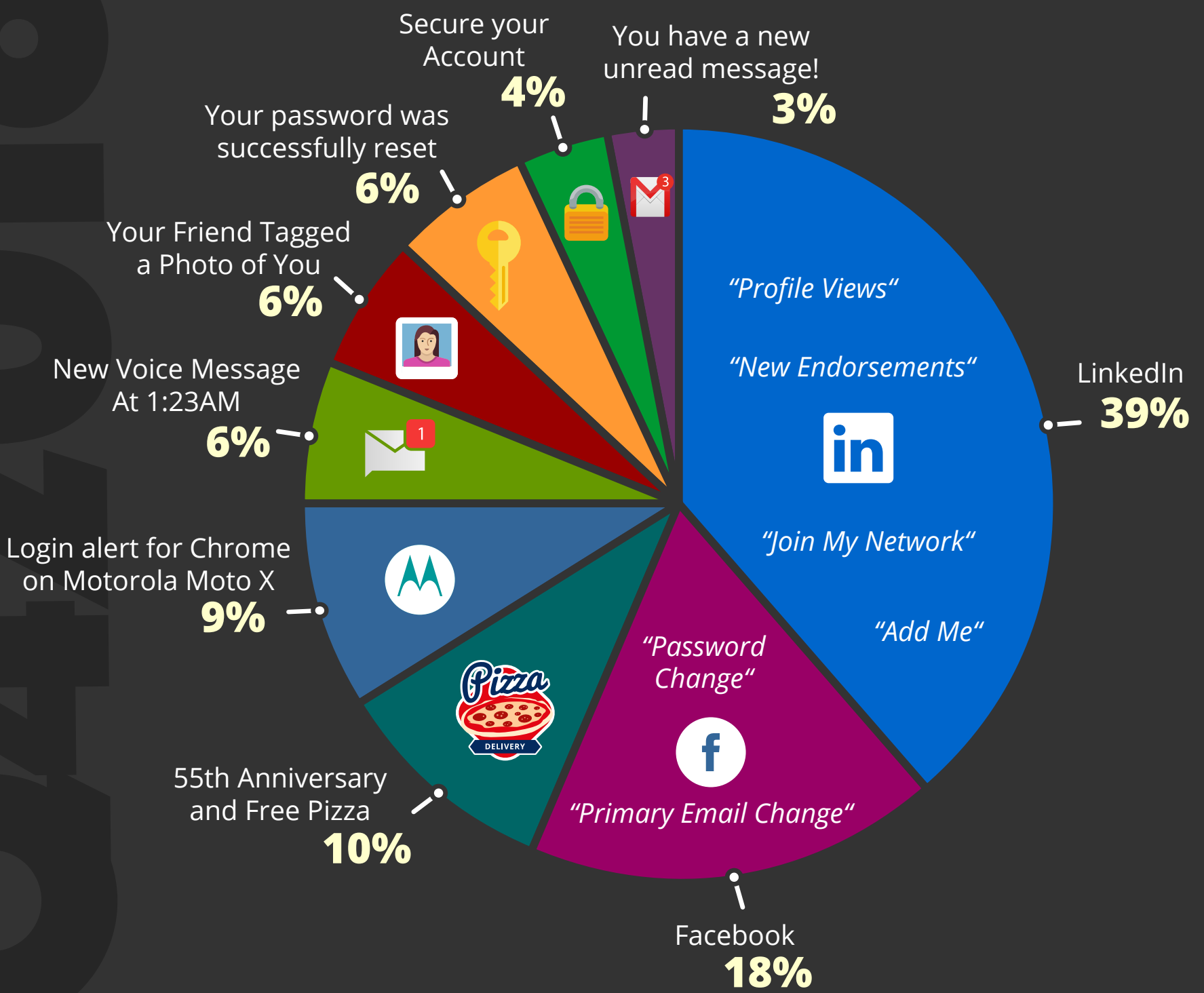


TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY



The curiosity and feeling of importance that a tagged photo, profile view or endorsement can sail past an individual's normal defenses. Other alerts that contain warning types of messages can bring about feelings of alarm and cause an individual to make a panicked decision. And everyone loves free pizza!

TOP 10 GENERAL EMAIL SUBJECTS

	Password Check Required Immediately	19%
	Your Order with Amazon.com/Your Amazon Order Receipt	16%
	Announcement: Change in Holiday Schedule	11%
	Happy Holidays! Have a drink on us.	10%
	Problem with the Bank Account	8%
	De-activation of [[email]] in Process	8%
	Wire Department	8%
	Revised Vacation & Sick Time Policy	7%
	Last reminder: please respond immediately	6%
	UPS Label Delivery 1ZBE312TNY00015011	6%

KEY TAKEAWAY



Hackers are playing into employees' desires to remain security minded. There's also an intrigue of mystery that often makes people curious enough to click (i.e., new voicemail, order on the way). Password management is a popular way to get people to click on a link.



COMMON "IN THE WILD" ATTACKS

- Apple: You recently requested a password reset for your Apple ID
- Employee Satisfaction Survey
- Sharepoint: You Have Received 2 New Fax Messages
- Your Support Ticket is Closing
- Docusign: You've received a Document for Signature
- ZipRecruiter: ZipRecruiter Account Suspended
- IT System Support
- Amazon: Your Order Summary
- Office 365: Suspicious Activity Report
- Squarespace: Account billing failure

KEY TAKEAWAY



The desire to receive communications intended for the individual is strong. The potential of something being wrong and/or at risk also plays into the human psyche, leaving the individual to think that he/she must act immediately to resolve the issue. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.