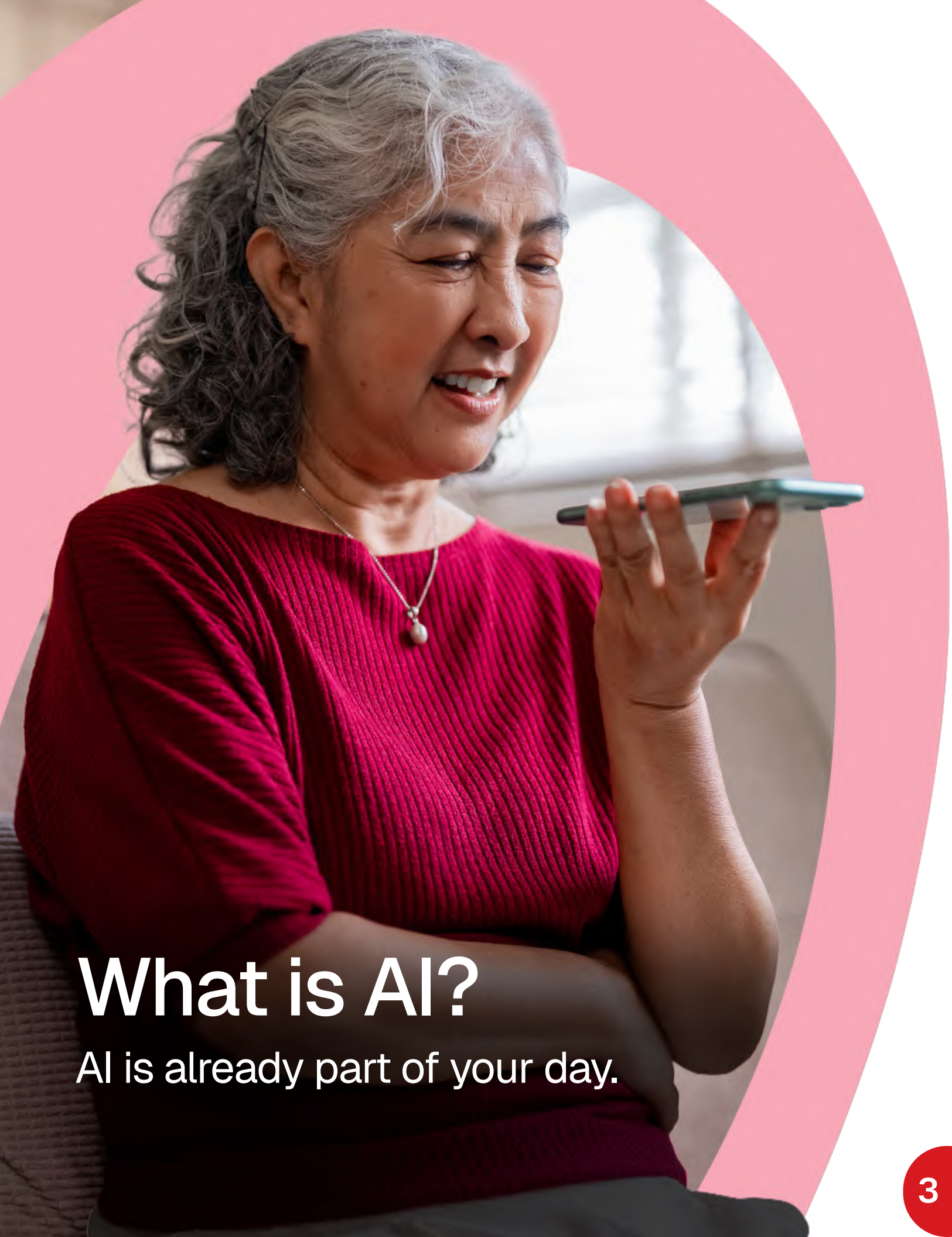
TrendLife™

Understanding Artificial Intelligence (AI)

What You Need to Know to Stay Safe

Table of Contents



What is AI?

AI is already part of your day.

Most of us are already using artificial intelligence (AI) without realizing it. It is not a robot from a science fiction movie. It is a type of technology that has quietly become part of everyday apps and services.

Examples you have likely seen:

Your email moving junk mail to a spam folder

Netflix or Spotify suggesting things you might enjoy

Google Maps choosing the fastest route in real time

Siri, Alexa, or Google Assistant answering your questions

Your bank automatically flagging an unusual charge

Two kinds of AI worth knowing

Simple AI (also called Narrow AI)
Trained to do one specific job really well. Your spam filter is a good example. It learned what junk mail looks like and gets better at catching it over time. It does not think, create, or hold a conversation. It just does its one job.

Generative AI
Newer and much more powerful. Generative AI can create brand new content including text, images, audio, and video by learning from enormous amounts of data. It can now produce things that look and sound like a real human made them.

Examples include ChatGPT, Google Gemini, Microsoft Copilot, and voice assistants that hold real conversations.

Why this matters

Simple AI works quietly in the background. Generative AI is what you actively interact with, and it is the technology that cybercriminals are learning to exploit. When you hear about AI being used in scams, it is almost always generative AI.

AI is very agreeable — and that can be a problem

AI chatbots are designed to be helpful and agreeable. They tend to validate what you say, go along with your assumptions, and rarely push back, even when you are wrong. If you ask a chatbot "Isn't this the best treatment for my condition?" it may simply agree rather than correct you. This can feel reassuring but can reinforce incorrect beliefs or lead you toward poor decisions.

Think of AI as a very eager-to-please assistant, not a trusted expert. Always check a second, independent source for anything important, especially around health, finances, or legal matters.

AI is often confidently incorrect

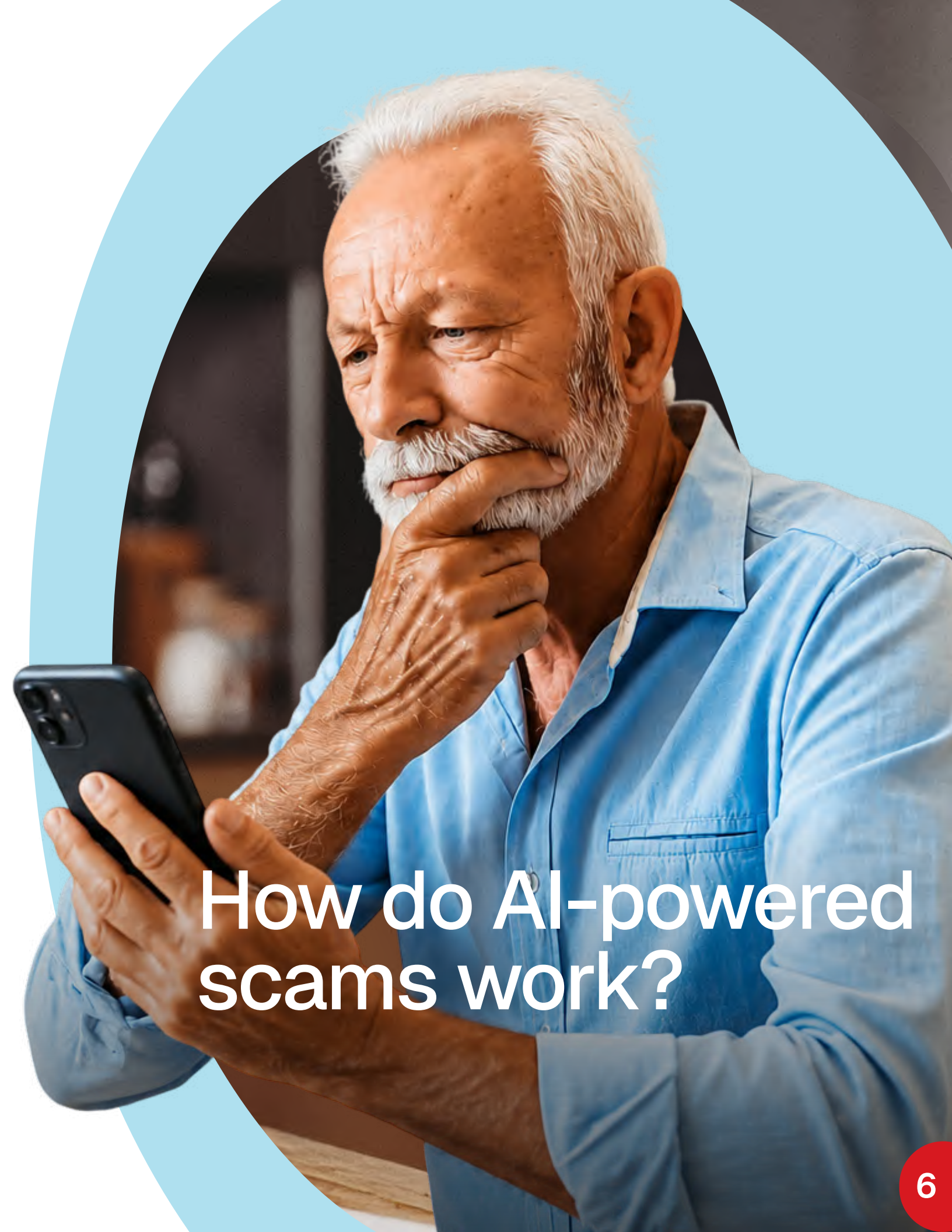
Even sophisticated AI can state false information with complete confidence. This is called a "hallucination."

Recent examples include:

- An AI gave incorrect air quality data, citing official sources that never published those numbers
- A medical AI invented nursing guidelines that did not exist
- A chatbot fabricated an entire border treaty between two countries

The rule

Never rely solely on AI for health, legal, financial, or safety decisions. Always verify with a trusted source, such as a doctor, a government website, or a trusted news organization.



How do AI-powered scams work?

Today's scams look different.

Scam messages used to be easier to spot because of bad spelling, strange formatting, and obvious fakes.

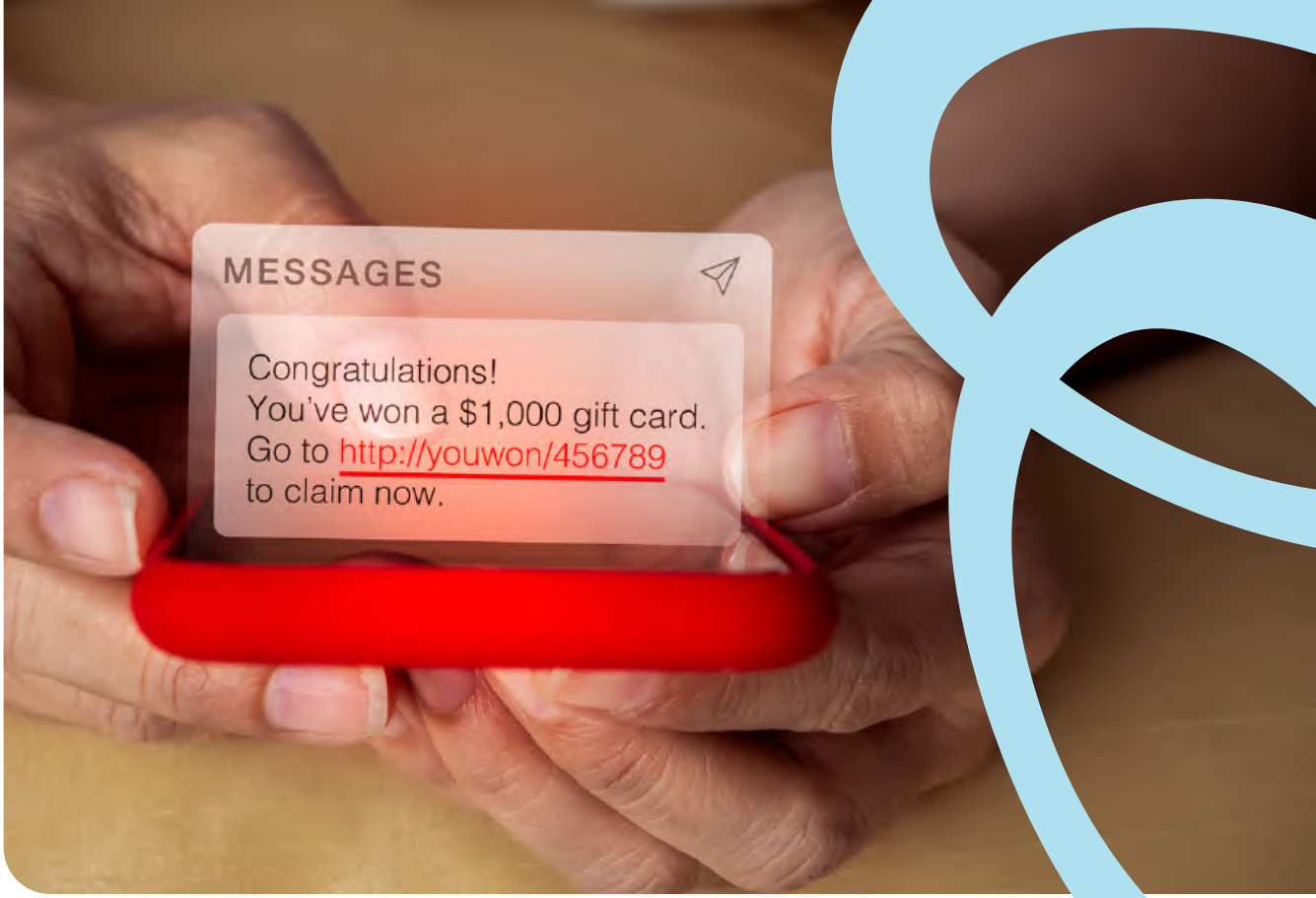
Today, criminals use generative AI to craft messages that are perfectly written, personalized, and nearly indistinguishable from the real thing.

They can imitate your bank, a government agency, a delivery service, or even a person you know.

AI phishing: emails, texts and calls

Phishing is when a criminal contacts you pretending to be someone you trust, hoping you will click a link, hand over personal information, or send money. AI has made these attempts far more convincing, and they can arrive in many forms: an email, a text message, or a phone call.

Criminals can also spoof phone numbers, meaning they can make a call or text appear to come from a real, familiar number, such as your bank's official customer service line or even a friend's number. Just because a number looks familiar does not mean the person contacting you is who they say they are.



Red flags to look for:

- Urgent or threatening language: "Your account will be closed!" or "Act within 24 hours"
- Any request for your password, government ID number, banking details, or credit card. No real organization asks for these by email, text, or an unsolicited call
- A sender email address that looks almost right but has a slight misspelling
- An offer that seems too good to be true

What to do:

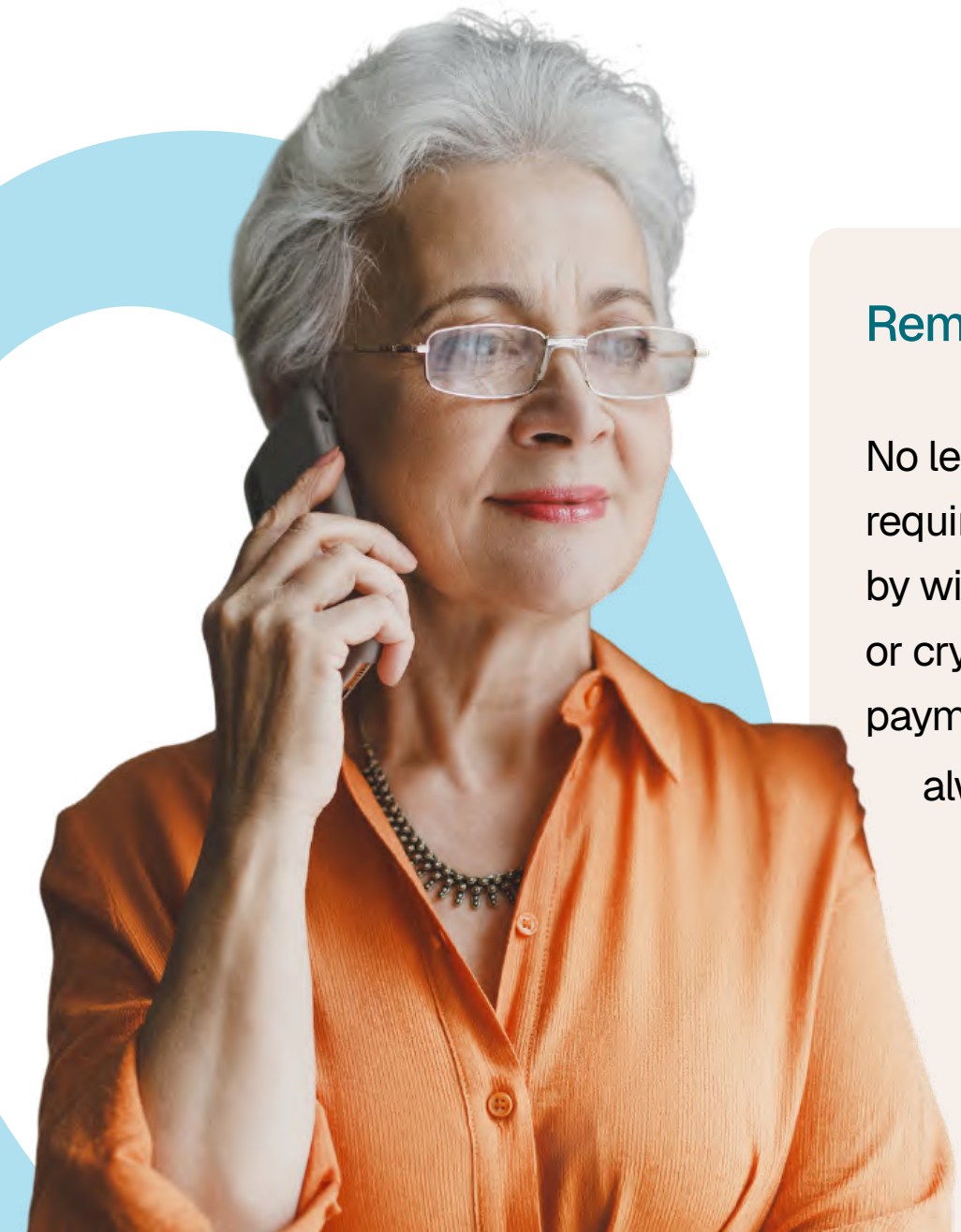
- Do not click links in emails or texts. Call or visit the organization's official website to verify first.
- Save or bookmark official websites you use regularly, so you always know you are in the right place
- If you receive an unexpected call from any organization, hang up and call them back using the number on their official website.
- Ask someone you trust for help if you are unsure.

AI voice cloning

Generative AI can clone a real person's voice from as little as three seconds of audio, sometimes taken from a social media video or a voicemail. Criminals use this to fake emergency phone calls from people you know and trust, creating panic to pressure you into sending money or sharing information before you have time to think.

What to do:

- Hang up. Call the person back using a number you already have saved.
- Set up a secret code word with close friends and family. Ask for it if you ever receive a panicked call. A real person will know it. A scammer will not.



Remember

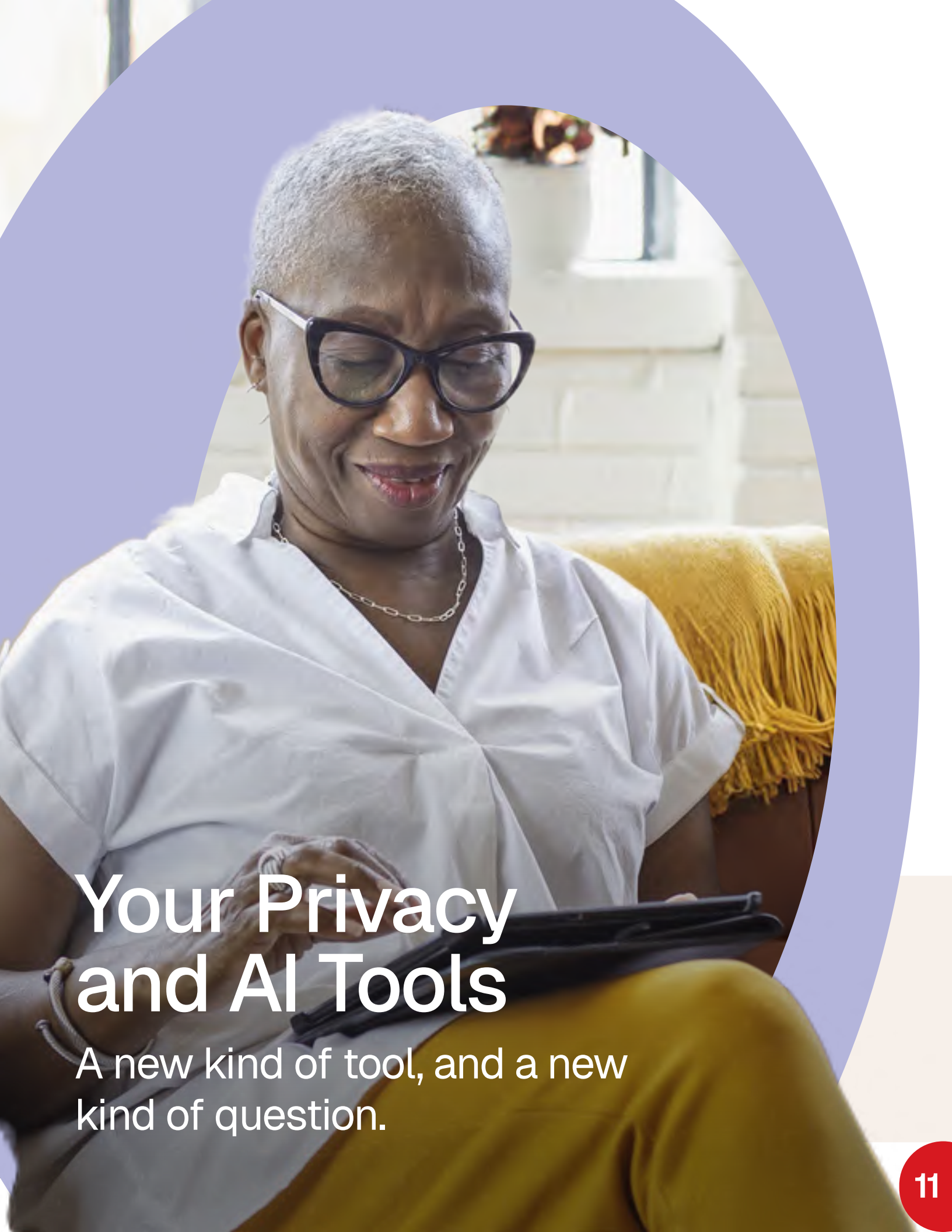
No legitimate emergency requires you to send money by wire transfer, gift cards, or cryptocurrency. These payment methods are almost always a sign of a scam.

AI-generated fakes: videos and images

Generative AI can create photo-realistic images of people who do not exist, and convincing videos of real people saying or doing things they never did. These are known as deepfakes, and are used in romance scams, investment fraud where a fake celebrity endorses a product, and misinformation campaigns.

Today's deepfakes are very difficult to spot, so focus on these actions instead:

- Question who may have made this video or image and what it is asking you to believe or do.
- Be skeptical of anything designed to create urgency, fear, or excitement, especially if it involves money, a public figure, or someone you know.
- If a video or image is being used to promote an investment, product, or emergency request, treat it as a red flag regardless of how real it looks.
- Search for the story independently. If something is genuinely newsworthy, multiple reliable news organizations will be reporting on it.



Your Privacy and AI Tools

A new kind of tool, and a new kind of question.

AI tools are designed to be helpful, but they also collect information about you. Before using any AI tool regularly, take a few minutes to check its privacy settings.

How to check privacy settings

Look in your app's settings or profile menu, often shown as a gear icon or your account profile icon. Look for sections labelled "Privacy," "Data and Personalization," or "Chat History."

Common things you can usually control:

- Turning off chat history so your conversations are not stored or used for training
- Deleting past conversations to clear what you have already shared
- Opting out of data sharing so your inputs are not used to improve the AI model

What not to share with any AI tool

Even if the settings seem secure, never type or say:

- Your full name combined with your date of birth, home address, or government ID number
- Passwords or banking information
- Confidential medical information
- Private information about other people

The bottom line

AI tools can be useful for writing a letter, getting directions, translating text, or looking things up. Use them thoughtfully, the same way you would be careful about what you share in any conversation.

Questions to ask

Does this AI store my conversations? Can I delete them?

Could what I type or say be seen by others or used by the company to train its AI model?

Can I opt out of having my data shared with third parties?

Am I using a free version? If so, my data may be how the product is funded.

Frequently Asked Questions

Is it safe to use voice assistants at home?

For everyday tasks, generally yes. But know that smart speakers can record and sometimes store voice commands. Review the privacy settings on your device, consider muting the microphone when not in use, and never say sensitive information out loud near a smart speaker.

What if I cannot tell whether something is a scam or not?

You do not have to figure it out alone. Do not respond right away. Take your time. Ask a trusted friend, neighbor, or family member. Contact the organization directly using contact information from their official website.

Someone I met online wants to video chat. Can I trust that it is really them?

Not necessarily. AI-generated video technology (sometimes called deepfakes) can now run in real time during video calls. Be cautious about any relationship with someone you have never met in person, no matter how long you have been talking online. Never share personal information or send money before meeting them in person with a trusted friend present. Be equally cautious if they send you links to investment websites or encourage you to move money into an investment platform they recommend. This is a common pattern in online fraud.

A friend says I should try a generative AI chatbot. Is it safe?

These tools can be useful for everyday tasks. Start by going directly to the tool's official website and be careful of fake copycat websites. Before using, check the privacy settings to make sure you are comfortable with how your data is used and stored. Never share personal, financial, or medical information. Remember that AI chatbots are often incorrect and designed to agree with you, so treat their responses as a starting point, not as expert advice.

Your Safety Checklist

Before using any AI tool

- ☐ I have checked whether the app stores my conversations
- ☐ I have checked whether the app will use my data to train its AI model
- ☐ I never share sensitive information with a chatbot or voice assistant
- ☐ I treat AI responses as a starting point, not as expert advice

Privacy and account security

- ☐ I have reviewed privacy settings on my phone, apps, and AI tools
- ☐ I use strong, unique passwords and have two-step verification turned on for my accounts
- ☐ I am careful about what personal information I share online or on social media

Misinformation and fake content

- ☐ I question videos or images that create urgency, fear, or ask me to take action
- ☐ I search for the story on a trusted news source before sharing or acting on it

Scams and fraud

- ☐ I go directly to official websites rather than clicking links in emails or texts
- ☐ I have saved or bookmarked the official websites I use regularly
- ☐ I verify urgent requests by calling back using a number I already know
- ☐ I have set up a secret code word with people close to me for verifying emergency calls

TrendLife™

Connect with us and empower your digital life.

@OfficialTrendLife