



Staying safe online

A guide for older people

Anyone can be targeted by a scam. These simple habits keep you safe. Keep this by the phone or the computer.



The one habit

Stop. Check. Call back on a number you trust.

- **Stop.** Don't let anyone rush you. If you're unsure, it is always fine to hang up.
- **Check.** Never use a number or a link that a caller or a message gives you.
- **Call back** on a number you trust: the back of your card, a bill you already have, or the official website.



Texts and phone calls

- Not expecting a text? Don't tap the link or ring the number in it.
- A caller may know your name and address. That doesn't make them genuine.
- Never give anyone a code sent to your phone.
- Asked to install an app, or to let someone into your computer or phone? Hang up.
- A landline call may not end until both sides hang up. Ring back from a different phone if you can.



They will never...

- **Your bank** will never ask for your full PIN, send someone to collect your card, or ask you to move money to another account.
- **The Gardaí** will never ask for your banking PIN or password, ask you to move money, or come to your home to collect your card or cash.
- **Revenue** will never text, email or phone you about a tax refund or a bill.
- **An Post** will never text or email you a link to pay for a parcel.

In danger, or is the scammer at your door now? Ring 999 or 112.



Emails and links

- Don't click links or open attachments in emails you weren't expecting.
- Go to a website by typing its address in yourself.
- Check who really sent it: look at the part after the @ sign.
- Being told to act now, or your account will be blocked, is a warning sign.
- A "reset your password" email you didn't ask for? Don't click it.



Passwords and two-step checks

- Make a password from three or more random words, with a number or symbol added. Aim for 12 characters or more.
- Use a different password for each important account, especially your email.
- Turn on two-step checks: a code to your phone as well as your password. Look in the account's settings or security section.
- Keep your passwords and PINs to yourself. A real helpdesk will never ask for them.
- Don't write your PIN down or keep it with your card.
- Keep your phone, tablet and computer up to date with the latest updates.



Online banking and shopping

- Shop with sellers you know. If in doubt, shop somewhere else.
- If you have a credit card, use it to shop online. It may give you more protection.
- The padlock beside a web address doesn't prove a shop is genuine.
- Don't bank or shop on public Wi-Fi. Use your mobile data instead.
- Look over your bank statements for anything you don't recognise.



Messages, social media and video calls

- A message from "your son" or "your daughter" on a new number, asking for money? Ring them on the number you already have before you send anything.
- Voices can be copied with AI. Take care even when a voice on the phone sounds familiar.
- Met someone online who asks for money? Don't send or receive money. Romance scammers always find a reason not to meet in person.
- Think twice before using your webcam with someone you have only met online.
- Keep your profile private. Don't post your date of birth, where you live or family details.
- A prize or a bargain that sounds too good to be true probably is.



If it has happened

It can happen to careful people. You have done nothing wrong by being targeted.

- 1 **Ring your bank now**, on the number on the back of your card. Ask them to stop any more payments.
- 2 **Stop all contact.** Don't reply, and block the number.
- 3 **Keep the evidence:** screenshots, numbers, dates, times and amounts.
- 4 **Report it** at your local Garda station, or any Garda station.
- 5 **Change your passwords** if you shared any: your email and online banking first.
- 6 **Tell someone you trust.** You don't have to sort it out alone.
- 7 **Beware of anyone offering to get your money back for a fee.** Don't send any more money.



Who can help

All the steps, in order: safeandsecure.ie/scamwatch/ive-been-scammed

- **Family or a friend.** Talk it over before you pay or share anything.
- **Your bank:** the number on the back of your card.
- **An Garda Síochána:** your local Garda station.
- **Crime Victims Helpline:** Freephone **116 006**, for support after a crime. Monday to Thursday 10am to 7.30pm, Friday 10am to 5pm, Saturday 2pm to 4pm.
- **Age Action's Getting Started:** free lessons with a volunteer tutor, to get online or use your phone or tablet with confidence. **0818 911 109**.
- **Is it a scam?** Look it up on ScamWatch: safeandsecure.ie/scamwatch



Keep these numbers to hand

My bank's fraud number _____ from the back of my card

My local Garda station _____

Someone I trust to ring _____

Never write a PIN or a password on this sheet.



One thing to do today

Copy the number from the back of your bank card into the box above. If a call or a text ever worries you, that is the number to ring.