Cyber Risk: Protecting Your Family During the Pandemic

The need to protect accounts, home networks and family members from cyber hazards has grown exponentially with the increase in work from home arrangements due to COVID-19. While insurance companies develop new policies and programs to protect consumers, individuals must proactively limit their personal cyber exposures.

Last spring, USI Insurance Services outlined strategies to keep safe while working from home. As we embark on a new year, it's time to reassess the current situation and consider what cyber safety measures need to be updated. USI personal risk experts recommend the following to help you limit your risk.

Recognize and Avoid Threats From Hackers and Bad Actors

In 2020, USI warned about the malicious threats that were taking advantage of the massive increase in employees working remotely. Threats included interactive maps purporting to track outbreaks of the virus, as well as phishing emails with malware and fake domains. Today, many of these same dangerous conditions still exist.

Clicking on a link in an email from an unfamiliar source remains one of the most common ways to infect your computer with a virus — or to aid a criminal in stealing your personal information or identity. When in doubt, do not click the link. Taking simple steps, such as hovering over the link to identify the actual site you will be directed to, can often reveal that the email is fraudulent. Alternatively, you can close the email and navigate to the website directly to avoid the trap of the email bait.

The latest threats are emails (phishing) or texts (smishing) that offer scheduling access to one of the approved COVID-19 vaccines. The U.S. Centers for Disease Control and Prevention (CDC) will not contact you via email or text, and there are no third parties sanctioned to make these arrangements.

Practice these cyber threat mitigation efforts:

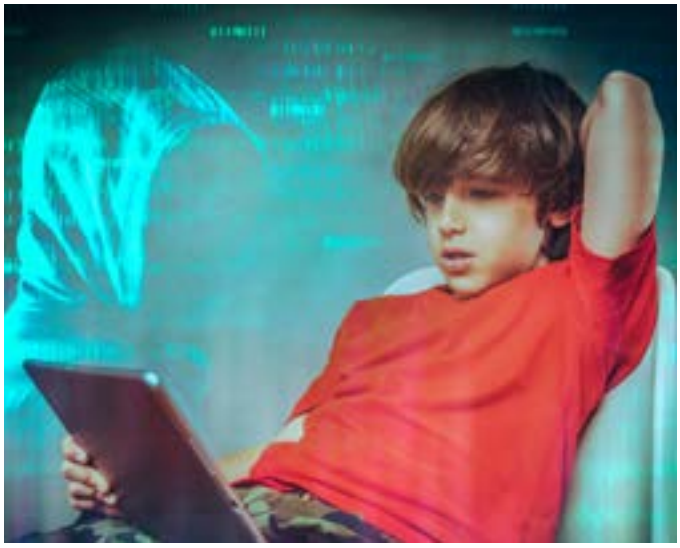
- If you do not recognize the sender, delete the text or email.
- Navigate directly to trusted sources via your web browser (if you're on your computer, your browser should be protected by antivirus and spyware software that you've purchased and installed).
- Be wary of social media offers, articles or links that promise vaccine information, as these can be fraudulent attempts to access your personal information.
- Never provide personal or financial information online or via a telephone solicitation.
- Do not allow your computer to autofill passwords.
- Do not access financial or other personal accounts on public Wi-Fi or on a mobile device.
- For more best practices, view USI's Cyber Safety Checklist below.

Conditions have changed very little since the onset of the pandemic — large numbers of employees continue to work remotely, providing an unprecedented opportunity for bad actors to gain access to a trove of confidential data from employers that could include employee and client information. The bad actors' methods remain largely the same, but they are switching the messaging to the vaccine rollout or protocol changes due to this winter's surge in COVID-19 cases.

Secure Your Network

If you hope to avoid these threats to your personal information and finances, you should also take security measures to prevent access to your network and Wi-Fi. Simple but practical steps can create enough obstacles to deter hackers.

For starters, change the name of your router — which serves as the gateway to your personal information — to one that does not identify you. For instance, having "[Your Family Name] Network" is a poor choice for a router name, as it identifies your last name to potential hackers. It's also a bad idea to have the router's manufacturer in the name (e.g., Linksys, Netgear), as that's also information perpetrators can use to compromise your network. Your router should also have WPA2 or WPA3 security, as well as a unique password that has a minimum of 12 characters and includes a mix of letters, numbers and symbols.



With the rise of smart devices and the smart home, the connection to appliances or other devices should be separate from the computer on which you store your financial information. Alexa, Xbox, refrigerators and other appliances should connect individually to a guest network (i.e., a separate network from your home network). Reserve the home network for your computer with your financial information saved on it.

Additional loss control measures you can take to secure access to your home Wi-Fi and internet:

- Change the administrator credentials on your network from the factory settings.
- Arrange a guest network for visitors, family, and mobile devices.
- Disable all smart home devices with recording capability when not in use.
- Enable security features offered in any devices, such as PINs, fingerprint and facial recognition.
- Consider using a password management system (e.g., LastPass, DashLane, NordPass).

Your first effort should always be to create obstacles to accessing the gateway into your home computer, and then to design and coordinate additional layers of protection. For more recommendations on cyber security related to COVID-19, please contact your USI personal risk advisor or visit USI's Public Health Emergencies site.

Cyber Checklist: Keep These Best Practices at Your Fingertips

Get proactive

- Review your credit report regularly.
- Lock credit for children and family members who don't need access to credit.
- Request a dark web scan and act when personal information is found.
- Sign up for monitoring services, e.g., Rapid ID Recovery.

Practice good password hygiene

- Create strong, unique passwords for all financial sites (e.g., phrases, song lyrics). Use a minimum of 12 characters.

Protect your network

- Utilize a secure router, preferably one not from an internet provider, and WPA2 or WPA3 security.
- Create virtual private networks (VPNs) to send and receive data more securely.
- Use one device (computer) for accessing all financial accounts.
- Create a separate guest network for all guests, smart devices, and additional family devices.
- Keep software up to date (e.g., antivirus and operating systems on computers/phones).
- Thumb drives should only be used if you purchased them — discard giveaways.

Act immediately after a suspected breach

- Notify: Contact financial institutions, credit bureaus, authorities, family members, and anyone with access or authority on accounts.
- Identify: Locate access points to personal or financial information and remedy the issue.
- Change: Update passwords, account numbers, and credit card numbers.
- Monitor: Check credit reports, bank and credit card accounts, and the dark web.

Trust, but verify

- Require financial institutions to provide verbal or written verification of fund transfers over a preset limit.
- Use dual authority for transactions (i.e., authorization from additional party such as a spouse or parent).
- Before clicking on links, verify if they are legitimate by hovering over the link to view the full web address (URL).
- Never follow links in an email to update personal information with financial institutions.
- Navigate to known websites from your browser in lieu of clicking a link.
- Avoid using public Wi-Fi, especially to access financial accounts.
- Protect usernames and passwords — utilize password utility programs (e.g., LastPass, DashLane, NordPass).
- Use multifactor authentication when possible.

The USI ONE Advantage®

To analyze our client's personal exposures and challenges our personal risk team leverages USI ONE®, a fundamentally different approach to risk management. USI ONE integrates proprietary business analytics with a networked team of local and national experts in a team-based consultative process to evaluate the client's personal risk profile and identify targeted solutions to address those risks. Clients then receive tailored recommendations for more efficient investment of premium dollars through customized personal insurance risk management programs that enhance coverage and manage rate control.