Mobile Device Security Tips

AmeriFirst Bank | Rev. 2026-10

Your phone or tablet may hold banking access, payment cards, email, photos, and verification codes. Protect the device and the accounts connected to it.

1. Use a strong screen lock

Use a strong device passcode or password; choose a longer code where supported and avoid birthdays, repeated digits, and simple sequences. Enable fingerprint or face recognition where available, backed by your passcode. Set a short automatic-lock period and conceal sensitive lock-screen notification previews. Do not share your passcode or let others watch you enter it.

2. Keep the device and apps supported and updated

Enable automatic operating system and app updates, and check for updates that require action. Replace devices that no longer receive security fixes. Keep built-in protections enabled; on Android, keep Google Play Protect on. Separate antivirus apps are not a universal requirement for every phone. Follow your manufacturer's guidance and use only trusted security products appropriate for the device.

Do not root or jailbreak the device or disable safeguards to install an app. For a work device, follow your employer's security and device-management requirements.

3. Choose apps carefully and limit permissions

Get apps from the official app store or another source you have independently verified. Check the developer and requested permissions; ratings alone do not prove an app is safe. Do not install apps or configuration profiles because an unexpected caller, text, or pop-up tells you to. Remove unused apps and limit access to contacts, photos, microphone, camera, and location to what each app needs.

Keep location and other settings required for device-finding and theft-protection features enabled. Review location access app by app rather than disabling every location feature.

4. Protect your accounts and phone number

Use long, unique account passwords and a reputable password manager. Enable multi-factor authentication (MFA), especially for email, your Apple or Google account, banking, and your mobile carrier. Use passkeys or security keys where supported; an authenticator app is another option. Never share sign-in verification codes with someone who contacts you or approve a login you did not initiate.

Protect your carrier account with a unique PIN or password and ask about number-lock or port-out protection. If calls and texts suddenly stop working, or you receive an unexpected SIM or number-transfer alert, contact the carrier immediately using another trusted device. An unexplained loss of service can have other causes, but it may indicate a SIM-swap attack.

5. Prepare before a device goes missing

Turn on the manufacturer's built-in device-finding and remote-lock features: Apple Find My or Google Find Hub, as supported. Enable additional theft protections, such as Apple Stolen Device Protection or Android theft-protection features, where available. Availability and setup vary by device and software version.

Keep encrypted or otherwise appropriately protected backups and check that you can recover them. Secure backup accounts and recovery methods. Know how to access the manufacturer's lost-device service from another trusted device.

Stay Safe on the Go

6. Use connections and charging safely

Avoid public or shared computers for banking. Disable automatic connection to unfamiliar Wi-Fi networks and confirm hotspot names with staff. Use your own cellular connection or hotspot if you are unsure about a network. On any connection, use the official app or verify the full website address and HTTPS. **Encryption protects the connection; it does not prove the website is genuine.** Never bypass certificate warnings.

Turn off unnecessary sharing or discoverability and decline unexpected pairing requests. You do not need to disable every mobile-wallet or wireless feature to use your phone safely; keep software current and use the manufacturer's security settings. Use your own wall charger and cable or power bank when possible, and decline unexpected prompts to trust a computer or share data.

7. Watch for mobile scams

Be cautious of unexpected delivery texts, toll notices, refunds, account warnings, QR codes, and calls claiming to be your bank or technical support. Open the organization's official app or type its known address instead of following a message's link. Caller ID, familiar voices, and realistic messages can be faked.

Do not move money to a supposed "safe account," share verification codes, install remote-access software, or share your screen during banking because an unexpected caller tells you to. End the contact and call the bank using a trusted number. Do not send confidential information through ordinary email.

8. If your phone is lost or stolen

Lock it promptly. Use the manufacturer's official lost-device service from a trusted device to mark it lost or lock it. Do not try to retrieve a stolen device yourself; contact law enforcement as appropriate. Do not trust a message claiming the phone has been found that asks you to sign in through a supplied link.

Contact your carrier. Ask about suspending service and protecting your number. Contact the bank or card issuer if mobile banking, payment cards, or wallet access may be exposed. Report a missing work device to your employer immediately.

Secure accounts and consider remote erase. Follow the manufacturer's instructions to secure your Apple or Google account and other affected accounts. Remote erase can help protect data, but may permanently remove information not backed up; it may wait until the device connects. Do not remove the device from your account or device-finding service unless the manufacturer's recovery or claim instructions direct you to do so.

Banking concerns and trusted resources

Contact **AmeriFirst Bank at 1-800-298-1763** immediately if you suspect unauthorized transactions or exposed banking access. Ask whether access can be secured or a payment stopped or recovered; recovery is not guaranteed.

Type these addresses into your browser; use a trusted device if yours may be compromised:

amerifirstbank.com - Bank website | **my.amerifirstbank.com** - Online banking
icloud.com/find - Apple lost-device tools
android.com/find - Google lost-device tools
ReportFraud.ftc.gov - Scam reporting | **IdentityTheft.gov** - Identity theft recovery