KnowBe4 Finds Email Subject Lines Focused on Personal Interests Prove Too Tempting for Employees

Submitted by: Origin Comms Ltd

Tuesday, 30 April 2019

KnowBe4 Q1 2019 top-clicked phishing subject lines reveals
LinkedIn messages to be most popular

York, UK (April 30, 2019) – World Social Media Week New York (#SMWNYC) starts today bringing attention to the fact that social media is now a part of everyday business and organisations can no longer limit employees' usage of platforms. KnowBe4 (https://www.knowbe4.com), the provider of the world's largest security awareness training and simulated phishing platform, revealed that simulated phishing tests that include "LinkedIn" in the subject line are clicked 50 per cent of the time by users of the platform.

This percentage is significant as many LinkedIn users, particularly those with business development responsibilities, have their accounts tied to their corporate email addresses, increasing corporate risk of a phishing attack, ransomware breach or other social engineering-related threat. Social media sites are also a hotbed for cybercriminal activity. According to recent research from Bromium, cyber criminals are earning at least $3.25bn per year from social media-enabled cybercrime.

"From the standpoint of a hacker, social media gives an all-access entry point into an organisation because some social media accounts are tied to corporate email addresses. I cannot stress enough that employees need to be hyper-vigilant about clicking on emails and links that come to their corporate email addresses," said Stu Sjouwerman, CEO, KnowBe4. "Clicking to view a new job posting or to identify who has viewed your LinkedIn profile could easily open the gates to bad actors who want to cause damage to the organisation."

People often rely on what they think are trusted sources to protect their information but fall victim to social media scams and end up offering up sensitive information. They need to make the extra effort to protect themselves and be mindful of methods being used by the bad guys.

"To best protect personal information and your organisation, you have to have a defence-in-depth security strategy that includes training your users to spot phishing emails," continued Sjouwerman.

KnowBe4's examination of simulated phishing tests showed that half of users clicked on spoofed LinkedIn emails that included the following subject lines:

- Join my network
- Profile Views
- Add me to your network
- New InMail Message

*Capitalisation and spelling are as they were in the phishing test subject line.
**Email subject lines are a combination of both simulated phishing templates created by KnowBe4 for clients, and custom tests designed by KnowBe4 customers.

In addition to sharing simulated phishing test results to identify social networks that tempt users, KnowBe4 has found that subject lines – both from simulated tests and 'in-the-wild' emails users receive and report – prey on what matters most to users. Subject lines that related to Human Resources and corporate policies, W-2 forms and Amazon ranked in the top 10 this quarter for both simulated tests and in-the-wild email subject lines.

Falling victim to a phishing email is avoidable. Organisations need to train their users to be their last line of defence. KnowBe4 has many free tools to test the users in their network, including the Phishing Reply Test, which quizzes organisations' users to see if they will reply to a highly targeted "spoofed" email attack and the Password Exposure Test to tackle at-risk employees. Learn more here (https://www.knowbe4.com)

About KnowBe4
KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 24,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organisations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognised cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organisations rely on KnowBe4 to mobilise their end users as the last line of defence.
Number 96 on the list Inc. 500 of 2018, number 34 on 2018's Deloitte's Technology Fast 500, and 2nd place in Cybersecurity Ventures Cybersecurity 500, KnowBe4 is headquartered in Tampa Bay, Florida, with offices in Brazil, England, the Netherlands, Germany, South Africa and Singapore.

For further information please contact:
Louise Burke
Origin Comms
Tel: +44 (0)7917 176095
Email: louise@origincomms.com