







Spot the red flags of invoice scams

Beat the scam by knowing the red flags

Criminals are impersonating businesses and organisations, sending fake invoices and payment details to unsuspecting customers. They're often able to do this by accessing the email accounts of businesses (known as Business Email Compromise).

Use our tips to learn how to protect your money and personal information.

Spot the red flags

-  **You're asked to click on a link, scan a QR code or download an attachment.** This is how criminals take over business email accounts, so be alert to these requests if you work for a business. It's a way for them to infect your device with a virus or direct you to a website that steals your usernames and passwords.
-  **Changes to payment details.** If a person or business tells you they have new account details for payments, it could be a sign that their email account has been taken over by criminals.
-  **You're asked for your usernames and passwords.** Never share these details with anyone. Remember, NAB will never ask for your log in details or to log in to your banking via a link or QR code.
-  **Requests to transfer money for a colleague.** If you work for a company or business, scammers may impersonate a colleague, usually someone more senior, asking for a funds transfer to be made on their behalf. Once this happens, it can be very hard to get the money back.

Tips for businesses

- Ask your customers to pay via your PayID or BPay Biller Code. This can help your customers avoid a scam impersonating your business.
- Ask new suppliers for their PayID, BPay Biller Code or ask to use e-invoicing. PayID allows you to see the legal name of the person or business you're paying before you confirm the transaction.
- Turn on Multi-Factor Authentication (MFA) for your email account. This adds extra steps to confirm your identity when you log in, such as your password plus a one-time code. So if a criminal has your password, they'll need additional information known only by you to log in. Learn more at nab.com.au/mfa.



more
than
money



Stop, Check, Protect

to minimise your chance of being impacted by a scam



Stop before you act

If someone sends you a link, QR code or attachment – even if it looks like they're from someone you trust – **stop** to consider, could this be a scam?



Check before you share

If you receive an email from a business with new bank account details, an invoice with updated payment instructions, or you're making a large payment to someone new for the first time, **check** the details are correct. You can do this by calling the company on their publicly-listed number or a number you already have. Don't rely on the contact details on the invoice or email, as they may have been altered by criminals.



Protect if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to **protect** your money and information, so if you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit nab.com.au/security. Business customers can visit nab.com.au/emailscams for tips on protecting your business.

