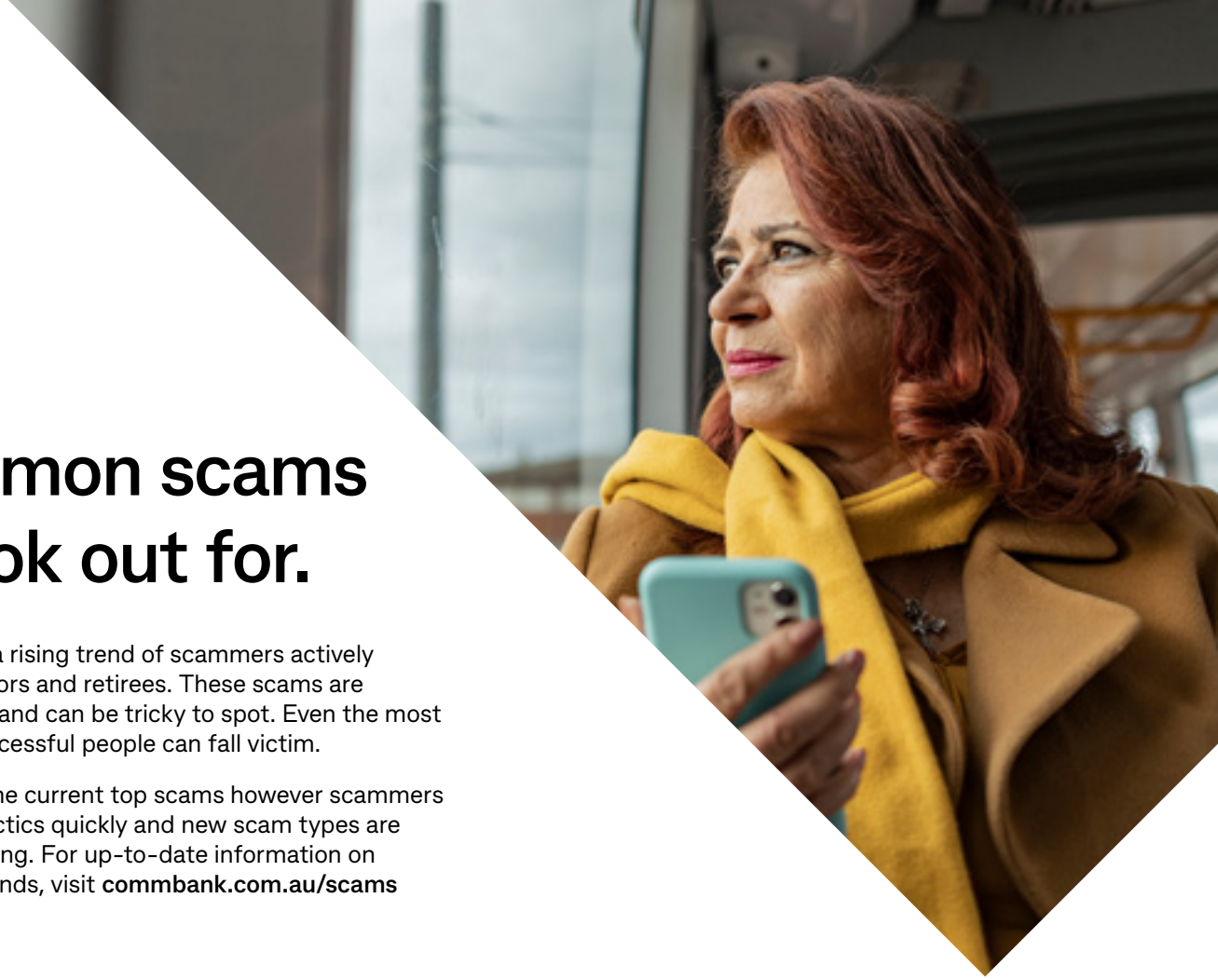

Common scams to look out for.

We're seeing a rising trend of scammers actively targeting seniors and retirees. These scams are sophisticated and can be tricky to spot. Even the most savvy and successful people can fall victim.

Below are some current top scams however scammers adapt their tactics quickly and new scam types are always emerging. For up-to-date information on scams and trends, visit **commbank.com.au/scams**

Common scams

Friendship or romance scams

Scammers attempt to gain your trust by developing a relationship with you that you believe is genuine. Usually meeting online, you may think you are speaking with a romantic partner, friend, or even a relative. However, their real intentions are often aimed at obtaining access to steal money or personal information from you.

Tip: Never send money or gifts to someone you only know online. Never give anyone access to your banking details or banking.

Impersonation scams

Where scammers pretend to be from organisations like banks, technology or government agencies. They might call, email or physically visit your house asking you to hand over identification documents, cards, cash, PINs, passwords or cheques.

Tip: CommBank will never ask for your banking information like your NetBank passwords PINs or NetCodes. If you're ever unsure, contact CommBank for help.

Investment scams

These scams attempt to entice you with the promise of high returns, often involving cryptocurrency, term deposits or other investment opportunities.

Tip: If an investment opportunity seems too good to be true - it probably is. Double check any investment opportunities with a trusted financial advisor.

Remote access scam (RAS)

Where a scammer contacts you and attempts to obtain access to your accounts or device, pretending to be from a well-known company. They usually ask you to download software to your computer or mobile device to gain access.

Tip: If you receive an unexpected phone call, text or email about your computer and remote access is requested, hang up or delete it immediately – even if they mention a well-known company.

Tips to stay safe

Remember 3 simple steps: **Stop. Check. Reject.**

1

Stop.

Does a call, email, text or visit seem off? The best thing to do is stop. Take a breath. Real organisations won't put you under pressure to act instantly.

2

Check.

Ask someone you trust or contact the organisation the message claims to be from. If available, always use an authenticated platform to contact the organisation (for example: the CommBank app).

3

Reject.

If you're unsure, hang up on the caller, delete the email, block the phone number and change your passwords.

If someone has physically visited you, report them to the police.

Tip: Create a support team of people you trust. This might include close friends, family members, or peers. You can also contact CommBank securely for help through the CommBank app or by visiting your local branch.

Before you decide, think about who might be best for your circumstances.

If you think you've been scammed:

1. Stop all communications with the suspected scammer immediately
2. Change your passwords and card PINs
3. Lock your bank cards via the **CommBank app** or **NetBank**
4. Message us in the **CommBank app 24/7** or call us on **13 2221** as soon as possible. For accessibility support visit **commbank.com.au/accessibility**

If you or a senior you know is:

being pressured for money or personal information, you can call the **National Elder Abuse** phone line on **1800 ELDERHelp (1800 353 374).**

a victim of identify crime, contact **IDCARE (1800 595 160).**

Remember, you are not alone and we're here to help.