



iPhone Safety Guide

Your iPhone holds keys to your personal life and financial accounts. Follow these steps to secure your device, protect your identity, and keep unauthorized users out of your banking apps.

Everyday Basics at Home or Traveling

- Use a strong screen lock. Do not use 1234, 0000, or your birthday.
 - Turn on **Face ID** or **Touch ID** so only you can unlock your phone.
 - Set Auto-Lock to 30 seconds or 1 minute in **Settings > Display & Brightness > Auto-Lock**.
 - Keep your iPhone updated in **Settings > General > Software Update** because updates fix security problems.
 - Turn on Find My iPhone in **Settings > [Your Name] > Find My > Find My iPhone**.
-
- Back up your phone with **iCloud Backup** so you can get your photos and apps back if it is lost.
 - Only download apps from the **App Store**.
 - Do not tap strange links in texts, emails, or pop-ups.
 - Be careful on public Wi-Fi. Avoid private tasks like banking on Wi-Fi you do not trust.
 - **Turn off Wi-Fi** and **Bluetooth** when you are not using them in busy places like airports and hotels.
 - Keep your phone in a front pocket, zipped pocket, or inside a bag while traveling.
 - If your phone is lost or stolen, tell a trusted adult or supervisor right away and use **Find My** to lock it or erase it.



(continued)

Extra Steps to Stop Account Changes

If a thief gets your phone and knows your passcode, they can try to lock you out of your digital life. Turn on these advanced settings to create a secondary line of defense for your most sensitive accounts.

1. Turn on Two-Factor Authentication

1. Open **Settings**.
2. Tap your **Name**.
3. Tap **Sign-In & Security** or **Password & Security**.
4. Turn on **Two-Factor Authentication**.

This means a thief needs your password and a second code sent to your trusted device.

2. Turn on Stolen Device Protection

1. Open **Settings**.
2. Tap **Face ID & Passcode**.
3. Enter your passcode.
4. Turn on **Stolen Device Protection**.
5. Set **Require Security Delay** to **Always** if you see it.

This makes Apple ID changes harder if someone knows your phone passcode.

3. Use Screen Time to Block Changes

1. Open **Settings**.
2. Tap **Screen Time**.
3. Tap **Use Screen Time Passcode** and make a code different from your phone passcode.
4. Tap **Content & Privacy Restrictions** and turn it on.
5. Tap **Account Changes > Don't Allow**.
6. Tap **Passcode Changes > Don't Allow**.

This adds one more lock so others cannot change your Apple ID or phone passcode easily.

4. Safe Habits

- Cover the screen when typing your passcode in public.
- Use **Face ID** or **Touch ID** when you can and never share your passcode or Apple ID password.
- Check your trusted devices in **Settings** and remove devices you do not know.

Your security is a top priority at First Oklahoma Bank. Contact our team if you suspect your financial information has been compromised. **918-392-2500**