KnowBe4 Releases Quarterly Top-Clicked Phishing Report for Q2 2017 - Results Show Human Error Continues to Be an Organisation's Weakest Link

Submitted by: Origin Comms Ltd
Wednesday, 12 July 2017

London July 12, 2017 – KnowBe4 (http://www.knowbe4.com), the provider of the world's most popular security awareness training and simulated phishing platform, today shared its Top 10 Global Phishing Email Subject Lines for Q2 2017. While the results show that users click most frequently on business-related subject lines ("Security Alert" is the highest ranked at 21 per cent), they still click with alarming frequency on subject lines not related to work topics and showing red flags.

According to Osterman Research, email has been the number one network infection vector since 2014. It's an effective method because it gives attackers more control than merely placing traps on the web and hoping that people will stumble over them. Instead, attackers craft and distribute enticing material to both random and targeted means. This method gives the cybercriminals greater control in selecting potential victims, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.

The Top 10 Global Most-Clicked Global Phishing Email Subject Lines for Q2 2017 include:

1. Security Alert – 21%
2. Revised Vacation & Sick Time Policy – 14%
3. UPS Label Delivery 1ZBE312TNY00015011 – 10%
4. BREAKING: United Airlines Passenger Dies from Brain Haemorrhage – VIDEO – 10%
5. A Delivery Attempt was made – 10%
6. All Employees: Update your Healthcare Info – 9%
7. Change of Password Required Immediately – 8%
8. Password Check Required Immediately – 7%
9. Unusual sign-in activity – 6%
10. Urgent Action Required – 6%

*Capitalisation is as it was in the phishing test subject line

"The subject lines we are reporting here actually made it through all the corporate filters and into the inbox of an employee. That's astounding. We are in a security arms race, and a multi-layered defence is critical because each layer has different points of effectiveness and ineffectiveness," said Perry Carpenter, Chief Evangelist and Strategy Officer at KnowBe4. "If crafted correctly, the right type of message can sail through all of the defences because it is finding the least effective point of each and playing into the human psyche of wanting to receive something you didn't know about or needing to intervene before something is taken away. Ultimately this means that a company's 'human firewall' is an essential element of organisational security because people truly are the last line of defence."

Businesses have to also be aware that social media messages to their users are potential landmines to their corporate networks. KnowBe4 evaluated the Top 10 Global Social Networking Subject Lines and found

that four of the top 10 spots equaling a full 44 per cent were related to LinkedIn messages, which users often have tied to their work email addresses.
As part of its ongoing research efforts, In October 2016 KnowBe4 evaluated more than 10,000 email servers and found that 82 per cent of them were misconfigured, allowing spoofed emails to successfully bypass endpoint security systems and enter an organisation's network. Aggregating information on the most clicked phishing test subject lines and sharing that data with clients is another way that KnowBe4 is helping protect against social engineering tactics that continue to plague businesses around the globe, resulting in growing ransomware, CEO fraud and other phishing-initiated attacks.

Businesses that are not already working with KnowBe4 to effectively train their workforce into a "human firewall" can utilise a number of free tools at www.knowbe4.com to test their users and their network.

About KnowBe4

KnowBe4, the provider of the world's most popular integrated new school security awareness training and simulated phishing platform, is used by more than 11,000 organisations worldwide. Founded by data and IT security expert Stu Sjouwerman, KnowBe4 helps organisations address the human element of security by raising awareness of ransomware, CEO Fraud and other social engineering tactics through a new school approach to security awareness training. Kevin Mitnick, internationally recognised computer security expert and KnowBe4's Chief Hacking Officer, helped design KnowBe4's trainings based on his well-documented social engineering tactics. Thousands of organisations trust KnowBe4 to mobilise their end-users as the last line of corporate IT defence.

Number 139 on the 2016 Inc 500 list, #50 on 2016 Deloitte's Technology Fast 500 and #38 in Cybersecurity Ventures Cybersecurity 500. KnowBe4 is based in Tampa Bay, Florida. For more information, visit www.knowbe4.com and follow Stu on Twitter at @StuAllard.

Contacts:

Louise Burke
Origin Communications for KnowBe4
M: +44 (0) 7917 176095
E: louise@origincomms.com