STAYING CYBER SECURE DURING COVID-19

As new cases of COVID-19 increase, more opportunities present themselves for cyber criminals to exploit and take advantage of organizations' and individuals' vulnerabilities. One of these vulnerabilities is remote working. Remote desktop protocol (RDP), when set up correctly, is a great tool for remote working. However, using it without multi-factor authentication (MFA) enabled or on an insecure network can open the gateway to hackers.

In fact, in 2019, 80% of the ransomware attacks we handled were initiated through RDP. In 2019, 80% of the ransomware attacks handled by CFC's cyber claims team were initiated through RDP. Businesses that start using RDP for remote working during the outbreak should be aware of some of the cybersecurity risks it can pose and ensure it is being used securely.

Employees should always log on within a trusted network and ideally work with their IT department to secure personal devices – and implement MFA, prior to remote working. We've provided recommendations below to help you and your clients.

RECENT SCAMS

- Interpol has warned of a large increase in fraudulent websites claiming to sell masks, medical supplies and other high demand items that simply take money from victims and never deliver the promised goods. It is advisable that internet users purchase items only from established and reputable sources.
- A Twitter user has identified another malware campaign purporting to be a "Coronavirus Update: China Operations." The emails have attachments linking to malicious software.

OUR RECOMMENDATIONS

TEST REMOTE LOGIN CAPABILITIES

Not only should personal devices be configured for secure remote working, businesses should also ensure that multi-factor authentication (MFA) is set up immediately. MFA is a process that requires more than a password to protect an email account or digital identity. It is used to ensure the user is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Implementing this reduces the chances of cybercriminals gaining access to your business's RDP.

BE VIGILANT

As this pandemic plays out, it is clear to us that cybercriminals are shifting tactics daily. If you see something on social media or receive an unsolicited email that seems too good to be true, it probably is. Aside from learning how to spot phishing emails, make sure to do your research, use reputable companies, and follow-up requests for money or information with a phone call using a number from a separate, trusted source.

TRAIN YOUR EMPLOYEES TO SPOT A PHISHING EMAIL

Make use of learning tools that assist with phishing attack recognition. As a cyber policyholder, you can get free access to a range of risk management tools, including tools that focus on phishing attacks. This valuable tool teaches people within your business to be more vigilant when in comes to opening attachments, clicking on links, transferring money, or sending sensitive information.

BE PREPARED FOR OPERATIONAL DISRUPTION

Put simply, prepare for the worst. As with so many cyber incidents, time is of the essence so ensure you have an incident response plan in place. And if you believe that one of your employees has fallen victim or that you are experiencing any kind of cyber event, notify your Cyber insurer or broker as soon as possible so that they can help you.