The common theme we see here is the push for action required. One message even has an exclamation point, which emphasizes the urgency of the message. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

Hackers are playing into employees’ emotions, causing them to panic when they see a de-activation of [email] in process. Their curiosity is piqued with delivery attempt messages and orders from Amazon. And who can resist HR-related messages that could potentially affect the daily work of employees?

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as “new message” or “add me.” Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as new message or a friend tagged a photo of you can make someone feel special and entice them to click.

COMMON "IN THE WILD" ATTACKS

- Wells Fargo: You have a new secure mail
- Undelivered Mail
- Etrade: Action Required!
- Microsoft Teams: Rick sent a message
- Microsoft/Office 365: Action required: Update your payment information now
- Stripe: Just now someone logged in to your account
- HR: Your Action Required
- Amazon: Refund Notification
- OneDrive: Your OneDrive is out of storage space
- HR: Download your W2 now

The common theme we see here is the push for action required. One message even fits an exclamation point, which emphasizes the urgency of the message. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.