Cyber Checklist: Keep These Best Practices at Your Fingertips

The ability to perform financial transactions online offers tremendous convenience, but also exposes assets to theft and cyber fraud. In addition, the Internet of Things (IoT), which connects home security systems and other smart devices, creates another access point to personal information and assets. As new technology surfaces, the need to protect accounts, home networks and family members from cyber hazards grows exponentially.

While insurance companies develop new policies and programs to protect consumers, it is critical for individuals to proactively limit their personal cyber exposures. USI Insurance Services personal risk experts recommend the following to help you limit your risk.

Prevent the Loss

Get proactive

- Review your credit report annually.
- 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, lyrics). Use a minimum of 12 characters if possible.
- Avoid using public Wi-Fi, especially to access financial accounts.
- Protect usernames/passwords (utilize password utility programs, e.g., Last Pass, Dashlane, NordPass).
- Use multifactor authentication when possible.

Protect your network

- Utilize a secure router, preferably one not from an internet provider and use WPA2 or WPA3 security.
- Create VPNs (virtual private networks) to send and receive data more securely.
- Use one device (computer) for accessing all financial accounts.
- Create a separate guest network for all guests 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.

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 an 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.

Reduce the Loss

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.