CRESTWOOD
ADVISORS

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.