

Family Cyber Safety Guide

Simple habits that protect your family from scams, account takeovers and AI fakes. No technical knowledge needed.

1 • Agree on a family safe word, today

Scammers can now copy a person's voice from a short video posted online. The "Mum, I've been in an accident, I need money now" call can sound exactly like your child. **Don't trust the voice. Verify.**

Choose a word only your family knows. Don't post it, text it or save it online. If anyone calls asking for urgent money or help, ask for the word. **No word, no money.** Then hang up and call them back on their usual number.

2 • Know the scams that reach families most

- **"Hi Mum/Dad, this is my new number."** A "new number" asking for money. Call the old number first.
- **Parcel and delivery texts.** "Pay €1.99 to release your parcel." Open the courier's app yourself.
- **"Your bank account is blocked."** Banks never ask for passwords, PINs or codes by text or phone.
- **Fake shops and travel sites.** Prices that seem too good to be true, or visa and booking sites found through ads. Type the address yourself.
- **Celebrity investment videos.** Deepfakes of famous people promoting "guaranteed" returns are scams.

3 • Lock the accounts that matter

Turn on 2-step verification (MFA) for everyone's **email, banking, WhatsApp** (Settings → Account → Two-step verification) and **social media**. And teach everyone the golden rule: **never share a verification code**, with anyone, for any reason.

• UNVERIFIED



```
> trust = 0; verify --all
```

Our family checklist

- ☐ We have a **family safe word**, and grandparents know it too
- ☐ **2-step verification** is on for everyone's email, banking and WhatsApp
- ☐ Phones, tablets and computers **update automatically**
- ☐ Photos and documents are **backed up** (cloud + external drive)
- ☐ The kids know they can tell us anything that happens online, **without getting in trouble**

Share it

Print it for the fridge, and send it to your family group chat. The people most likely to be targeted are often parents and grandparents.

Why Alphatechs

24/7 security operations with a 30-minute response, penetration testing, and Sphere TI, our own threat intelligence platform.

Take the Next Step

More free guides and posters for home and work: alphatechs.al/cyber-month

4 · Kids and teens

- No game cheats, “free” skins or modded games. They're a top source of password-stealing malware.
- Only download apps from official app stores.
- Keep gaming and school accounts separate from parents' accounts and cards.
- Tell them: if someone online asks for photos, codes or secrecy, come and tell us, and **you won't be in trouble**.

5 · Parents and grandparents

- They're often the first targets of voice-clone and “bank” calls. Share the safe word with them too.
- Agree they'll **always call you** before sending money to anyone who contacts them unexpectedly.
- Help them turn on automatic updates and MFA.
- Remind them it's fine to hang up on anyone, even “the police” or “the bank”.

6 · If someone in the family gets hacked

1. From a **different, clean device**, change the email password first, then other accounts.
2. Turn on 2-step verification and **log out of all devices** (Settings → Security).
3. Money involved? **Call the bank immediately**, using the number on the card.
4. Warn friends and family not to trust messages “from” the hacked account.
5. Report it to the platform, and to the police if money was lost.

> ONE RULE FOR THE WHOLE FAMILY

Trust nothing. **Verify everything.**

A message, a voice or a video can be faked. A call back to a number you already know can't. When in doubt, hang up, check, and ask someone you trust.

Safe word

the simplest defence against voice-clone calls

2-step

verification on email, bank and WhatsApp

Call back

on a number you already have, every time