HideMyDataNow

FREE GUIDE

Stay safe online in the age of AI

How scammers and AI agents find you, the scams they use, and simple steps to stop them.

> **In seconds, an AI agent can find your home address, phone number, employer and even your voice online. Then it writes the perfect scam message for you. This guide shows you how to make that much harder.**

Inside this guide

1. How AI agents find you
2. 5 scams AI makes easier, and how to spot them
3. Quick wins: three things to do today
4. The 12-step checklist to stay safe
5. Red flags cheat sheet

HOW EXPOSED ARE YOU?

Check your own risk score

See what an AI agent can find about you, scored out of 100. Free, takes under a minute.

Scan the code or visit www.hidemydatanow.com

1 · THE PROBLEM

How AI agents find you

AI agents can search the whole web for a name in seconds and combine everything into one profile. These are the four places they look first.

People search sites and data brokers

Hundreds of sites collect and sell your address, phone number, age, relatives and job. An AI agent reads them in seconds.

Social media and old accounts

Photos, posts, friends and check-ins show who you know, where you go and how you write. That's enough to impersonate you.

Leaked databases

Every hacked webshop or app leaks emails and passwords. Attack tools try them on your email and bank within hours.

Videos, podcasts and voice messages

A few seconds of your voice is enough for AI to fake a phone call from you.

2 · KNOW THE TRICKS

5 scams AI makes easier

None of these are new. AI just makes them cheaper, faster and far more convincing.

1. The "Mum, I'm in trouble" call

An AI copy of a loved one's voice calls from a new number and urgently needs money.

What to do: Agree a family safe word. Hang up and call back on the number you already have.

2. The perfect phishing email

No spelling mistakes, your name, your job, even a recent purchase. It asks you to log in or pay.

What to do: Never use the link. Go to the website or app yourself.

3. The fake invoice or urgent boss

"Our bank details have changed" or "Please make this transfer today, and keep it quiet."

What to do: Confirm every change of bank details by phone, on a number you already know.

4. The account takeover

Criminals log in with a password that leaked years ago, then lock you out.

What to do: A password manager and two-step login stop almost all of these.

5. The deepfake video call
A familiar face on video asks for money, codes or access. The image looks a little off.
What to do: Ask something only the real person knows, or call them back.

3 · START HERE

Quick wins: do these today

Twenty minutes in total. These three stop the most common attacks.

5 min	**Turn on two-step login for your email**
5 min	**Agree a safe word with your family**
10 min	**Install a password manager and change your email password**

4 · TAKE ACTION

The 12-step checklist to stay safe

Tick them off one by one. Five minutes each, most of them free.

- [ ] **1. Use a password manager**
  Bitwarden (free), 1Password, or the one built into your phone. It gives every account its own strong password, so one leak can't open the rest.
- [ ] **2. Turn on two-step login**
  On your email first, then your bank and social media. Choose an app code or a passkey over SMS where you can.
- [ ] **3. Change any leaked password**
  Every password from a known leak, everywhere you used it. Your password manager makes this quick.
- [ ] **4. Agree a family safe word**
  Anyone who calls or video-calls asking for money must say it. This beats AI voice-clone scams.
- [ ] **5. Hang up and call back**
  When a bank, boss or relative asks for money or codes, call back on a number you already have. Never use the one in the message.
- [ ] **6. Lock your phone number**
  Ask your mobile provider for a PIN or extra check before anyone can move your number to a new SIM.
- [ ] **7. Turn on bank alerts**
  Get a notification for every new payee and every large payment, so you spot fraud straight away.
- [ ] **8. Share ID copies safely**
  Use the KopieID app (Netherlands) or cross out your ID number and photo before sending a copy.

- [ ] **9. Tighten your social profiles**
  Hide your phone number, birthday and friend list. Delete old accounts you no longer use.
- [ ] **10. Watch what search shows**
  Turn on Google's "Results about you" to get an alert when your address, phone or email appears.
- [ ] **11. Keep a human in the loop with AI assistants**
  Don't give one assistant your inbox, payments and sending all at once. Approve anything that sends money or mail.
- [ ] **12. Update everything automatically**
  Turn on automatic updates on your phone, laptop and home router.

5 · KEEP THIS HANDY

Red flags cheat sheet

See one of these? Stop, hang up, and check through a channel you already trust.

- ! **It's urgent, and you must act right now**
- ! **You're asked to keep it secret**
- ! **Bank details or a phone number have "changed"**
- ! **Payment by gift card, crypto or a new account**
- ! **Someone asks for a code you received by text**
- ! **A link asks you to log in or confirm details**

HIDEMYDATANOW

Want us to do the hard part?

We remove your personal data from the web and keep watching, so scammers, hackers and AI agents can't find you again. Free during beta.

+ **We find what AI can find**
  We search the web the way an AI agent or scammer would, and check for leaked passwords.
+ **We remove it for you**
  We send legal GDPR removal requests in your name, chase companies that don't answer and read their replies.
+ **We keep watching, every week**
  Data brokers put details back up. We rescan weekly, remove anything new and warn you about new leaks.
+ **We guide you, one step a week**
  One short email a week walks you through this checklist, about five minutes each.

HOW EXPOSED ARE YOU?

Get your free risk score

See what an AI agent can find about you, scored out of 100. Free, takes under a minute.

Scan the code or visit www.hidemydatanow.com

Know someone who should read this? Forward this guide to family and friends. It's free.