

# Online Banking Security Tips



## Mobile Device Security

Configure your device to require a passcode to gain access.

Avoid storing sensitive information. Mobile devices have a high likelihood of being lost or stolen, so you should avoid using them to store sensitive information. If sensitive data is stored, enable encryption to secure it.

Keep your mobile device's software up-to-date.

Review the privacy policy and data access of any applications (apps) before installing them.

Disable features not actively in use, such as Bluetooth, Wi-Fi, and infrared. Set Bluetooth-enabled devices to "non-discoverable" when Bluetooth is enabled.

Delete all information on a device before the device changes ownership. Use a "hard factory reset" to permanently erase all content and setting stored on the device.


"Sign Out" or "Log Off" when finished with an app, rather than just closing it.

Utilize antivirus software where applicable (i.e., Androids, Windows, etc.).

Do not jailbreak or otherwise circumvent security controls.

## Online Security

Never click on suspicious links in emails, tweets, posts, or online advertising. Links can take you to a different website than their labels indicate. Typing an address in your browser instead of clicking a link in an email is a safer alternative.

Ensure your information is protected as it travels across the Internet by only submitting sensitive information to websites that use encryption. Verify the web address begins with "https://" (the "s" is for "secure") rather than just "http://". Some browsers also display a closed padlock. 

Do not trust sites with certificate warnings or errors. These messages could indicate your connection is being intercepted or the web server is misrepresenting its identity.

Avoid using public computers or public wireless access points for online banking and other activities involving sensitive information, when possible.

Always "Sign Out" or "Log Off" of password protected websites when finished to prevent unauthorized access. Simply closing the browser window may not actually end your session.

Be cautious of unsolicited phone calls, emails, or texts directing you to a website or requesting information.



## General PC Security

Maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.

Update your software frequently to ensure you have the latest security patches. This includes your computer's operating system and other installed software (e.g., web browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.).

Automate software updates, when the software supports it, to ensure it's not overlooked.

If you suspect your computer is infected with malware, discontinue using it for banking, shopping, or other activities involving sensitive information. Use security software and/or professional help to find and remove malware.

Use firewalls on your local network to add another layer of protection for all the devices that connect through the firewall (e.g., PCs, smart phones, and tablets).

Require a password to gain access. Log off or lock your computer when not in use.

Use a cable lock to physically secure a laptop when the device is stored in an untrusted location.



## Passwords

Create a unique password for all the different systems/websites you use. Otherwise, one breach leaves all your accounts vulnerable.

Never share your password over the phone, in texts, by email, or in person. If you are asked for your password, it's probably a scam.

Use unpredictable passwords with a combination of lowercase letters, capital letters, numbers, and special characters.

The longer the password, the tougher it is to crack. Use a password with at least eight (8) characters. Every additional character exponentially strengthens a password.

Avoid using obvious passwords such as names (e.g., your name, family members' names, business name, user name, etc.), dates (e.g., birthdays, anniversaries, etc.), and dictionary words.

Choose a password you can remember without writing it down. If you do choose to write it down, store it in a secure location.

## Learn More

To learn more about information security, visit any of the following websites:

- [OnGuardOnline.gov](https://www.onguardonline.gov)
- [StaySafeOnline.org](https://www.staysafeonline.org)
- [BBB.org/Data-Security](https://www.bbb.org/Data-Security)
- [US-CERT.gov](https://www.us-cert.gov)