KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

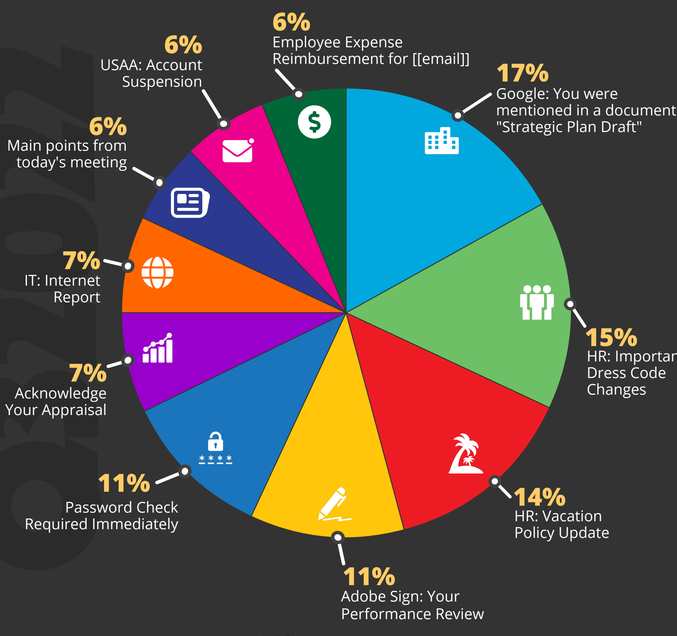
COMMON *"IN THE WILD"* ATTACKS

- Equipment and Software Update
- Mail Notification: You have 5 Encrypted Messages
- Amazon: Amazon - delayed shipping
- Google: Password Expiration Notice
- Action required: Your payment was declined
- Wells Fargo: Transfer Completed
- DocuSign: Please review and sign your document
- IT: IT Satisfaction Survey
- Zoom: [[manager_name]] has sent you a message via Zoom Message Portal
- Microsoft: Microsoft account security code

KEY TAKEAWAY

Business phishing emails are the most clicked subject category across the world. These range from messages purporting to be from internal organizational departments, to external requests for information that convey a sense of urgency and entice users to take an action.

TOP EMAIL SUBJECTS GLOBALLY



KEY TAKEAWAY

We have seen a lot more business related subjects coming from HR/IT/Managers in recent months. 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.

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

Credentials Landing Page
Phishing Link Directs User to Data Entry or Login Landing Page

KEY TAKEAWAY

This is a ranking of top attack vector types used in KnowBe4 Phishing Security Tests. Unsurprisingly, the #1 vector for the past quarter from our phishing tests and those seen in the wild are phishing links in the email body. When these links are clicked they often lead to disastrous cyberattacks such as ransomware and business email compromise.