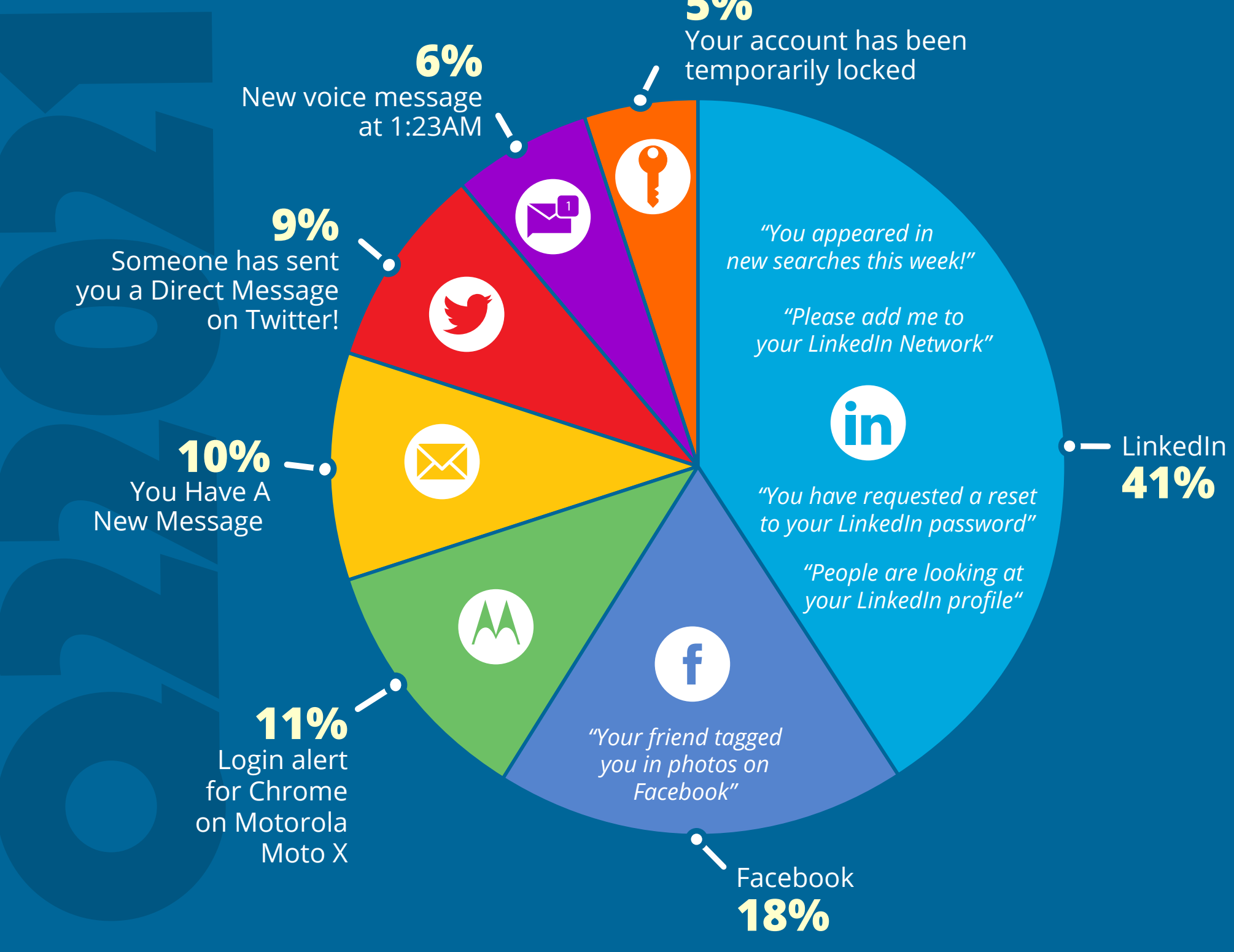
KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY

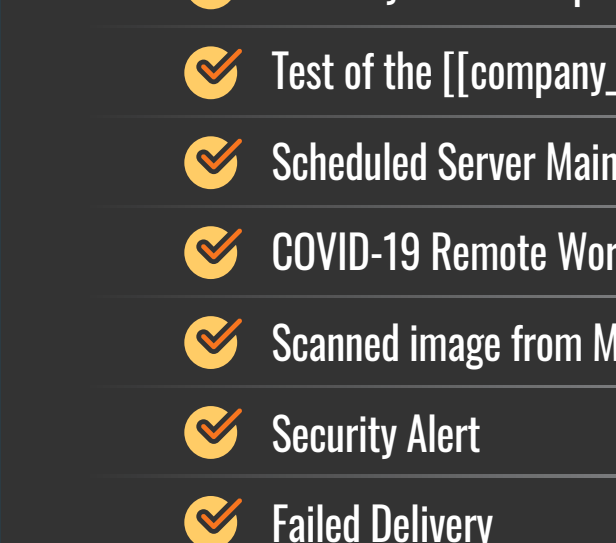
LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or you have a new message can make someone feel special and entice them to click.

TOP 10 GENERAL EMAIL SUBJECTS

Password Check Required Immediately	23%
Vacation Policy Update	17%
Important: Dress Code Changes	13%
ACH Payment Receipt	10%
Test of the [[company_name]] Emergency Notification System	8%
Scheduled Server Maintenance -- No Internet Access	7%
COVID-19 Remote Work Policy Update	6%
Scanned image from MX2310U@[[domain]]	6%
Security Alert	5%
Failed Delivery	5%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. There is only one subject around COVID-19 this quarter, it seems users are now more savvy to those types of ploys. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.



COMMON *"IN THE WILD"* ATTACKS

- Zoom: Important issue
- IT: Information Security Policy Review
- Mastercard: Confirmation: Your One-Time Password
- Facebook: Your account has been temporarily locked
- Google: Take action to secure your compromised passwords
- Microsoft: Help us protect you - Turn on 2-step verification to protect your account
- Docusign: Lucile Green requests you to sign Mandatory Security Training documents
- Internship Program
- IT: Remote working missing updates
- HR: Electronic Implementation of new HRIS

KEY TAKEAWAY

This quarter we see more security-related warnings, account activity messages and half of them are work-related. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.