

FREE CHECKLIST

How to protect yourself, your family and your business from AI scammers

Today anyone's voice and video can be cloned, and hackers using artificial intelligence break into websites and services many times faster than before. The good news: simple agreements and a few settings stop most of these attacks. Here is what you need to do.

If you're not sure how to set something up, ask ChatGPT, Claude or another AI. Ready-made prompts are under the items, just copy them.

Personal life

- ☐ Warn the people close to you. Tell your parents, grandparents and anyone less familiar with technology plainly: a voice and even a video call can be faked.
- ☐ A family code word. Agree on a word only you know. Agree on it in person, not in a chat. "Your son" calls and asks for money: ask for the word.
- ☐ Hang up and call back. Unsure about a call, even with a familiar voice or on video? Call back yourself on the number saved in your contacts.
- ☐ Two-factor authentication, not by SMS. Email, bank, social media, messengers: an authenticator app, a passkey or a physical security key (for example, YubiKey). Protect your email first: it is used to reset all your other passwords.

ASK AI How do I turn on sign-in with an authenticator app instead of SMS in [service]?
- ☐ A password manager for every account. A long, unique password for every service, no repeats. For example, 1Password, Apple Passwords or Google Password Manager.

ASK AI Help me choose a password manager and move all my passwords into it. I use [iPhone or Android] and [Windows or Mac].
- ☐ Updates. Phone, computer, browser, apps. Turn on automatic updates.
- ☐ Don't tap links in "urgent" messages. "Your account is blocked", "your parcel is delayed", "confirm now": open the website or app yourself.
- ☐ Less of your voice and face in public. Make your social media private or limit who sees your videos and stories.

ASK AI How do I make my Instagram account private and limit who sees my stories?
- ☐ A PIN with your mobile carrier, so your number can't be moved to someone else's SIM card.

Note for your parents

PRINT IT AND KEEP IT BY THE PHONE

- 1 "Family" calls and asks for money? Ask for our code word.
- 2 No word, or not sure? Hang up and call back yourself on the number in your contacts.
- 3 A voice and even a video can be faked.
- 4 Rushing you and asking you to tell no one? It's a scammer.
- 5 Never tell anyone codes from SMS, passwords or PINs. Your bank never asks for them.
- 6 Don't tap links in messages. Call the bank on the number on your card.
- 7 Not sure? Call me: _____

Business

- ☐ Everyone who can move money has their own code phrase. Each employee with the right to pay, change bank details or grant access gets their own phrase. Any call or video call asking for money, access or data: the phrase comes first. Sign with each of them that the phrase has the force of their signature and that they are responsible for keeping it secret: if they share it with anyone, the consequences are theirs. Don't keep the phrases in a work chat.
 - ☐ Call back on a known number. "The director", "a supplier" or "the bank" calls: hang up and call back on the number from your own records, not from the message.
 - ☐ Bank details change only after a check. A supplier or employee sends new bank details: first call back on a known number, then pay.
 - ☐ The four-eyes rule. Payments above a limit and changes of bank details are confirmed by two people. The second person is not on the same call.
 - ☐ Payment limits, including for every employee who can make payments.
 - ☐ Review permissions. Who can pay, change bank details, grant access? Everyone gets only what they need for their work. Someone leaves: close their access the same day.
- ASK AI** Make a simple access-rights table for a company of [number] people: who pays, who changes bank details, who grants access.
- ☐ Cover rules in advance. Who confirms a payment if the responsible person is away. Written down, not decided on a call.
 - ☐ No exceptions for urgency or secrecy. "Urgent, confidential, tell no one" means: check. Tell your team out loud that double-checking even "the director" is right and will never be punished.

- ☐ A 10-minute briefing for the team. Voice and video can be faked, everyone has their own code phrase, here is the call-back rule.

ASK AI Write a 10-minute staff briefing on fraud with fake voices and video, with examples and verification rules.

- ☐ Two-factor authentication and a password manager for all work accounts. Email, bank, accounting, CRM, company social media. Share passwords only through the password manager, never in a chat.

- ☐ Update your website and systems. Is your website on WordPress or other PHP? Ask your developer or hosting provider whether the PHP fix from 21 October 2026 is installed, and ask for confirmation.

ASK AI How do I check which PHP version my website runs and whether it needs an update?

A couple of agreements today cost less than one call from "the director" tomorrow. Send this checklist to someone whose safety matters to you.

Some items come from the digital hygiene checklist by Andrej Karpathy (one of the founders of OpenAI), simplified for everyday use.

YANIS LUBINS • AI AUTOMATION FOR OWNER-LED BUSINESSES

Find out how AI can double your team without extra payroll

Setting up AI agents in a small business is like hiring extra staff for the work you always needed done but never had the budget for

SEE HOW IT WORKS ►

yanislubins.com