Video transcript – Business email compromise scams

[Female voice over]

When it comes to the emails you receive, everything isn't always as it seems.

Targeting businesses of all sizes, business email compromise scams are rampant, amounting to billions of dollars of losses globally.

Using emails that are made to look like they are from someone you know like your boss, your supplier or your customer, these scams ask for a payment to be made to a fraudulent account.

A quick phone call could prevent your business from being scammed out of thousands of dollars, so here are two common examples of this scam you need to be able to spot and protect against.

Supplier email scams occur when a fraudulent request for payment looks like a legitimate expected invoice, or it could be a fake email requesting you update a supplier's payment details for future payments.

Scammers can also masquerade as your boss, emailing a request to make an urgent or confidential payment, often in a way that's different from your usual process.

So what can you do to avoid being caught by one of these scams?

You can start by dead-bolting the doors to your email accounts by using strong and unique passwords for each account, and enabling two-factor authentication where available.

Then, establish a clear payment approval process that involves multiple approvers.

Most importantly, remember to always pause before you pay, especially when making payments to new accounts - even if the request comes from your boss.

Verify payment requests received by email by calling a trusted number from the supplier or customer's website, or speaking to the requestor in person, to confirm the details are correct before creating the payment.

Questioning the legitimacy of a payment request could save your business thousands of dollars.

If you think you may have been scammed, contact Bankwest immediately, then make sure you reset your passwords and enable two-factor authentication on your email accounts.

Learn more at bankwest.com.au/security-centre