Using Online / Mobile Banking Securely

At Pentucket Bank we do everything possible to keep your personal information secure. But in today's "high-tech" world the security of your personal information is a collaborative effort between you and the bank. While Technology continues to provide the convenience of banking anywhere and anytime, that convenience carries with added security risks. Here are a series of best practices you can use to help protect yourself from these risks.

- Create a strong, unique password that is easy to remember, but hard to guess. Don't use common words, names, birthdays or any personal information in your password.
- Use your mobile device's auto-lock feature. We recommend you set your auto-lock to take effect 5 minutes from the last activity.
- Log out after each Banking session immediately to ensure your account information is not easily accessed if your PC or mobile device is compromised.
- Delete Mobile Banking text messages after viewing. Once you've received and reviewed the account information you requested via text message, delete the message to ensure the information cannot be viewed by others if your phone is lost or stolen.
- Back up your data regularly. We recommend synching your mobile device with your PC.
- Delete any text messages or emails that contain sensitive information. We recommend that you never disclose sensitive, personal information about yourself via a text message or email. Sensitive personal information can include your driver's license number, social security number, password, and account numbers.
- Prior to making a purchase or conducting a transaction online, review the web address for security. Websites that contain "https:" in the web address indicates the site has taken measures to secure your personal information.
- Mobile device companies regularly provide updates for your mobile device operating system which include security patches. Keep all mobile software up-to-date by routinely checking with your device manufacturer.
- Be aware that Malware (viruses and Trojans) and fraudulent applications exist. Only download mobile applications from authorized application stores like the Apple App Store or the Android Play Store.
- If you believe your device has been lost, stolen, or compromised, immediately go online through your home computer and change passwords for financial and personal accounts to prevent any identity theft or fraud.
- If you lose your mobile device, report the loss immediately to your carrier (if you've lost a cell phone) or your company (if you've lost a company-owned mobile device).
- Don't "jailbreak" or "root" your mobile device. Jailbreaking or rooting means you are overriding some of the software features and limitations of the mobile device and this may prevent you from accessing your online banking accounts. It can also void warranties and render your phone completely unusable.
- Contact Pentucket Bank immediately if your mobile device is lost or stolen or if you suspect fraudulent transactions on your account.