KnowBe4 Finds Holiday-Themed Emails Entice Employees to Click

April 13, 2022

KnowBe4 releases Q1 2022 global phishing report

TAMPA BAY, FL, April 13, 2022 /PRNewswire**/ --** KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, today announced the results of its Q1 2022 top-clicked phishing report.

"In our latest quarterly phishing report, we found that holiday-themed emails were the most tempting for employees to click on," said Stu Sjouwerman, CEO, KnowBe4. "HR-related messages such as a change in the schedule for the holidays likely piqued interest from employees to see if they would receive an extra day off or shortened work schedule due to the holidays. It is important to remember that cybercriminals utilize various tactics such as preying on people's emotions when executing their malicious scams. Remaining vigilant and adopting a heightened sense of suspicion around emails that trigger an emotional response can end up preventing a detrimental cybersecurity attack."

Global Holiday Emails

1. HR: Change in Holiday Schedule
2. Someone special sent you a Valentine's Day ecard!
3. St. Patrick's Day: Employee Behavior/Company Policies
4. Our Valentine's Day Gift To You
5. Starbucks: Happy Holidays! Have a drink on us.

Top 10 Email Categories Globally:

1. Business
2. Online Services
3. Human Resources
4. IT
5. Coronavirus/COVID-19 Phishing
6. Banking and Finance
7. Phishing for Sensitive Information
8. Mail Notifications
9. Social Networking
10. Current Events

Top phishing email subjects were broken out, comparing those in the U.S. to those in Europe, Middle East and Africa (EMEA). In Q1 2022, KnowBe4 examined tens of thousands of email subject lines from simulated phishing tests. The organization also reviewed 'in-the-wild' email subject lines that show actual emails users received and reported to their IT departments as suspicious. The results are below.

Top Phishing Email Subjects:

The U.S.

1. HR: New requirements tracking Covid vaccinations
2. Password Check Required Immediately
3. HR: Vacation Policy Update
4. HR: Important: Dress Code Changes
5. Acknowledge Your Appraisal

EMEA

1. Authorize Pending Transaction on your Wallet
2. HR: Registration for COVID-19 Study
3. IT: End of Year Password Policy
4. HR: Code of Conduct
5. Your Benefit Account Has Been Updated

*Capitalization 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.

Common "In-the-Wild" attacks:

- IT: Software Update
- Google Forms: Your Voice Engagement Survey
- Zoom: You missed a Zoom meeting
- Project Notice
- Dropbox: Updates about your account

*Capitalization and spelling are as they were in the phishing test subject line.
**In-the-wild email subject lines represent actual emails users received and reported to their IT departments as suspicious. They are not simulated phishing test emails.

For more information on KnowBe4, visit 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 47,000 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:https://www.prnewswire.com/news-releases/knowbe4-finds-holiday-themed-emails-entice-employees-to-click-301524072.html

SOURCE KnowBe4