PHISHING QUICK REFERENCE

Report suspicious activity immediately to David or Jason	
Phone: 03 9038 8188	Email: helpdesk@youritcrew.com.au

1. Is this a Phishing Attack?

Most common indicators include:

- Unexpected emails requesting personal information, passwords, or financial details.
- Emails with urgent requests for immediate action or threats of consequences.
- Hyperlinks that seem legitimate but redirect to suspicious or unrelated websites.
- Attachments that you were not expecting, especially if they come from unknown senders.
- Emails from seemingly trusted sources with odd grammar or spelling mistakes.

2. Avoid engaging with the suspicious email

If you suspect an email is a phishing attempt, take the following steps:

a) **Do Not Click Links or Open Attachments:** Any interaction with malicious content can lead to further compromise.
b) **Do Not Reply or Forward to Other Employees:** Refrain from engaging with the email sender, as it may confirm your email is active to attackers.
c) **Hover Over Links:** Without clicking, hover your mouse over links to verify their destination.

3. Verify the Sender's Identity

Check the sender's email address for inconsistencies:

- Is it spelled correctly, or does it mimic a legitimate address?
- Does the email domain match the company it's claiming to represent?
- Contact the person or organization directly using a known, trusted communication method to confirm the legitimacy of the message.

4. Report and delete the Phishing email

Immediately forward any suspicious email to the Your IT Crew helpdesk@youritcrew.com.au for analysis and then delete the email to prevent accidental interaction.

If you use Inbox Defender, the email & Outlook can be used to train the app to prevent spam to others in the organization.

It's important to stay vigilant

- Always thoroughly check messages and emails you receive
- Always question unsolicited requests for sensitive information.
- Avoid links that ask you to log in or reset your password
- Be extra cautious with emails containing urgent requests or threats.
- Use complex & unique passwords, stored securely in a password manager.
- Turn on multi-factor authentication

YOUR IT CREW