BOLSTER

Beyond Email: The Rise of Multi-Channel Phishing Attacks

Highlights from Bolster Research's Phishing in Focus: A 2024 Mid-year Report on AI, Disinformation, Election and Identity Fraud

Read the Full Report →

KEY FINDINGS

38K+ New daily phishing sites launched over the first half of 2024.

170% Increase in phishing attacks originating from social media.

102% Increase in attacks from Feb to June 2024 originating from mobile app stores.

75% Of threat actor groups targeting the election are from China, Russia and Iran.

514% Increase in domains using "election", which reflects growth in election-specific scam sites.

2X More phishing sites in May 2024 than in May 2023 which is the hotspot month for scam activity.

40+ Phony and lookalike CrowdStrike domains created after the outage.

#1 Technology is the most heavily targeted industry for phishing scams.

15% Increase from 2023 to 2024 in payment-based phishing scams.

The Bolster Research **Phishing in Focus 2024 Mid-Year Report** provides insight into the trends around the evolving landscape of phishing attacks and scam techniques. Leveraging CheckPhish data from the Bolster Research Lab, the report covers a seven-month period from January through July 2024. This document summarizes the key findings from this report.

AI Ignites Unprecedented Surge in Scam Wave

Hackers use AI to create realistic scams and phishing attacks across various platforms at new levels of speed and scale. The daily count of new phishing attacks keeps climbing, with over 38,000 new sites launched each day the first half of 2024.

Phishing Attacks Have Diversified Beyond Email

Cybercriminals now use a multi-pronged approach that includes text messages, social media, email, malicious domains and voice calls to reach a wider audience and increase their chances of success. Phishing sites from social media increased by 170% from March through April, and attacks originating from mobile app stores increased by 102% from February to June.

Foreign Actors Launch US Election Themed attacks

Nation-state threat actors are launching US presidential related phishing attacks, spam campaigns and data breaches that enable fraud, data, identity and financial theft. China, Russia and Iran drive 75% of the activity.

Sun, Sand and Scammers

Phishing attacks spike during the summer shopping season, particularly in May and June, with fake online stores and fraudulent vacation deals. There were 2x more phishing sites in May 2024 than May 2023.

CrowdStrike Outage Creates the Emergence of Phishing Sites

Capitalizing on the disruption following the CrowdStrike outage, threat actors created phishing and phony lookalike domains targeting CrowdStrike users. In the first 24 hours of the outage alone, over 40 CrowdStrike typosquat domains were created

ABOUT BOLSTER RESEARCH'S CHECKPHISH DATA

CheckPhish collects a massive amount of data on phishing and scam activities through its URL scanning service. Bolster Research uses insights from this data to understand the overall phishing threat landscape and to contribute to the Bolster Research Phishing in Focus reports.

Technology, Finance, E-Commerce, Entertainment and Marketing Are Prime Targets

These sectors are the top five most vulnerable to phishing and scam attacks because of their abundance of valuable data and digital assets, making them prime targets for financial gain.

United States, Germany and Canada Lead Phishing Domain Registrations

Economic prosperity, widespread internet use, and a trusting public make the U.S., Germany, and Canada lucrative targets for phishing attacks. Sites hosted on U.S. based Cloudflare and Amazon comprise two-thirds of all phishing sites.

Payment-Related Phishing Attacks are Thriving

Payment and transaction providers are increasingly targeted by phishing attacks due to the lucrative rewards and the ease of selling stolen payment data on the dark web. Payment-based phishing scams have increased 15% so far from last year.

Stealing Sensitive Data Is the Top Intent Category For Phishing

Threat actors are still executing their phishing attempts primarily to steal sensitive data. Domain parking and domain purchasing are ranked next in intent, with the goal of conducting brand impersonation.

Summary

Phishing is evolving in 2024 because of GenAI, which enables cybercriminals to launch more sophisticated and widespread attacks across multiple channels. Nation-states and organized criminal groups are capitalizing on this technology to target individuals and businesses. The heightened emotions surrounding the presidential election provide an ideal environment for these cybercriminals to succeed.

Bolster is on a mission to make the internet a safer place by eradicating threats from your online experience. We deliver phishing and scam protection for companies fo all sizes by automating the detection and takedown process through generative AI. Attackers are leveraging different channels to impersonate organizations and individuals as well as launch their online attacks. Because we think everyone deserves a safe internet experience, we also created CheckPhish, a community tool to help anyone discover and monitor sites for phishing or scam activities.

Backed by leading investors like M12, Thomvest, Cervin, and Crosslink, and founded by threat research leaders, many of the world's leading brands over 20% of Fortune 500 rely on Bolster and CheckPhish today.