



Aware*and* **Safe**

BE AWARE. STAY SAFE.

SAFE IN THE AGE OF AI

The Small Business Guide to AI Security

FREE SAMPLE · CHAPTER 1

How AI Changed Fraud

From “The Small Business Guide to AI Security” — read the full first chapter free.

How AI Changed Fraud

Three years ago, fraud against small businesses looked like this: a badly written email pretending to be from your bank, a phone call from "tech support" with a thick accent reading from a script, an invoice from a supplier you'd never heard of with the wrong logo.

You could spot most of it. Your staff could spot most of it. The fakes were *fake* — wrong tone, wrong details, wrong everything.

That world is gone.

What changed

Artificial intelligence didn't invent fraud. It industrialized it. Here's what that means in practice:

Research at machine speed. Before AI, a scammer targeting your business had to manually research you — browse your website, scroll your social media, guess at your suppliers and processes. It took hours per target, so they only bothered with big fish. Now they feed your public footprint into an AI tool and get a complete profile in minutes: your team members' names and roles, your recent projects, your tone of voice from your own marketing copy. Every business is now worth researching, because research is nearly free.

Writing that passes the smell test. The old phishing email failed because it *sounded* wrong. AI writes in fluent, natural business

English — or French, or Mandarin, or whatever your business uses. It mimics the formality of a real invoice email. It gets the jargon right. The "broken English" tell that protected a generation of small businesses is extinct.

Voice and video impersonation. This is the big one, and it gets its own chapter. Thirty seconds of your voice — from a voicemail greeting, a podcast appearance, a video on your website — is enough for AI to generate new sentences in your voice saying anything the criminal types. Video is catching up fast. The "I'll know it's really them because I can hear their voice" defense is dead.

Scale without cost. A single criminal with a laptop can now run personalized attacks against hundreds of small businesses simultaneously. The economics flipped: it used to cost more to research and craft a convincing attack than most small businesses were worth stealing from. Now the marginal cost of one more target is essentially zero.

A walkthrough: how they'd research you

To make this concrete, here's what an afternoon of AI-assisted reconnaissance looks like against a fictional business — "Lakeside Dental," a six-person clinic. Every step uses only public information and free tools:

2:00 PM — The website. The criminal opens lakesidedental.ca. From the "Our Team" page: Dr. Patel (owner), Maria (office manager), two hygienists. From the blog: a post about their new CEREC crown machine — expensive equipment, recently purchased. That tells the criminal the practice spends money and Maria probably handles payments.

2:15 PM — Social media. Dr. Patel's LinkedIn shows 400+ connections, including "Henry Wu — Patterson Dental Supply." Maria's Facebook (public) shows she just got back from a cruise — posted the dates. The criminal now knows the owner's supplier by name and that the office manager was recently away (useful for timing).

2:30 PM — The voice. The clinic's website has a "Meet Dr. Patel" video — 90 seconds of clear speech. The local news site has a clip of him at a charity fundraiser. That's more than enough audio to clone his voice.

2:45 PM — The build. The criminal feeds all of this into an AI tool with a simple prompt: "Write a professional email from Dr. Patel to Maria asking her to urgently wire a deposit to a new equipment supplier. Reference the CEREC machine. Keep it short and natural." The AI produces a flawless email in Dr. Patel's communication style — because it learned that style from his own blog posts.

3:00 PM — The attack. Maria receives the email. It references the real supplier relationship, the real equipment purchase, and sounds exactly like her boss. If she hesitates, a follow-up "call" from Dr. Patel's cloned voice seals it.

Total criminal investment: one hour, zero dollars. Potential payoff: tens of thousands. And nothing in this walkthrough required hacking, malware, or technical skill — just a web browser and patience.

Your business has the same public footprint. The only question is whether your processes can survive an attack this well-prepared.

The numbers behind the shift

You don't need precise statistics to understand the trend — but the direction is unmistakable. Business email compromise (fraudulent emails impersonating executives or vendors) has been the costliest form of cybercrime for years, measured in billions annually. AI hasn't created this category; it's made every attack in it more convincing and dramatically cheaper to run.

The pattern to internalize: **attacks are getting more targeted, more convincing, and more frequent simultaneously.** That's the triple threat AI introduced. Any one of those trends alone would be manageable. All three together is why this book exists.

Why small businesses specifically

It's worth being blunt about why criminals prefer you over larger targets:

- 1. You have money but not security staff.** You process payments, hold customer data, and maintain banking relationships — everything worth stealing — without a single person whose full-time job is protecting those things.
- 1. Your processes are informal.** In a five-person company, the owner says "wire the deposit" and someone wires it. There's no procurement department, no dual authorization, no

verification callback. That informality is efficient — and it's exactly what impersonation attacks exploit.

1. You trust your tools. Small businesses run on email, and email was designed in an era when impersonation was hard. AI made impersonation easy, but the trust stuck around.

1. You're busy. The owner is selling, hiring, fixing, and firefighting. Security is the thing you'll get to "next quarter." Criminals are counting on next quarter never arriving.

None of this is a criticism. It's the reality of running a small business, and the defenses in this book are designed for that reality — not for a company with a chief information security officer.

What hasn't changed

Here's the reassuring part, and it's important: **every fraud still needs a human being to do something.** Click the link. Approve the transfer. Share the password. Send the data. AI made the *bait* more convincing, but the *hook* still requires your action — or your employee's.

That means the defenses that matter most aren't technical. They're procedural: verification rules, clear policies, and habits that don't depend on anyone being clever enough to spot a perfect fake. You don't need to outsmart AI. You need processes that work even when the fake is flawless.

That's what the next five chapters build.

This week's action

Before you read further, do one thing: **ask yourself who in your business can authorize a payment, and what would stop them from sending money to a convincing impersonator of you.** If the answer is "nothing, really" — Chapter 2 is the most important thing you'll read this month.



Enjoyed this chapter?

This was Chapter 1 of *The Small Business Guide to AI Security*, 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/product/the-small-business-guide-to-ai-security-ebook-audiobook-bundle/>

Ebook

\$6.99

Premium PDF — read on any device.

<https://awareandsafe.com/product/the-small-business-guide-to-ai-security-ebook/>