Keep your business safe:
Know who you're paying

Scammers catch us all off guard. They don't target one group over another.

Scammers may impersonate your business, contact your customers and provide false payment details.

This results in payments being made to an account controlled by the scammer.

When this happens, it's often very difficult for you, or your customers, to get money back.

PayID, BPay and e-invoicing will show who you're paying - before you pay.

How can scammers compromise your business emails?

Imitate an email account or website (spoofing)
Slight variations on legitimate addresses (john.smith@yourcom.com.au vs. john.smith@yourecom.com.au) trick customers into thinking fake accounts are authentic and following instructions in the email to pay funds into a different account controlled by the scammer.

Send phishing emails
These messages look like they're sent from a trusted sender to trick victims into revealing login details and passwords, allowing scammers access to your email account or IT systems. Scammers then issue legitimate invoices with the scammer's account details rather than your details.

Use malware
Malicious software can infiltrate your IT systems and allows a scammer to intercept and issue legitimate invoices inserting the scammer's account details rather than your details.

Australian Government | Australian Small Business and Family Enterprise Ombudsman | COSBOA Council of Small Business Organisations Australia | Australian Banking Association

How to protect yourself from business email compromise

For a new supplier, ask them directly for their BPay biller code, PayID, or ask to use e-invoicing.

For existing suppliers, only use the payment details stored in your records or system that you have confirmed in the past.

If you get a request to change payment details, call the supplier using the number from your records or from their website to verify the new details.

When you are asking customers for payment, ask them to pay to your PayID or BPay biller code wherever possible. This can help your customers avoid a scam impersonating your business.

Turn on multi-factor authentication to protect your email account. This provides an extra layer of security to your email account to prevent unauthorised access.

What is Multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is a security measure that requires two or more forms of identity to grant you access.

Multi-factor authentication typically requires a combination of something the user knows (pin, secret question), something you have (card, token) or something you are (finger print or other biometric).
Businesses should implement MFA wherever possible. Some MFA options include, but are not limited to:

- Physical token
- Random pin
- Biometrics / fingerprint
- Authenticator app
- Email
- SMS

Visit cyber.gov.au/mfa for more information, and more ways to protect your business.

Important note: This fact sheet gives information of a general nature and is not intended to be relied on by you as advice in any particular matter. You should contact your bank on how this information may apply to your circumstances.