CYBERSECURITY CHECKLIST

Fort Washington Investment Advisors, Inc.
A member of Western & Southern Financial Group

Technology continues to evolve and impact a significant portion of our daily lives and activities. Technological progress has achieved a variety of benefits. However, with these benefits also comes news risks and vulnerabilities. Cybersecurity is one area where individuals must be prepared for these new risks and vulnerabilities. Cyber threats, such as hacking, data breaches, identity theft, and malware attacks, pose significant dangers to individuals. Some of these dangers are financial losses, reputational damage, or even physical harm. Therefore, taking steps to protect your cybersecurity is crucial. The checklist below outlines multiple actions that can be taken in several key areas in order to improve your cybersecurity.

1. Have I created strong passwords and am I managing my passwords correctly?

- Length—At least 12 characters should be used when generating a password. More characters in a password make it harder for cybercriminals to crack.
- Complexity—Uppercase and lowercase letters, numbers, and special characters should be included in your password to increase its complexity. More types of characters increase potential combinations making it harder for cybercriminals to figure out. Use a passphrase like Maryhad@littlelamb.
- Avoid common passwords—Refrain from using common phrases or words in your password, such as "password", which are less challenging for hackers to guess.
- Avoid personal information—Exclude personal information from passwords, such as your birthday, which can make it easier for hackers to guess.
- Unique password—Every one of your accounts should have its own unique password. Different passwords across accounts will reduce your account exposure in the event of a password breach. Especially keep your financial and health account passwords different.
- Update periodically—Change your password periodically to limit the time risk exposure.
- Two-factor authentication—Enroll in two-factor authentication to increase security by adding a second layer of verification.

2. Am I safely navigating social media?

- Be prudent with what you share online—You should not share personal information or details that could be leveraged by cybercriminals in an attack. What may appear to be an innocent detail, can provide clues to these criminals. Think before you post.
- Be informed—Know how to identify social media scams and be alert to the most recent scam trends.
- Tighten your privacy settings—Modify your privacy settings to narrow the list of people who can view your posts and your profile. Blocking strangers from viewing these details will limit your exposure to cybercriminals.
- Manage friend requests—Be skeptical of unfamiliar people requesting to be your friend on social media. They may have malicious intent. Check to see if you are already friends with the person as your friend's account could have been compromised.
- Monitor for suspicious activity—If you see suspicious or inappropriate activity of social media, report it.
- Be wary of online quizzes—These quizzes can manipulate you into sharing personal information, providing answers to security questions, or expose you to malicious links.

3. Am I consistently monitoring my key financial information?

- Frequently review your account statements—Reviewing your account statements will enable you to detect unauthorized activity in the event that it occurs.
- Enroll in account alerts—Account alerts will notify you of activity on your accounts as it occurs. Activities can include transactions or updates to your user profile, such as login credentials or verification methods. This can be very helpful with spotting fraudulent activity.
- Lock accounts that you use infrequently—Most credit/debit accounts now allow you to lock accounts through an application on your phone or computer. This feature can allow you to freeze accounts if you do not plan to or use them infrequently.
- Monitor your credit report—periodically check your credit report to verify there is no unauthorized activity or account openings.
- Avoid sharing sensitive information—Avoid sharing sensitive information such as your Social Security number, bank account details, or credit card information unless necessary.
- Use reputable financial partners—Only utilize and conduct business with reputable financial partners. Review what financial protection and assurances your partners provide to you.
- Consider use of an ID theft protection provider—ID theft protection providers can assist with the monitoring of your accounts, provide alerts, and offer ID theft insurance.

4. Am I taking the necessary steps to protect my devices?

- Keep your software up-to-date—Ensure the versions of your operating system, software, and apps are the latest versions. Enroll in automatic updates to enable timely installation.
- Utilize anti-virus software—Install reputable anti-virus software on your devices to detect and remove malicious software.
- Enable firewall protection—Enable firewall protection on your devices to prevent unauthorized access. Check to see if your at-home router contains a firewall.
- Backup data regularly—Backup your data regularly to prevent data loss in case of a cyber-attack or hardware failure.
- Secure your network—Secure your network by changing the default password and using a strong password for your Wi-Fi network. Contact your provider for assistance.
- Shut down your device when not in use—Shutting down the device will limit the time your device is potentially exposed to hackers. If your device is exposed to a hacker, then turning it off will cut off the connection the hacker has.

5. Am I safely browsing the web?

- Verify website authenticity—Verify the authenticity of websites before entering sensitive information. Verify the website address is correct.
- Don't click on suspicious links—Be cautious of suspicious links in emails, messages, and social media posts. Hover over (don't click) links to verify the URL before clicking.
- Use ad-blockers—Use ad-blockers to avoid malicious ads that can harm your device or steal your personal information.
- Be cautious of public Wi-Fi—Be cautious when using public Wi-Fi as it may not be secure. Avoid logging into sensitive accounts or sharing personal information on public Wi-Fi. Verify the exact spelling of the WiFi prior to connecting to it.
- Don't download from untrusted sources—Only download software and files from trusted sources to avoid downloading malware or viruses.
- Delete your browser history—Your browsing history can store accounts you visit online along with the login credentials. Deleting the history and stored information can limit the information a cybercriminal has access to in the event of an attack.

ADDITIONAL RESOURCES

To learn more about cybersecurity, how to protect yourself, or to report an issue, visit the Cybersecurity & Infrastructure Security Agency (CISA) website, **https://www.cisa.gov/**. CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

If you identify suspicious activity or believe you are a victim of a cybersecurity attack that impacts your financial information, please contact Fort Washington at **888.244.8167**. Furthermore, if you receive unusual communications identified as Fort Washington that seem fraudulent, please contact us to verify the communications.

Fort Washington
Investment Advisors, Inc.

A member of Western & Southern Financial Group