KnowBe4 Takes a Bite Out of Phishing With New Phishing Reply Test

Submitted by: Origin Comms Ltd
Tuesday, 2 April 2019

No-Cost IT security tool tests organizations' users to see if they will reply to a highly targeted "spoofed" email attack

York, UK (April 2, 2019) – KnowBe4 (https://www.knowbe4.com), the provider of the world's largest security awareness training and simulated phishing platform, today announced a new, complimentary tool aimed to gauge how many employees will reply to a phishing email called the Phishing Reply Test (PRT).

Highly targeted phishing attacks, known as Business Email Compromise or CEO fraud are used by the bad guys to impersonate a C-level executive and trick high-risk users, often Accounting, HR, or Executive teams and even IT because they own the keys to the kingdom. PRT is a web-based tool that cybersecurity professionals can use to test employees on these common scenarios for targeted attacks used by the bad guys.

The IT Pro can select and send an email template to users under the guise of a trusted sender within the organisation and phishes for a response. This tool provides insight into how many of an organisation's users will fall for this type of phishing scenario so that proper training can be administered to help prevent an actual phishing attack.

"At KnowBe4, it's our goal to make the jobs of cybersecurity professionals easier by providing them with tools to help better train their users," said Stu Sjouwerman, CEO, KnowBe4. "Our new Phishing Reply Test tool will help educate users on the importance of always verifying requests for sensitive and/or confidential information before hitting the reply button."

The majority of impersonated email attacks do not involve any link: it's simply a plain text email. The problem with this type of attack is that people can unknowingly provide sensitive and/or confidential information to the bad guys.

These highly targeted attacks are clever because they bypass traditional approaches to email security which focus on scanning and filtering the content of the email. These spoofed emails contain no links, no attachments. They are pure social engineering attacks that target users and their vulnerability to deception.

In July 2018, the FBI reported that organisations have lost over $12.5 billion since 2013 through the use of technically simple, but very effective emails that impersonate C-level executives or other high-profile employees.

For more information on KnowBe4's Phishing Reply Test, visit https://info.knowbe4.com/phishing-reply-test.

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.

Media Contact:

Louise Burke
Origin Comms
Tel +44 (0) 7917 176095
Email: louise@origincomms.com