SLASHNEXT SECURITY

The State of PHISHING

2024 Mid-Year Assessment

A mid-year look at the LATEST phishing trends that are sweeping the globe and what is required to stop them.

KEY FINDINGS

341%

INCREASE IN MALICIOUS EMAILS
In the Last 6 months

856%

INCREASE IN MALICIOUS EMAILS
In the Last 12 months

4151%

INCREASE IN MALICIOUS EMAILS
Since Launch of ChatGPT
(November 30, 2022)

29%

INCREASE IN BUSINESS EMAIL COMPROMISE
Since January 2024

45%

ALL MOBILE THREATS ARE SMISHING
In the Last 6 months

11%

ALL PHISHING EMAILS ARE QR BASED PHISHING
In the Last 6 months

59K

AVERAGE NEW THREATS PER DAY HOSTED ON TRUSTED DOMAINS
In the Last 6 months

217%

INCREASE IN CREDENTIAL PHISHING
In the Last 6 months

EXECUTIVE SUMMARY

The State of Phishing report published in October 2023 unveiled a stark reality: the threat landscape had been dramatically altered by the introduction of ChatGPT in November 2022. Cybercriminals had swiftly adapted, using large language model (LLM) chatbots to launch a multitude of highly targeted phishing attacks at an alarming scale. The surge in phishing attacks we reported in late 2023 prompted us to conduct a comprehensive analysis at the six-month mark. The goal was to determine if the upward trend in phishing attacks was continuing and to identify the types of threats organizations were facing from October 2023 to March 2024.

The battle against cyber threats is an ongoing struggle, with hackers demonstrating a relentless pursuit of innovative methods to exploit generative AI. From jailbreaks to malicious LLMs, they are constantly evolving their tactics to breach cybersecurity. The threat of credential phishing,

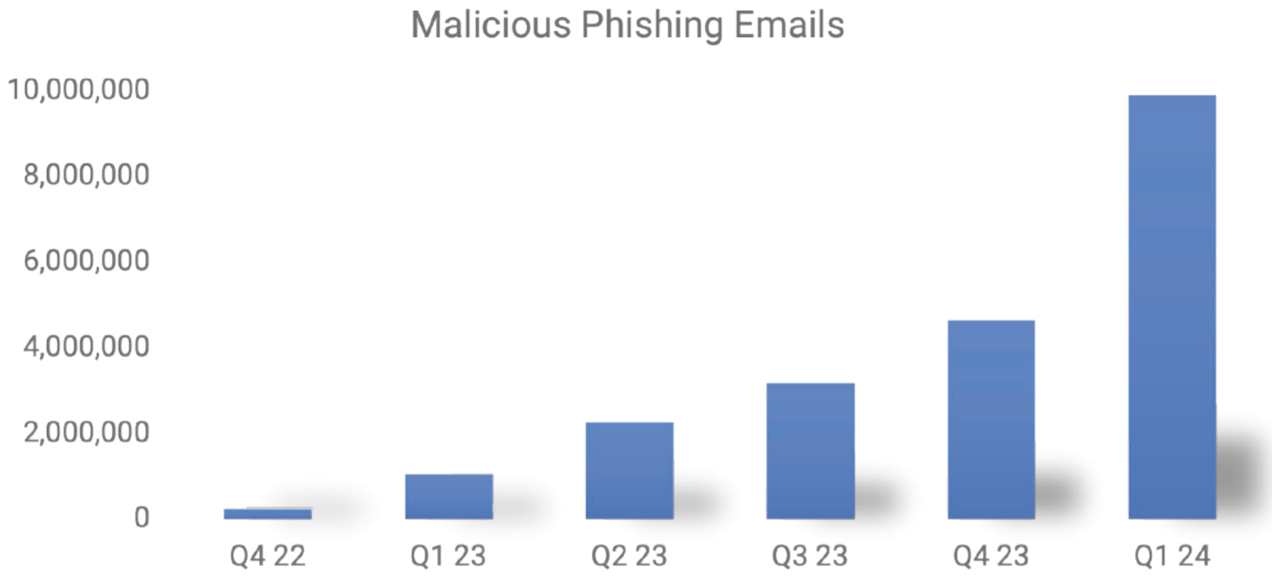


Exhibit 1: Phishing has increased by 341% in the last six months and 856% in the last 12 months.

BEC, and trusted services attacks remains significant. QR-based phishing now constitutes a substantial 11% of all email phishing threats.

This half-year report urgently underscores the evolving landscape since the last State of Phishing report, with certain trends escalating at an alarming rate. In the past six months, SlashNext Threat Labs witnessed a staggering 341% surge in malicious emails, catapulting the 12-month increase to a daunting 856%. Since the advent of ChatGPT in late 2022, the number of malicious emails has skyrocketed by 4151% (Exhibit 1).

Text-based BEC attacks have surged by another 29% since the beginning of 2024, and mobile phones persist as the most utilized and vulnerable communication channels, with 45% of all mobile threats reported as smishing. The use of generative AI has undeniably fueled the phishing surge, and security teams that are not leveraging generative AI to counter these attacks are perilously close to a breach.

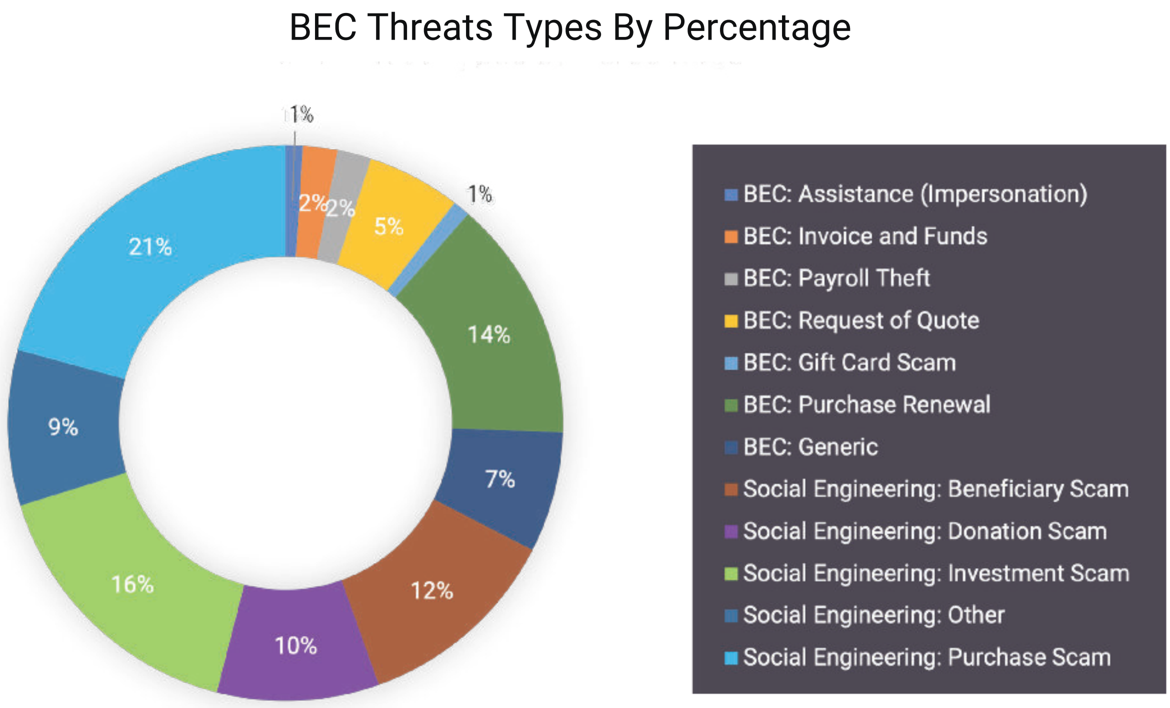

BEC Threats Types By Percentage

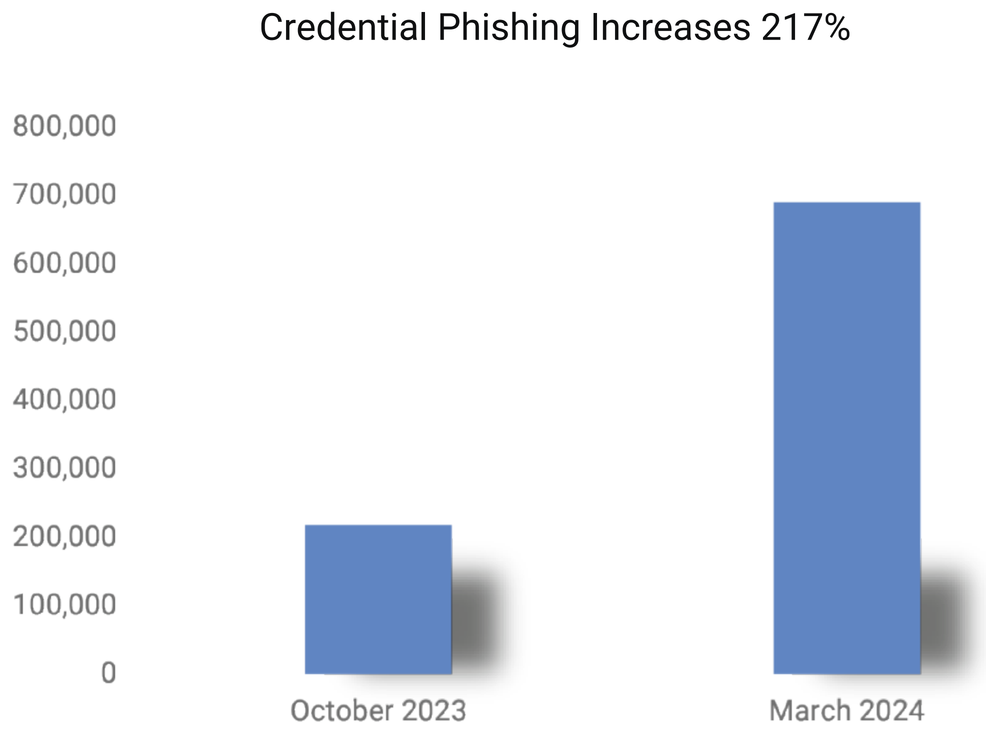
Exhibit 2: Types of BEC Threats.

GENERATIVE AI IS STILL A BIG TREND IN 2024

Generative AI has witnessed an astounding surge in the past 16 months, with a remarkable 86% of IT leaders foreseeing its pivotal role in their company's future (Salesforce). By 2026, an estimated 90% of online content could be AI-generated (Europol). This rapid expansion poses significant challenges for both the defenders and perpetrators of cybercrime, from IT departments to the Dark Web, underscoring the urgent need for the infosec community to develop robust countermeasures.

For cybercriminals, the advent of generative AI tools has ushered in a new era of sophistication, enabling more advanced BEC attacks (Exhibit 2), refined social engineering tactics, and enhanced malware. This dynamic landscape necessitates the infosec community to stay ahead of the curve, as generative AI holds the promise of better detection. Security vendors who are proactive in developing generative AI technology are well-positioned to tackle these evolving threats.

Despite the strides in technological advancements, it's crucial to remember that people remain an organization's most targeted and vulnerable aspect. The surge in multi-stage attacks across various platforms, including email, mobile, and collaboration tools, serves as a stark reminder of



how cyberattacks have evolved, with hackers now targeting less protected channels like mobile. This human element of cybercrime underscores the imperative need for comprehensive security measures.

Credential phishing is the number one access point for breaches. According to the Verizon 2024 Data Breach Investigations Report, the rate of users falling for phishing attacks and clicking on embedded links has increased, with a median time of 21 seconds to click on a malicious link after the email was opened, and then only another 28 seconds for the user to enter their data. Credential phishing is big business for hackers looking for access to ransomware, data exfiltration, and intellectual property. It has the biggest volume of all phishing campaigns and spans email, mobile, social, and collaboration, with a spike in growth since October of 217%. (Exhibit 3)

Cybercriminals still favor using legitimate, trusted services to hide phishing and malware. By using trusted domains, attackers have more anonymity. It's hard for users to identify these types of attacks, and taking down this malicious content is often more complex, which gives hackers more time to perpetrate these attacks. Microsoft Sharepoint, AWS, Salesforce, and other trusted service vendors are the most popular legitimate infrastructures to host phishing and malware.

Cybercriminals are steadily becoming more clever by investing in more sophisticated ways to deceive users and the security tools in place to protect them. Two big trends that are increasing are QR code phishing and CAPTCHA-based attacks.

CAPTCHA-based attacks have increased and are being used to mask credential harvesting forms. CAPTCHA is used to prevent automated bots from creating fake accounts or submitting spam. Attackers are exploiting this tool by generating thousands of domains and implementing CloudFlare's CAPTCHAs to hide credential phishing forms from security protocols that are unable to bypass the CAPTCHAs.

QR-based email attacks have grown across all companies, from SMBs to large enterprises. There was a spike in these types of attacks in 2023, and now 11% of all malicious emails are QR-based attacks. Security vendors and organizations need technology that can identify malicious QR codes in emails and all messaging channels, including personal email and mobile apps, to stop these threats before they experience a costly breach.

SLASHNEXT GENERATIVE AI

Email is still the primary tool for communication and collaboration, and it’s a rich target for cybercriminals seeking to exploit user vulnerabilities. Generative AI has exacerbated this issue, enabling attackers to launch Business Email Compromise (BEC) and advanced phishing attacks like executive impersonation, invoice fraud, QR phishing, and ransomware with unprecedented scale and ease. In addition, attackers are expanding their focus to adjacent communication channels such as SMS, Teams, and Slack. These sophisticated attacks can only be stopped by augmenting Microsoft Defender for Office 365.

SlashNext’s advanced AI platform is purpose built to anticipate and stop sophisticated BEC threats, phishing, and ransomware. The service delivers industry leading 99.9% detection rate and 1 in 1 million false positive rate by utilizing Gen AI, natural language parallel prediction, computer vision, relationship graphs, and contextual analysis for:

- Broad threat coverage due to large and diverse LLMs
- Highest accuracy and a 48-hour detection advantage to stop sohisticated zero-hour threats
- Increased SecOps and user productivity from using a solution with the highest detections and the lowest false positives rates
- 360° protection with threat protection across all messaging channels: in email, mobile and web

The SlashNext AI Security platform includes:

- **Cloud Email Security:** Next Gen AI detects BEC and advanced phishing threats for inbound, outbound, and internal emails, with 48-hour detection advantage.
- **Comprehensive Threat Coverage**: Uniquely trained AI classifiers identify all forms of BEC, social engineering and advanced phishing threats with accuracy and precision.
- **AI Threat Insight**: Delivers advanced security analytics, offering comprehensive insights into the rationale behind AI’s classification of threats.

- **Spam/BulkMail**: Automatically detects and removes unsolicited bulk emails from user inboxes to improve employee productivity and reduce SecOps hours spent on abuse inbox management.
- **Email+ Security**: Extends protection to adjacent channels, such as SMS, Slack, Zoom, Teams, Gmail and other messaging apps on mobile devices and computers.
- **Unified Administration Console**: A single pane of glass for deployment, configuration, and reporting.
- **API Integration Ecosystem**: Seamlessly ingest advanced security events into Microsoft Sentinel, Splunk, or any SIEM solution.

Get a Customized Email Security Risk Assessment

See if your organization's current email security stops the latest Business Email Compromise (BEC), malicious attachments, and malicious exploits by plugging into SlashNext Cloud Email Security in observability mode. Deploy in minutes with no impact on your existing email infrastructure or mail flow. Receive a customized report detailing the attacks missed by your current email security.

- Fast and Easy: With one click, deploy in minutes a read-only API integration with no impact on your existing email infrastructure. We will analyze your current email for security threats and deliver a customized report of attacks.
- Actionable Insights: The customized report provides a clear and insightful view of your organization's email security. Our goal is to offer data-driven insights to make informed decisions, fortify your cybersecurity measures, and ensure your organization's protection.
- Comprehensive Summary: Receive a summary of the impact on your organization and where your current security defenses stand today. See how you can improve security readiness and save valuable SOC time and operating expenses.

For more information visit https://slashnext.com/risk-assessment/

Report data and methodology: The report data represents threats detected by SlashNext security products. SlashNext analyzed billions of link-based, malicious attachments and natural language threats scanned in email, mobile, and browser channels during a 6-month period from Q4 2023 to Q1 2024. The organizations in our sample ranged in size from 500 to 250,000 users, spanning a variety of industries.

About SlashNext

SlashNext Complete™ AI Security for Email, Mobile and Browser

At SlashNext, we know that the demands of a changing and growing threat landscape increase the need to protect people where they work in real time. That's why SlashNext Complete delivers zero-hour protection for how people work today across email, mobile, and browser apps. With SlashNext's generative AI to defend against advanced business email compromise, Smishing, spear phishing, executive impersonation, and financial fraud, your people are always protected anywhere they work. Request a demo today. slashnext.com/request-a-demo/

Contact Us

6701 Koll Center Parkway, Suite 250
Pleasanton CA 94566

Contact Sales 1(800) 930-8643

Request a Demo https://www.slashnext.com/request-a-demo/