Scams & Threats

Household Digital Security Agreement

A signed plan for how your household handles suspicious calls.

About 10 minutes together Steps checked October 11, 2026

By Jason Phillips, Founder

General information, not professional advice. You decide which steps fit your situation.

The short answer

Sit down together for ten minutes, choose a private safe word and a Co-Pilot to call before money moves, and agree on five habits: let strangers wait, ask for the safe word, call the real number yourself, call your Co-Pilot first, and never send hard-to-reverse payments or codes. Then sign it.

What you will need

- This page or the printed PDF
- A pen
- Your phone and bank cards
- Everyone in the household, plus your Co-Pilot

Why this matters

Scammers do not just attack computers. They attack people. They use fear, urgency, and secrecy to bypass our good judgment. Sometimes they even use familiar voices to keep us from checking in

with someone we trust. With new technology, these scams are getting harder to spot. A call might sound exactly like your child, your spouse, your bank, or a government agency. But a familiar voice, an official-looking message, or an urgent deadline doesn't mean a request is real.

The good news is that most scams start the same way. They usually involve an unexpected request to act quickly, keep a secret, send money, share a code, or hand over access. This agreement gives everyone in the household a simple, calm response: pause, verify independently, and call each other before taking action. Your family can move from uncertainty to confidence, together.

This is not about being paranoid, and it is not about anyone being naive. Today's scams are designed to fool smart, careful people by creating fear, urgency, and confusion. Taking 10 minutes to agree on a few shared habits means your family has each other's backs before the pressure starts.

How to use this agreement

1. Read the five protocols together.
2. Choose a safe word and name your Co-Pilot team.
3. Complete one Reference Card for each household member. It is the last page of the printable PDF.
4. Sign the agreement.

Do this first: set up your safety team

Before you start, choose two things: a safe word your family can use to prove an emergency is real, and a Co-Pilot team to call before money moves.

Action 1: Create the family safe word

A safe word works because a scammer can copy a voice, but not a private word your family chose ahead of time.

1. Choose an ordinary phrase that is meaningful only to your household.
2. Avoid anything searchable, such as birthdays, pet names, addresses, or social-media inside jokes.
3. Pick something everyone can say and remember under stress.
4. Write it on paper only.

> **Good examples**
> Try "Italian Seasoning" or "Stuck at Three." Easy to remember, unlikely to appear online.

Our family safe word

Keep this on paper, not in a phone, note app, email, password manager, or cloud folder.

Action 2: Name your family Co-Pilot

Your Co-Pilot is the person you call before acting on a payment, account, or urgent request that feels unexpected, rushed, or secret. This is a no-shame check. Calling your Co-Pilot is a security step, not a test.

1. Choose a person everyone can call without hesitation.
2. Choose a Backup Co-Pilot in case the first person is unavailable.
3. Choose one person your Co-Pilot can call for a second opinion.
4. Agree that no request is too small to check first.

Role	Name	Phone
Family Co-Pilot		
Backup Co-Pilot		
Who our Co-Pilot calls		

Protocol 1: Let strangers wait

Almost every scam starts with someone you did not expect: a call from an unknown number, a knock at the door, a friend request from a stranger. You do not owe any of them an answer on the spot. A real caller will leave a message, and a real business will leave something in writing.

1. **Send unknown callers to voicemail.** Save family, doctors, and your Co-Pilot in your contacts first. Then turn on your phone's setting to silence unknown callers, and make sure your voicemail is set up and not full.
   - **iPhone:** Open Settings, tap Apps, then Phone. Under Screen Unknown Callers, choose Silence. Calls from numbers you have not saved go straight to voicemail.
   - **Samsung Galaxy:** Open the Phone app and tap the three dots. Tap Settings, then Block numbers. Turn on Block calls from unknown numbers.
   - **Other Android phones (Google's Phone app):** Open the Phone app and tap More. Tap Settings, then Blocked numbers. Turn on Unknown. This blocks calls that hide their number.
   - Menus change with updates. If yours looks different, search your phone's settings for "unknown."

2. **Use your phone line, then hang up.** "I do not do business over the phone. Goodbye." You do not need to explain, and you do not need to feel rude.

3. **Use your door line.** "I do not do business at my door. Please leave me something to review." No one comes inside without an appointment we made ourselves.

4. **Keep your profiles private.** Set social media to friends only, turn down friend requests from people you have not met, and skip posting birthdays, hometowns, or family details. Scammers use them to sound like they know you.

Protocol 2: Defeat AI voice and video fakes with your safe word

A convincing AI (artificial intelligence) fake can sound exactly like someone you love, and it can now show their face on a video call too. That is why your eyes and ears alone are not a reliable check. A safe word gives your family one thing a scammer cannot fake.

1. Ask for the safe word first.
2. If the caller cannot give it, end the call, even if it looks or sounds exactly like them.
3. Reach your family member another way, using a number you already know.

Practice the word together every six months so everyone can recall it under pressure.

Protocol 3: Always call the real number yourself

Caller ID, sender names, and links are easy to fake. This protocol creates a simple security airlock between an unexpected message and any action involving your money or accounts. A real institution will never mind you hanging up to call back.

1. **Disconnect.** End the unverified call. Do not reply, click, or call any number in the message.
2. **Find the official number.** Check the back of your card or a statement you already have, never the number the caller or text gave you. Never use a customer service number from an online search. Scam ads can show a real company's name with a criminal's number.

3. **Call the real number yourself.** Dial that number to reach a real representative and ask about the request.

For texts and emails, the same rule applies: do not tap the link you were sent. Open the app you already use, or type the address yourself.

> **Caller ID is not proof**
> A text can show a sender name like "IRS.gov" and still be fake. Neither caller ID nor a sender name proves who is really contacting you.

Protocol 4: Call me first

Scammers want you to pay in ways that cannot be reversed. They ask for gift cards, wire transfers, cryptocurrency, gold, payment-app transfers, or remote access. Once this money is sent, it almost never comes back. They also try to keep you alone. They tell you to keep the call a secret so no one can stop you. This protocol gives your family one habit that catches all of them at once.

1. **Pause the transaction.** Stop what you are doing. Scammers rely on artificial urgency to force a mistake.
2. **Leave the channel.** Hang up the phone, close the text thread, or close the email.
3. **Call your Co-Pilot.** There is no threshold too small and no reason too minor. A real request can wait for one phone call.

This is a no-shame, no-judgment check. The goal is not to prove anything, only to slow a decision before money or access changes hands. The same pause applies before a new investment account, a cryptocurrency purchase, or calling a number from a pop-up or security warning.

The one that outranks all of them

"Don't tell your kids, they will just worry." "You are under a gag order." Any request to keep a money conversation secret from your Co-Pilot is itself the warning. It does not matter how reasonable the rest of the call sounded.

Protocol 5: Three things we never do

Most scams end with the same few asks: send money in a hard-to-reverse form, give someone access to your device, or hand over a code that unlocks an account. Your family does not have to identify the scam. It only has to recognize the ask.

1. We never send gift cards, cryptocurrency, gold, or cash by courier to someone who contacted us, and we never send money to someone we have only met online. Before any wire or payment-app transfer (Zelle, Venmo, Cash App), we verify the recipient using a number we already trust.
2. We never give remote access to a device. No screen sharing, no support software, no control, unless we placed the first call.
3. We never share a one-time code, password, recovery code, or PIN. Not with anyone who contacted us.

The pop-up number tell

Treat any unexpected pop-up on your computer screen urging you to call a number as a scam until you verify it independently. Do not call the number. Close the window or restart the device.

The prize tell

Any prize, lottery, or sweepstakes win that asks you to pay a fee first is a scam, every time.

Confirm your household is ready

Go through this together, out loud. Tick a box only when every person in the room can say it is true.

- [ ] The family has chosen a safe word, and it is written on paper, not stored on any device.
- [ ] The family has named a Co-Pilot, a Backup Co-Pilot, and someone the Co-Pilot can call.
- [ ] Every phone in the house sends unknown callers to voicemail, everyone knows the phone and door lines by heart, and our social media profiles are set to friends only.
- [ ] Everyone knows to ask for the safe word and is comfortable hanging up if it cannot be given.
- [ ] Everyone knows to disconnect, find the official number independently, and call that number instead. This applies to texts as well as calls.
- [ ] Everyone agrees to call the Co-Pilot before any unexpected payment request, any new payee, or anything that feels rushed or secretive.
- [ ] Everyone agrees to never send gift cards, cryptocurrency, gold, or cash by courier to someone who contacted us unexpectedly, and to verify any wire or payment-app transfer independently before sending.
- [ ] Everyone agrees to never give remote access, screen sharing, or device control to anyone who contacts us.
- [ ] Everyone agrees to never share a verification code, password, recovery code, or PIN with anyone who contacted us unexpectedly.

Formalize the family commitment

By signing below, we agree to follow these five protocols every time, and to support one another without pressure, blame, or judgment. If someone in this house makes a mistake, we help first and we never shame. Reporting fast matters more than feeling embarrassed, no matter the amount.

Name	Signature	Date
Family member		
Family member		
Family member		
Family member		
Co-Pilot		

Optional: add a trusted contact to your financial accounts

A trusted contact is a person you name on a bank or brokerage account. If the company cannot reach you, or sees signs that someone may be pressuring or defrauding you, they are allowed to phone this person. That is all it does. Naming one gives away no control at all. A trusted contact cannot see your balances or activity, cannot move money or place trades, and cannot make decisions about your account. It is not a power of attorney.

1. Log in to your bank or brokerage account, on the website or app.
2. Open your Profile or Security settings.
3. Find "Trusted Contact." It is usually near your profile or your beneficiaries.
4. Enter your Co-Pilot's name, phone number, and email.
5. Save, then tell your Co-Pilot they are listed, so a call from the company is never a surprise.

Many banks and brokerages offer this. If you cannot find it, call the number on your statement and ask. Repeat for each account you want covered.

If it already happened

Act fast, no blame

If money or access went to a scammer, act immediately. Contact your bank, card issuer, payment app, or gift-card issuer right away and ask whether the transaction can be canceled, reversed, frozen, or recalled. Then change affected passwords from a known-safe device. If you gave someone remote access, disconnect the device from the internet first, then change passwords from a different device. Report the scam at reportfraud.ftc.gov and tell your Co-Pilot the same day. Fast reporting gives you the best chance of recovery.

Where to get help

- **Report fraud.** Federal Trade Commission at reportfraud.ftc.gov or 877-382-4357.
- **Report online crime.** Federal Bureau of Investigation Internet Crime Complaint Center at ic3.gov.
- **Talk it through.** AARP (American Association of Retired Persons) Fraud Watch Network Helpline, 877-908-3360.
- **Watch together.** AARP has good advice on spotting fraud. If you want to see it, its short "Pause. Reflect. Protect." video walks through the red flags: aarp.org/money/scams-fraud/pause-reflect-protect.

About this guide

General information to help you make safer choices online, not legal, financial, tax or professional security advice. You decide which steps fit your situation. No tool or checklist can prevent every kind of fraud or identity theft; these steps lower your risk but cannot remove it. Companies named here reflect our independent view and are not paid endorsements. Caveo is not affiliated with any agency or company named here. Steps checked against official sources on October 11, 2026; corrections to hello@joincaveo.com. Terms and Privacy Policy.