GO PHISH!

We all know about Phishing scams and of course it's good to have a reminder on how to remain vigilant. But are you also aware of the other hacker hobbies of Spear-Phishing, Whaling, Smishing and Vishing?

PHISHING VS SPEAR-PHISHING

Phishing and spear phishing share similar techniques in that they wish the target to open an attachment or click on a malicious link. However, Phishing is on a large scale with the hope that a small percentage of email attacks will be successful and once information such as bank account details are stolen the attack is usually complete.

Spear-phishing is a targeted version of phishing whereby the fraudulent emails target specific organisations and the theft of personal information is then used to gain access to the target network. Additional spear-phishing tactics include impersonation and targeting specific employees using social media information garnered from Twitter, Facebook or LinkedIn to customise the email for specific individuals which adds authenticity.

WHALING:

Whaling attacks are so called because of the size of the target - meaning these attacks are aimed at high-ranking senior managers within a company. Both spear-phishing and whaling take much more time and effort to execute than the broader phishing attack because the attackers strive to make the emails seems as legitimate as possible through their social media research and inclusion of personal details.

WHAT CAN WE DO?

Make it a habit in your company of regularly educating staff, particularly senior management about the effects of phishing and whaling attacks and how to spot them. Train these employees on the common characteristics of phishing attacks like hoax sender names, unsolicited requests, unlikely attachments, or spoofed hyperlinks.

Encourage senior staff to set privacy restrictions on their profiles across their social media use. This will stop unknown individuals from viewing their personal information like birthdays, hobbies, friends and holiday locations.

Earmark external emails: Many whaling emails are intended to look like they come from someone high up within the organization. A good way to spot potential whaling attacks is to flag emails that are sent from outside of the corporate network. In Outlook you can set up a Flag for all emails, except ones sent from internally or from a specific address book.

In your Outlook mail box perform the following steps:

- From the Home Ribbon, go to Rules / Create Rules / Advanced Options to open the Rules Wizard

- Step one: Check the box to apply the Rule to Emails 'sent only to me'.

Step two: Check the box to 'Display a specific message in the Alert Window'. Click the hyperlink in the lower section to customise your text to something like 'External Email'. This will be visible in the email notification window that appears when an email arrives.

Step Three: In the Any Exceptions window, check the box for 'except if the sender is from a specific address book'. In the lower section of the window, click the hyperlink to select your Global Address list.

Step Four: To Finish the Rule, give it a name like 'External Email rule' *and check the box to turn this rule on.*

Also establish a verification process within your company: If an unusual request is made from within the company, the safest option is to get confirmation of the request by another method of communication.

EMAIL HIJACKING

Be aware also that email hijacking is widespread. Once a scammer has guessed a password and hacked an email account, they will have access to all the contact addresses. So even if you receive an email from someone you know, if you aren't expecting a link or attachment then it's wise to make a quick phone call to the sender to verify.

This of course reminds us all about password security. Do not use the same password across multiple sites and make sure it is cryptic.

VISHING

Vishing is slightly different in that a voice mail or email directs the target to ring a number to verify information, usually around activity on their credit card. The term is a combination of "voice" and "phishing." The number given is actually a VoIP (Voice Over IP) phone and the keystrokes of the credit card number can be recorded as the caller is prompted to enter card and password information. Often these phone numbers look legitimate because they have local area codes. Ring your bank directly to confirm any suspicions.

SMISHING:

Smishing (SMS or text) Phishing is gaining popularity as an alternative method to trick people into releasing their personal information. Typically, the text messages sent are urgent in nature asking you to directly call a number or click a link to verify your information.

A Smishing text might say you are told you have won a prize and you are asked to click a link. You might be asked to call your bank or internet company urgently regarding unusual activity against your account. Don't reply to the message or click any of the links in the message. You can contact the company directly to confirm if they sent you the message. You can also report the number that sent you the message to your mobile phone provider.

REPORTING ATTACKS

New to New Zealand as of April 2017, is CERT – a government organisation established to improve cyber security in New Zealand. CERT stands for Computer Emergency Response Team, which consists of an expert group of people that handles cyber security incidents. There are more than 100 CERT organisations worldwide and now New Zealand has its own. Go to www.cert.govt.nz to report any incidents. There is information there for individuals as well as IT professionals.

EDUCATING STAFF:

Remind staff to watch email addresses carefully and check web addresses of any links given. Check for misspellings, unsolicited attachments or unusual requests - all of these are common features of phishing and just through this careful consideration of emails, an attack could be prevented.

These are all actions that can be taken by the employee, because despite the best IT infrastructure in place, it’s often people who are the weakest link.