- Computer crimes

Protect yourself from WFH online scams

The Manila Times · 26 Apr 2020 · B6

As insidious as it sounds, there are people who use disasters and crises as opportunities to seek financial gain with complete ethical disregard. There is considerable evidence pointing to a sharp increase in cyberattacks in the Philippines and worldwide, with the coronavirus disease 2019 (Covid-19) being used as a means to illicit ill-gotten gains.

This evidence includes over 100,000 new domains being registered in the last few weeks, containing words like “covid,” “virus” and “corona,” among others. Although some might be legitimate, these new domains are most likely interlinked and used as a means to spread malware to unsuspecting visitors.
For the millions of people working from home, security measures taken at the office must still be followed. In the current situation where real-time information about the disease is highly sought after, people working from home are easier to scam than in the workplace, where security is stricter.
Here are eight ways to protect yourself against common cyberattack methods while working from home:

Online searches

Remember those 100,000 new domain names? Beware! Cyber criminals have been found to leverage online search terms by placing links to malware-distributing or ad-filled websites in web search and social media results. Allow or enable website filtering on your antivirus software or stick to your trusted media sites for information.

Gaming

If you are sharing your device with family members, it is common for the same device to be used to access company servers and used for personal activities such as gaming. Traffic to online gaming sites has increased significantly because of work from home (WFH) directives, home quarantine/ self-isolation, students studying at home, etc. Criminals often pepper third party sites with malware-infected apps, so only download from Google Play and Apple stores.

Video conferencing

Many attacks such as meeting "bombing," malicious chat links and unauthorized attendees, can be remedied through a few steps. These include enabling passwords, reviewing privacy settings, turning on notifications so you know when someone joins, disabling the "join before host" function and the usage of your office security irrespective of which video conferencing tool you choose to use.

If you want to hold virtual gatherings with your friends, best to use your personal smart-phone, laptop or other devices. (See infographic for helpful tips.) Like any application, ensure that you are using an up to date version and using the security features, which are part of the application.

Internet of Things

In an age when fridges, TVs and other home appliances may be connected to the internet, these again offer a cyber criminal an easy attack method. Since many Internet of Things items are manufactured with little regard to security, it is imperative that passwords are changed upon purchase. It may sound minor but what would you do if your smart fridge is turned off remotely or your smart TV is switched to a pay channel without your authorization?

Virtual private networks

There is so much focus on business continuity, but very little on connectivity to the enterprise network from home. Home routers are connected to an internet service provider and in place for a long time, often without dated firmware. This makes home routers very vulnerable and an easy solution is to ensure the latest updates are in stalled and passwords changed. When was the last time you checked if your router needed an up date?Now would be a good time as cyber attackers know that we are working from home.

Phishing

Information stealing through phishing is a popular method of attack in the Philippines because it involves the bulk sending or specially crafted individual emails/messages. These messages utilize marketing techniques to hook you into signing up for Covid-19 updates, for example, and encourage you to click a link leading to malware. Make sure your work email is accessed via a corporate firewall and be on guard for anything being offered for free whether via email, chat apps, social media, etc. Be wary of emails and be sure to think before you click as cyber attackers will prey on us having our guard down as we are working from home.

Online scams

Buying products online and sending them overseas to those in desperate need due to scarcity of supply is something else scammers leverage. There are many cases, including overseas government procurement departments, where health care providers desperate for personal protective equipment are getting scammed. Buy only from trusted online retailers or platforms.

Cloud

Since the cloud plays an important role in delivering software as a service, check with your information technology staff that the corporate firewall infrastructure is using threat intelligence to look at traffic coming in and out of the network. This means your home devices are protected from attacks whenever you access the corporate network.

Scammers. Never. Sleep.

Their modus operandi is to search, select and scam targets all day either manually or through automation. A crisis on this scale is like music to their ears and they have zero care about their victims. However, following the tips above and having a general awareness supported by sophisticated technologies help combat cyber-criminals. Every successful attempt blocked or reported goes a long way in protecting you and your personal information. We're all in this together, so let's ensure that we stay smart while working online at home.