

Online Banking Security

Protect yourself online with the following tips:

Password Protection / Identity Theft Protection

- Never share your passwords or PINs with anyone.
- Never provide personal or account login information over the phone.
- Never write your passwords down where they could be easily found by others.
- When creating passwords, don't use information that could be easily linked to you (like your birth date, Social Security number, phone number, or the names of pets or hobbies).
- Use passwords that contain letters and numbers, preferably not recognizable words (example: Ter8sdF).
- Visit the Federal Trade Commission (FTC) website for helpful password tips.
- Select a unique and complex password and security questions/answers for each system. Always use a different password and/or security questions for each system you access.
- Change your online account passwords often. We recommend that you change your passwords every 30 days.

Online Security

- If you are providing financial information or placing an order online, be sure the site is secure. Look for a URL that begins with "https://" and the "closed padlock" () in the lower right hand corner of your browser.
- Do business only with financial institutions and online merchants that you know and trust.
- Watch out for copycat sites that may try to look like a financial institution. Be sure you are using the correct web address for your bank.
- Avoid downloading programs from unknown sources.
- Be aware and cautious of suspicious emails. Don't reply to any e-mail or pop-up message that requests you update or provide personal information.
- Never leave your computer unattended while using any online banking or investing service.
- Always log off completely and close your browser when you are finished with a secure session.
- Only access your personal financial information from a computer you "trust." Internet kiosks and cyber cafes are not as secure as your personal computer.
- Install, use and regularly update anti-virus and anti-spyware software on your computer.
- Maintain a current browser. Make sure your computer is up-to-date with security patches for your operating system and applications. Windows users should turn the Auto-Update feature on. Security patches may be found at vendor's websites. Check the sites periodically as these patches are frequently updated.
- Install a personal firewall and intrusion prevention system to prevent hackers from invading your personal computer, especially if you are using DSL or a cable modem to access the Internet. A firewall can make you virtually "invisible" online and will help to block out communications from unauthorized sources.
- If you use wireless networking, make sure to turn on all security features such as WPA encryption. Change the default password and SSID on your wireless router.

William Penn Bank will not contact customers on an unsolicited basis to request any personal information.

Review your bank account statements on a regular basis. Report any unauthorized charges to us right away.

To report any suspicious or unauthorized account activities, including a suspicious email if received or opened, please contact us at 215-945-1200.

For more information, visit the FDIC and FTC websites.