TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS

Q3 2017

5% Unread Message

9% New Voice Message

9% Free Pizza

12% Tagged Photo

24% Login Alert

"Add Me"

"Join Network"

LinkedIn **41%**

"Reset Password"

"New Message
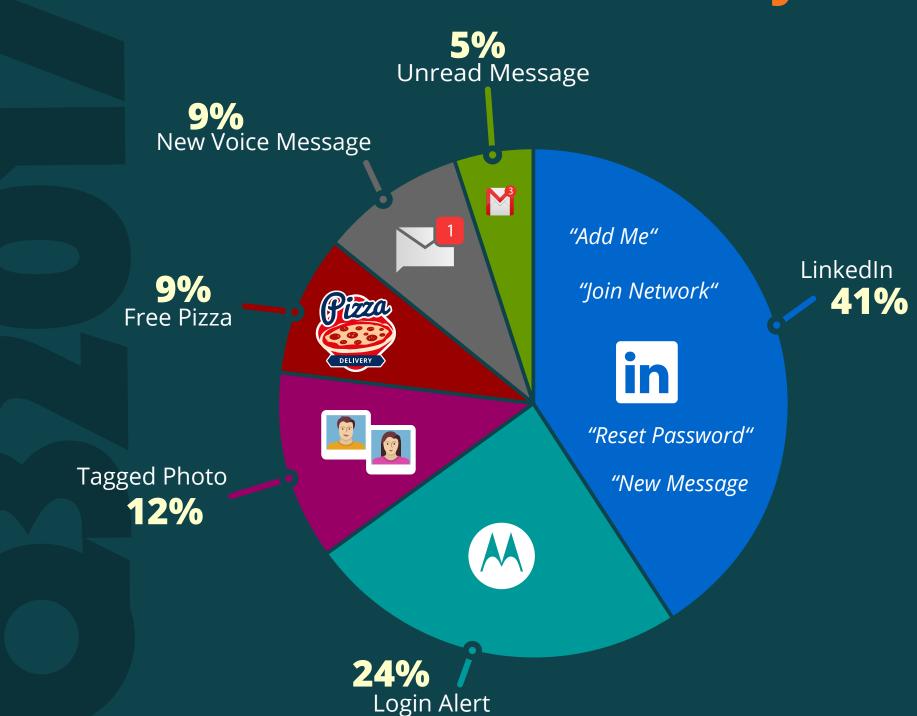
KEY TAKEAWAY

Certain types of messages sail through personal security defenses because they play into the human psyche. Whether it is wanting to be popular or recognized, these types of email make someone feel important. And people love free pizza!

TOP 10 GENERAL EMAIL SUBJECTS

Subject	%
Official Data Breach Notification	14%
UPS Label Delivery 1ZBE312TNY00015011	12%
IT Reminder: Your Password Expires in Less Than 24 Hours	12%
Change of Password Required Immediately	10%
Please Read Important from Human Resources	10%
All Employees: Update your Healthcare Info	10%
Revised Vacation & Sick Time Policy	8%
Quick company survey	8%
A Delivery Attempt was made	8%
Email Account Updates	8%

KEY TAKEAWAY

Email is an effective way to phish users when disguised as legitimate email. These methods allow attackers to craft and distribute enticing material for both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.

COMMON *"IN THE WILD"* ATTACKS

- LinkedIn: Important Security Update
- Amazon: Kindly update your account with Amazon to avoid shutdown
- Email account will be closed
- Office 365: Incoming mail on hold
- We have created your ticket for server upgrade
- Credit Card Details Follow Up
- USAA: E-Money Pending Approval
- PayPal: Problem with Account ID
- Synchrony Bank/Walmart: Account Alerts
- COURT NOTICE FILED AGAINST YOU

KEY TAKEAWAY

These attacks are effective in that they are using the personal rewards of the target as the lure. Also, a single-stage phish is easier to accomplish than multi-stage because it exploits an immediate psychological 'knee jerk' impulse.