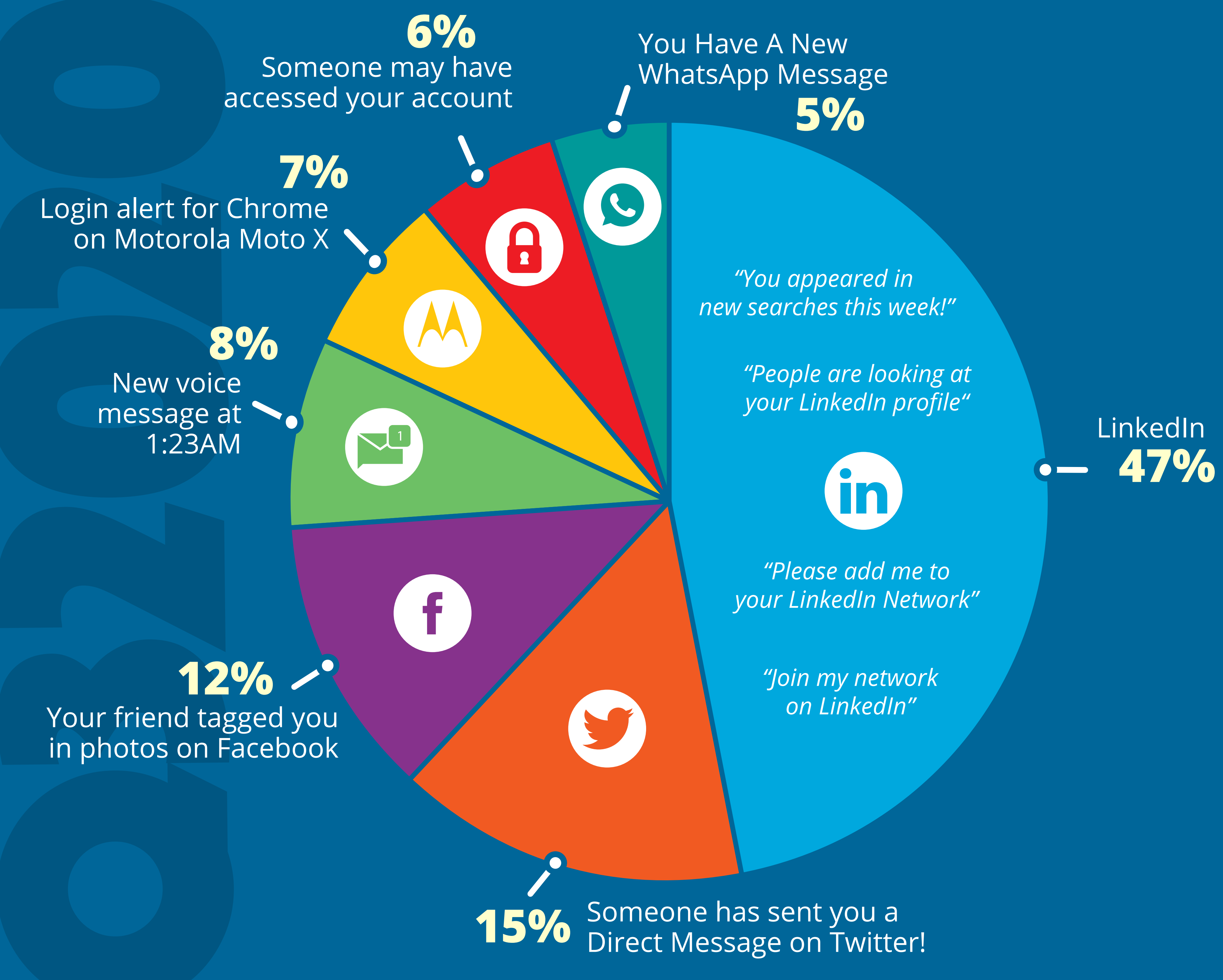
KnowBe4
Human error. Conquered.

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

✓ Payroll Deduction Form	33%
✓ Please review the leave law requirements	12%
✓ Password Check Required Immediately	9%
✓ Required to read or complete: "COVID-19 Safety Policy"	9%
✓ COVID-19 Remote Work Policy Update	7%
✓ Vacation Policy Update	7%
✓ Scheduled Server Maintenance -- No Internet Access	7%
✓ Your team shared "COVID 19 Amendment and Emergency leave pay policy" with you via OneDrive	6%
✓ Official Quarantine Notice	5%
✓ COVID-19: Return To Work Guidelines and Requirements	5%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. Half of the top subjects for this quarter were around COVID-19 once again. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.

COMMON *"IN THE WILD"* ATTACKS

- Microsoft: View your Microsoft 365 Business Basic invoice
- HR: Pandemic Policy Update
- IT: Remote Access Infrastructure
- Facebook: Account Warning
- Check your passport expiration date
- TeleMed Appointment Reminder
- Twitter: Confirm your identity
- Apple: Take part in our iPhone 12 trial and enter for the chance to win a FREE iPhone12
- Exchange ActiveSync service disabled for [[email]]
- HR: Benefit Report

KEY TAKEAWAY

Here again we see subjects related to working from home. 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.