PHISHING ATTACKS AND HOW TO PROTECT AGAINST THEM

INTRODUCTION

A growing number of data breaches involve employees of Victorian Public Sector (**VPS**) organisations experiencing phishing attacks. This resource explains what phishing attacks are; how to identify them; and steps VPS organisations and employees can take to protect themselves.

WHAT IS PHISHING?

Phishing is a type of scam. It involves scammers sending communication (usually email but may also be a phone call or SMS) disguised as being from a trusted sender in order to steal confidential information or to make it unavailable.

In the VPS, phishing attacks often involve an employee receiving a scam email containing a hyperlink or an attachment. Where the employee clicks on the link or opens the attachment, they are typically taken to a website where malicious software is installed on their device or they are asked to provide confidential information (such as a username and password). The scammer will then often try to gain access to the employee's device and accounts.

These phishing emails are often designed to look genuine by copying the format used by the organisation or individual that the scammer is disguised as. In some instances, the phishing emails have even been sent from another VPS employee's email address where that employee has had their email account compromised.

Where a scammer gains access to your information through phishing, they will often use it to carry out further fraudulent activities. The scammer may:

- attempt to gain access to information you hold on your device;
- steal money from you or others at the organisation you work for; or
- attempt to use your email to send further phishing attempts to your contacts, possibly while masquerading as you.

Below are two examples of the phishing attempts which highlight the various methods scammers use and the potential impact they could have.

Example 1

Robert and Jennifer both work at Victorian Water, a VPS organisation. Robert received an email which appeared to have been sent from Jennifer's Victorian Water email address.

The email stated: "Hey Robert, click here to view the financial statements for the year." Robert clicked the link which took him to a website, where he was asked to enter his Victorian Water Office365 username and password to view the document.

In this example, the scammer had already compromised Jennifer's Victorian Water Office365 account allowing them to send further phishing attempts disguised as being from Jennifer.

The link in the email that Robert clicked sent him to an illegitimate website setup by the scammer. By Robert entering his Victorian Water Office365 username and password, the scammer was able to steal this information.

The scammer then used this information to login to Robert's Victorian Water Office365 account; view all of the documents he has access to; and send further phishing emails from Robert's Victorian Water email address, perpetuating the scam.

Example 2

Robert works at Victorian Water, a VPS organisation. Robert received an email which claimed to be from a local that he frequently deals with.

The email included a PDF attachment but no text. Robert was curious to see what was in the PDF, so he opened the PDF. This caused a malicious program to be installed on Robert's PC.

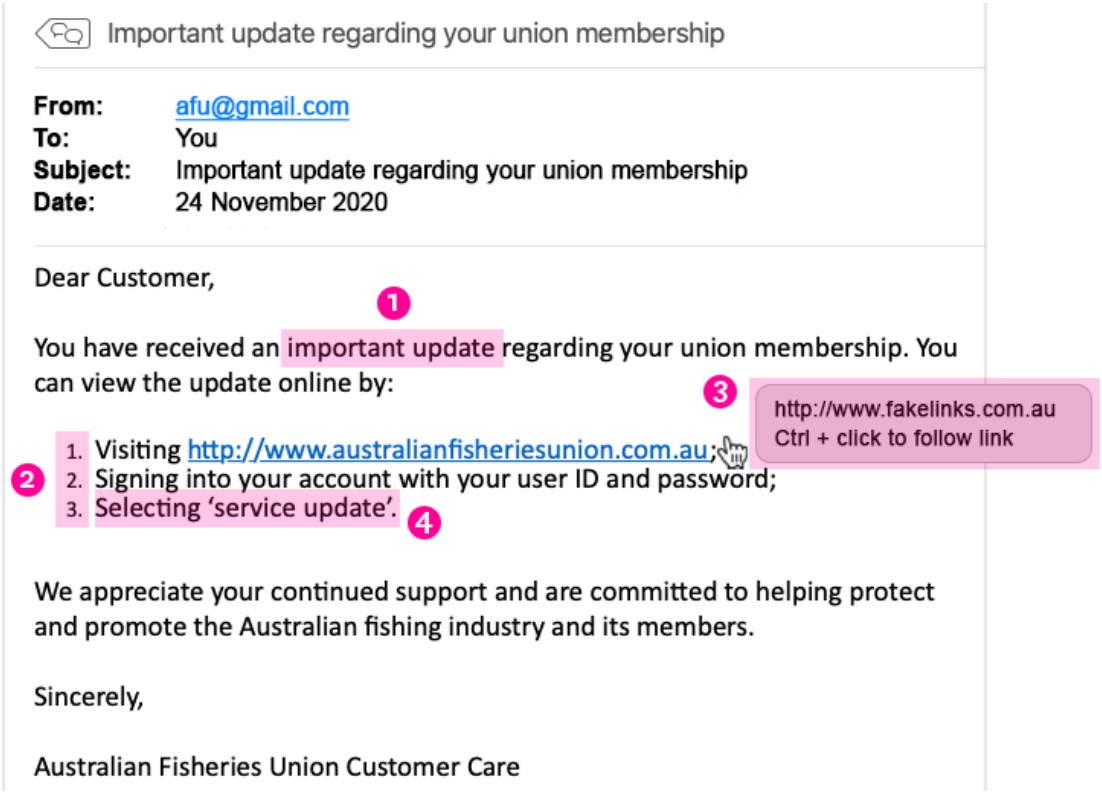
The malicious program created a rule in Robert's Outlook email client, which forwarded to the scammer, emails in Robert's email account, with key words such as 'invoice' or 'credit card.'

Robert was unaware of this rule, and so it went unnoticed for a period of 3 months. During the 3 months, the rule sent over 300 emails from Robert's email account to the scammer.

The emails contained financial information belonging to Victorian Water's customers, which the scammer could try to further exploit.

HOW CAN YOU IDENTIFY A PHISHING ATTEMPT?

The below example illustrates some common signs that a communication is a phishing attempt.



1. **It is unexpected or creates a sense of urgency for you to do something –** This might be by sending you an email that is unexpected so you don't know how to react (e.g. telling you that you have received a missed call and sending you to a website to hear it) or by creating a sense of urgency so that you don't have time to think about how to react (e.g. telling you that one of your accounts is about to be terminated unless you act quickly). In the example above, the scammer uses the wording 'important update' to create a sense of urgency for you to click on the link they have provided.

2. **It asks you to click a link, open an attachment or sends you to a website which asks you to enter your information –** For the phishing attempt to be successful, the scammer needs you to perform an action. In the example above, the scammer asks recipients to click on a link and enter their union username and password combination.

3. **The link suggests that it will take you to a legitimate website but, when you hover over the link, it shows that it is actually for a different website –** In the example above, the link appears legitimate, sending recipients to www.australianfisheriesunion.com.au. However, recipients who hover over the link will see that if they click on it, it will actually send them to a different website at www.fakelinks.com.au.

4. **It asks for information that the real or legitimate sender would not necessarily need to know** – In the example above, the scammer would send the recipient to a fake website where they would ask them to enter their real username and password combination that the recipient uses for their union membership.

WHAT STEPS CAN VPS ORGANISATIONS TAKE TO PROTECT AGAINST PHISHING ATTACKS?

- **Include security awareness in your organisation's culture.**
  By raising awareness of the signs and dangers of phishing attacks, VPS employees will be able to identify them; be less likely to fall for them; or at least be able to flag an issue and report it to you so you can take timely steps to contain the incident.

- **Use spam filters or secure email gateways to block deceptive emails from reaching VPS employees.**
  Spam filters and secure email gateways monitor incoming emails for unwanted or fraudulent content. Once identified, they prevent them from ever reaching a VPS employee's inbox.

- **Enable multifactor authentication (MFA) and anomaly login policies.**
  Even if an employee provides information to a scammer, these measures decrease a scammer's ability to gain access to the employee's work account and increase your ability to detect and respond to incidents in a timely manner.

- **Report phishing attempts to CIRS and OVIC.**
  You should report phishing attempts to the Victorian Government Cyber Incident Response Service by emailing cybersecurity@dpc.vic.gov.au who can help you respond to the incident.

  You should also report security incidents to OVIC by emailing a copy of our incident notification form to incidents@ovic.vic.gov.au or contacting us at privacy@ovic.vic.gov.au for privacy advice.

WHAT STEPS CAN VPS EMPLOYEES TAKE TO PROTECT AGAINST PHISHING ATTACKS?

- **Watch out for fake links or attachments.**
  Where you suspect an email to be a phishing attempt, contact your IT team. Do not open any attachments, click any links or forward the email to another device.

- **Do not provide information to unverified sources.**
  If you are unsure about whether you should be providing your information, check with your Privacy Officer or IT team. If the email is from someone familiar but the contents appears surprising or suspicious, contact them on the phone number you already hold to verify if they actually sent it.

- **If you receive a phishing email, notify your IT department.**
  If you think you have fallen for a phishing attempt or notice suspicious activity on your device, immediately disconnect from the internet and notify your IT team. Do not shut down or restart your device.

Disclaimer: The information in this document is general in nature and does not constitute legal advice.