Cyber Security NSW

HEIGHTENED RISK OF PHISHING ATTACKS

The NSW Government has been advised by the Australian Cyber Security Centre (ACSC) that there is currently a heightened risk of phishing attacks. This relates to a current national phishing campaign known as **Emotet**.

WHAT YOU SHOULD LOOK FOR:

Emotet phishing emails can masquerade as a legitimate email correspondence by **reusing victims' contact lists and previous email correspondence**. These emails appear to come from the known or trusted person. However, when you preview the email in outlook, you will see that the sender's email address will not be the legitimate sender's email address.

- Phishing emails re-use of a victim's previous email correspondence and subject lines. These are recognisable as they will contain a generic email message asking the user to open or examine the attached document, but **the message may appear misaligned with the email's flow of conversation**.
- Emails may be an **out of sequence response, an unrelated reply or a forward of an old email conversation**. The email may have an attached malicious word or PDF document and will come from an email address that may not be the legitimate contact's email address.

Phishing emails often include malicious documents with a wide range of topics to lure victims into opening the file or link enclosed.

Be aware of any emails with the following types of attachment names:

- **MAIL**_[random numbers and letters].doc
- **ATO_Tax_payment**_[current date].doc
- **Comments**_[random numbers and letters].doc
- **DETAILS**-[current date].doc
- **INFO**_[current date].doc

HOW TO KEEP YOURSELF SECURE:

- If you have received a suspicious email, or other suspicious email from a contact or a vendor, **DO NOT** open the attachment. Speak to your IT security team first and only forward them the email if they request it.
- **DO NOT** attempt to contact the sender of the email, either by replying to the email or any other means.
- **DO NOT** forward the email to others who do not have a need to see it. This includes your personal email address.
- If you have forwarded the email to any other party, the ACSC requests that you inform the recipients and advise them to delete it. Please also advise your IT security section of those email addresses. If it was sent to your personal email address, delete it at the first available opportunity.

If you see any of the above –
report this to your IT security team immediately

NSW GOVERNMENT