even at the highest level, it is a coin toss if they will fall for the attack.

The good news is that even if a link is clicked, that does not automatically mean that your account has been compromised. Catching when a link takes you to an unexpected location and stopping there may be enough to stop the attack in its track. Although this is not always the case and there are multiple zero-click email threats that have been discovered, ensuring that you pay attention to the location that a link takes you to is a very good second step.

As the attack progresses, it is extremely important to gather as much information and ensure that you can talk a user through this while also ensuring that they are giving truthful information is a skill that takes time to master but once it is, can be the difference between stopping an attack in its tracks or the complete loss of an account or even an entire network. Of course if a link is clicked, whether the user inputs their credentials or not, the first mitigating step to take is to change the account passwords. If credentials where entered, it is also suggested to check signin logs if you are an admin or have the access to do so and then forcing a sign out of any active sessions. This will help ensure that if a foot hold has happened, the

attack must start from scratch. It is also good to verify if the account has multifactor authentication. If it is not enabled, look at why it is not. The security experts stress that this can help minimize the takeover of an account and if it is available that it be enabled.

Now that you have addressed the account, it is time to look at the computer or device itself. If the attack happened on a phone, ensuring that the OS is fully up to date is a good place to start. If the attack happened on a computer, there are a few steps to take as a precaution. First and foremost, running a full system scan for viruses and malware will ensure that if any payloads were able to detonate, they are caught. One thing to note here is that this does have an asterisk. The malicious payload is only going to be caught if the software running the scan has the definitions for the malicious software. While the scan is running, there are a few places to check to make sure things like persistence have not been put in place. Verifying the startup applications in three locations can help determine if this has happened. First, check the startup apps within the system settings. Once you verify this, it is time to check the startup apps in the app data folder. This can help to ensure that there is nothing hidden that the system's settings did not show you. Finally, you can check the startup applications within the registry. Looking for things that are out of the ordinary, like a PowerShell script that is run on startup or unusual applications are good indicators that persistence has been put in place.

While there are other places for malicious software to hide, like the services that run on a computer, doing these steps will help ensure that most threats are mitigated. Knowing when to ask for help can be more important than just assuming. As always, this is not meant to be the only source of information and I implore you to keep learning as knowledge is the best weapon against the on going battle for data.

Thank you,

Caleb Leggett