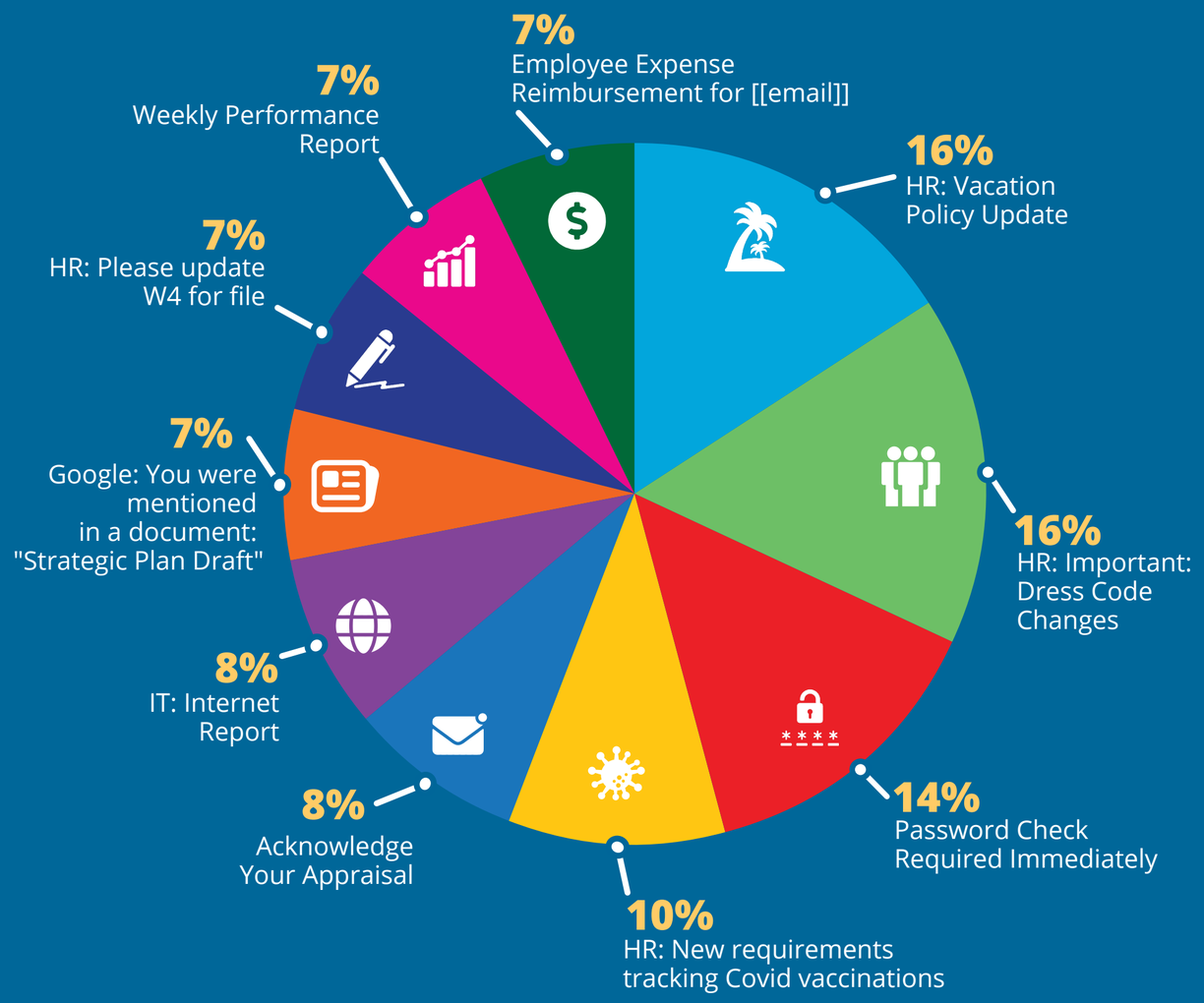
TOP-CLICKED PHISHING TESTS

2022 | TOP EMAIL SUBJECTS GLOBALLY



Key Takeaway

We have seen a lot more business related subjects coming from HR/IT/Managers in the past year. Others involve logins on new devices and password resets. These attacks are effective because they could potentially affect users' daily work, and cause a person to react before thinking logically about the legitimacy of the email.

2022 | COMMON "IN THE WILD" ATTACKS

- IT: Software Update
- HR: Your performance evaluation is due
- Google: You were mentioned in a document: "Strategic Plan Draft"
- Mail Notification: You have 5 Encrypted Messages
- LinkedIn: LinkedIn Customer Service Survey
- Amazon: Amazon - delayed shipping
- Microsoft: Update your security settings
- Action required: Your payment was declined
- Your fax is pending for preview
- Zoom: [[manager_name]] has sent you a message via Zoom Message Portal

Key Takeaway

In 2022 we saw mostly IT and online service notifications that could potentially affect users' daily work. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

2022 | TOP 5 ATTACK VECTOR TYPES

Link
Phishing Hyperlink in the Email

Spoofs Domain
Appears to Come From the User's Domain

PDF Attachment
Email Contains a PDF Attachment

Branded
Phishing Test Link Has User's Organizational Logo and Name

HTML Attachment
Email Contains an HTML Attachment

Key Takeaway

This is a ranking of top attack vector types used in KnowBe4 Phishing Security Tests. The #1 vector we saw in 2022 by a large margin was phishing links in the email body. When these links are clicked they often lead to disastrous cyberattacks such as ransomware and business email compromise.