

Winchester Savings Bank works diligently to protect our customer's information and accounts from cybercriminals. The following security tips should be used to help ensure the safety of your information **online** and when using **Mobile Banking**. For more information, please visit our website at www.winchestersavings.com, and check out the Online Education Center under Resource Center.

How does Winchester Savings Bank help?

- We will never request your login information or any other personal financial information by phone or email.
- We suggest you change your password at least every 90 days.
- We use multi-factor authentication.
- We use 128-bit encryption on internet connections.

How can you help?

- Always log in to websites by typing the web address directly into a browser- never click on a link in an email. Cyber thieves can make it look legitimate.
- Avoid using the same login id and or password on financial sites/multiple sites.
- Avoid using common family or pet names or other easily-obtained information as your password. Social engineers & cyber thieves use social media sites to gather information.
- Always use special characters *)^\$@(), numbers and upper and lower case letters in your password to enhance the security. HINT - make up a phrase and take a letter/number from each word to create your password.
- Do not access any financial transactions on a public computer or Wi-Fi network.
- Use a reliable anti-virus software product to scan your computer regularly and make sure it is kept updated.
- Install a firewall especially if using a broadband connection - DSL or cable modem connection.
- Update your computer operating system and browser with security related patches regularly. Look into the automated update feature when applicable.

Additional tips for smart phones - Remember that your smartphone or other mobile devices are actually a small computer with lots of data.

If you use an app, verify that it is the official app provided by your bank by downloading it from your bank's site.

- In most cases you should only download an app from an official app store. (For example: Amazon Market, Apple iTunes, Google Play Store and BlackBerry App World.)
- Beware of free apps from unknown sources, because they may contain malware or viruses that can create potential security threats.
- Password-protect your smartphone or other mobile device to protect access to your personal information in case the device is lost. Notify the Bank immediately to help change your login and password.
- In your settings, configure your smartphone to lockout after a short period of inactivity and require a code to reactivate it.
- Never store user IDs or passwords on your phone.
- Don't respond to unsolicited messages, texts or voicemails that request a PIN or password.

Did you know?

After you enter the Bank's web address and hit enter, the Internet address will change from "http" to "https." This indicates you have entered a secure site. If you do not see the https or padlock on the webpage, do not go any further and please report this to the Bank.

These safeguards are provided as a tool to help you prevent potential harm to your personal information or computer. The use of the information is not a guarantee. Contact the Bank at (781) 729-2130 if you have any concerns about an email or phone call that you received stating they are calling from Winchester Savings Bank.