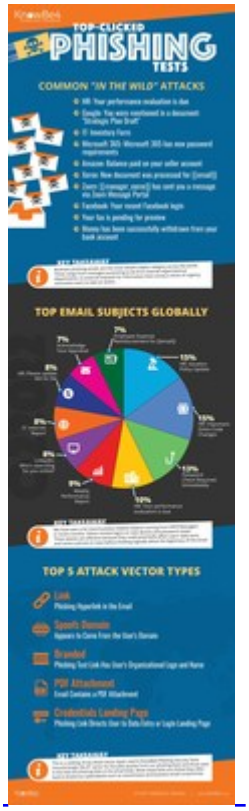
KnowBe4 Phishing Test Results: Employees Most Frequently Fall for Emails That Look Like They Came From Human Resources or IT

July 25, 2022

In phishing tests conducted on business emails, more than half of the subject lines clicked imitated Human Resources communications.

TAMPA BAY, Fla., July 25, 2022 /PRNewswire/ -- KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, has released the most frequently clicked phishing methods, including the top email subjects clicked on in phishing tests. Half of those that were clicked on had subject lines related to Human Resources, including vacation policy updates, dress code changes, and upcoming performance reviews. The other top category was IT requests, including password verifications needed immediately. Test results are available on KnowBe4's website.



By now most people know that if they receive a text message confirming an $1800 order they never placed, or telling them they've just won a new grill, they shouldn't click on it. But what if it's from their HR Department about an upcoming performance review? Or, what if the attachment is a draft of a Strategic Plan that mentions their name?

Business phishing emails are particularly effective because, left unanswered, they could potentially affect the user's daily work, enticing employees to react quickly before thinking logically about the email's legitimacy. The email source may be hidden by a spoofed domain, making it even easier to miss, and may even have the company name and logo (sometimes even the employee's name) in the email body. Most include a phishing hyperlink in the email or a supposed PDF attachment.

"We already know that more than 80% of company data breaches globally come from human error," said Stu Sjouwerman, KnowBe4's CEO. "New-school security awareness training your staff is one of the least costly and most effective methods to thwart social engineering attacks. Training gives employees the ability to rapidly recognize a suspicious email, even if it appears to come from an internal source, causing them to pause before clicking. That moment where they stop and question the email is a critical and often overlooked element of security culture that could significantly reduce your risk surface."

To download a copy of the KnowBe4 Phishing Infographic, visit KnowBe4.

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 50,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations 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 recognized 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 organizations rely on KnowBe4 to mobilize their end users as their last line of defense.

Media Contact
Amanda Tarantino
Public Relations Officer
KnowBe4
amandat@knowbe4.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/knowbe4-phishing-test-results-employees-most-frequently-fall-for-emails-that-look-like-they-came-from-human-resources-or-it-301592461.html

SOURCE KnowBe4