AFP

JPC3
JOINT POLICING CYBERCRIME COORDINATION CENTRE

Bank impersonation scams edition

ClickFit

Stakeholder Kit — April 2026

Stop your scroll — Check with your bank — Protect your account

Contents:

Impersonation scams: Not your real bank

Bank impersonation scams are designed by criminals to create urgency and fear, so people make fast decisions before they have time to think. They use simple emotive tactics to pressure people to **"act fast because your money is at risk."**

Bank impersonation scams come in many forms, and criminals continue to evolve the tactic, contact, and request for money/ account details to deceive victims:

⚠️ **Tactic** *("unauthorised payment", "new payee", "account locked")*

📲 **Contact** *(SMS, phone call, email, social media)*

💳 **Request** *(bank/personal details, security or one-time passcodes (OTPs), passwords, remote access, transfers)*

Criminals do this by creating realistic emails, text messages and phone calls to impersonate banks and trusted organisations replicating their brand, tone, and messaging.

These scams are often urgent, alarming and highly believable — ***and that is exactly the point.***

Despite a stable belief in our ability to spot scams, those who 'always' check for phishing signs fell from 51% to 36% over the past five years.*

This is where *ClickFit* comes in.

To help Australians navigate their online banking safely, it's important they can recognise the warning signs of bank impersonation scams:

- Stop, think before you click
- Check with your bank directly
- Protect your codes & passwords
- Do not transfer money on request
- Secure your accounts
- Report immediately to bank

ClickFit will make it easier for Australians to steer clear of impersonation scams and keep their online banking on the right track.

* CybSafe. (2023). *Oh behave: The cybersecurity attitudes and behaviors report 2021–2025.*

What is *ClickFit:* Impersonation scams?

***ClickFit:* Impersonation Scams** is designed to get Australians to **stop** their scroll, **check** with their banks, and **protect** their accounts from cybercriminals.

Think of ***ClickFit*** as a road-safety campaign for digital banking: every online user is being urged to slow down, swerve around bank impersonation scams and stay one step ahead of cybercrime.

ClickFit: **Impersonation Scams** is a part of a 12-month national awareness campaign to encourage Australians to take simple steps to protect themselves online.

The campaign will launch on Monday 30 March and conclude in June 2026.

Are You Fit to *Click-Bank*?

ClickFit is a few steps that everyone can introduce into their online banking to help protect themselves from cybercriminals.

Get ready to click-bank in six simple steps:

STOP, THINK BEFORE YOU CLICK
If you get a call, text, or email from your "bank" pause before you act. Real banks won't rush or pressure you.

CHECK WITH YOUR BANK DIRECTLY
Don't trust unexpected contact. Contact your bank using their official app, website or number on your card.

PROTECT YOUR CODES AND PASSWORDS
Your bank will never ask you to disclose an OTP, password, or PIN over the phone.

DO NOT TRANSFER MONEY ON REQUEST
Banks will never ask you to move money to a "safe account". If asked - stop and contact your bank.

SECURE YOUR ACCOUNTS
Use strong passphrases and multi-factor authentication (MFA). Keep your devices updated.

REPORT IMMEDIATELY TO BANK
If something feels off - act fast. Report to your bank immediately. Have you lost money? Report to police at cyber.gov.au/report.

How to support *ClickFit:* Impersonation Scams?

Stakeholders can help Australians better protect themselves online by sharing ***ClickFit*** content across their channels and networks.

Distribute the campaign material (digital and print) through your social media, website, workplace, newsletters and community groups.

Campaign material include:

- Social media assets
- Factsheets & flyer
- 'ClickFit Scam Check'
- Stickers & graphics
- Newsletter copy

Download ClickFit: Impersonation Scams assets here

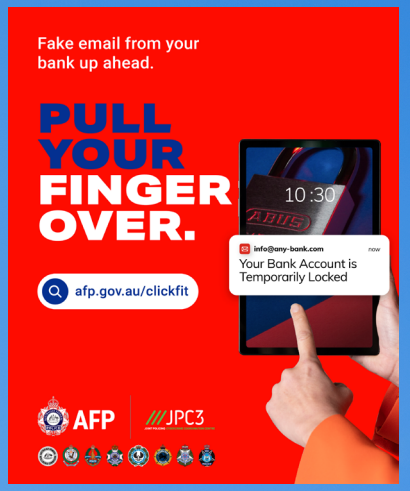
ClickFit: Social media assets

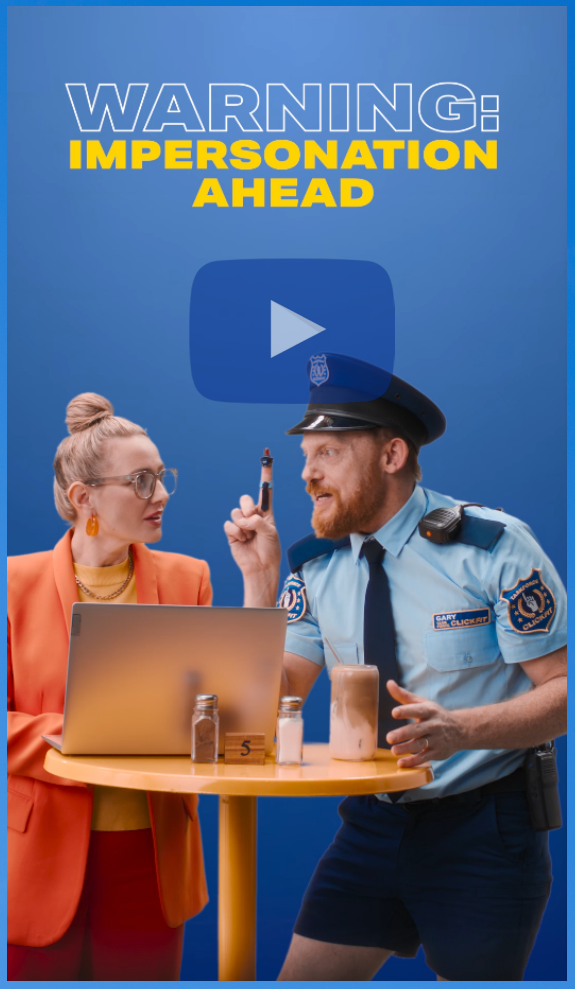
Cybercriminals pretend to be your bank, the police, or even a friend, all to steal your information or money.

If someone contacts you out of the blue and asks for payment or personal details, stop and double-check.

Only trust what you can verify yourself.

Get ClickFit at www.afp.gov.au/ClickFit





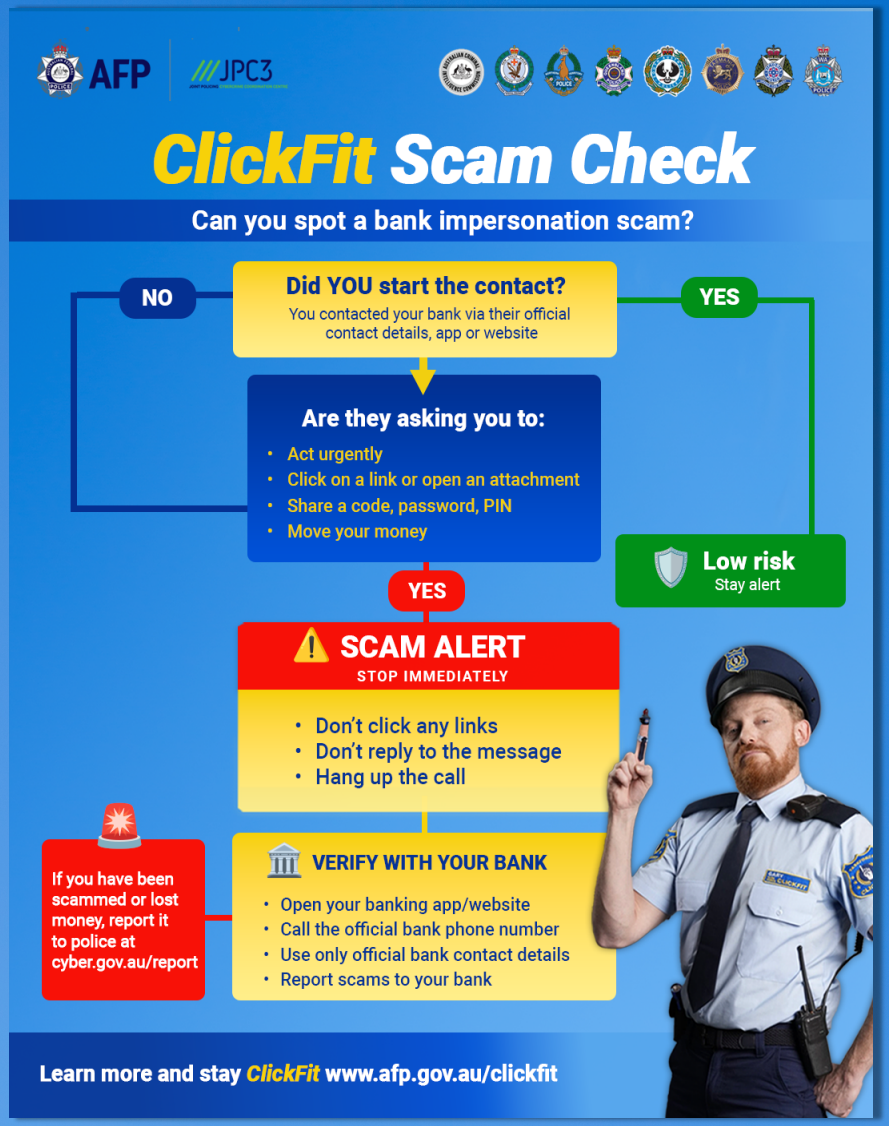
Share the campaign video or images across Facebook, Instagram, X (Twitter), YouTube, LinkedIn and TikTok, and get ready to ***Click-Bank***!
Don't forget to include ***#ClickFit*** in your posts and tag AFP with the following social media handles:

AusFedPolice ***ausfedpolice*** ***AusFedPolice*** ***AustFederalPolice*** ***Australian Federal Police***

ClickFit: Scam Check

***ClickFit* Scam Check** is a step-by-step chart designed to get people to stop, think and check whether a text, call or email from their bank is legitimate.

It will help people recognise the warning signs of bank impersonation scams and verify contact through their offical bank before taking immediate action.



ClickFit: Factsheets (Interactive + Print)

'Are You Fit to Click-Bank?' is a factsheet (print and interactive) and flyer, available via **www.afp.gov.au/clickfit.** The interactive version allows users to test the digital blind spots of impersonation scams and help protect themselves from cybercriminals.

Factsheet

Flyer

ClickFit: Newsletter copy

Campaign copy to use for agency/organisation newsletters. Please edit according to in-house style guides and character restrictions.

ClickFit: Are You Fit to Click-Bank?

ClickFit: Impersonation scams is designed to get Australians to stop their scroll, check with their bank, and protect their accounts from cybercriminals. Think of ClickFit as a road-safety campaign for digital banking: every online user is being urged to slow down, swerve around bank impersonation scams and stay one step ahead of cybercrime.

Why ClickFit Matters?
Bank impersonation scams are designed by criminals to create urgency and fear, so people make fast decisions before they have time to think. They use simple emotive tactics to pressure people to "**act fast because your money is at risk.**"

To help Australians navigate their online banking safely, it's important they can recognise the warning signs of bank impersonation scams. ClickFit will make it easier for Australians to steer clear of impersonation scams and keep their online banking on the right track.

Get Ready to Click-Bank in Six Steps:

- Stop, think before you click
- Check with your bank directly
- Protect your codes & passwords
- Do not transfer money on request
- Secure your accounts
- Report immediately to bank

Get Involved!
Visit www.afp.gov.au/clickfit to download resources and social media content. Share campaign assets, tag @AusFedPolice, and use #ClickFit to support the campaign. Stay ClickFit!

ClickFit: Additional assets

Additional campaign graphics and colours for website use, email signature blocks, stickers, newsletters or social media.

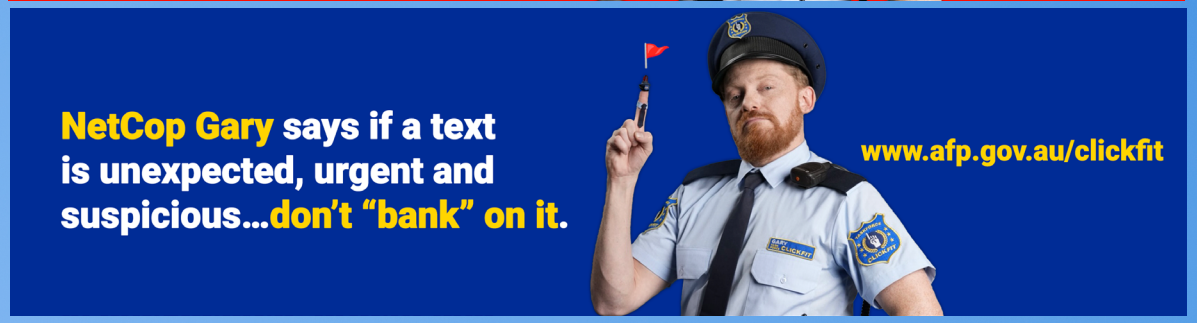
Suitable for email signatures and website banners

RED
HEX #FD0C00
R253 G12 B0
C0 M99 Y100 K0

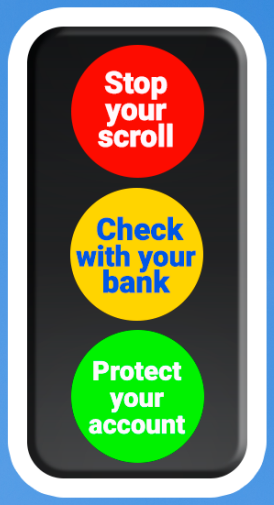
BLUE
HEX #043092
R4 G48 B146
C100 M92 Y10 K2

YELLOW
HEX #FDD302
R253 G211 B2
C2 M15 Y100 K0

ClickFit: Additional assets



Suitable for printing stickers



ClickFit: Scam-aware language

We urge stakeholders to use scam-aware language when promoting *ClickFit*.

Scamwatch has *'dos and don'ts'* to avoid victim-blaming language and focus on tactics used by criminals rather than the actions of those targeted.

Use ✅
Deceive
Manipulate
Victim of a scam
Scams are crimes/Scammers are criminals
Scam tactics
Scam methodologies
Stolen by scammers
Financial theft

Don't Use 🛑
Trick
Fool
Fooled by a scam / scammer
Fallen for a scam
Scammers are tricksters
Scam tricks
Lost to scammers
Gave to scammers
Handed over to scammers

The Joint Policing Cyber Coordination Centre (JPC3) comprises of state and territory police, government agencies, and industry partners, working together to combat, disrupt and prevent cybercrime in Australia.

For *ClickFit* questions please contact jpc3-prevention@afp.gov.au