Gallagher

Tips for Managing Your Cyber Security

Cyber crime is expected to cost the world $10.5 trillion annually by 2025, which, if compared to a country, would make it the third-largest economy after the US and China.* Protecting your personal information and assets is vital. You can help reduce your risk of becoming a victim to fraud and loss by following these tips.

SECURE YOUR ACCOUNT ACCESS

- Set strong passwords using letters (upper and lower case), numbers, and special characters
- Use a password manager to track passwords rather than writing them down
- Change passwords every 120 days, or if there's a security breach.
- Don't share, reuse, or repeat passwords.
- Use multi-factor authentication to verify your identity (for example, entering a code sent in real-time by text message or email) when available.
- Do not share your account information with friends or most family members. If you must share information with a spouse or trusted advisor, do not share information via text message or email.
- Do not provide third parties personal information of any kind without verifying their credentials independently.
- Update your contact information when it changes, so you can be reached if there's a problem.

MONITOR YOUR ACCOUNTS

- All accounts holding your personal financial and/or health information should be considered (retirement accounts, bank accounts, HSA, etc.)
- Register for your online account to deter cybercriminals from registering in your place
- Routinely monitor your accounts to maintain access and check for irregular changes.
- Monitor your existing lines of credit.
- Select multiple communication options (text, email, paper alerts, or a combination)
- Sign up for account activity notifications.
- Close or delete unused accounts. The smaller your on-line presence, the more secure your information.

* Source: Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)

MANAGE YOUR DEVICES

- Apply available software updates as they act as "preventative care" for your device. Allowing auto-install options will keep your updates timely.
- Run an antivirus product on work and personal computers
- Be cautious when downloading applications, and use reputable sources like the App Store rather than third parties
- Back-up your data on a regular basis

BE ALERT IN YOUR DAILY LIFE

- Limit how much and what you share on social media and keep privacy settings set.
- Use a reliable email provider for your personal email.
- Be wary of free Wi-Fi. Networks such as those at airports, hotels, or coffee shops pose security risks that may give criminals access to your personal information.
- Refrain from using public USB ports or charging cords.
- Beware of phishing attacks that try to trick you into sharing passwords or other account information.
    - Be suspicious of texts, emails, or calls from an unfamiliar party requesting personal information

KNOW HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS

The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:

- https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
- https://www.cisa.gov/report

Gallagher

Insurance | Risk Management | Consulting