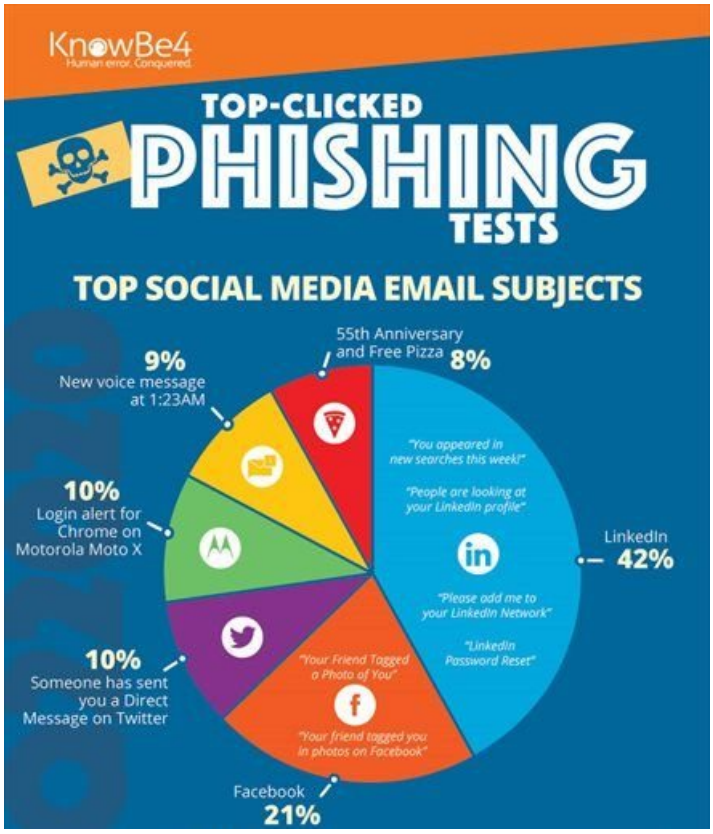
Phishing email attacks surge amidst pandemic

KnowBe4, a provider of security awareness training and simulated phishing platform, revealed the results of its Q2:2020 top-clicked phishing report.



click to enlarge

The results found that phishing email attacks related to Covid-19 remained frequent in Q2:2020. Covering the entire second quarter, simulated phishing tests with a message related to the coronavirus were the most popular, with a total of 56%.

Social media messages are another area of concern when it comes to phishing. Within the same report, KnowBe4's top-clicked social media email subjects reveal password resets, tagging of photos and new messages.

"It's no surprise that phishers and scammers are using the avalanche of new information and events involving the global coronavirus pandemic as a way to successfully phish more victims," said Stu Sjouwerman, CEO, KnowBe4.

“These phishing scams are becoming more aggressive and more targeted as this pandemic continues. Everyone should remain very sceptical of any email related to Covid-19 coming into their inbox.”

In Q2:2020, KnowBe4 examined tens of thousands of email subject lines from simulated phishing tests. The organisation also reviewed ‘in-the-wild’ email subject lines that show actual emails users received and reported to their IT departments as suspicious.

Top 10 General Email Subjects

- Password Check Required Immediately
- Vacation Policy Update
- Branch/Corporate Reopening Schedule
- Covid-19 Awareness
- Coronavirus Stimulus Checks
- List of Rescheduled Meetings Due to Covid-19
- Confidential Information on Covid-19
- Covid-19 - Now airborne, Increased community transmission
- FedEx Tracking
- Your meeting attendees are waiting!

Note: Capitalisation 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.

When investigating ‘in-the-wild’ email subject lines, KnowBe4 found the most common throughout Q2 2020 included:

- Microsoft: Abnormal log in activity on Microsoft account
- Chase: Stimulus Funds
- HR: Company Policy Notification: Covid-19 - Test & Trace Guidelines
- Zoom: Restriction Notice Alert
- Jira: [JIRA] A task was assigned to you
- HR: Vacation Policy Update
- Ring: Karen has shared a Ring Video with you
- Workplace: _name invited you to use Workplace
- IT: ATTENTION: Security Violation
- Earn money working from home

Note: Capitalisation 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.