Unfortunately, over the past couple of weeks, cybercriminal enterprises have increased their activity. The COVID-19 pandemic provides them a single issue to take advantage of, preying on individuals worldwide.

As most of us are now working from home, we need to be aware of potential cyberattacks against our personal and work environments. Cybercriminals have been observed using the COVID-19 pandemic to impersonate local/national governments, regional/global health organizations, and popular news sources. Besides phishing emails, cybercriminals are utilizing:

- Text messages to cell phones claiming to be from official entities
- Fake COVID-19-related websites hosting malware and malicious apps
- Impersonation of VPN/portal representatives to capture employee credentials

It is important to continue to follow common-sense best practices when it comes to your company’s VPN, along with other standard company-issued resources. Any changes to processes should be well-documented, reviewed by management, and exchanged via your normal internal communication methods.

Every employee plays an important role in mitigating risk:

- Maintain a heightened level of caution when reading emails, especially external emails related to the COVID-19 pandemic
- Use only company-provided equipment to perform company functions
- Utilize your company email and voice tools for all company-related functions
  - Do not utilize or respond to emails from other employees' personal email for company-related tasks
- Avoid the potential impulse to improvise and utilize tools/websites not previously approved by the company
  - Such sites introduce a high risk of the service being impersonated and/or theft data/content
- Retrieve information or click on links only from known, reliable sources
- Do not install any apps or software related to tracking the COVID-19 pandemic
- Escalate any barriers to your normal job function to your management and/or IT support teams
Other ways to be vigilant:

- Do not use company-provided equipment for personal use unless connected to the VPN
- Ensure your home network and router have strong passwords
- Beware of phishing and texting scams across social media accounts
- Verify a charity’s authenticity independently before donating
  - Monitor credit cards and bank accounts after making donations

When managing a distributed workforce, communication is the key to success. Make a point to stay in touch with employees who are remote to keep best practices top of mind when it comes to security, such as the following:

- Exercise proper cyber hygiene on any devices used for work-related purposes, including how to identify when an email is coming from an external source
- Reinforce the importance of safeguarding confidential information, including login and account passwords, personal, identifiable information of customers and others, and sensitive business and market information, particularly because employees may be working on shared devices and in shared spaces
- Delete confidential, personal, or other sensitive data when no longer reasonably required for business purposes

For more related articles, visit CounselLink COVID-19 Resource Center.