



Aware *and* Safe

BE AWARE. STAY SAFE.

SAFE IN THE AGE OF AI

The Family Guide to Outsmarting AI Scams

FREE SAMPLE · CHAPTER 1

The New Family Threat

From “The Family Guide to Outsmarting AI Scams” — read the full first chapter free.

The New Family Threat

Imagine a burglar who never has to leave home. Instead of picking your lock, they pick through your family's public life — the videos, the photos, the school announcements, the "so proud of Emma's first day of Grade 9!" posts — and build a key cut precisely for your front door. That is what modern scamming looks like. And artificial intelligence just gave that burglar power tools.

This chapter is about understanding the threat clearly, without hype and without panic. Because here's the thing most coverage gets wrong: AI hasn't made scammers smarter. It's made impersonation *cheaper*. That distinction matters, because it tells you where to aim your defences.

What AI actually does for criminals

Let's strip away the mystery. "Artificial intelligence" in the hands of scammers comes down to three capabilities, and it helps to know each one by name.

1. Voice cloning. Software can now take a short recording of someone's voice — a few seconds from a social media video, a voicemail greeting, a clip from a school concert posted online — and generate new speech in that voice saying anything at all. The quality varies, but on a crackly phone call, with emotion in the mix, it's convincing enough to fool a parent or grandparent. This is the engine behind the fake emergency calls in Chapter 2.

2. Face and video fakery ("deepfakes"). AI can put a real person's face onto video, or animate a still photo to look like a live video call. The technology is improving fast. Right now, most scam attempts still use voice alone, because it's easier and phone calls create urgency. But video-call scams — "it's your grandson, look, it's really me" — are increasingly common, and your family should know they're possible.

3. Personalised writing at scale. AI can write fluent, natural messages — texts, emails, social media DMs — tailored to a specific person using details scraped from their public profiles. The old giveaway ("the email is full of spelling mistakes") is gone. A message to your teenager can now reference their real friends, their real school, their real interests, and sound like it came from someone who knows them.

That's the toolkit. Notice what's *not* on the list: mind reading, hacking your phone by calling you, or anything magical. Every AI scam still needs you to *do* something — send money, share information, click a link, keep a secret. The technology is new. The ask is always old.

Why your family specifically

Criminals are businesspeople, in the worst sense. They go where the return is highest for the effort. Families offer four things that make them ideal targets.

A visible map. Your family's life is partially public. Social media posts, school websites with team rosters, obituaries naming grandchildren, real estate listings with family photos — each piece is harmless alone. Together, they let a stranger learn your

children's names, your parents' voices, your routines, and your relationships. You don't need to delete your online life. You do need to know it's being read by people you didn't invite.

Emotional shortcuts. Every family has them: the panic when a child might be hurt, the instinct to help a parent in trouble, the embarrassment that keeps a teenager from asking for help. Scammers don't hack computers here — they hack these shortcuts. The most effective scams don't feel like scams. They feel like emergencies.

Multiple generations, multiple weaknesses. A criminal targeting your family gets options. Grandparents tend to answer the phone and trust voices. Teenagers live online and trust messages that look like they're from friends. Busy parents are distracted and make fast decisions under pressure. One family, three attack surfaces.

Money in motion. Families constantly move money for legitimate reasons — allowances, school fees, gifts, emergency help. A request for money doesn't automatically look strange in a family context. That's what makes the fake emergency so effective: "wire money quickly" is something real families actually do.

What's hype and what's real

Because fear sells, you'll hear dramatic claims about AI scams. Let's sort them honestly.

Real and happening now: voice-clone emergency calls. AI-written phishing messages personalised with real details. Fake explicit images used for extortion. Scam video calls (early but

growing). These are documented, reported by fraud agencies, and worth preparing for — which is exactly what this book does.

Real but rare: fully interactive real-time deepfake video calls that hold up under scrutiny. The technology exists, but most criminals don't bother — a voice call is easier and works. Don't dismiss it, but don't lose sleep over it either.

Mostly hype (for now): AI "hacking into" your phone just by calling you, or taking over your devices through a text message alone. That's not how phones work. Be suspicious of anyone who tells you otherwise — including anyone selling you expensive "protection" against it.

The honest summary: the threat is real, it's growing, and it's specifically shaped around families. But it's also *narrow*. Every attack in this book is defeated by the same small set of habits. Learn those habits and the hype stops mattering.

Your family's digital footprint: a quick audit

You can't protect what you can't see. Before the next chapter, take twenty minutes for a simple exercise — ideally with your teenager, who will find things you won't.

- 1. Google your family's names.** What comes up? School pages, sports rosters, social profiles, news mentions? Note what's public.
- 2. Check social media privacy settings together.** Who can see posts, friend lists, and photos? "Friends only" is the minimum; "public" is an invitation.

3. **Listen to voicemail greetings.** Does anyone's greeting say their full name? A name plus a voice sample is starter material for cloning.
4. **Look at what's posted *about* your kids by others.** Grandparents' public Facebook posts are a goldmine for scammers — full names, schools, voices in videos. Have the conversation kindly; this isn't about blame.
5. **Search your home address.** Real estate listings often include interior photos and family details long after you've moved in.

You're not trying to disappear from the internet. You're mapping what a stranger could learn in an afternoon — because that's exactly what the professionals do before they call.

KEY TAKEAWAYS

- 1. AI made impersonation cheap, not criminals smart.**
Voice cloning, fake video, and personalised messages are the three tools — and every scam still needs you to *do* something.
- 2. Families are targets because they're visible, emotional, multi-generational, and move money.**
That's the business logic; understanding it removes the mystery.
- 3. Your ears and eyes are no longer sufficient proof of identity.** A familiar voice on the phone proves nothing by itself anymore.
- 4. Audit your family's public footprint together.**
Google names, check privacy settings, and look at what grandparents post publicly — kindly, not as an accusation.
- 5. Don't buy fear.** Real threats are specific and addressed in this book; anyone selling panic (or expensive "AI protection") is selling you something, not protecting you.

LINE TO REMEMBER

Trust is now something you verify, not something you hear.

The "Emergency" Scam

The phone rings at 9:40 on a Tuesday night. The voice on the other end is your son's — you'd know it anywhere — except he's crying, and he's saying he's been in a car accident, and he needs you to wire bail money right now, and please don't call Dad, he'll handle it, just please hurry.

Your hands are shaking. You're reaching for your banking app before he's finished talking.

Stop. Breathe. Read this chapter first — or better yet, read it *before* that call ever comes, because preparation is the only thing that works when your heart is pounding.

How the scam works, step by step

Understanding the machinery takes away its power. Here's the playbook, refined over years and supercharged by AI:

Step 1: Reconnaissance. The criminals learn about your family first. Social media, school websites, obituaries, public posts by proud grandparents — they collect names, relationships, voices, and details. They know your son's name. They may know what car he drives, where he goes to school, who his friends are.

Step 2: The call. It usually comes late at night or early in the morning — when you're groggy and emotional. The voice sounds like your child or grandchild: upset, crying, whispering, or with a bad connection "explaining" any oddness in the audio. AI voice

Enjoyed this chapter?

This was Chapter 1 of *The Family Guide to Outsmarting AI Scams*, part of the *Safe in the Age of AI* series by Aware and Safe. The complete handbook includes every chapter, all the checklists, and the companion resources — available now in the edition that suits you.

Ebook + Audiobook Bundle

\$8.99

Everything together — the best value.

<https://awareandsafe.com/safe-in-the-age-of-ai/family-guide/#formats>

Ebook

\$6.99

Premium PDF — read on any device.

<https://awareandsafe.com/safe-in-the-age-of-ai/family-guide/#formats>

Audiobook

\$4.99

Full MP3 narration + companion PDF.