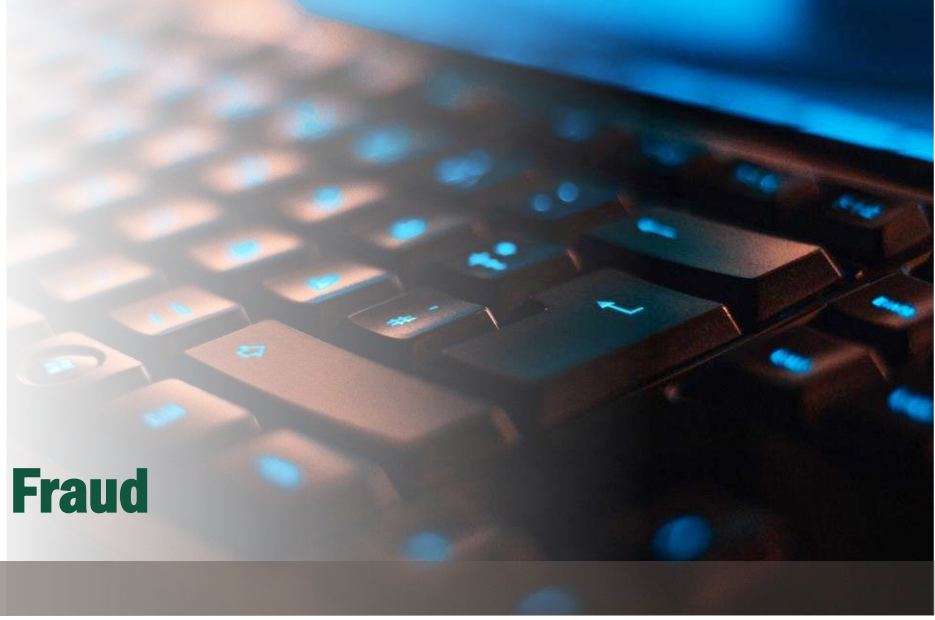
Acadia INSURANCE
| a Berkley Company



Precautions to Prevent Fraud

Disruption in the world has created significant opportunity for fraud in many unimaginable ways. We encourage you to take additional steps to make certain that actions you take in connection with sharing information and making payments to third parties do not result in unintended consequences. Spoofing and phishing emails, amongst other strategies by fraudsters, are even more prevalent in an environment where so many of us are working remotely. Please be careful and take the extra time to fully and completely validate any such interactions you may have with third parties, particularly prior to making payments. Please note that this is for general information purposes only, and nothing herein is intended to constitute legal advice or the provision of professional consulting services.

Although there are unfortunately many ways during the COVID-19 pandemic for fraud and criminal activities, there are few common means of being victimized electronically. Common means of cyber fraud committed against individuals and organizations are through phishing, spoofing, and ransomware attacks.

Phishing

Phishing is when emails are sent to members of your organization appearing to come from a legitimate source. In reality, they are hackers attempting to trick people into revealing sensitive or personally identifying information, while posing as someone else.

Spoofing

It is called *spoofing* when a person or party downloads malware onto your computer or network with the purpose of taking over an identity, phone number, email address or even an IP address in an effort to trick a third party. In these situations, they may be requesting payments, account numbers, or other sensitive information for their own fraudulent gain.

Ransomware Attacks

A *ransomware attack* occurs when a criminal or group gains access to an individual computer or network, making it inoperable until a ransom demand is met. This may involve locking or encrypting a system or set of files until a payment is made. Ransomware attacks can be the result of phishing emails, opening unknown attachments, or by visiting websites from which the malware is downloaded.

To help protect your organization from cyber fraud, we recommend the following practices:

- Make sure your networks and computers are secure and are satisfactory with the challenge of the increased number of employees working remotely.
- Install antivirus software updates as soon as they are available.
- Train employees to spot phishing attempts and have a means for reporting them.
- Do not give out personally identifying information, passwords, or financial information as a result of an email, phone call, or text request.
- Have caution opening an email from an unknown/unexpected sender or subject line.
- Only open attachments from a trusted and verified sender.
- If using a Wi-Fi network at home, make sure security is up-to-date and the network is password protected.
- Verify the sender's email address. For example, an email from a bank representative with a domain of @gmail.com or a misspelled company name is likely to be a cyber-criminal.
- Hover your cursor over hyperlinks to view and verify the whole URL before clicking.
- Avoid visiting unfamiliar websites.
- Turn on your computer's pop-up blocking feature.
- Implement a policy requiring employees to change their passwords at a minimum of every 90 days. Passwords should be unique and consist of a combination of upper and lowercase letters, special characters, and numbers.
- Implement a policy for internet use while using a company-owned device or any device using the company's network.
- Regularly backup valuable internal documents and customer information, and store backups remotely or on the cloud.

During this time of our nation standing together and helping one another, charitable donations are on the rise. Unfortunately, this is another opportunity for cyber fraud criminals to pose as an organization to obtain your financial information. Please ensure the validity of a charity to which your funds are intended. Two means of doing so are through charitynavigator.org and charitywatch.org.

For more information regarding cyber security or precautions to prevent fraud, please contact Acadia's Virtual Loss Control Team at 207-874-5701 or virtuallc@acadia-ins.com.

05/04/2020