

 **STOP. THINK. DON'T CLICK.**

Phishing Awareness:

How to Spot a Scam Before It's Too Late

Phishing is when cybercriminals trick you into giving away sensitive information – like passwords or credit card numbers – by pretending to be someone you trust. Here are some common signs of a Phishing Email:

1

Urgent or threatening language

"Your account will be locked!" "Action required immediately!"

2

Suspicious links or attachments

The link may look legit, but hovering reveals a strange or misspelled address.

3

Unfamiliar sender or unexpected request

Would your manager really ask you to buy gift cards via email? Always verify.

4

Poor spelling or grammar

Professional organisations rarely send out sloppy emails.

5

Too good to be true

You didn't enter a competition - but you've won a prize? Be cautious.

Over 90% of cyber attacks begin with a phishing email. That's why it's essential to stay vigilant.

Even one wrong click can open the door to malware, data loss, or fraud.

Staying alert protects you and your whole organisation.


Tips to Stay Safe

- **Pause and think** before clicking links or downloading attachments.
- Check the **sender's email address** - does it look legitimate?
- **Hover over links** to preview the URL before clicking.
- **Report anything suspicious** to our Service Desk.
- **Never share passwords** or login details via email.


Got a suspicious email?

Don't click – report it to:

support@businessworks.com.au

 **1300 732 810**

 **info@businessworks.com.au**

 **www.businessworks.com.au**