CYBER SAFETY QUICK-REFERENCE GUIDE

Tips to help protect yourself, your assets and personal information.

CONGRESS WEALTH MANAGEMENT

10 KEY CYBER SAFETY TIPS

1. Never click on a link in an email until you validate the source
2. Never enter personal information in an email or text message
3. Use antivirus software and keep it up to date
4. Limit web usage in the office to core, business-related sites
5. Make minimal use of unsecured, public networks
6. Create strong passwords and change them every 2-3 months
7. Do not use the same password for multiple accounts
8. Create separate email accounts for work, personal use, alert notifications and other interests
9. At home, set up a primary network and another for guests
10. Be prudent in what you share about yourself and your job via social media

Passwords

- Create passwords that are at least 10–14 characters. Be sure to use a mix of numbers, upper- and lowercase letters and symbols
- Change passwords at least quarterly if not monthly
- Store in a safe place or utilize a password management tool
- Turn on **two-factor authentication** whenever an ecommerce site offers it
- Never select "remember my password" on websites you visit
- Do not create common passwords
- Do not use the same password for multiple accounts/sites

Email

- Create separate email accounts for work, personal use, alert notifications and other interests
- Password protect sensitive files before emailing them *or* use a secure file exchange portal like Fidsafe.com
- Use spam filtering to stop unwanted email from reaching your in-box
- Do not open emails from unknown senders
- Do not reply to requests for financial/personal info

Virus and Malware Protection

- Keep software/browser/systems up to date
- Install antivirus software
- Turn on firewall to highest level
- Regularly back up your data
- Do not install or use pirated software
- Do not install P2P file-sharing programs
- Do not set email to auto-open attachments

Internet Usage ("Surfing the Web")

- Download software only from trusted sources
- Always log out of sites instead of simply closing the window
- Look for f**https://** in web addresses or secure session validation when available
- Do not click on links from unknown or untrustworthy sources
- Do not allow ecommerce sites to store your credit card information
- Do not click on pop-up windows to close them; instead use the "X" in the upper right hand corner of the screen

Mobile Phones and Tablets

- Keep screen lock on; choose strong passwords
- Select a device with anti-theft features
- Turn off Bluetooth when it's not needed
- Regularly update apps (e.g., security patches)
- Securely back up your data
- Do not click on ads when surfing the internet public Wi-Fi/hot spots
- Disable ad hoc networking
- Turn off auto connect to non-preferred networks
- Turn off file sharing
- Do not use public Wi-Fi

Home Networks

- Create one network for you, another for guests
- Change your router's name and password
- Change the password to your wireless network
- Turn on your router's WPA2 encryption and firewall
- Do not use default user names/passwords
- Do not broadcast your home network

Social Media

- Telephone the person who sent the email to confirm its authenticity if you suspect it may be fraudulent
- Limit the amount of personal information you give out
- Use privacy settings online wherever possible
- Do not respond to requests for personal or financial information in an email
- Do not assume that every email you receive is authentic (or its attachments

Put these safeguards in place as soon as possible if you haven't already!

CYBER SAFETY QUICK-REFERENCE GUIDE

Choosing services, software, hardware and equipment.

Email Providers

If your email is hacked, your personal information (accounts, communications, phone numbers, SSN, etc.) can potentially be stolen. The best email providers surround your information with several layers of security.

Features to Look For:

- *Authentication*
  A high-quality email service will provide secure authentication to prevent spam and spoofing.
- *Virus Scanning*
  Email is scanned for malicious content by the provider.
- *Anti-spam*
  Reputable email service providers filter spam messages from your in-box.
- *Phishing Protection*
  Some service providers will identify potential phishing emails.

Password Protection

Weaknesses stem from how users choose and manage passwords, which can make it very easy for hackers to access them and break into individual accounts. Password management tools help users store and organize passwords and can even provide additional features, such as form filling and password generation.

Features to Look For:

- *Synchronization*
  A good password manager will allow access from anywhere and synchronize across devices.
- *Password Generator*
  Automatically generates strong, complex passwords.
- *Encryption*
  Passwords are stored encrypted, and the master password is not retrievable.
- *Two-factor Authentication Support*
  An example of a second 'factor' is the user repeating back something that was sent to them through an out-of-band mechanism (like a security code received via text).

Virus and Malware Protection

If you use a computer for web surfing, shopping, banking, email and instant messaging and do not have proper protection, you are at high risk of being victimized. Running real-time antivirus products and keeping them up to date is an essential step to reduce risks from malware and can reduce infection by more than 80%.

Features to Look For:

- *Detection*
  High-quality software detects existing and new variations of malicious software.
- *Cleaning*
  Effectively quarantines or removes malicious software from an infected device.
- *Protection*
  Helps maintain a healthy system by proactively preventing malicious infection.
- *Performance*
  Good antivirus software will not slow down your system.
- *Parental Controls*
  Optional feature that will secure your systems when used by children.
- *Backups*
  Many applications provide optional back-up protection in case of system failure.

Wireless Routers

A wireless router allows you to connect devices to the internet and communicate with other devices on your network. Routers are computers, with their own operating systems, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log keystrokes and access your accounts.

Features to Look For:

- *Protection*
  Prevents high-volume malicious attacks to your home network.
- *Firewall*
  Secures your network from intrusion.
- *Guest Network*
  Allows for separate network and credentials for temporary access.

CONGRESS WEALTH MANAGEMENT

250 Northern Avenue - Suite 310 - Boston, MA 02210
8 Wright St. - Westport, CT 06880
www.congresswealth.com