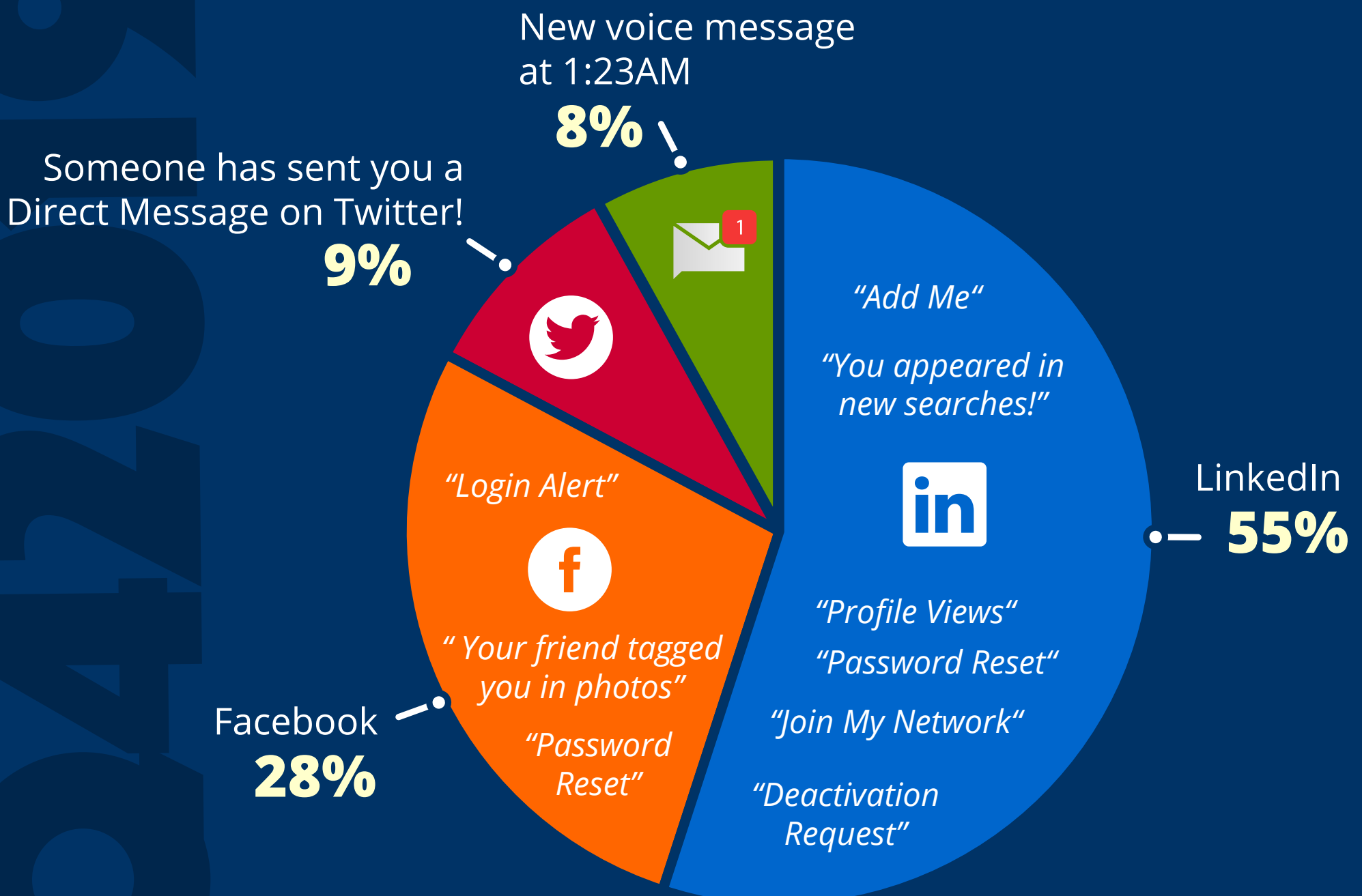


TOP-CLICKED PHISHING TESTS

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 "you appeared in new searches" 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%
	Please review: Appropriate Halloween costumes	14%
	Change of Password Required Immediately	14%
	Starbucks: Free Drink for the Holidays	11%
	New Message about [[company_name]] Holiday Party	7%
	You have been drawn a name for Holiday Gift Exchange	6%
	IT: Scheduled Server Maintenance -- No Internet Access	6%
	FYI - Important information about your insurance	6%
	HR: Revised Vacation & Sick Time Policy	6%
	Microsoft/Office 365: De-activation of Email in Process	5%

KEY TAKEAWAY



Hackers are playing into employees' desires to remain security minded. Their curiosity is piqued with delivery attempt messages and HR-related messages that could potentially affect their daily work. At the end of the year, holiday-related and seasonal message get users to click without thinking twice.



COMMON "IN THE WILD" ATTACKS

- SharePoint: Approaching SharePoint Site Storage Limit
- Microsoft: Anderson Hauck has shared a Whiteboard with you
- Office 365: Medium-severity alert: Unusual volume of file deletion
- FedEx: Correct address needed for your package delivery on [[current_date_0]]
- USPS: Your digital receipt is ready
- Twitter: Your Twitter account has been locked
- Google: Please Complete the Required Steps
- Cash App: Your Account Has Been Closed
- Coinbase: Important Please Resolve Error Now
- Would you mind taking a look at this invoice?

KEY TAKEAWAY



The potential for gaining something of value is a common reason for clicks; several of these messages refer to transactions. Another common theme is a push for action required. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.