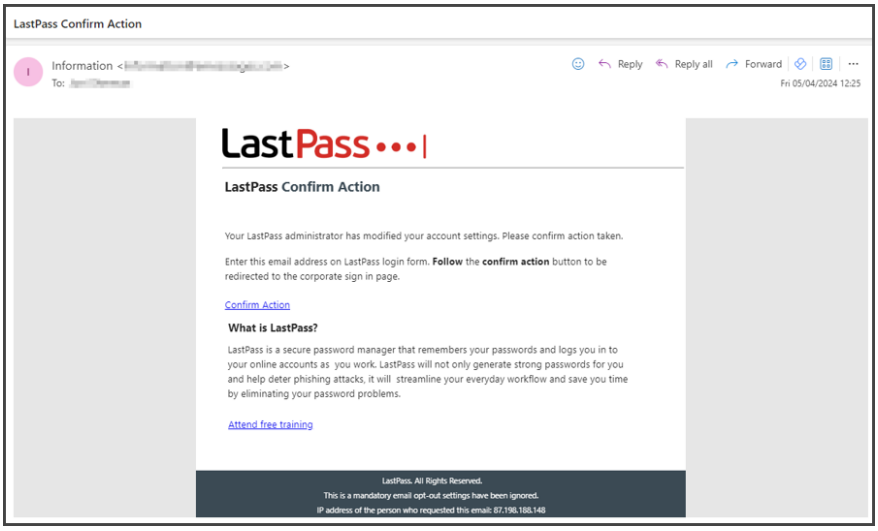
Phishing Simulation:
Sample Lures

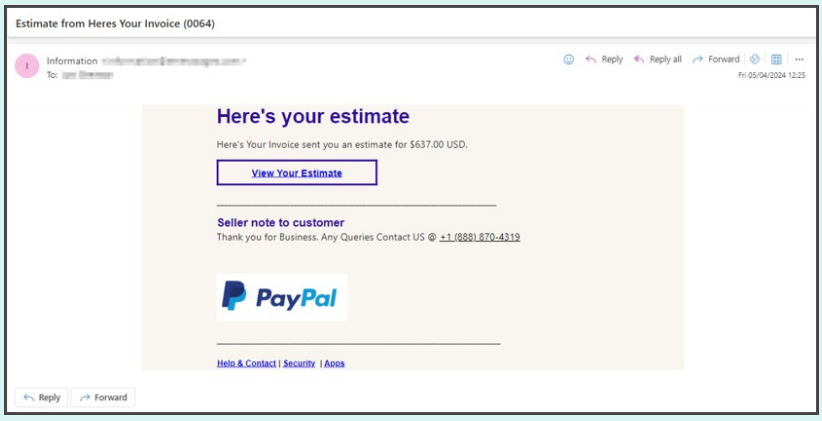
TitanHQ's specialized phishing simulation emails —lures— are uniquely designed to protect your organization against ever increasing cyber threats. By leveraging our comprehensive set of carefully created lures in a phishing simulation, you can raise awareness, build resilience, and help users mitigate against the risk of falling victim to a phishing attack.

Every TitanHQ lure is tailored to a specific phishing threat category. Read on for a brief description and sample lure for each category.

Threat Category: Urgent Account Verification & Subscription Alerts

This threat category mimics urgent requests to verify account details or renew subscriptions and are often used by attackers to elicit sensitive information. These lures enable employees to identify common indicators of fraudulent emails and respond appropriately to safeguard their accounts and personal information.



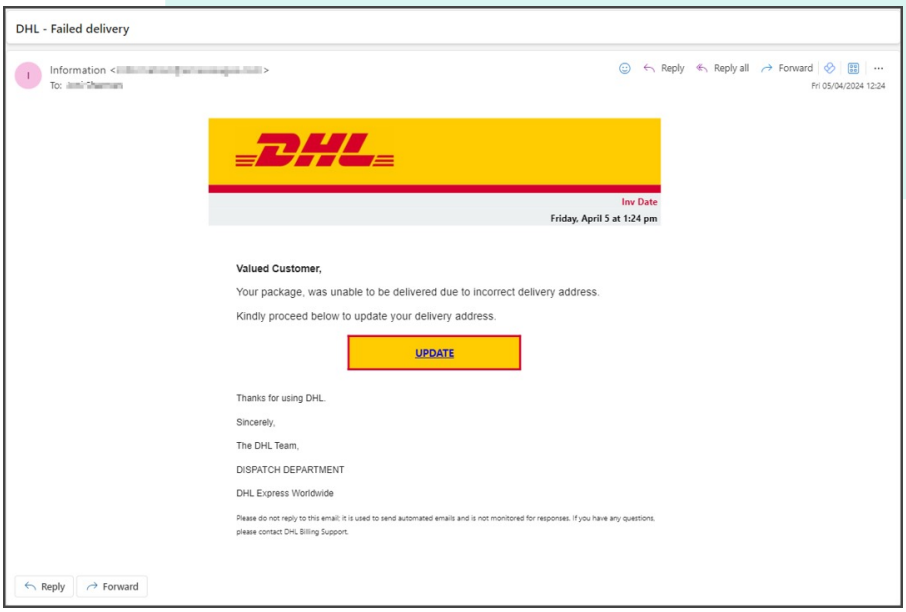


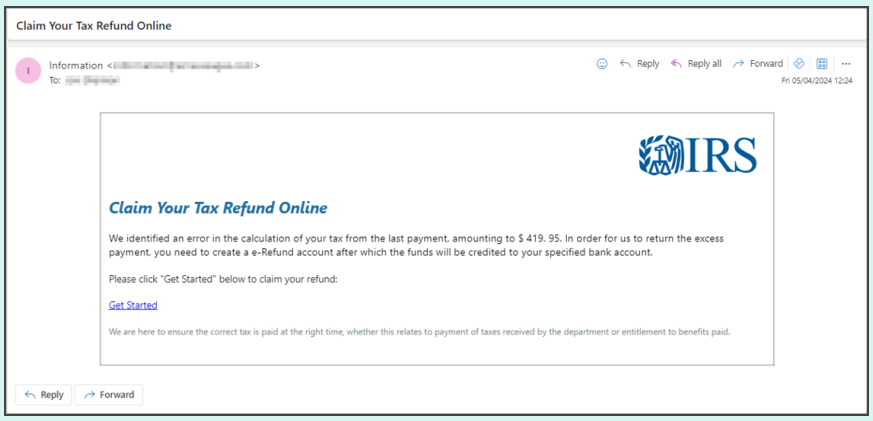
Threat Category: Fake Invoices or Payment Requests

Lures containing counterfeit invoices or fraudulent payment requests are designed to trick recipients into making unauthorized payments or revealing financial details. With these lures, employees learn to scrutinize invoice details, verify sender authenticity, and confirm payment requests through trusted channels, minimizing the risk of financial fraud.

Threat Category: Shipping and Delivery Notifications

Shipment tracking and delivery notifications are often exploited by phishing attackers to lure recipients into clicking malicious links or downloading malware. This category of lure helps employees learn how to verify the authenticity of shipping notifications, cross-reference tracking numbers, and exercise caution when interacting with unfamiliar delivery-related emails.



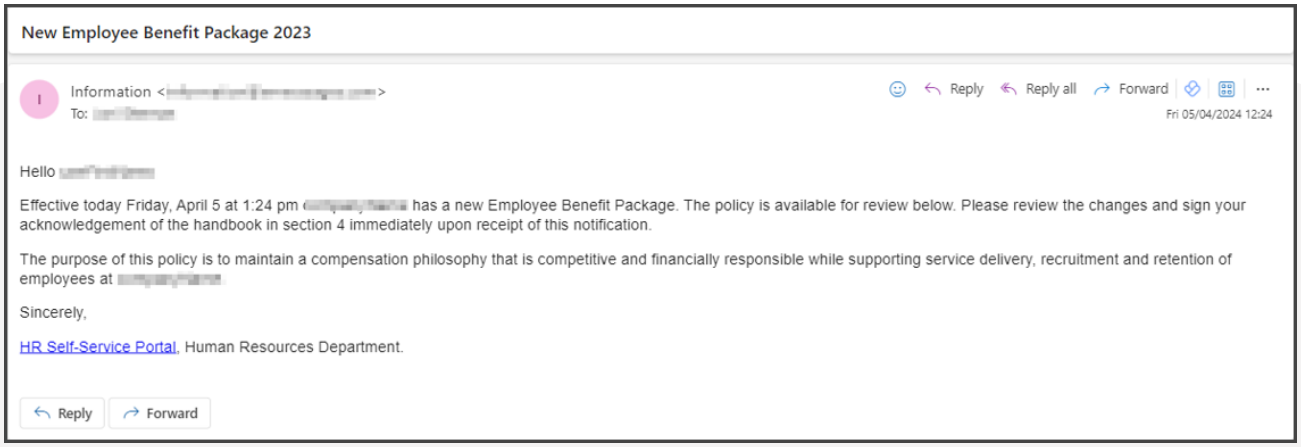


Threat Category: IRS & Tax Scams

Lures in this category purport to be from tax authorities or government agencies, falsely claiming owed taxes or promising refunds in exchange for personal information. These lures help users to recognize common characteristics of tax scams, such as unsolicited requests for sensitive data or threats of legal action, and report suspicious communications promptly.

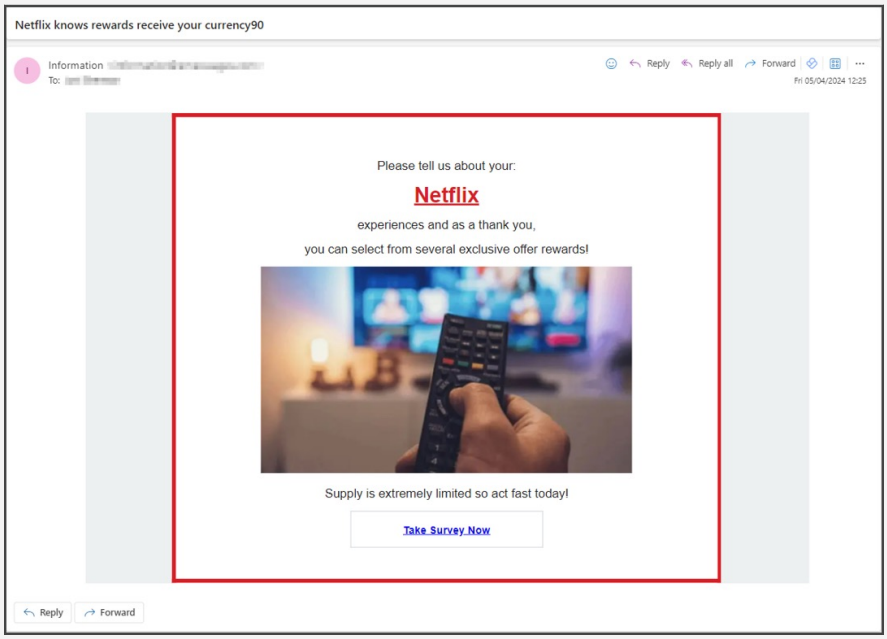
Threat Category: Job Offers, Benefits & Work-From-Home Opportunities

Emails that offer enticing employment opportunities, or attractive benefits, are often used to lure job seekers into divulging personal or financial information. These simulation emails equip employees with the skills to verify the legitimacy of job offers, research company backgrounds, and avoid falling victim to employment-related scams.



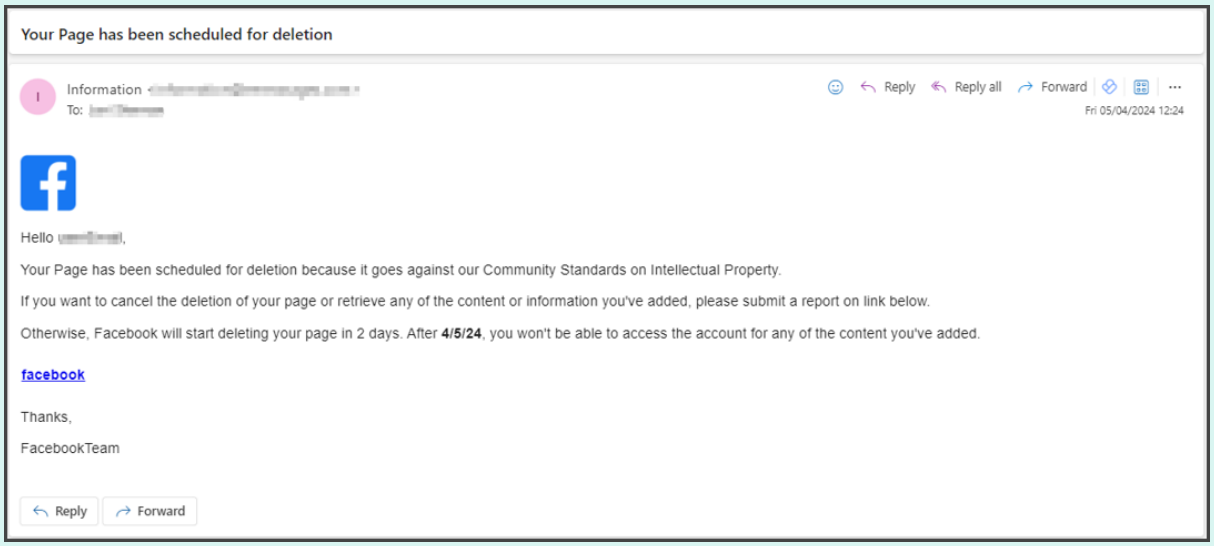
Threat Category: Gift Card Giveaways & Surveys

Lures promising free gift cards or rewards in exchange for participating in surveys, or providing personal information, are commonly used by phishing attackers to harvest sensitive data. With these lures, employees learn to distinguish between genuine promotional offers and deceptive schemes, minimizing the risk of identity theft or financial exploitation.



Threat Category: Social Media Alerts & Work Messengers

Simulated notifications, or messages resembling legitimate social media alerts or internal communication platforms, are often exploited by phishing attackers to distribute malware or initiate social engineering attacks. These lures help employees to verify sender identities, scrutinize message content for suspicious links or attachments, and exercise caution when engaging with online communications.



TitanHQ

About TitanHQ

TitanHQ offers a best-in-class SaaS Cybersecurity Platform delivering a layered security solution to prevent user vulnerability. Our MSP-centric platform enables our partners to generate recurring revenue through the sale of our solutions to SMBs and to scale and effectively manage their businesses.