Coronavirus Advisory:

Cybersecurity Measures

As the COVID-19 pandemic unfolds, there are cyber criminals who will likely take advantage of individuals working remotely, as well as people seeking information about the pandemic. It is important businesses remain vigilant as they work to mitigate these threats.

Cybersecurity for Organizations

As organizations explore various alternate workplace options in response to COVID-19, the Cybersecurity and Infrastructure Security Agency (CISA) recommends examining the security of information technology systems by taking the following steps:

- Secure systems that enable remote access.
  - Ensure Virtual Private Network (VPN) and other remote access systems are fully patched.
  - Enhance system monitoring to receive early detection and alerts on abnormal activity.
  - Implement multi-factor authentication.
  - Ensure all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.
- Test remote access solutions capacity or increase capacity.
- Ensure continuity of operations plans or business continuity plans are up-to-date.
- Increase awareness of information technology support mechanisms for employees who work remotely.
- Update incident response plans to consider workforce changes in a distributed environment.

Cybersecurity Actions for Employees

Malicious cyber actors could take advantage of relaxed privacy practices as well as increased public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. Organizations should guard against such acts by informing and regularly reminding employees of company policies and extra precautions they can take to minimize risk to themselves and the company at large. Recommended steps include:

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information. This includes following links sent in email.
- Use multi-factor authentication for all outside communication to ensure you are speaking with or granting access to the appropriate person(s). This includes conversations with vendors and over messaging services such as Skype.
- Avoid Social Engineering and Phishing Scams:
  - Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
  - Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
  - Don't send sensitive information over the internet before checking a website's security.
  - Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure — rather than "http."

- Look for a closed padlock icon — a sign your information will be encrypted.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, anti-phishing features, and email filters to reduce some of this traffic.
- Watch for Invoice Manipulation Fraud and be on HIGH alert for ANY change in payment instructions and verify via an external method (Ex.: phone call to the contact listed in the original customer or vendor contract) before sending a check or changing EFT or wire instructions.

- Avoid COVID-19 related scams:
  - Don't click on links from sources you don't know. It could download a virus onto your computer or device.
  - Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying that they have information about the virus.
  - Ignore online offers for vaccinations.
  - Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don't let anyone rush you into making a donation. If someone wants donations in cash, by gift card, or by wiring money, don't do it.
  - Be alert to "investment opportunities."
- Use trusted sources — such as legitimate, government websites — for up-to-date, fact-based information about COVID-19.
- Trust but verify.

Cyber Liability Coverage

It is important for every business to maintain appropriate cyber insurance coverage and limits. Contact your McGriff representative to better understand cyber liability insurance options available for your company. An important question may also arise during an event of this magnitude, which is whether your company should file a claim. It is always McGriff's recommendation that any claim or potential claim be filed with the carrier as soon as possible for consideration.

For more information – please visit our Coronavirus Resource Center.