FREE GUIDE

Scam-proof your phone in 10 minutes

Ten settings that stop most scams before they reach you, and the one rule that stops the rest.

The one rule

If a call, text or email asks you to **act fast**, **pay in an unusual way** or **share a code**, stop. Hang up and call back using a number you already trust: the one on your card, your statement, or the company's own website.

Ten minutes of settings

Phones label these differently, so type the **bold words** into your phone's Settings search.

1. **Updates.** Turn on automatic updates for the phone and for apps. Updates close the holes scammers use.
2. **Screen lock.** Use a six-digit passcode plus face or fingerprint unlock, and set the screen to lock after one minute.
3. **Unknown callers** or **spam calls.** Turn on spam call filtering or silence unknown callers. Real callers leave a voicemail.
4. **Unknown senders.** Filter texts from people not in your contacts into their own list, and don't tap links in them.
5. **Two-step sign-in.** Turn it on for your email first, then your bank and your phone company account. Where a site offers a passkey, use it.
6. **Account PIN** with your phone company. Log in or call them and add an account PIN or "number lock", so nobody can move your number to their phone.
7. **Find my device.** Leave it on, so a lost phone can be located, locked or erased.
8. **App permissions.** Take away location, contacts, camera and microphone access from apps that don't need them.
9. **Backup.** Turn on automatic backup for photos and contacts, so a lost or wiped phone isn't a disaster.
10. **Emergency.** Add an emergency contact and medical information that shows on the lock screen.

Red flags

- A text saying your account is locked, a package is held or you owe a toll, with a link to tap.
- Anyone asking for gift cards, a wire transfer, cryptocurrency or a payment-app transfer.
- A caller asking you to read back a code that was just texted to you. Real companies never ask for it.
- A pop-up with a phone number saying your device is infected.
- Pressure to act right now, or to keep it from your family or your bank.
- A QR code stuck on a parking meter or flyer that asks you to pay.

If you already clicked or paid

1. Call your bank or card company using the number on the back of your card, and tell them what happened.
2. Change your email password first, then any account that uses the same password.
3. Turn on two-step sign-in anywhere it was off.
4. Report it at reportfraud.ftc.gov.
5. If your phone suddenly loses service, call your phone company right away: your number may have been moved.

Want it done for you?

I'll set it up at your place in New Orleans and walk you through it. Call or text (504) 350-8238, or ask at chonola.com/help.