AFP | JPC3 JOINT POLICING CYBERCRIME COORDINATION CENTRE

Combatting cybercrime through collaboration

Cybercrime Alert

Surge in BEC Scams Targeting Australia's Construction Sector

25 September 2025

The AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) is issuing a critical warning following a sharp rise in Business Email Compromise (BEC) attacks aimed at the construction industry.

What is a BEC Scam?

A Business Email Compromise (BEC) scam involves cybercriminals impersonating a business or its employees via email to deceive victims into redirecting legitimate payments to fraudulent accounts.

Why Construction?

The construction industry is a prime target due to its high-value transactions, frequent invoicing, and often limited cybersecurity resources – especially among small, family-run businesses. Many operators lack dedicated finance teams and are time-poor, making them vulnerable to sophisticated scams that exploit trust and urgency.

How These Scams Work

Criminals are deploying highly targeted and socially engineered attacks using two main tactics:

- **Tender Surveillance**: Threat actors monitor publicly listed government tenders, which often reveal contract details, awardees, project scope, and payment amounts.
- **Invoice Impersonation**: Criminals pose as legitimate suppliers and impersonate known companies.

Criminals will then send fraudulent invoices to government agencies or building contractors, embedding their own bank details. To boost credibility, they may call ahead, impersonating finance staff and claiming the invoice is overdue, pressuring the recipient to act quickly. Once the payment is made, the funds are deposited into criminal-controlled accounts, which are often based overseas and unrecoverable.

The Sophistication Behind the Scam

These attacks use advanced social engineering, real-time surveillance, and psychological manipulation to bypass even cautious targets. They mimic tone, formatting, and internal processes with alarming precision, sometimes even referencing previous legitimate communications which criminals may have intercepted.

How to Protect Yourself

To defend against BEC scams, follow these best practices:

- **Verify payment requests** through a trusted contact, not via phone numbers or emails listed in the invoice. Even if the request comes from the business' "finance team," confirm directly with your trusted contact.
- **Implement ACSC's Essential Eight** mitigation strategies to strengthen your cyber posture.
- **Contact your financial institution immediately** if you believe you've made an incorrect payment.
- **Report suspicious activity** to police via ReportCyber.

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.