Passwords

MAKE IT UNIQUE

Create a unique password for each website you use. If you do not, one breach leaves all your accounts vulnerable.

MAKE IT COMPLEX

The longer the password, the tougher it is to crack. Use a password with at least 14 characters. Avoid using obvious passwords, like names, dates, or standalone dictionary words.

DO NOT SHARE

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

USE A PASSWORD VAULT

Choose passwords you can remember without writing it down. If you cannot remember all your passwords, consider using a password vault.

Learn More

To learn more about securing your online banking activities, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- CISA.gov

CYBERSECURITY AWARENESS

Online Banking Security Tips

TXN BANK

Mobile Device Security

AUTHENTICATE
Require a passcode and/or biometrics to access your device.

INSTALL UPDATES
Install patches and updates as soon as possible once they become available.

SIGN OUT
“Sign Out” or “Log Off” when finished with an app, rather than just closing it.

LOCK THE SCREEN
When your device is not in use, lock the screen to prevent unauthorized access to it.

SECURE THE DEVICE
Enable security features (e.g., auto-wipe, auto-lock, biometrics, etc.). Install anti-malware, when possible. Do not jailbreak or otherwise circument security controls on your device.

DISPOSE CAREFULLY
Before disposing of your mobile device or when changing ownership, delete all information from the device. Use a “factory reset” to permanently erase all content and settings stored on the device.

Online Security

SUSPICIOUS LINKS
Never click suspicious links in emails, on social media posts, or via online advertising. Links can take you to a different website than the labels indicate.

WHEN IN DOUBT, DO NOT CLICK.

ENCRYPT DATA
Protect your data by only submitting sensitive information to websites that encrypt your data Make sure the URL begins with https:// instead of just http://. (The “s” means your data will be encrypted when you submit it.) Some browsers also display a closed padlock.

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

BE CAUTIOUS
Always be cautious if you receive an unsolicited phone call, text, or email directing you to a website or requesting sensitive information.

Computer Security

WATCH FOR MALWARE
Maintain active and up-to-date anti-malware protection provided by a reputable vendor. Schedule regular scans of your computer, alongside real-time scanning, when possible.

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

UPDATE SOFTWARE
Update your computer software frequently to ensure you have the latest security patches. This includes your computer’s operating system, as well as other installed software (e.g., web browsers, Adobe programs, Microsoft Office, etc.). Automate software updates, when possible, to ensure it is not overlooked.

PHYSICAL SECURITY
Keep your computer in a secure location. Do not leave laptops unattended in untrusted locations (e.g., car, restaurant, airport, etc.).