MEMO: SPOOF EMAIL AWARENESS

To: All Staff
From: IT
Date: 13/5/26
Effective From: Immediately
Attachments: NONE

Summary

Due to an increase in SPAM and spoof emails attempting to impersonate employees, internal email addresses, and retailers, all staff are reminded to remain vigilant when reviewing incoming emails.

These messages may appear legitimate at first glance, but often use misleading display names or compromised email accounts to trick recipients into responding or clicking unsafe links.

Below is an example of an email purporting to be from Michael Mackin to Michael Ostroburski with a fake Gmail email address. This was sent to both Michael O's work and personal email address.

Key Points:

- Staff must always check the actual sender email address, not just the displayed "From" name, as spoof emails may use familiar names while being sent from unrelated or invalid addresses.
- If there is any doubt about whether an email is genuine, staff should contact the purported sender directly where possible, using a known and trusted contact method.
- Staff may also contact itsupport@assemblynow.com.au for assistance with suspicious emails.
- Never click a link unless the sender is trusted and the link was expected.

- If a link is unexpected, it must be verified before clicking, as legitimate email accounts can be compromised and used by bad actors to send malicious emails from real addresses.
- Vigilance and caution from all staff is essential in reducing security risks across the business.

Ways to stay safe:

1. Checking Sender Details:
   - Review the **full sender email address** before taking any action.
   - Do not rely solely on the sender name shown in the "From" field.
   - Be cautious of addresses that imitate staff names, company contacts, or retailers but do not match legitimate domains.

2. Verifying Suspicious Emails:
   - If an email seems unusual, unexpected, or out of character, verify it before replying or clicking any links.
   - **Contact the sender directly using a known phone number, previous email thread, or other trusted contact method.**
   - If direct contact is not possible, forward the email to IT Support for review.

3. Handling Links and Attachments:
   - Never click a link or open attachments **unless you are expecting to receive a link or attachments from the sender** *and* you trust the sender.
   - Do not open attachments from suspicious or unverified emails.
   - Remember that even legitimate-looking emails may be unsafe if the sender's account has been compromised.

4. Reporting Concerns:
   - Report suspicious emails to itsupport@assemblynow.com.au as soon as possible.
   - Prompt reporting helps reduce the risk of broader security incidents affecting other staff or systems.

Additional Help and Support

For assistance with suspicious emails or other IT security concerns, contact itsupport@assemblynow.com.au.