Have a conversation with your team about scams

Scammers can target businesses of all sizes. They often impersonate trusted suppliers, customers or colleagues to try and steal money or sensitive information.

Having regular conversations with your team about scams can help your business recognise warning signs and know what to do if something doesn't seem right.

Common scams targeting businesses and how to help start the conversation

Invoice and payment redirection scams

Scammers impersonate a supplier and request a change to bank or payment details - often just before an invoice is due.

Conversation starters:

"If a supplier asked us to update their bank details, how would we verify it's genuine?"

"When was the last time we reviewed our supplier payment details, and who's responsible for approving changes?"

Business Email Compromise (BEC)

Scammers pose as a leader, colleague, supplier or customer to request an urgent payment, gift cards or sensitive information.

Conversation starters:

"If an urgent payment request came in, what should we do before actioning it?"

"If a colleague suddenly asked us to buy gift cards or make an urgent transfer, what would raise a red flag?"

Phishing and impersonation scams

Fake emails, texts, calls or websites pretending to be a trusted organisation, like your bank, the ATO or a tech or utility provider, designed to steal logins or business data.

Conversation starters:

"How do we check whether a message from a 'trusted' brand is legitimate?"

"If someone in the team clicked a suspicious link by mistake, what should they do next and who should they tell?"

Business scam prevention checklist

This checklist can help to protect your business against some common scams.

STOP Pause before acting on unexpected requests.	✓ Treat urgent payment requests or changes to payment details with caution. ✓ Question anything that feels unusual or out of the ordinary. ✓ If unsure, know who to contact internally for a quick check.
CHECK Verify before making a payment or sharing information.	✓ Confirm payment detail changes by calling the supplier on a trusted number you've used before — never rely on email alone. ✓ Apply extra checks and dual approvals for large or unusual payments. ✓ Check for signs of phishing - unexpected links, urgency, or unusual requests. ✓ Use multi-factor authentication where available.
REJECT If something doesn't feel right, don't proceed.	✓ Never click suspicious links or open unexpected attachments. ✓ Don't share passwords, PINs, MFA codes or sensitive information. ✓ Stop the process if you suspect a scam at any point. ✓ Report and escalate concerns immediately.

What to do if you or your business has been scammed

- Stop all communications with the suspected scammer immediately.
- Change passwords, PINs and lock cards in the CommBank app or NetBank.
- Contact us on 13 1998 and select option 4 as soon as possible, or message us securely in the CommBank app 24/7.

CommBank is committed to helping keep our customers safe from scams and fraud.

More resources are available at **commbank.com.au/scam-tips**

CommBank Safe

Commonwealth Bank of Australia ABN 48 123 123 124 AFSL and Australian credit licence 234945.

CBA6456 070325