Family Anti-Fraud Playbook

Oct 4, 2026 · @Howard Bouk

Why this exists

A single convincing phone call can be enough for a scammer to take over someone's phone number, email, and shopping accounts in one evening. It happens to people of every age, including careful and tech-savvy people. These scams are run by professionals and built to feel real.

How a phone number gets hijacked (SIM swap)

- The scammer calls pretending to be from your phone company, bank, or another business you trust. Caller ID can be faked to show the real company name, and they often already know your name, address, or account details from past data leaks.
- They create urgency: fraud on your account, a charge you didn't make, or service about to be cut off.
- They ask you to "verify" by reading back a code that was just texted to you. That code is really signing them into your account.
- They may ask for photos of your ID or a selfie, which helps them pass the phone company's identity checks.
- Once inside your account, they move your number to a SIM or eSIM in their own phone. Your phone loses service, and your calls and texts go to them.

How an email account gets taken over

- Many accounts send sign-in or password-reset codes by text. With your texts going to the scammer, they click "forgot password" on your email and receive the code themselves.
- Sometimes they simply ask for the email code during the same phone call.
- Once in, they change the password and recovery details to lock you out, and may set up hidden forwarding so they keep seeing your mail.

Why linked services fall next

- Your email is the master key. Most websites and apps reset passwords by email, so whoever controls it can get into almost anything.
- Accounts you open with "Sign in with Google," Apple, or Facebook open straight away.

- Shopping, travel, and food delivery apps are targeted first because they let the scammer spend money immediately.

The risk of saved credit cards

Any site or app that stores your card is only as safe as your login to it. Once a scammer is in, nothing stops a purchase: they can book travel, order electronics, or ship goods to a new address. Every place that keeps your card is another door. Payment wallets that ask for your face or fingerprint, and instant purchase alerts, close most of that gap.

Falling for one of these calls is not a sign of carelessness. The rest of this playbook closes each weak point: the call, the code, the phone number, the email account, and the saved card.

The 5 rules

These five rules block every step of the attack described above. Learn them before anything else.

1. **Don't answer numbers you don't know. If they called you, hang up and call back.** Caller ID can be faked, so the name or number on your screen proves nothing. Turn on Silence Unknown Callers (see setup below) so unknown numbers go to voicemail. A real business will leave a message. Call back using the number on your card, your bill, or the company's app, never a number the caller gives you.
2. **Never give a code to someone who called you.** A code texted to you is a key to your account. Banks and other companies sometimes do ask you to read a code to their staff, and that is only safe when *you* started the contact: you are in the branch in person, or you called them on a number you trust. If they called you and ask for a code, hang up.
3. **Never send photos of your ID to someone who contacted you.** Only show ID in person, or upload it in an official app you opened yourself.
4. **Pressure is the warning sign.** "Act now," "your account will be locked," and "don't hang up" are scammer lines. Slow down, hang up, and call someone in the family.
5. **No phone service suddenly? Treat it as an emergency.** If your phone shows "No Service" or "SOS only" and it isn't a known outage, call your carrier from another phone right away. Then follow "If it happens" below.

One extra for family calls: if a family member calls asking for money or help in a hurry, ask for the family code word. AI can now copy a voice from a short clip.

Setup (30 to 45 minutes)

Do this once per person, ideally together with someone who has done it before. Everything here is free and uses tools already on your phone, except the optional password manager, which may cost a small fee.

Optional: Set up a password manager (15 minutes)

A password manager remembers every password, 2FA code, and passkey for you. It keeps them in sync on all your devices, so they come back on a new phone. Choose one:

- **1Password** (paid): works on iPhone, Android, Mac, and Windows, and syncs passkeys across all of them.
- **Bitwarden** (free plan): stores passwords and passkeys on all your devices. Keeping 2FA codes in it, and letting a trusted family member recover your account, both need the low-cost Premium plan.
- **Built into your phone** (free): Apple Passwords (iPhone, iPad, Mac, and Windows through iCloud) and Google Password Manager (Android and Chrome) both sync passkeys. These work best when all your devices are Apple, or all are Android.
- **Others:** Proton Pass, Dashlane, Keeper, and NordPass also sync passkeys, with free or paid plans.

- [ ] Install the app from the App Store, Google Play, or the company's official website. Create your account, and write the master password and any recovery code in your recovery kit.
- [ ] Use it for all your passwords, 2FA codes, and passkeys. When a website offers to save a password or create a passkey, let the password manager do it.
- [ ] In your phone's settings, set it as the password AutoFill app so it fills in sign-ins for you.

Phone carrier (10 minutes)

- [ ] Call your carrier at the number on your bill or in their app.
- [ ] Set an account PIN or passcode. Ask that it be required for any SIM change, new eSIM, or number transfer.
- [ ] Ask what other number-transfer or SIM-swap protection they offer, and turn it on.
- [ ] Give the carrier account a new password that you use nowhere else. Let your phone create and save it.
- [ ] Send unknown callers to voicemail. iPhone: Settings > Apps > Phone > Silence Unknown Callers (older iPhones: Settings > Phone). Android: in the Phone app's settings, look for blocking or screening unknown callers.

Email account (10 minutes)

Your email can reset almost every other account, so it gets the most protection.

- [ ] Run the security checkup: Google Security Checkup for Gmail, or Settings > your name > Sign-In & Security on iPhone.
- [ ] Add a passkey so you sign in with your face or fingerprint instead of a texted code.
- [ ] Where you can, turn off text-message codes as a sign-in method once the passkey works.
- [ ] Check that the recovery email and phone number are yours or belong to another person you trust.
- [ ] Check for mail forwarding and filters you didn't create, and delete them.
- [ ] Remove **all** connected apps and services from your email account, and any signed-in devices you don't recognise. If you used "Sign in with Google" or Facebook for an app, first give that app its own email and password or passkey, then remove the connection.
- [ ] From now on, never choose "Sign in with Google" or "Sign in with Facebook." If that one account is broken into, every app connected to it opens too.
- [ ] Print or write down backup codes and put them in your recovery kit (next section).

Payments (5 minutes)

- [ ] Add your cards to Apple Pay or Google Pay and use those at checkout. Each purchase needs your face or fingerprint.
- [ ] Delete saved cards from shopping sites and apps you rarely use.
- [ ] Turn on instant purchase alerts in your bank and credit card apps.

Family (5 minutes)

- [ ] Agree on a family code word. Never text or post it.
- [ ] Make sure at least one family member can help you recover your email if you lose access.

Passkeys and losing your phone

Losing or replacing your phone does not lose your passkeys, as long as you can sign in to your Apple or Google account on the new phone. You don't need a paid app for this.

- **iPhone:** passkeys save to iCloud Keychain and come back when you sign in to your Apple Account on a new device.

- **Android or Chrome:** passkeys save to Google Password Manager and come back when you sign in to your Google account.
- **Paid managers like 1Password** are optional. They help mainly if you mix Apple and Windows or Android devices and want everything in one place.

The real risk moves to one place: your Apple or Google account itself. Protect it with a recovery kit.

Recovery kit (paper, kept at home)

- [ ] Your Apple Account or Google account email and password, written down.
- [ ] Google backup codes, or your Apple recovery key if you set one up.
- [ ] Your carrier account PIN.
- [ ] A trusted family member set as your recovery contact (Apple: Recovery Contact; Google: a recovery email you trust).

Keep the kit in a drawer or envelope at home, not in your phone or email. A thief who gets into your phone can't reach it.

If it happens

Speed matters most in the first hour. Work through these steps in order, from another phone or computer if yours has lost service. If you can, have a family member or friend with you to help work through the steps and keep track of what is happening. Ask them to bring their own phone and laptop so you can make calls and fix accounts at the same time.

1. **Call your carrier** at the number on their website or bill. Say your number was transferred without permission and ask them to lock the account.
2. **Call your bank and credit card companies** at the number on the back of the card. Freeze or replace the cards and dispute any charges you didn't make.
3. **Take back your email.** Use account recovery, change the password, sign out all other devices, and remove forwarding rules, filters, and recovery details you didn't add.
4. **Change passwords on shopping and delivery apps** that had a saved card or were linked to your email. Remove the saved cards.
5. **Call a family member** so someone else is helping and keeping track.
6. **If ID was shared:** place fraud alerts with Equifax Canada and TransUnion Canada, and replace the document (ServiceOntario for an Ontario driver's licence).
7. **Report it** to the Canadian Anti-Fraud Centre and your local police. Keep the report numbers; banks and merchants often ask for them.

8. **Watch for 90 days** for strange emails, new-account notices, credit-check letters, or your phone losing service again.

Setup tracker

Use this table to track each person's progress through the setup. Write each person's name in a row and tick a box when that step is done.

Name	Password manager (optional)	Carrier PIN	Email passkey	Recovery kit	Wallet payments	Code word
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐