Cyber Risk Due to COVID-19

PERSONAL RISK UPDATE

Be on High Alert to Avoid Cyber Attacks

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.

The Threat of Malware and Bad Actors is Real and Growing

- The Johns Hopkins COVID-19 infection rate map was laced with suspicious malware by bad actors exploiting human desire for information on the pandemic
- Consider that malware software such as keyloggers are being hidden in emails, notifications, and social media posts, and may appear to be from trusted government agencies such as WHO and CDC
- Watch out for fake domains for meeting and school applications such as Zoom, Google Classroom and other trusted platforms
- Expect to see additional phishing emails from hackers posing to as delivery companies, online sellers, brokers and investments firms

There is the potential of a devastating impact as the result of the loss of personal information, such as login credentials to financial institutions. At a minimum it could lead to the theft of funds and fraudulent charges, damaged reputations and even more.

Follow Mitigation Best Practices

- Exercise caution in handling any email ("phishing"), text message ("smishing") or voice calls ("vishing") with a COVID-19-related subject lines/attachment/hyperlink/topics or headers
- If you don't recognize the sender, you should delete without opening
- Don't trust links, documents or texts – hover over links and check for misspellings and unrelated addresses (e.g. googloclassroom\.com)
- Navigate directly to trusted sources e.g. CDC, FEMA, NIH for updates and new information

- Be cautious of social media pleas/articles/links related to COVID-19 – these may be phishing items
- Do not provide personal/financial information in response to online/offline phone solicitations
- "Remember password" functions should always be turned off on computer
- Do not access financial or other accounts from mobile devices or through public Wi-Fi
- For additional best practices view USI's Personal Risk Cyber Checklist

Network Protection Practices

- Do not use the internet provider's router—purchase a separate router network for home
- Ensure home wi-fi networks are secure—use WPA2 or WPA3 security and a unique password
- Passwords should be a minimum of 12 characters
- Change administrator credentials from factory settings
- Set-up a guest network for all visitors, family and your mobile devices
- Use one device for financial transactions and keep it on the home network
- Disable all "smart home" devices with recording capability when discussing confidential matters, especially voice activated "smart speakers" such as Alexa, etc.
- Enable security features on any devices—PINs, fingerprint authentication, or facial recognition
- Use password management systems such as Last Pass or Keeper to protect your credentials

View USI's full report, ***Cyber Exposures and the COVID-19 Quarantine***, to learn more about protecting your company and employees from these exposures. **Please also visit the USI COVID-19 Resource Center for additional updates, tools and resources at www.usi.com/public-health-emergencies.**

How Can We Help?

For more information about cyber exposures or to discuss potential insurance solutions for you and your family, please contact your USI Personal Risk Advisor or visit us at www.usi.com.

Sources:

https://www.fastcompany.com/90476868/cybercrooks-see-the-coronavirus-as-an-opportunity-to-steal-your-data
https://thehackernews.com/2020/03/zoom-video-coronavirus.html
https://www.tomsguide.com/us/home-router-security,news-19245.html
https://www.hellotech.com/blog/which-router-security-option-should-you-choose
https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/
https://www.cnet.com/how-to/strong-passwords-9-rules-to-help-you-make-and-remember-your-login-credentials/
https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/
http://www.digitaljournal.com/tech-and-science/technology/hackers-are-exploiting-coronavirus-to-gain-access-to-it-systems/article/568557