



newzealand.govt.nz

Media release

Kiwis hooked by online phishing expedition

12 October 2016 – A KPMG test on the cyber security of New Zealand businesses as part of [Connect Smart Week](#) has revealed one in ten Kiwis could fall for a phishing attack.

Phishing is the practice of sending an email pretending to be from a reputable company or organisation in order to trick individuals to reply with personal information, such as passwords and credit card numbers.

Ahead of Connect Smart Week, KPMG conducted a phishing experiment with 35 organisations, who agreed to be involved, with a total of 8,333 staff.

Employees in each organisation were sent an email indicating their organisations had signed up to a password quality checking website. The email contained a link and asked the recipient to go to the website to check the quality of their password.

KPMG found that 1,009 people (12.1%) clicked on the link and, once through to the website, 702 (8.4%) entered their password details.

Philip Whitmore, KPMG Partner and head of KPMG Cyber, said the exercise was a great way to educate employees and start a discussion in the workplace, but also a real warning sign for organisations.

“Unfortunately the results were not surprising – as phishing emails are becoming increasingly convincing and sophisticated. If the phishing emails had been real, then cyber-criminals would have acquired the passwords of a significant number of people in every organisation,” said Mr Whitmore.

“With many organisations still relying upon username and password for remote access, it would have meant it was game over for many of the organisations involved.”

Whitmore indicated there were a few simple warning signs in the phishing email which should have raised alarm bells.

“We made the email look like it was sent from an employee within the organisation, but the name did not match the email address. The email also did not include a signature block, and there was no personalised greeting – a couple of red flags.

The Connect Smart website has advice for individuals looking to improve their cyber security, including a tip sheet on how to recognise and avoid phishing attacks,” says Mr Whitmore.

Director of the National Cyber Policy Office Paul Ash urged people to “think before they click”. “Employees should look out for suspicious, unsolicited emails requesting personal information or other information relating to their workplace. They should

take care to verify links or attachments are genuine before clicking on them.”

“Individuals can take simple steps to protect themselves and their workplace. Workplace cyber security is about protecting information – whether it is the organisation’s intellectual property, financial information, details of customers or personal staff details,” says Mr Ash.

This Connect Smart Week is hosted alongside [Stay Smart Online](#) Week, run by the Australian Government. The theme of Connect Smart Week 2016 is improving the cyber security capability of employees.

For more information about Connect Smart Week and initiatives during the week, visit ConnectSmart.govt.nz

Tips to prevent against phishing:

- **Know how to recognise valid emails:** Is the email from someone you know or have received an email from before? Is it something you were expecting? Does it look strange (e.g. unusual spelling or other errors in the email address or domain names)? Has it passed the anti-virus test?
- **Think before you click:** Do not open suspicious links in emails, tweets, social media posts, online ads, messages or attachments – even if you think you know the source.
- **Verify the email:** If you are unsure about whether an email is from a legitimate company or government department, try calling the organisation that appears to have sent the email.

About Connect Smart:

Connect Smart is a public-private partnership that promotes ways for individuals, businesses and schools to protect themselves online. Connect Smart is led by the government’s National Cyber Policy Office (NCPO) within the Department of the Prime Minister and Cabinet (DPMC), in partnership with over 100 organisations from across the private, government and NGO sectors.

The Connect Smart initiative has been developed in partnership with the public sector and NGOs, with support from Platinum Partners ASB, BNZ and Spark; Gold Partners ANZ, Datacom, Deloitte, Facebook, FireEye, Hewlett Packard Enterprise, KPMG and Microsoft; and Silver Partners Dimension Data, International Underwriting Agencies and Marsh.

For further information on how to Connect Smart, or to become a Connect Smart partner, visit www.connectsmart.govt.nz, and follow us at [@ConnectSmartNZ](https://twitter.com/ConnectSmartNZ)

ENDS

For further information, or to speak with NCPO Director Paul Ash, please contact:

Emma Ward, Acumen Republic for Connect Smart

E: eward@acumenrepublic.com

T: 04 494 5121

M: 021 151 6594

