WESTAMERICA BANK
Your Community Banker™

Helpful Security Tips

For Online / Internet Banking

• Protect your online passwords. Don't write them down or share them with anyone.

• Change your passwords regularly and use combinations of letters, numbers, and special characters such as (@, #, %, *).
Do not use your online banking username and passwords as credentials for other online accounts.

• Protect your answers to security questions. Select questions and provide answers that are easy for you to remember, but hard for others 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.

• Use secure websites for transactions and shopping. Shop with merchants you know and trust. Make sure internet purchases are secured 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" means that the website is using secure settings.

• Always log off from any website after using your credit card, debit card, or other sensitive information. If you cannot log off, close your browser to prevent any potential unauthorized access to your account information.

• Close your browser when you're not using the internet.

• Be cautious when using public hot-spots (such as coffee shops, fast food restaurants and libraries) and consider your Wi-Fi auto-connect settings. You should never automatically connect to a "Free" hot-spot.

For Email / Phishing

• Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.

• Be careful to click on links from known senders. Links can get hacked in transit. It is better to copy the link and paste it into the browser, or just re-type the link all together.

• If you receive a suspicious email that you think is a phishing (an attempt to get information from you), do not respond or provide any information. If the email is from a known company or person, call them on the phone and verify that the email was sent before opening it.

For Your Computer / Laptop

• Avoid downloading programs from unknown sources. Toolbars, "PC Fix" software and other programs are specially made to attract mal-ware.

• Install, run, and keep anti-virus and other software updated.

• Keep your computer operating system up to date to ensure the highest level of protection.

• Turn your computer / laptop off completely when you are finished using it – do not leave it in sleep mode.

• Be careful when conducting online banking sessions on computers that are shared by others. Public computers (computers at internet cafes, copy centers, libraries, etc.) should be used with caution, due to shared use and possible tampering. Online banking sessions and viewing or downloading documents (statements, etc.) should be conducted, when possible, on a computer you know to be safe and secure.

• Ensure your computer operating system (Windows / iOS), software; browser (Safari, Chrome, Firefox and others) version and plug-ins are current. Before downloading an update to your computer program, first go to the company's website to confirm the update is legitimate.

• Configure your devices to prevent unauthorized users from remotely accessing your devices or home network. For example, if you use a home wireless router for your home internet connection, follow complex password suggestions and consult the manufacturer's recommendations to configure the router with appropriate security settings.