







Spot the red flags of remote access scams

Beat the scammers by knowing the scam

Remote access scams can give criminals access to your computer or mobile phone from anywhere, anytime. This can let them steal your information, transfer money out of your accounts, run up debts in your name, monitor your incoming and outgoing emails, and lock your computer files and demand a ransom to unlock them.

Our tips can help you safeguard your personal information and money.

Spot the red flags

-  **You receive a call or text you weren't expecting, or a strange pop-up message on your device.** Scammers will make contact out-of-the-blue, often pretending to be from an internet or phone provider, your bank, or the police.
-  **You're asked to download software.** They'll claim this will fix a problem on your computer or a fraud issue on your bank account. You might even be asked to pay for the software.
-  **Requests for your NAB Internet Banking log in details and security codes.** Never provide these details to a third party, even if they say they're calling from NAB – our authorisation text messages always say 'Don't share this code with anyone, even NAB'.
-  **You're asked to transfer money to a 'safe' account.** Scammers may claim there's fraud on your account and direct you to move your money – either online or by visiting a branch – to keep it safe. They might even say that branch staff are involved in the fraud and tell you to lie about why you're making a withdrawal. Remember, NAB will never ask you to transfer money to a safe account – it's safe where it is.

Did you know?

Multi-Factor Authentication (MFA) is quick and easy to set up on your banking, email and online accounts. It adds extra steps to confirm your identity when you log in, such as your password plus a one-time code. So if a criminal has your password, they'll need additional information known only by you to log in. Learn more at nab.com.au/mfa.



more
than
money



Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

If someone contacts you and asks for access to your devices to fix a problem, tells you to download software or instructs you to transfer money to a 'safe' account, **stop** communicating with them immediately and hang up.



Check before you share

If you're ever unsure if a message or phone call is legitimate, **check** the identity of the person contacting you before sharing any information. You can do this by calling the real organisation on their official, publicly-listed phone number.



Protect if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to **protect** your money and information, so if you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit nab.com.au/security.

For tips on protecting your business, visit nab.com.au/remotearchesscams

