Beware of COVID-19 Scams

With the media consumed with COVID-19 information and the economic stimulus package passed by Congress, hackers are having a field day. What a great opportunity for hackers to engage with people during this stressful time. They are hoping to catch people off their guard and get them to click on a fake link or give out personal identifiable information without thinking.

During this time, train your employees to be on their best "cyber-guard" behavior. Discuss some of the following potential scams and make sure your employees think before they click.

COVID-19 Scams

- Emails claiming to be from the Center for Disease Control (CDC) and providing a link giving out information regarding COVID-19.
- Emails claiming you can get your stimulus money immediately asking you to provide banking information to deposit your stimulus check.
- Emails asking you to donate money to a charitable foundation to assist with COVID-19 supplies and hospital bills.
- Robo-calls providing information on obtaining vaccinations or home test kits.
- Calls or emails claiming to have the ability to ship you essential supplies, with the main goal of stealing your credit card information.

As more people are working remotely, hackers will take advantage of the lack of home cyber-security. Be sure your business has processes in place for Work From Home (WFH) employees.

One of the major tools for hackers are Phishing emails. Phishing emails appear to be from a legitimate source, but in reality they are from hackers trying to acquire your data or install malware on your device. Here are a few tips that will help your staff determine if they have a potential phishing email.

Tips for Recognizing Phishing Emails

Fake Links - Many phishing emails will contain a fake link directed to a site that will download malicious software to your device. If you hover your cursor over the link, you will see the actual URL. If this looks suspicious do not click on the link. Remember, many of these fake links will resemble a real URL so be very careful.

Immediate Action Needed - Most emails that insist on immediate action are fake. Their goal is to frighten you into immediate action before you have time to think. Take your time and carefully review the email.

Email will ask you to fill out or confirm personal information – Some of these fake emails will ask you for personal identifiable information that could be used to open up fake accounts or steal your identity. Never give out personal information.

Incorrect Spelling – Yes, many phishing emails will have spelling and grammatical mistakes. Some will come from foreign actors and the translation might not be 100% correct. So keep your eye out for bad grammar and spelling.

Unsolicited Attachments - Never click on an attachment unless you are expecting something from that individual and it is probably still a good idea to verify it with the sender. There have been many cases of individuals receiving emails with attachments and later found out the attachment installed malware on their device.

Remember to never click on any link or attachment that you do not know the sender. If the email looks suspicious, review the tips listed above. When in doubt delete the email.