

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:

1 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.

2 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.

3 PROTECT AGAINST IMPERSONATION

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

4 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.

5 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.

6 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

