10 simple ways to stay a step ahead of scams.

A few useful changes. A moment to double-check. Pick one step today, or work through this guide with someone you trust.

1–4 Set up your devices and accounts

5–9 Check before you act

10 Sign up for Bernie

“You don’t have to work it all out at once. Start with one thing.”

A guide from Bernie · Updated October 30, 2026

1 Keep your devices up to date

1. Open your device's Settings and install available updates.
2. Turn on automatic system updates where offered.
3. Turn on automatic app updates, too.

Android menus vary by phone maker. Most Android system updates install automatically; restart when prompted.

Full device settings on page 11.

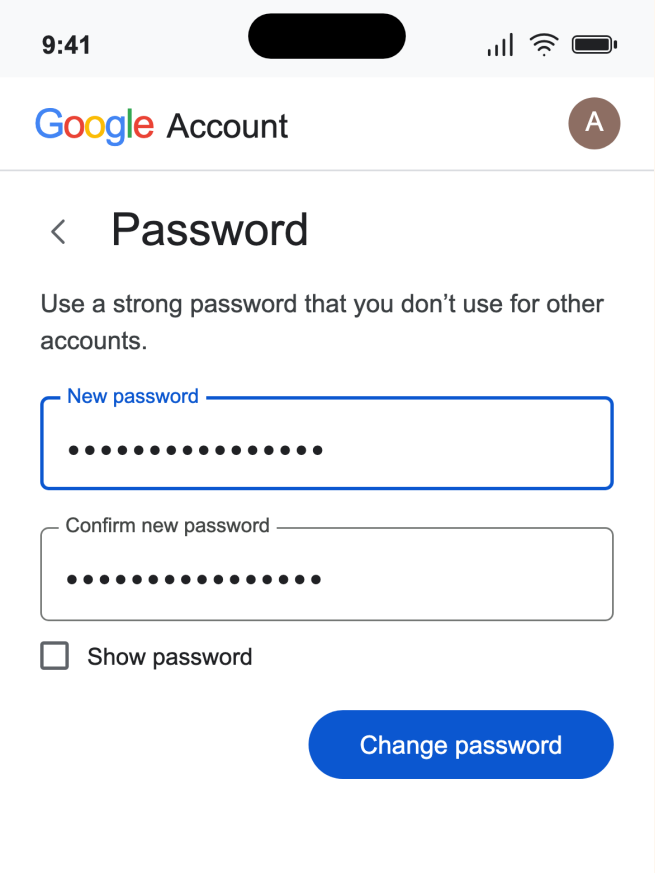


iPhone · Automatic Updates screen mockup. Labels vary by iOS version.

2 Replace weak or reused passwords

1. Start with your email. Open the official app or website yourself.
2. Find Account or Security, then Change password.
3. Create a long, unique password and save it in your password manager.

Change weak, reused or exposed passwords. You don't need to change a strong password just because it is old.



Google Account · Password screen mockup, with fictional details.

3 Use a password manager

1. Choose LastPass or 1Password. Follow its setup guide, then save or import your current logins.
2. Use its built-in security check to find weak, reused or exposed passwords, where supported.
3. Change flagged passwords on each account's actual website or app. Use a unique generated password, then save the new password in your manager.

Editing a saved password alone does not change the account password. Features vary by plan and device. Keep your manager's recovery instructions secure.

LastPass

Setup guide

Security Dashboard guide

1Password

Setup guide

Watchtower guide

Official guides. Choose the manager that works for you.

4 Turn on two-factor authentication

1. When prompted, turn on two-factor authentication (2FA), also called multi-factor authentication (MFA). It is like double-locking your doors. Follow the setup instructions.
2. No prompt? Open the account or app's settings. Look under Security or Privacy and Security. Labels vary by service.

Save recovery codes securely. If text codes are the only option, use them. Approve sign-in prompts only when you are signing in.

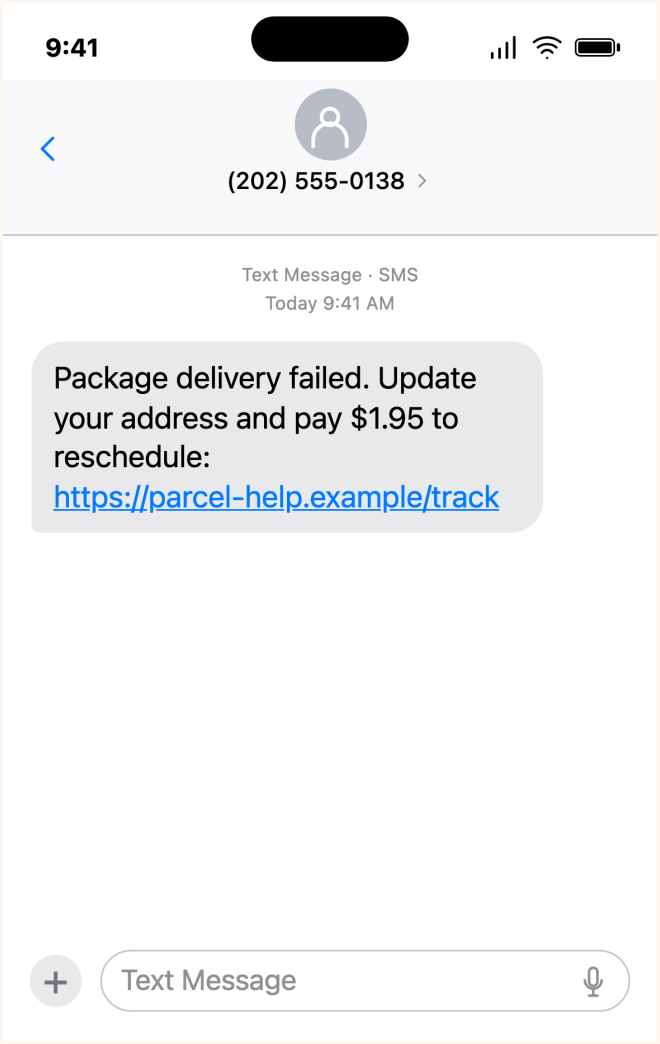


iPhone · Sign-In & Security screen mockup. Tap Two-Factor Authentication.

5 Don't just click on any link.

1. Pause before opening an unexpected link or attachment.
2. Open the company's official app, or type a web address you already know.
3. Check for the message there. Still unsure? Call a trusted number.

Use a saved bookmark or an address from a statement. Don't use contact details in the suspicious message.

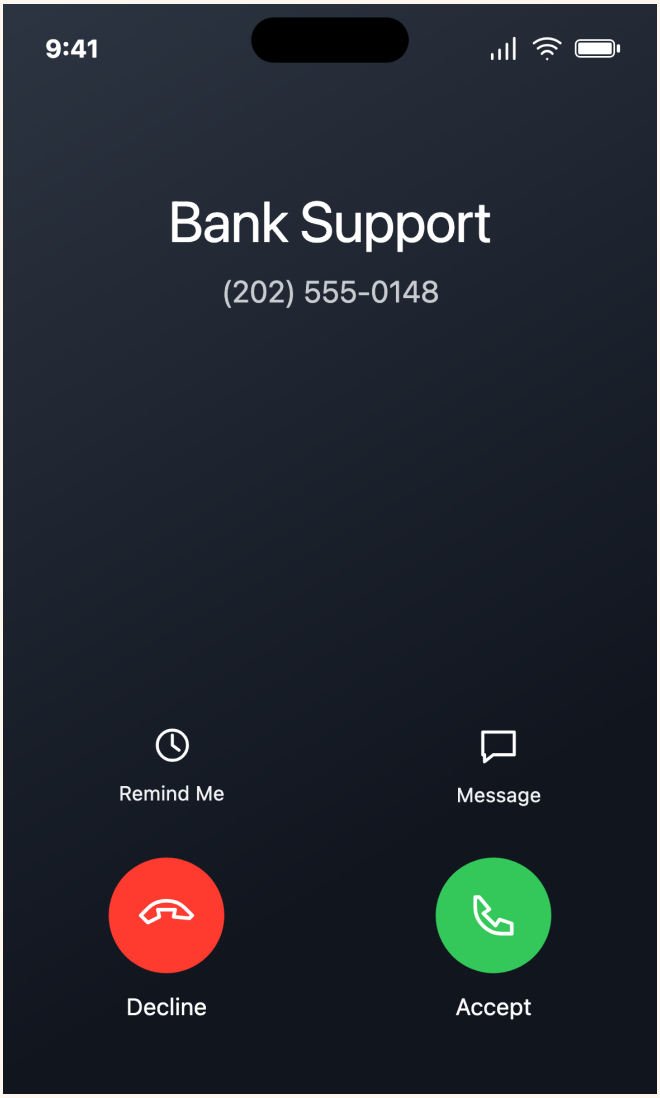


iPhone Messages · Sample scam text. The example link is not real.

6 Hang up and call a number you trust

1. Say, 'I'll call you back,' and end the call.
2. Find the number in saved contacts, on your bank card or on a statement.
3. Call that number yourself and check the request before acting.

Use a number you already trust, even if the caller gives you a number to call back.



iPhone · Sample incoming call. Caller ID can be faked.

7 Choose a private family safe word

1. Privately agree on a word or phrase for your family to use as a password.
2. Don’t share it or post it on social media.
3. Ask for it whenever a request or someone’s identity is in question.

Call back on a number you already trust as an additional check. A safe word alone does not prove who is calling.

8 Keep sign-in codes to yourself

1. Never read or send a login code to an unexpected caller or message.
2. Enter it only in the official app or website where you started signing in.
3. Didn't request a code? Don't share it or approve a sign-in prompt.

If you're worried, open the official app yourself and check your account's security settings.

9 Don’t give unexpected callers remote access

1. If an unexpected caller asks, don’t install remote-control software or share your screen.
2. Don’t give them access to your phone or computer. End the call.
3. If you need help, contact a support provider you already know and trust.

Already gave access? Disconnect from the internet and get help from trusted support. Contact your bank if you shared financial details.

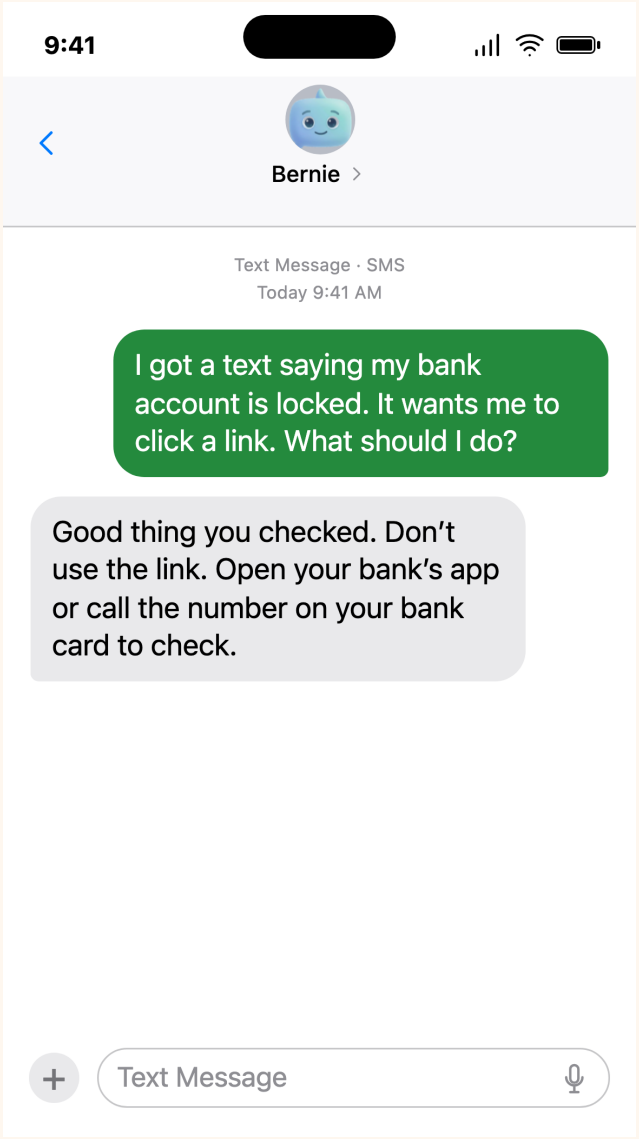
10 Sign up for Bernie for extra protection.

Text Bernie anytime something suspicious or unfamiliar comes in.

Sign up for Bernie

textbernie.me/signup

Bernie flags suspicious requests and advises. No service prevents every scam.



Sample conversation in an iPhone Messages mockup. Not a real customer message.

More help finding the settings

1. Keep your devices up to date

iPhone system: Settings > General > Software Update > Automatic Updates. Turn on Automatically Install.

Android system: Settings > System > Software updates. Follow the prompts. If this path differs, search Settings for 'update'.

iPhone apps: Settings > Apps > App Store > App Updates: On.

Android apps: Play Store > profile picture > Settings > Network preferences > Auto-update apps. Choose Update over Wi-Fi only, or a data option you prefer.

Bernie is a product of AI for the People LLC. These steps reduce risk; no checklist or service prevents every scam.