neoRhino
IT SOLUTIONS

DEFENDING YOURSELF AGAINST COVID-19 SCAMS

Cyber-criminals are capitalizing on the fear of COVID-19 by using online scams to steal personal and financial information from victims worldwide.

Below are 10 examples of why you must stay alert and decrease your chances of falling victim to a Coronavirus scam.

FAKE COVID-19 EMAILS

Numerous emails are circulating that contain links or attachments that alledegly provide information on COVID-19 but are hidden malware threats. Scrutinize every email you get regarding Coronavirus, especially if it is from an unknown source or the message contains grammar/spelling errors.

WORLDWIDE ATTACKS

Security researchers have identified malicious attempts from various countries to capitalize on the COVID-19 situation. The attempts usually involve cyber-criminals hiding malware in documents that allegedly contain information on the pandemic, or links to websites containing viruses.

IMPERSONATION

Cyber-criminals are not only using the Coronavirus scare to distribute malware via email but many are impersonating health authorities to trick users into clicking a link that contains malware. These attacks often are in the form of Trickbots or other trojans.

MALICIOUS WEB LINKS

Thousands of new domains containing the phrase “Coronavirus” were created near the beginning of the pandemic. Unfortunately many of them host phishing sites that can spread malware. Hover your mouse cursor over any hyperlinks BEFORE you click to see where they lead.

MALICIOUS APPS

Several malicious apps have been discovered in the Google Play and Apple App Store that are disguised as Coronavirus news sources, but were actually aapps created to track location data and install malware on their device. Verify all apps for legitimacy before downloading.

MISINFORMATION

False information regarding the pandemic is running rampant and is normally meant to get people to take actions they wouldn't otherwise take, such as a clicking a Phishing scam. Attackers also pretend to be from official organizations, such as the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC).

FRAUDULENT PRODUCTS

Cyber-criminals have also begun advertising fraudulent products claiming to help people cope with the situation, such as fake links to purchase face masks or hand sanitizers, often disappearing after receiving the money. Verify any source you are purchasing from.

CHARITY SPOOFING

If you wish to donate money to charity organizations, donate directly through their official websites or phone numbers. Bad actors often spoof victims through fake charity campaigns. While they may seem legit, you could be giving your credit card credentials directly to a cyber-criminal.

AVOID "ACT NOW" ADS

Avoid emails or advertisements that encourage you to "act now" to avoid being a victim of the virus. This sense of urgency is meant to capitalize on the panic and pressure people into making an irrational decision. Be vigilant and steer clear of these advertisements.

GO THE DISTANCE

This may be a sensitive time for everyone but cyber-criminals prey on that sensitivity and hasty decisions that are made too often in a crisis. Double check before clicking any links or giving to "charity" donation. Verify any news source regarding COVID-19. It is up to you to stay vigilant.

For more information and tips visit our website at www.neorhino.com.