PROTECT YOURSELF, PROTECT YOUR DATA

CYBER CRIME IS SPREADING

With the COVID-19 pandemic impacting the globe, opportunistic cyber criminals are leveraging our fear and need for information to gain access to individuals' computers and personal information through phishing and other spoofing schemes. These major threats require risk mitigation, risk management and/or risk transfer strategies as the crisis unfolds.

STEP 1: **Be Wary**

EMAIL SCAMS

About 90% of all cybercrime starts with an email. Check the sender's address and be skeptical of anything that doesn't look or feel right. If it doesn't look right don't open it. "When in doubt, delete it out."

INVOICING SCAMS

Scammers will monitor personal news: births, deaths, new homes and more, and then send fake invoices for payment. For example, after finding a widow on the Internet, scammers will pretend to be a collection agency calling about the recently deceased's debts.

CHARITABLE DONATIONS SCAMS

Beware of requests for money immediately after a disaster. Scammers set up fake websites with names similar to real charities and solicit donations.

INVESTMENT SCAMS

Scammers will set up seminars or websites where they suggest investing in specific funds or unusual assets has made them rich.

PERSONAL SCAMS

With so much information available online — through social media or online dating apps — scammers may be using blackmail or personal scams in addition to just economic scams.

SMALL BUSINESS SCAMS

About half of all small businesses experience a cyberattack because they generally have a moderate amount of data and often have minimal cybersecurity.

COVID-19 RELATED PHONE SCAMS AND PHISHING ATTACKS

It is being reported that callers claiming to be representatives of the Centers for Disease Control and Prevention (CDC) are beginning to surface. These calls are scams. Be wary of answering phone calls from numbers you do not recognize.

Malicious cyber criminals are also attempting to leverage interest and activity in COVID-19 to launch coronavirus-themed phishing emails. These phishing emails contain links and downloads for malware that can allow them to takeover healthcare IT systems and steal information.

STEP 2: **Do These Ten Things Now**

START by incorporating these behaviors into your digital life	**RAISE YOUR GAME** by using these technology solutions:
1 Do not provide personal/financial information in response to online/offline phone solicitations; never send money without a phone call and verification.	6 Keep computer software up to date, including firmware on routers and modems.
2 https: websites that begin with https (as opposed to just http) have a layer of encryption called the secure sockets layer, or SSL. Never enter your credit card information or other sensitive data into a site without the "s."	7 Install antivirus/malware software like Norton, McAfee or Total AV on all devices (even your Apple computers and mobile devices).
3 "Remember password" functions should always be turned off on computer. Never auto-save your user name and password information.	8 Ensure home wi-fi networks are secure—use WPA2 or WPA3 security and a unique password (call your internet provider if not sure what you have).
4 Do not access financial or other accounts from mobile devices or through public Wi-Fi. Financial transactions should only be conducted on a trusted virtual private network or VPN.	9 Enable security features on any devices and/or websites — PINs, fingerprint authentication, facial recognition or multi factor authentication.
5 Disable all "smart home" devices with recording capability when discussing confidential matters, especially voice activated "smart speakers" such as Alexa, etc.	10 Use password management systems such as Last Pass or Keeper to protect your credentials. These secure websites will help you better manage your user names and passwords. Passwords should be a minimum of 12 characters and contain a mixture of upper- and lower-case letters, numbers and symbols.

PROTECT YOUR BUSINESS through training and third-party services:
Small businesses should secure their Wi-Fi networks, train employees on cyber security, and consider using third-party security companies to protect their data. Cyber liability insurance can help a small business survive cyber-attacks by paying for customer notification, credit monitoring, legal fees and fines after a data breach.