New Zealanders get hooked by phishing attacks

Phishing attacks are a reality that all organisations have to deal with. Criminal organisations are readily using phishing as an attack method, with attacks occurring with increased frequency and with an increased level of sophistication. The risks are real both in a business environment and in our personal lives.

As part of Connect Smart Week, the KPMG Cyber team undertook a phishing exercise to gain insights into how security aware New Zealanders are. With Connect Smart Week having a theme of "increasing the cyber security awareness and capability of individuals in the workplace", a phishing exercise to provide a snapshot of how security aware New Zealanders are seemed ideal.

Thirty five organisations with a total of 8,333 staff agreed to participate in the exercise. The staff were sent an email from a fake email address indicating the organisations had signed up to a password quality checking website, and asking them to go to a (fake) website to check the quality of their passwords.

The results were unfortunately not surprising. While the emails should have clearly stood out as being fake, of the 8,333 people phishing emails were sent to, 1009 people (12.1%) clicked on the website link in the email, and 702 (8.4%) entered their password into the fake website.

The first person entered their password into the fake website less than a minute after the phishing emails were sent.

"Had the phishing emails been real, that would have meant cyber-criminals would have had the passwords for a significant number of people in most organisations" says Philip Whitmore, KPMG Partner and head of KPMG Cyber. "With many New Zealand organisations still relying upon just username and password for remote access; that may have also meant it was game over for many of the organisations involved" says Whitmore.

The percentage of staff within an organisation that provided their passwords ranged from just under 1% to over 25%. The size of an organisation did not seem to affect the results, with staff from both small and large organisations falling for the phishing emails.

8,333

PEOPLE RECEIVED PHISHING EMAILS

1009

PEOPLE CLICKED ON THE WEBSITE LINK IN THE PHISHING EMAIL

702

PEOPLE ENTERED THEIR PASSWORD INTO THE FAKE WEBSITE

Today's reality

Organisations and the public are at risk of increasingly sophisticated phishing attacks.

Organisations that fail to investigate in preventative measures and do not have a rapid response plan are particularly vulnerable to attacks by cyber-criminals.

Organisations need to educate staff about the dangers of phishing and train them on what to look for and how to react.

Phishing, Spear Phishing and Whaling

Phishing – A deceptive process by which a cyber-criminal attempts to make you divulge sensitive or confidential information (such as passwords or credit card information), or attempts to make you undertake specific actions (such as downloading malware or making a payment to them).

Typically carried out via email, phishing attacks may also come via other technologies such as instant messaging, text messages or phone calls. The phishing correspondence commonly appears to come from a legitimate party you may a relationship with.

Spear Phishing – A targeted and more sophisticated form of phishing. Unlike standard phishing schemes that use mass communication, spear phishing targets individuals that fit a certain profile. For example, they may only target senior staff of a specific organisation, or users of a specific website.

Whaling – Phishing for the bigger fish. Phishing attacks targeted at senior members of staff, such as C-level executives. This can include, for example, a phishing email to the Chief Financial Officer appearing to come from the Chief Executive, in an attempt to get fraudulent payments made.

Combating Phishing Attacks

The need for sound security practices and controls is imperative to help protect against a growing swell of sophisticated cyber threats. Phishing attacks, including targeted spear phishing attacks and whaling attacks, have become commonplace. It is almost certain that these attacks will increase in frequency and sophistication as organisations expand the use of digital assets and unstructured data. Organisations stand to lose far more than their intellectual property and money in the aftermath of a phishing attack. Damage to reputation and brand can be just as devastating as theft of money and secrets.

The increased headlines we see should serve as a loud wake-up call to organisations as just how difficult it is to prevent cyber-attacks, especially those with social-engineering aspects. A single employee can inadvertently cause a serious breach that could have a cascading effect throughout an organisation, as well as its customers and clients.

There are however, several proactive steps an organisation can take to minimise the likelihood of a successful attack. Organisations must understand that a sound cyber security program requires maturity across people, process and technology, as no one element is sufficient.

People

1 **Adopt a strategic vision and communicate it** – An organisation's leadership must adopt a clear, strategic vision of how to protect and secure critical information assets across people, process and technology. This message needs to be communicated throughout the organisation and continually reinforced.

2 **Educate and train all staff** – It is critical to provide ongoing training and education for all staff, including C-level executives, in order to increase security awareness. Remember it only takes one staff member opening an attachment in a targeted email to open the door for cyber criminals and potentially compromise an organisation's network.

Process

3 **Develop a data governance strategy** – Organisations need to develop a strong data governance regime that includes the classification and monitoring of critical or sensitive data.

4 **Perform simulated phishing attacks** – Organisations should perform simulated phishing attacks to measure the effectiveness of their end-user education and incident response processes. These simulations can help an organisation identify individuals and groups that require additional training and help to identify gaps in security controls and policies.

5 **Develop an incident response process** – By developing an incident response process that defines key roles and responsibilities as well as internal and external coordination steps throughout the incident life cycle, an organisation can prepare itself for potential cyber-attacks. In addition, the organisation should test its plan periodically to help ensure that staff are prepared to respond to an incident and that the planned steps are effective.

Technology

6 **Update patching and antivirus programs** – Effective patch management and up-to-date applications, including web browser add-ons such as Java and Adobe Flash, are critical components of an effective defence. An organisation should confirm that its antivirus programs, operating system patches, and application patches are up-to-date in order to increase its overall security posture and protect against cyber-attacks.

7 **Implement two factor authentication** – Organisations should implement two factor authentication for remote access. Two factor authentication requires both something you know (such as a password) and something you have (such as a cellphone that a text message is sent to) to gain remote access. If, for example, a staff member inadvertently discloses their password as part of a phishing attack, unauthorised access will not be able to be gained as the attacker will not have the second factor.

8 **Limit who has administrative access of their workstation** – Most staff members do not have a need to have administrative access of their laptop or desktop computer. By limiting administrative access to those staff that absolutely need it to undertake their jobs, limits the ability for any malware delivered by a phishing attack to run.

To minimise the likelihood of being phished

- Do not click on unsolicited attachments or website links.
- Be wary of:
  - Emails where the from name does not match the sending email address
  - Emails signed with a generic closing, such as "Customer Service"
  - Emails from organisations you have no relationship with
  - Too good to be true offers
  - Emails from generic mail services such as Gmail or Hotmail
  - Emails where the URL (website address) differs to that displayed when you hover your mouse over it.
- Do not bypass standard processes because of an unexpected email.
- If someone emails you and asks you to make a payment or send personal information, do not complete the request until you have confirmed it is a genuine request – and not via replying to the email. Standard payment processes should always be followed.

Contact us

Philip Whitmore
Partner – KPMG Cyber
Auckland
T +64 (09) 367 5931
E pwhitmore@kpmg.co.nz

@KPMGNZ_cyber

KPMG-Cyber

connect SMART
Protect yourself online
GOLD PARTNER 2015/16

kpmg.com/nz/cyber

This document is made by KPMG, a New Zealand Partnership and a member firm of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity, and is in all respects subject to the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.