

General Online & Mobile Security Tips

Online Security Tips

- Use a current web browser such as [Microsoft Internet Explorer](#), [Mozilla Firefox](#), or [Apple Safari](#), depending on the device and/or system you are using or personal preference, and ensure that all available security upgrades are downloaded and installed.
- Avoid downloading programs or opening attachments from unknown sources.
- Do not use your Social Security Number as a username or password. Change your usernames and passwords regularly and use combinations of letters, numbers, and "special characters" such as "pound" (#) and "at" (@) signs as permitted by the system you are using.
- Protect your online passwords. Don't write them down or share them with anyone. Avoid using the same username and password across websites, and ensure to differentiate and safeguard those used established for financial and transaction purposes.
- Protect your answers to security questions. Select questions and provide answers that are easy for you to remember, but hard for anyone else to guess. Do not write down your security questions or answers or share them with anyone. If you have selected security questions on other websites, avoid using the same questions for financial and transaction purposes.
- Use secure websites for transactions and shopping. Shop with merchants you know and trust. Make sure internet purchases are secured with encryption to protect your account information. Look for "secure transaction" symbols like a lock symbol in the lower right-hand corner of your web browser window, or "https://..." in the address bar of the website. The "s" indicates "secured" and means the web page uses encryption.
- Always log off from any website after making a purchase. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.
- Close your browser when you're not using the Internet.

Mobile Banking Security Tips

- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password-protect your device so that nobody else can use it or view your information. Also be sure to store your device in a secure location.

- Frequently delete text messages from your financial institution, especially before loaning out, discarding, or selling your mobile device.
- Never disclose via text message any personal information (account numbers, passwords, or any combination of sensitive information like your Social Security Number or birth date that could be used in ID theft).
- Text Banking users, if you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile with your financial institution and contact customer service at your institution.
- Always read and follow instructions and guidance from your financial institution regarding securing your mobile banking experience.

Mobile banking applications are programs you can download to your mobile device. Applications or "apps" that let you monitor your finances and conduct certain transactions are increasing in popularity.

- To ensure the safety of your personal and account information, download mobile apps from reputable sources only. Consult your financial institution for specific guidance regarding app authenticity.
- For your security, sign off when you finish using a mobile banking app rather than just closing it.