AFP | JPC3 JOINT POLICING CYBERCRIME COORDINATION CENTRE

Combatting cybercrime through collaboration

Cybercrime Alert

Cybercriminals impersonate conveyancers to target Australian property buyers in 'settlement-scam'

4 February 2026

The AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) is issuing an urgent warning following increased reports of criminals impersonating Australian conveyancer emails to target and scam property buyers.

What is a BEC Scam?

A Business Email Compromise (BEC) scam involves cybercriminals impersonating a business email or an employee's email to deceive victims into redirecting legitimate payments to fraudulent accounts.

Why conveyancers?

Criminals are actively targeting Australians involved in property transactions by impersonating conveyancer firms or employees' using spoofed or compromised email accounts.

- Spoofed emails – scammers create emails that look legitimate e.g. accounts@ozzieconveyancer.com.au (legitimate) vs accounts@ozzieconveyancer.com (spoofed).
- Compromised email accounts – cybercriminals have gained unauthorised access to the business email account or an employee's email account, allowing them full access to read/send emails, intercept financial information, reset passwords or steal data.

The scam is designed to intercept legitimate property communications and redirect settlement funds to criminal-controlled bank accounts, often during the final stage of purchasing a property when pressure and urgency is high.

The property transactions usually involve multiple large sums of money, making buyers a prime target for cybercriminals.

The trend:

- Reports of the scam through ReportCyber began increasing in December 2025.
- Victims have reported an email from their "conveyancer firm" or "settlement officer" during the final stages of purchasing a property.
- The scammer is spoofing email addresses and impersonating employees from conveyancer firms.
- The scammer requests the victim send the deposit for their purchase to a bank account controlled by criminals.
- The types of property transactions requested by the scammer include full settlement, deposit or partial settlement, and pre purchase building inspections.
- The victim will send either a deposit or the full amount in multiple transactions.
- In most cases, banks or financial institutions alert victims that a transaction is suspicious and block it. However, this is usually by the second or third transaction.

Indicators of a convincing spoofed email:

- An 's' or 'au' is either added or removed from the legitimate email address:
  - **Real email:** info@helpingbuyhomes.com **Spoofed address:** info@helpingbuyhomes.com.au
  - **Real email:** example@conveyancers.com **Spoofed address:** example@conveyancer.com
- The email signature includes the conveyancer firm's branding or employee's photo to look legitimate.

What you can do:

- **Report suspicious activity** to police via ReportCyber at cyber.gov.au/report
- **Visit the small business hub** - Follow the 'how to' guides to protect your business and learn how to recover after a cyber incident.

What to advise your clients to do:

- **Verify payment requests** by calling the conveyancer firm or settlement officer directly via their phone number on the official company website – not the phone number in the email signature.
- **Do not reply to the email or click on links** if it looks suspicious, it is likely a scam.
- **Contact your financial institution immediately** if you believe you've made an incorrect payment**.**
- **Report suspicious activity** to police via ReportCyber at cyber.gov.au/report
- **Get ClickFit** – improve your cyber safety awareness and stay alert to emerging scams by getting ClickFit at afp.gov.au/clickfit

The AFP-led JPC3 brings together the powers, experience, investigative and intelligence capabilities of all Australian policing jurisdictions and key international law enforcement and industry partners. It identifies organised cybercriminals targeting Australia, disrupts their criminal activities and prevents further harm and financial loss to the Australian community.