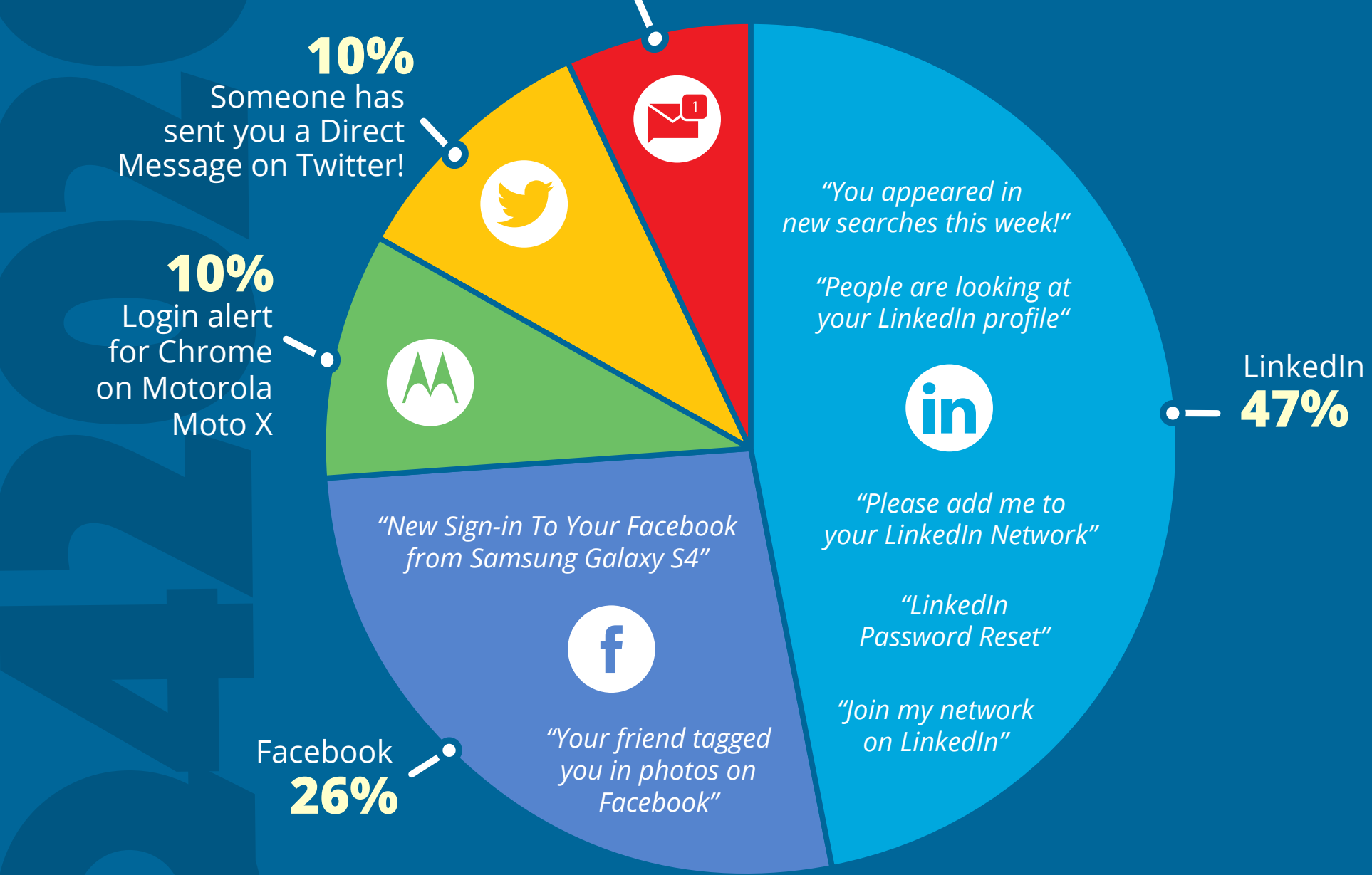
KnowBe4
Human error. Conquered.

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

TOP 10 GENERAL EMAIL SUBJECTS

Password Check Required Immediately	25%
Touch base on meeting next week	14%
Vacation Policy Update	11%
COVID-19 Remote Work Policy Update	11%
Important: Dress Code Changes	10%
Scheduled Server Maintenance -- No Internet Access	7%
De-activation of [[email]] in Process	6%
Please review the leave law requirements	6%
You have been added to a team in Microsoft Teams	5%
Company Policy Notification: COVID-19 - Test & Trace Guidelines	5%

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

- IT: Annual Asset Inventory
- Changes to your health benefits
- Twitter: Security alert: new or unusual Twitter login
- Amazon: Action Required | Your Amazon Prime Membership has been declined
- Zoom: Scheduled Meeting Error
- Google Pay: Payment sent
- Stimulus Cancellation Request Approved
- Microsoft 365: Action needed: update the address for your Xbox Game Pass for Console subscription
- RingCentral is Coming!
- Workday: Reminder: Important Security Upgrade Required

KEY TAKEAWAY

Again this quarter we see subjects related to working from home and a new one around stimulus payments. 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.