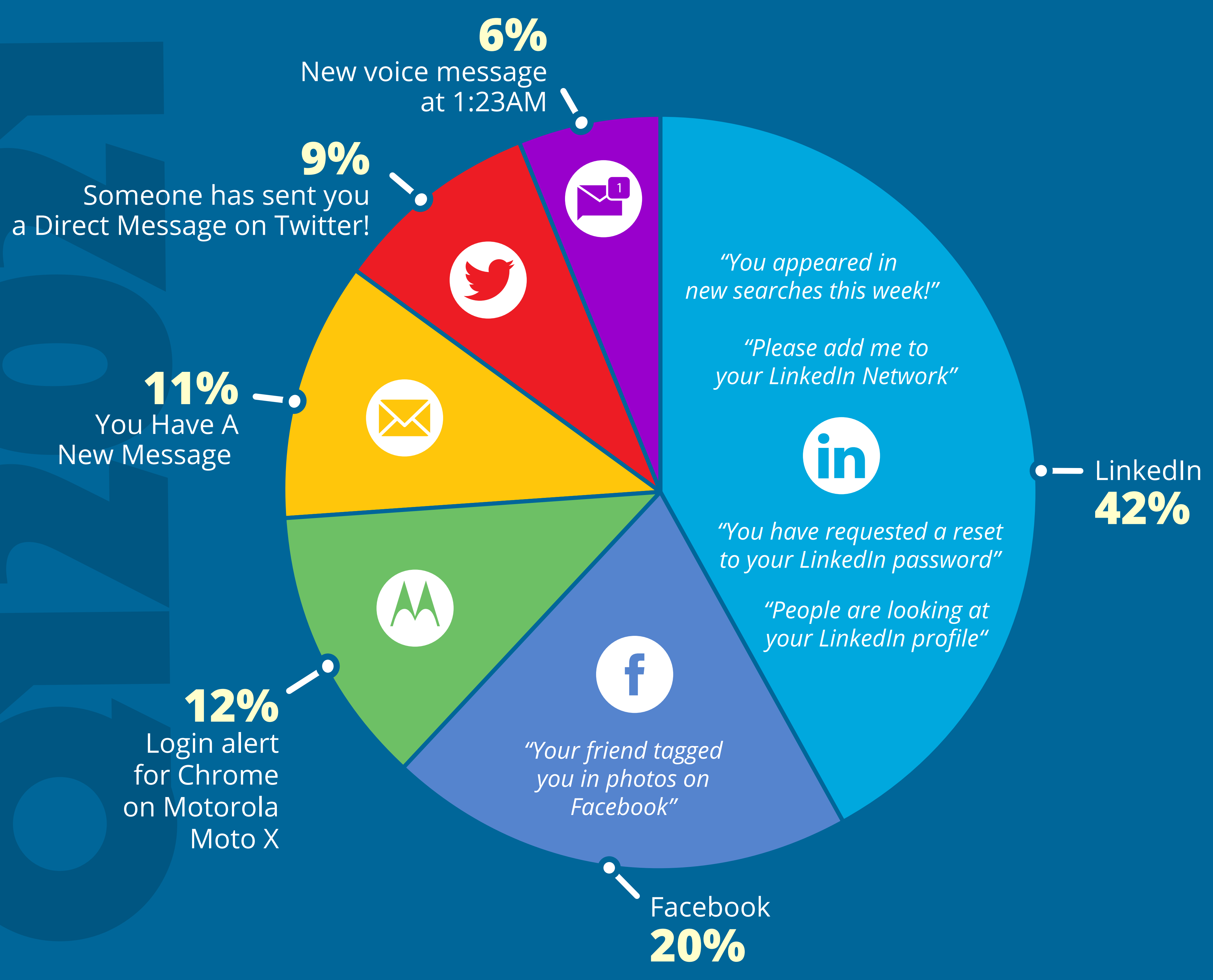
KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS

Q1 2021



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 mentioned you can make someone feel special and entice them to click.

TOP 10 GENERAL EMAIL SUBJECTS

✓ Password Check Required Immediately	31%
✓ Revised Vacation & Sick Time Policy	15%
✓ COVID-19 Remote Work Policy Update	13%
✓ COVID-19 Vaccine Interest Survey	10%
✓ Important: Dress Code Changes	7%
✓ Scheduled Server Maintenance -- No Internet Access	6%
✓ De-activation of [[email]] in Process	5%
✓ Test of the [[company_name]] Emergency Notification System	5%
✓ Scanned image from MX2310U@[[domain]]	4%
✓ Recent Activity Report	4%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. We are still seeing some subjects around COVID-19, but it seems users are getting 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

- Microsoft 365: Scheduled Server Backup
- IT: IT-Help Ticket Survey Invitation
- Warning: Your E-mail account has just sent 260 E-Mails
- Amazon Prime: Action required - Card on file has been declined
- License Update
- Google: Take action to secure your compromised passwords
- Apple: Prize winner! We need your confirmation
- Zoom: You missed a Zoom meeting
- HR: Your payroll details needs updating
- Facebook: Important message regarding your Facebook profile

KEY TAKEAWAY

This quarter we see more security-related warnings, account activity messages and even a "prize winner" notification. 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.