West View Savings Bank
wvsbank.com

Personal Cybersecurity Checklist & Tips

Consider these tips to help protect your accounts, identity, and electronic devices.

Protect Your Accounts and Identity

Cybercriminals love to target accounts by using compromised login credentials, attempting to impersonate a phone rep, or contacting you directly and pretending to be from a legitimate company.

- **Create unique login identities and passwords,** particularly for your financial, email, phone and social media accounts. Avoid using your email address as a login identifier. Don't re-use passwords and avoid weak or commonly used passwords, e.g., 123456. Consider using passphrases, e.g., "I LOVE Ice Cream".
- **Enable two-factor authentication,** particularly with your financial, email, phone and social media accounts. It's easy to set up and use, and -- many smartphone apps support native device biometrics, such as thumbprint and facial recognition.
- **Provide current digital contact information** to financial institutions you do business with so you can be contacted in real-time in case of fraud or high risk transactions.
- **Use biometrics where available** to protect your account from cybercriminals in the voice channel. Many smartphones and apps support native device biometrics, such as thumbprint and facial recognition.
- **Don't click on untrusted links or attachments** in email or text—known as phishes or smishes (SMS/text message phish). Hover over links to verify it's a trusted site before you click.
- **Consider using a password vault/manager for lower risk accounts.** If you do use one, be sure to protect it with a strong, unique password or passphrase.
- **Be aware of scams.** From remote access to imposter to lottery and grandparent scams, cybercriminals use clever scams to defraud millions of people each year. If you or a loved one are faced with one of these scams, remember, in every scenario, the first step is to STOP communicating with the person immediately! And never give an unverified individual remote access to your computer.

Monitor your accounts and credit

After compromising your account, cybercriminals will attempt to move money. Monitor your accounts and credit score for suspicious activity.

- Check for any suspect activity including profile/contact information changes, transaction attempts, etc., and review any alerts you receive.

Freeze your credit to prevent credit fraud. Contact Equifax (800-525-6285), Experian (888-397-3742), and TransUnion (800-680-7289).

- Be sure to remember your PIN, username and password, as they'll be required for any freeze/unfreeze account activity. Consider purchasing identity theft protection.

Secure Your Electronic Devices

Cybercriminals will also attempt to gain control over your devices with malware, by sniffing your network traffic, or by taking over your cell phone account.

- **Use a personal firewall and anti-virus software on your personal devices,** and routinely apply security patches, anti-virus signature updates and operating system upgrades.
- **Use trusted devices for conducting sensitive transactions.** Avoid systems used for social media, video streaming or gaming, which are prone to malware.
- **Avoid conducting sensitive activities, such as online shopping, banking or sensitive work, over a public Wi-Fi connection.** Use encrypted connections whenever possible. Additionally, routinely apply security patches to your wireless access point (WAP), and protect access to your Wi-Fi network and WAP with a strong password or passphrase.
- **Secure your mobile services.** Ensure that your cell number cannot be transferred to another device without additional authentication, such as an authentication app. Consider using a mobile security app that scans URLs and checks Wi-Fi connections. Use built-in device features, such as biometrics, automatic screen lock, automatic updates, "Find my phone" feature, and minimize location access for required apps only.
- **Update/patch your Internet of Things (IoT) devices.** Routinely apply security patches and change the default usernames and passwords. Consider turning off smart digital assistants when discussing important personal matters

Safeguard Your Data, Mail and Online Shopping

Cybercriminals will ransom your data, compromise legitimate e-commerce sites, and even steal your mail, looking for checks and credit cards.

- **Backup your data to a secure cloud location.** Most modern personal computers offer secure cloud storage capabilities that are built-in and easy to use. Enable autosave for your apps, and routinely backup your data to the cloud.
- **Practice safe online shopping.** Consider using trusted payment systems and never use debit cards for online purchases. Do business with reputable vendors and make sure your connections are encrypted by checking websites for a closed padlock icon ( ) and a URL that begins with https://.
- **Protect your US mail.** Sign up for USPS's free Informed Delivery service to help prevent mail fraud or theft. Digitally preview your mail and manage your packages scheduled to arrive. Protect your email account that receives these notifications with a strong password/passphrase and Dual Factor Authentication (2FA), so cybercriminals don't see the email and then steal your mail.

Additional Resources:

- Cybersecurity and Infrastructure Security Agency (CISA) Password Tip Card
- FTC Guidance to help you avoid fraud from common online scams
- CISA Mobile Security Tip Card
- CISA Privacy and Mobile Device Apps
- CISA Securing Wireless Networks
- CISA IoT device security tips
- CISA Security tips for shopping safely online
- Cybercrime Support Network

- **If you're a victim of online crime**, file a complaint with the Internet Crime Complaint Center, or visit the FTC's free, one-stop resource, www.IdentityTheft.gov