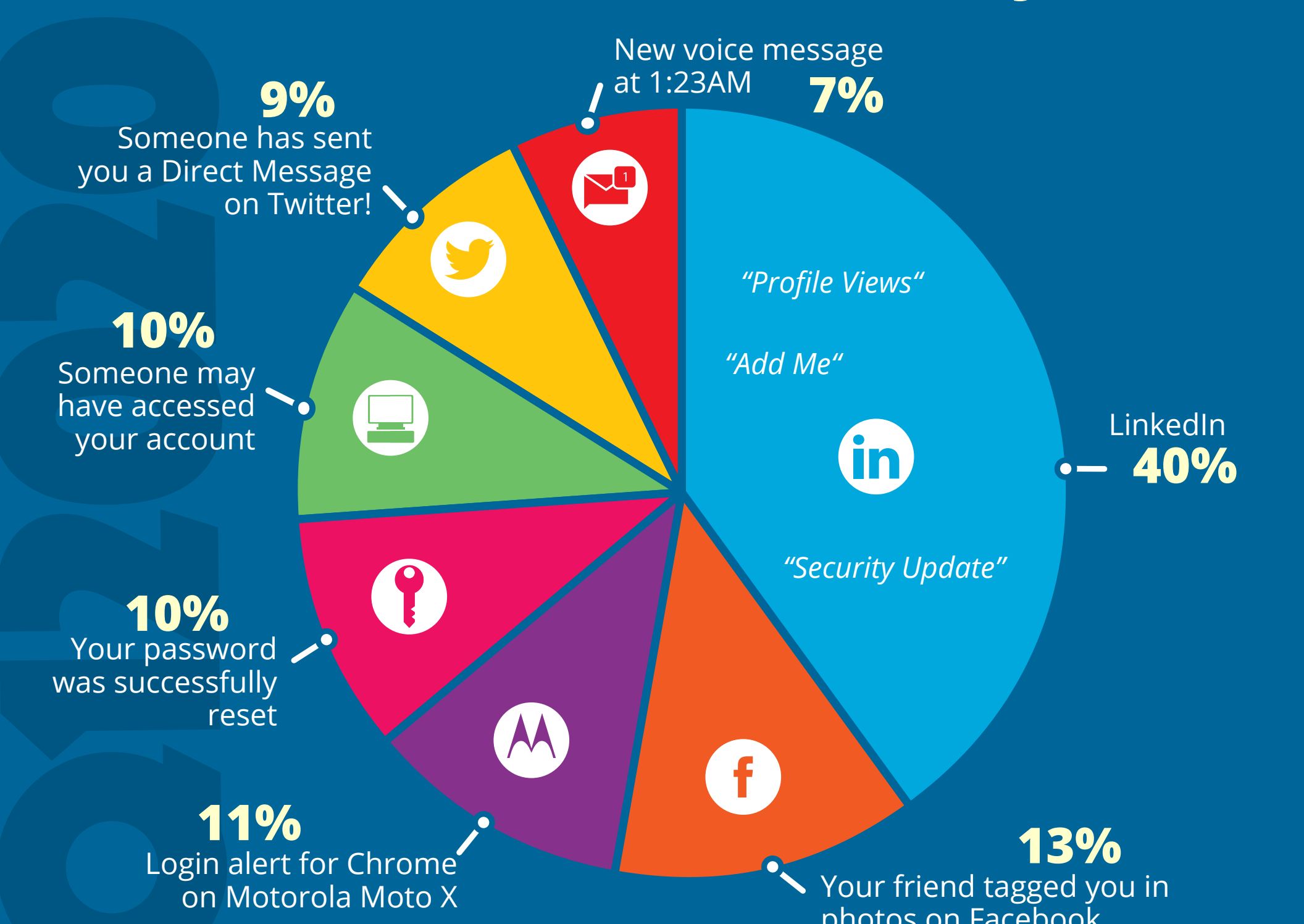
KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY

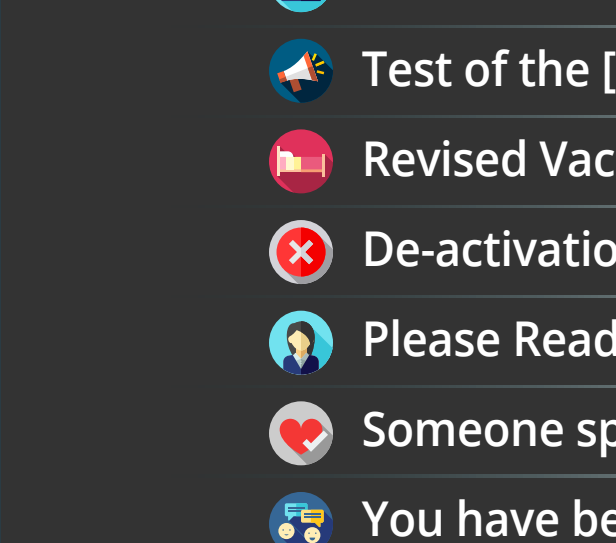
LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged 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	45%
CDC Health Alert Network: Coronavirus Outbreak Cases	10%
PTO Policy Changes	7%
Scheduled Server Maintenance -- No Internet Access	7%
Test of the [[company_name]] Emergency Notification System	6%
Revised Vacation & Sick Time Policy	5%
De-activation of [[email]] in Process	5%
Please Read Important from Human Resources	5%
Someone special sent you a Valentine's Day ecard!	5%
You have been added to a team in Microsoft Teams	5%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. Unsurprisingly, one of the top subjects for this quarter was about the novel Coronavirus. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.



COMMON *"IN THE WILD"* ATTACKS

- List of Rescheduled Meetings Due to COVID-19
- SharePoint: Coronavirus (COVID-19) Tax Cut Document
- Confidential Information on COVID-19
- IT: Work from home - VPN connection
- Comcast: Notification from Carl Vargas
- Microsoft: Your meeting will begin soon
- HR: New Employee Stock Purchase Plan
- Vodafone: Caller Alert: Msg Received Today
- Amazon Chime: Vonage invites you to join vonage_303136
- Parking Authority: Parking Ticket: Pay Charge

KEY TAKEAWAY

Here again we see subjects related to the Coronavirus and working from home, **Coronavirus related phishing email attacks are up over 600%.** 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.