



BEC scams edition

ClickFit

Stakeholder Kit — October 2026



Stop your scroll — Check before you pay — Protect your business

Contents:

**P3 Business Email
Compromise (BEC)**

P4 What is ClickFit?

P5 Get ClickFit

P6 Support ClickFit

P7 Social media

P8 ClickFit: BEC Safety Kit

P9 Factsheets

P10 Newsletter copy

P11 Additional assets

P14 Scam language



BEC: Fake email = real losses

Business Email Compromise (BEC) is a form of cybercrime where criminals impersonate trusted people or organisations to deceive victims into redirecting payments, transferring money or sharing sensitive information.

They often impersonate suppliers, customers, employees, senior executives, lawyers, conveyancers or trusted business partners and their goal is simple: **convince someone to transfer money to an offender-controlled account.**

A common tactic involves criminals gaining access to a legitimate email account and monitoring communications for weeks or even months. During this time, they gather valuable information about business operations, payment workflows and invoicing processes.

They **will strike at the right moment** by changing invoice payment instructions or bank account details to redirect a legitimate payment.

Common BEC warning signs include:

- Requests to change bank or payment details
- Minor changes to email addresses or domains
- Newly registered domains designed to resemble a legitimate business
- Emails that appear genuine because they originate from a compromised account
- Unsolicited follow-up calls confirming payment instructions
- Unprompted MFA or device logins
- Unfamiliar attachments or documents

Criminals often pressure people into acting quickly by:

- Claiming a payment is overdue, often before a weekend or public holiday
- Claiming urgent payment is required to avoid penalties or delays
- Imposing tight timeframes
- Requesting confidentiality to bypass approval processes
- Making follow-up calls that appear local or legitimate

The consequences of BEC scams can cause significant financial losses, operational disruption, recovery costs, reputational damage, loss of trust and emotional hardship.

Criminals will target any business regardless of its size. Any person or business involved in processing invoices or payments can be targeted.

This is why being **ClickFit** is so important to help Australians recognise BEC warning signs and protect their business from cybercriminals:

- Stop before you pay
- Check payment details carefully
- Protect against impersonation
- Verify before making payment
- Be alert to urgency
- Report immediately

What is *ClickFit*: **BEC**?

***ClickFit*: BEC** is designed to get Australians to **stop** their scroll, **check** before they pay and **protect** their business from cybercriminals.

Think of ***ClickFit*** as a road safety campaign for Australian businesses: whether you're a CEO, small business owner or sole trader, everyone is encouraged to slow down, steer clear of suspicious emails, and avoid fake payment hazards.

***ClickFit*: BEC** 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 1 October and conclude by December 2026.

P5

Get *ClickFit* before you **pay**:

ClickFit is a simple six step approach that helps businesses and employees identify BEC warning signs and verify payments before money is sent.

Check before you pay
in **six simple steps**:

STOP BEFORE YOU ACT

Pause before you action any invoice, email, payment request or bank detail changes. Criminals are counting on you to rush. Always double-check.

CHECK PAYMENT DETAILS CAREFULLY

Compare bank account details with previous invoices and be alert to changes in bank details, payment processes and email addresses.

PROTECT AGAINST IMPERSONATION

Watch for slight changes in email addresses or domains, unexpected emails, calls or shared documents, and unusual requests for payment.

VERIFY BEFORE MAKING PAYMENT

Always verify payment requests or changes to bank details using a trusted phone number or in person. Never use contact details provided in the email.

BE ALERT TO URGENCY

Be suspicious of urgent payment requests, demands for secrecy, or attempts to bypass normal approval processes. Criminals create pressure to stop you from checking.

REPORT IMMEDIATELY

If you have transferred money or something doesn't feel right, call your bank via their official contact, notify your IT team and report it to police through cyber.gov.au/report

How to support **ClickFit: BEC?**

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

Campaign materials can be distributed through your social media, website, newsletters, email signature, workplace communications, and community groups.

Campaign material include:

- Social media assets
- Factsheets & flyer
- ClickFit: BEC Safety Kit (for employers/employees)
- Stickers & graphics
- Newsletter copy

[Download ClickFit: BEC assets here](#)

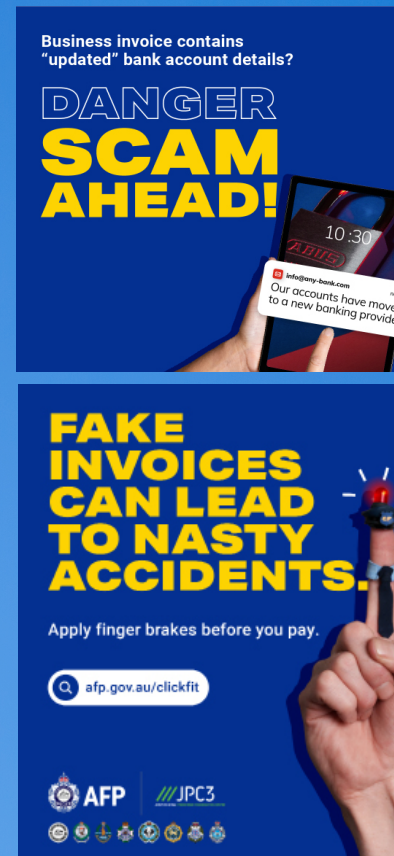
ClickFit: Social media assets

Cybercriminals will try and reroute legitimate payments straight into their own bank accounts by impersonating a business, supplier, coworker, or client.

They will pressure you with urgent or overdue deadlines (e.g. before a weekend or end of day), provide unusual instructions or ask you to update your personal or bank details.

Do not send money or provide any personal information. Always verify by calling or contacting the person or business via their official website.

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



Share the campaign across Facebook, Instagram, X (Twitter), YouTube, LinkedIn and TikTok.
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: BEC Safety Kit

The **ClickFit: BEC Safety Kit** helps Australians safeguard their business, staff and finances from Business Email Compromise (BEC). It includes practical guides for employers and employees, along with a BEC Bingo activity to build scam awareness and detection skills.

AFP JPC3

ClickFit BEC Safety Kit:

Employers / business owners / sole traders

Any business can be a target for business email compromise (BEC).



Protect Your Business

Put safeguards in place to prevent BEC:

- Establish clear payment verification processes
- Use Multi-Factor Authentication (MFA) across business systems
- Require strong, unique passphrases for all accounts
- Limit public information about your business and staff online
- Keep domain registrations current and consider registering similar domains
- Have a clear process for staff to report suspicious requests or activity.

Prepare Your Staff

Build the skills to spot and stop BEC:

- Recognise BEC warning signs
- Verify payment requests independently
- Check email addresses carefully for subtle changes
- Be cautious of unexpected links and attachments
- Think critically before acting on unusual, urgent, or confidential requests
- Know how and where to report suspicious emails or requests

Report immediately

- Did you make payment?** Contact your bank using official details
- Report to police** via cyber.gov.au/report
- Notify your IT** or cybersecurity team

Learn more and stay **ClickFit** www.afp.gov.au/clickfit

AFP JPC3

ClickFit BEC Safety Kit:

Employees / self-employed / freelancers

Any person or business involved in processing invoices or payments can become a business email compromise (BEC) target.



ClickFit is six simple steps to take before making a payment to help protect your workplace or business from cybercriminals:

- STOP BEFORE YOU ACT**
Pause before you action any invoice, email, payment request or bank detail changes. Criminals are counting on you to rush. Always double-check.
- CHECK PAYMENT DETAILS CAREFULLY**
Compare bank account details with previous invoices and be alert to changes in bank accounts/details, payment processes and email addresses.
- PROTECT AGAINST IMPERSONATION**
Watch for slight changes in email addresses or domains, unexpected emails, calls or shared documents, and unusual requests for payment.
- VERIFY BEFORE MAKING PAYMENT**
Always verify payment requests or changes to bank details using a trusted phone number or in person. Never use contact details provided in the email.
- BE ALERT TO URGENCY**
Be suspicious of urgent payment requests, demands for secrecy, or attempts to bypass normal approval processes. Criminals create pressure to stop you from checking.
- REPORT IMMEDIATELY**
If you have transferred money or something doesn't feel right, call your bank via their official contact, notify your IT team and report it to police through cyber.gov.au/report

Learn more and stay **ClickFit** www.afp.gov.au/clickfit

AFP JPC3

ClickFit BEC Bingo

Can you spot a business email compromise scam?

HOW TO PLAY

- Mark each warning sign you recognise
- Complete a row, column, or diagonal of red flags to get **BEC BINGO!**

New supplier account	Urgent payment request	Pressure to make same-day payment	Threats of delays or fines if payment is not received
Unexpected change to bank details	Slightly different email address	Unusual invoice amount, timing or supplier	Sender asks to keep payment confidential
Pressure to act immediately	Payment redirected to a different account	Unfamiliar link, document or attachment	Unexpected changes to bankroll or employee details
New contact details	Payment request outside of normal hours	Generic email greeting, 'hello customer'	Unexpected login to device or MFA

Report immediately

- Did you make payment?** Contact your bank using official details
- Report to police** via cyber.gov.au/report
- Notify your IT** or cybersecurity team

Stop your scroll. Check before you pay. Protect your business.

Learn more and stay **ClickFit** www.afp.gov.au/clickfit

ClickFit: Factsheets (Interactive + Print)

Are You ClickFit to Pay? 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 BEC scams and help protect themselves from cybercriminals.



Are You ClickFit to Pay?

Stop your scroll Check before you pay Protect your business

Do you independently verify changes to bank details before making payment? **YES** **NO**

Do you check for slight changes in email addresses or domains? **YES** **NO**

Do you confirm unusual payment requests via a trusted phone number? **YES** **NO**

Your Results

If you answered **NO** don't worry!
You can build stronger online business habits with ClickFit.

ClickFit takes **six simple steps** before you pay to protect your business from cybercriminals.

Factsheet



Get ClickFit in six steps before you pay:

- 1 Stop before you act
- 2 Check payment details carefully
- 3 Protect against impersonation
- 4 Verify before making payment
- 5 Be alert to urgency
- 6 Report immediately

Click the digital BEC blind spots

Lookalike email address

Urgent request for payment

Generic greeting ('Customer')

New bank details

Stop your scroll!

Check before you pay

Protect your business

Learn more and stay ClickFit www.afp.gov.au/clickfit



Are You ClickFit to Pay?

ClickFit takes **six simple steps** to help protect your business from cybercriminals

- 1 Stop before you act
- 2 Check payment details carefully
- 3 Protect against impersonation
- 4 Verify before making payment
- 5 Be alert to urgency
- 6 Report immediately

Learn more and stay ClickFit www.afp.gov.au/clickfit

Flyer

ClickFit: Newsletter copy

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

Are You ClickFit to Pay?

ClickFit: BEC is designed to get Australians to stop their scroll, check before they pay and protect their business from cybercriminals. Think of **ClickFit** as a road safety campaign for Australian businesses: whether you're a CEO, small business owner or sole trader, everyone is encouraged to slow down, steer clear of suspicious emails, and avoid fake payment hazards.

Why ClickFit Matters?

Business Email Compromise (BEC) is a form of cybercrime where criminals impersonate trusted people or organisations to deceive victims into redirecting payments, transferring money or sharing sensitive information. Criminals will target any business regardless of its size. Any person or business involved in processing invoices or payments can become a victim.

This is why being **ClickFit** is so important to help Australians recognise BEC warning signs and protect their business from cybercriminals.

Get ClickFit in Six Steps:

- Stop before you pay
- Check payment details carefully
- Protect against impersonation
- Verify before making payment
- Be alert to urgency
- Report immediately

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!

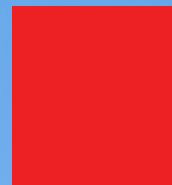
ClickFit: Additional assets

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

New bank details?
NetCop Gary says pick up
the phone not the payment.



www.afp.gov.au/clickfit

NetCop Gary says don't
let one fake invoice cost
you your business.



www.afp.gov.au/clickfit

Don't let cybercriminals
redirect your payment. Take
control, verify before you pay.

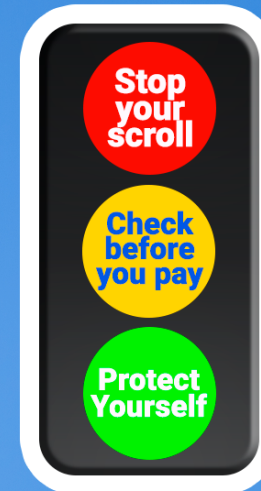


www.afp.gov.au/clickfit

Are you ClickFit
to pay?



I'm ClickFit
to pay.



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 	Don't Use 
Deceive	Trick
Manipulate	Fool
Victim of a scam	Fooled by a scam / scammer
Scams are crimes/Scammers are criminals	Fallen for a scam
Scam tactics	Scammers are tricksters
Scam methodologies	Scam tricks
Stolen by scammers	Lost to scammers
Financial theft	Gave to scammers
	Handed over to scammers



AFP



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