SLASHNEXT

NEXT GEN AI EMAIL+ SECURITY

Prepare for 2025

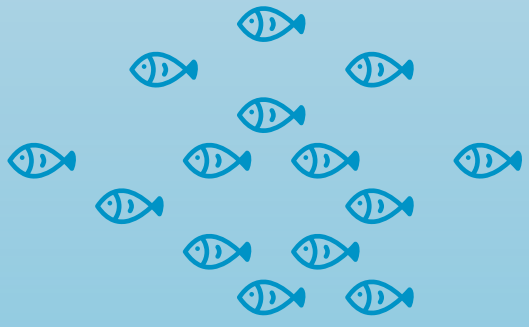
2024 Phishing Intelligence Report

Table of contents

Executive Summary

The 2024 phishing landscape reveals an unprecedented surge in attack volume, with a 202% increase in phishing messages in the second half of 2024, and credential phishing attacks rising 703% in the same period. Organizations face nearly one advanced attack per mailbox weekly, while mobile users encounter up to 600 threats annually, highlighting the critical shift from email-only to multi-channel attack vectors. Our analysis shows that 80% of malicious links in attacks are previously unknown zero-day threats, demonstrating that traditional threat intelligence and signature-based detection methods are increasingly ineffective against modern, AI-powered attack campaigns.

Looking ahead to 2025, we expect this rapid evolution to accelerate, with AI-generated attacks becoming more sophisticated and harder to detect, while attackers increasingly target messaging platforms beyond email, including business collaboration tools, SMS, and social media. The bottom line is phishing isn't an email-only problem anymore; it is a broader messaging security problem that requires a fundamental shift in how organizations approach threat detection and prevention.



Introduction

Welcome to SlashNext's 2024 State of Phishing report, where we uncover the most critical insights from the current threat landscape. We analyze the key attacks and trends of the past year, using data to determine whether phishing threats are escalating, stabilizing, or declining. Discover what to expect in 2025 and the emerging attack vectors you must watch out for.

Key Findings

Before diving into the detailed analysis, let's examine the critical insights that emerged from our research. These key findings highlight the most significant trends and developments that security leaders should consider when evaluating their threat prevention strategy.

Email Attacks

Overall email attack volumes increased 202% in the second half of 2024, trending up as we approach 2025.

Up 202% ↗

Advanced Phishing

Users receive at least 1 advanced phishing link every week that bypasses traditional network security controls.

Users get advanced phishing every week!

Mobile Threats

Users encounter up to 600 mobile threats annually on average.

600 threats/yr

Top Email Attack Vector

Malicious email link-based attacks are the top email attack vectors, with email text-based attacks following close behind.

#1. Link-based
#2. Text-based

Attacks Inside and Outside of Email

Top attack technique categories, link-based and text-based, can change as fast as weekly; organizations must have a comprehensive strategy for all attack types inside and outside of email.

Attacks changing weekly!

Social Engineering

Social engineering continues to be ever-present, rising 141% throughout the second half of 2024.

Up 141% ↗

New and Unknown Threats

On average, 80% of the links in email link-based threats are new and unknown.

80%!

Credential Phishing Up

In the second half of 2024, credential phishing is up 703%.

Up 703% ↗

Overview of Phishing

Phishing remains one of the most significant cyber threats impacting organizations worldwide. By deceiving individuals into revealing sensitive information or installing malware through seemingly legitimate communications, phishing attacks can lead to severe financial losses, legal issues, and damage to an organization's reputation. To combat these threats effectively, it is crucial to understand the various types of phishing attacks and the tactics employed by cybercriminals.

Phishing is a cyberattack where attackers deceive people into revealing sensitive information or installing malware through fraudulent communications that appear legitimate. Phishing attacks, including spear phishing, BEC, and credential phishing, can severely impact organizations by compromising sensitive data, leading to financial losses, legal liabilities, and reputational damage. These attacks exploit social engineering tactics and can result in unauthorized access to systems, financial fraud, data breaches, and loss of customer trust, ultimately affecting the organization's bottom line and operational integrity.

Multichannel Phishing

Phishing attacks that exploit multiple communication channels beyond email to deceive victims, such as browser links, QR codes, SMS, or cloud-based collaboration tools.

Spear Phishing

A targeted phishing attack aimed at specific individuals or organizations through personalized malicious emails.

Credential Phishing (Credential Harvesting)

A type of cyber-attack focused on tricking individuals into revealing their login credentials through deceptive emails, websites, or messages.

Social Engineering

A set of tactics used to manipulate, influence, or deceive people into divulging sensitive information or performing actions that aid cyber-attacks. For example, attacks categorized as business email compromise (BEC) fall into this category.

Browser Messaging Phishing

Phishing attacks that leverage browser messaging services, direct messaging platforms like LinkedIn, social media, chat services like Slack or Microsoft Teams, or personal communication tools (e.g., personal Gmail accounts) to trick users into clicking malicious links.

Mobile Phishing

Phishing attacks targeting mobile devices through links to malicious mobile websites, SMS text messages (SMiShing), or QR code phishing.

Overall Phishing Trends

Let's look at the overall trends for email-born attacks over the year in Figure 1 below. When you look at these graphs, please note all figures presented represent advanced threats detected per 1,000 mailboxes and delivered on a weekly basis (unless otherwise noted). We measure the prevalence of threats per 1,000 mailboxes to provide a clear, consistent view of risk across businesses of all sizes. This allows for an apples-to-apples comparison, whether an organization has 100 mailboxes or 100,000. Notably, these advanced threats bypass legacy and first-generation AI email security systems.

Our mid-year State of Phishing report showed a significant increase in email attacks from February to March. This surge was noticeable across all email attachment methods. We won't spend a lot of time repeating what we've already reported; instead, we will focus on the interesting trends emerging in the latter half of 2024.

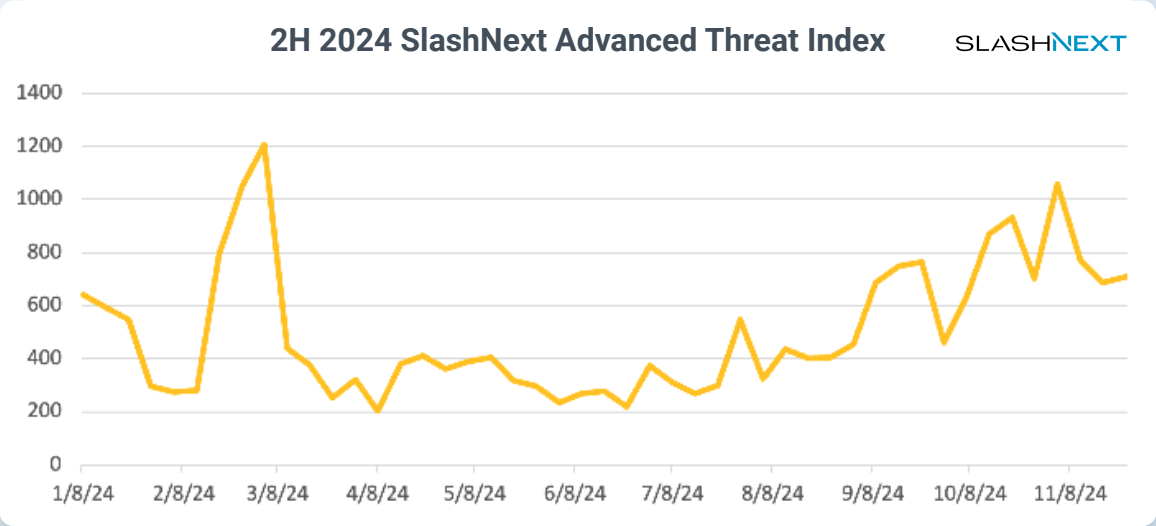


Figure 1. Overall advanced threat index covering all email-based threat types

A 202% rise! ↗

Instead of experiencing a large, sudden spike in attacks like in the first half of 2024, we saw a steady and consistent rise in the overall volume of phishing attacks. As you can see in Figure 2, mapping the changing nature of the volume of phishing attacks and adding an overall trend line shows this consistent rise.

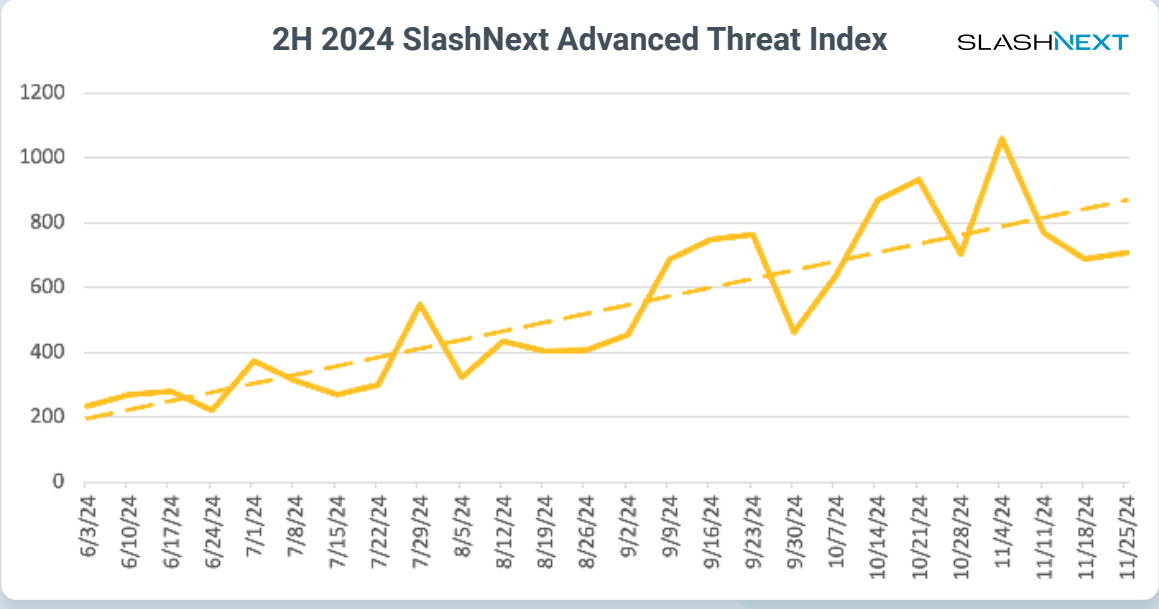


Figure 2. Second Half of 2024 overall email threat trend and trendline

Since June, the number of attacks per 1,000 mailboxes each week has increased linearly. Currently, we are capturing close to one advanced attack per mailbox each week. As we reach the 1,000 threshold, this translates to nearly one advanced attack for every single mailbox each month. This steady increase indicates a substantial volume problem that individual efforts cannot handle effectively.

Unfortunately, this rise in the volume of attacks isn't a huge surprise. Throughout the year, we've shown evidence of attackers having access to unique phishing kits (see New FishXProxy Phishing Kit Lowers Barriers for Cybercriminals) designed to evade detection, automate their processes, and target victims at scale). Our data shows that these diverse phishing methods have been consistently employed from the beginning to the end of the year. Since our mid-year report, there has been a remarkable **202% increase** in the number of phishing messages delivered per 1,000 mailboxes.

This trend underscores a significant shift in email security dynamics. We are now operating in what can be described as a "volume game," where the sheer number of attacks overwhelms traditional security measures. Relying solely on Security Operations Center (SOC) analysts to manually manage this influx is proving unsustainable and may set organizations up for failure.

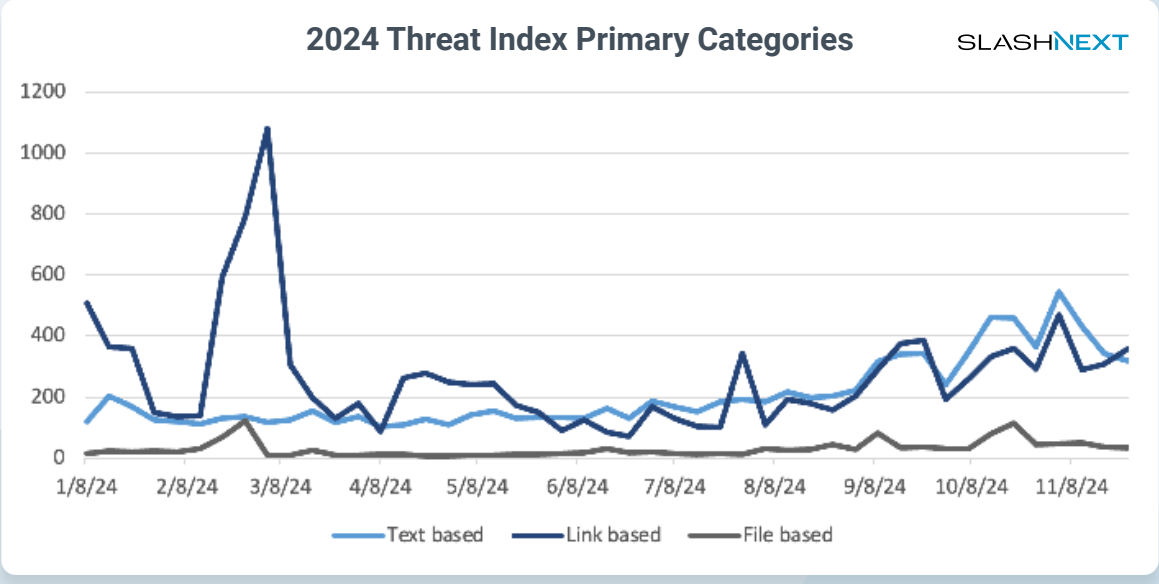


Figure 3. Email Threat Categories (Text, Link, and File based) trends over time

Let's break this down a bit further.
The image above shows the breakdown of email threat vectors into three main categories:

- **Text-based threats** (no attached payload)
- **Link-based threats** (malicious links as payload)
- **File-based threats** (file attachment as payload)

No single threat category consistently dominates

While text-based threats have gained wide attention since the FBI began tracking them in 2013, link-based threats remain the primary challenge in terms of volume. Text-based threats like Business Email Compromise (BEC) attacks, a subset of Social Engineering attacks, are important attack vectors that should be addressed. At the same time, the data in Figure 3 shows that link-based phishing is the primary vector, and text-based threats are second. The data shows these attack methods alternate throughout the year in prevalence—**no single threat category consistently dominates**. This reinforces why browser-based threat defense is a critical and necessary part of a phishing defense strategy.

File-based threats remain constant, though they're generally less prevalent than other attack vectors in our context.

This reduced frequency can be attributed to several factors:

- Organizations implementing restrictive file-based policies
- Enhanced email security infrastructure
- Secure file transfer mechanisms
- Improved operational procedures

Modern file-based threats have evolved beyond traditional self-executing files.
They now often incorporate techniques like HTML smuggling and don't always contain the malicious payload themselves but instead side-load that content once the file is executed.

These more advanced file attacks focus on:

- Credential harvesting
- Personal Identifiable Information (PII) theft

Overall, the past year has seen a dramatic rise in email phishing attacks, with a particularly steady increase in the second half. Attackers are utilizing sophisticated and automated techniques, resulting in nearly one advanced attack targeting every mailbox each week. This escalation presents a major challenge for email security, highlighting the need for more robust, automated defenses rather than relying solely on manual intervention by SOC analysts.

Threat Category Breakout Analysis

The current threat landscape shows several prominent attack vectors, with some key trends emerging:

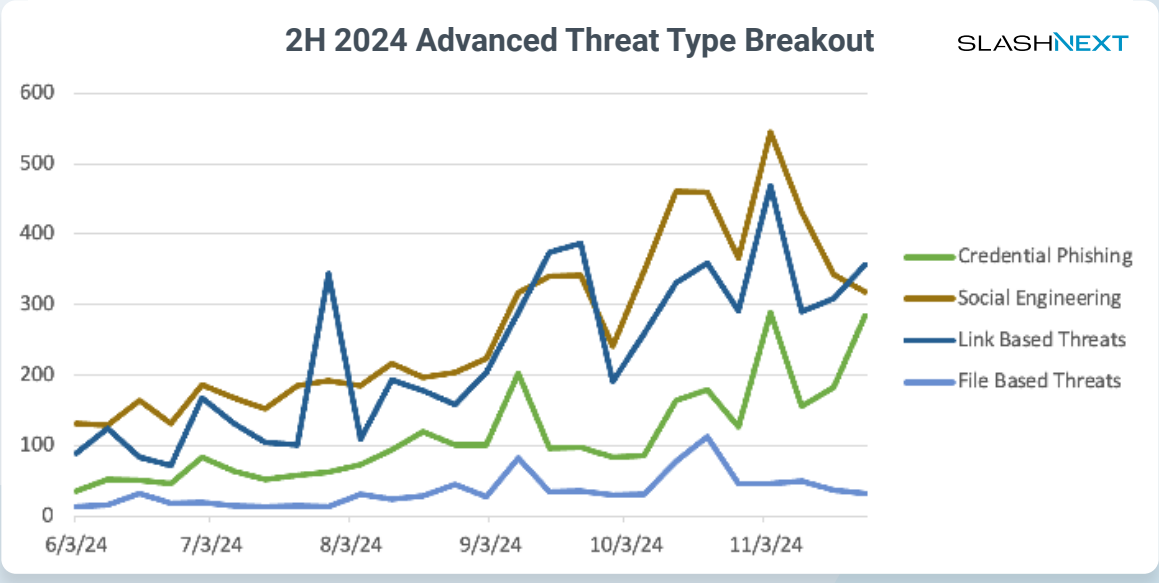


Figure 4. Specific Threat Type Breakout focusing on Credential Phishing and Social Engineering

Recent data shows a significant rise in both credential phishing and link-based threats. In the second half of 2024, shown in Figure 4, credential phishing is up **703%**. These attack methods frequently overlap, as many credential phishing attempts incorporate malicious links as part of their strategy. However, while there's substantial overlap, they're not entirely the same. Recent data indicates a late surge in these tactics as we move towards the holiday season. This was associated heavily with the major phishing campaign abusing DocuSign APIs in October and November.

Social Engineering attacks are up 141%, maintaining a consistent presence throughout the year and showing steady growth.

Credential phishing is up 703% ↗

Credential Phishing

Credential harvesting attacks begin when a malicious email bypasses security filters and reaches a user's inbox. The attacker's primary goal is to lead victims to a webpage where they will enter their login credentials. Let's use the recent DocuSign campaign as a sample.

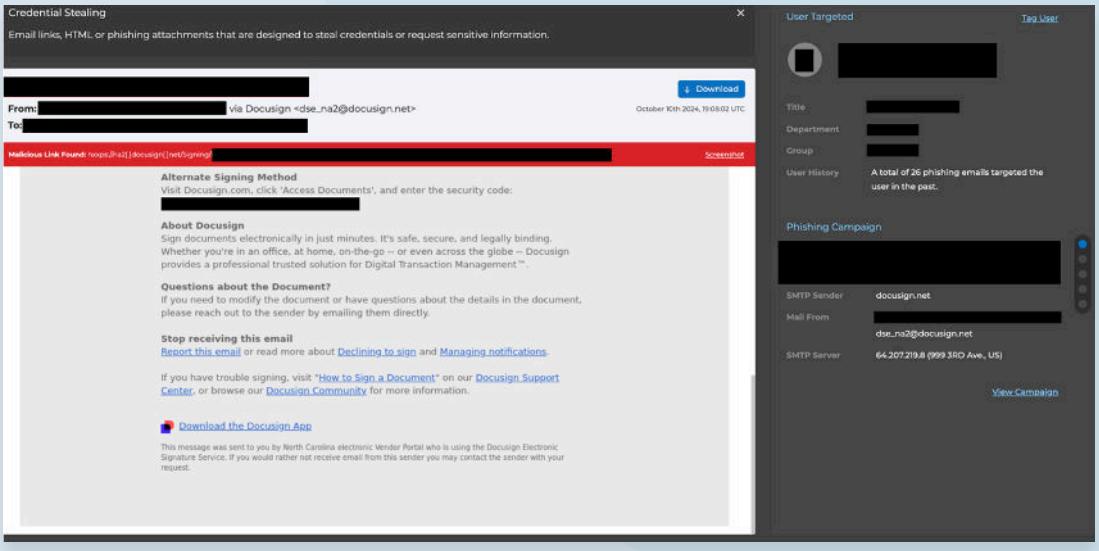


Figure 5. Legitimate emails sent from trusted vendors leveraged by threat actors

Figure 5 shows an email that successfully passed through email filters because it originated legitimately from DocuSign, a legitimate business service. The email can't be blocked without impeding normal business operations, as employees need to exchange DocuSign documents with customers. The security challenge arises because while the email legitimately uses DocuSign's cloud infrastructure, it contains a direct link within its environment that leads to malicious content.

There are three main methods attackers use to direct users to these malicious pages:

Direct links **QR codes** **Attachments**

Taking the simplest case of a malicious link, the attack flow includes multiple layers of obfuscation:

First, attackers employ redirectors and intermediate sites to mask the destination. They often implement testing mechanisms to filter traffic—either based on specific criteria like browser age and source or sometimes random filtering for high-volume campaigns. This helps keep their phishing pages active longer by making them harder for security services to detect.

When users reach the destination, they typically encounter a "human verification" test.
This might appear as:

- CloudFlare turnstile services
- Google CAPTCHA pages

After passing these verification steps, users face the actual phishing attack: a spoofed login page designed to capture credentials.

This is a two-stage process:

1. First, users enter their initial login credentials.
2. Then, attackers intercept the legitimate two-factor authentication process by displaying their own spoofed 2FA prompt.

Once attackers have both the initial credentials and the two-factor authentication details, they can successfully compromise the account.

Social Engineering

Social engineering continues to be ever-present, as shown in Figure 4, rising 141% throughout the second half of 2024.

Social engineering encompasses several attack styles, including but not limited to:

- Quote requests for vendor partnerships
- Fake loan and purchase scams
- Business Email Compromise (BEC)

There are also BEC subcategories within Social Engineering that include:

- Payroll theft
- Reconnaissance
- Invoice fraud

Social engineering attacks are up 141% ↗

While BEC attacks receive significant market attention and can cause substantial financial damage, they represent a small percentage of the total attack volume. Organizations have improved at detecting traditional BEC, leading attackers to change tactics frequently as we noted previously.

The most dangerous attacks now involve compromised external accounts, where recipients are accustomed to communications from the sender. Without social graph analysis to understand relationship patterns, these attacks are particularly effective. We capture these by leveraging machine learning, neural networks, or generative AI.

The most dangerous attacks now involve compromised external accounts

A notable development is the Black Basta campaign, which introduced a new multi-channel approach:

- Flooding inboxes with legitimate service registration emails creates confusion
- Appearing as account compromise
- Following up through alternate channels (Teams chat) posing as Microsoft support
- Delivering the actual attack through QR codes, links, or files

Social engineering attacks have increased in the second half of this year from where they started, with trends showing:

- Integration with other phishing techniques
- More sophisticated multi-dimensional approaches
- Combination of social engineering, link-based threats, and multi-channel phishing
- Some variants include malicious files for endpoint compromise

The trend indicates continued steady growth with increasing complexity rather than one-dimensional attacks.

Live Scanning and Link-Based Phishing

The image below illustrates the detection methods for link-based threats, currently the leading category of email-borne attacks. The graph shows two categories: known threats detected through existing threat intelligence (dark blue) versus threats detected through real-time scanning of previously unseen URLs (red). The primary takeaway is that, on average, **80%** of the links in email link-based threats are **unknown**. These pages are created moments before being sent last for a very short period and are de-weaponized just as fast. In other words, most malicious links will slip past controls relying on known threat feeds. We utilize a proprietary virtual browser to analyze and live scan URLs when analyzing email threats.

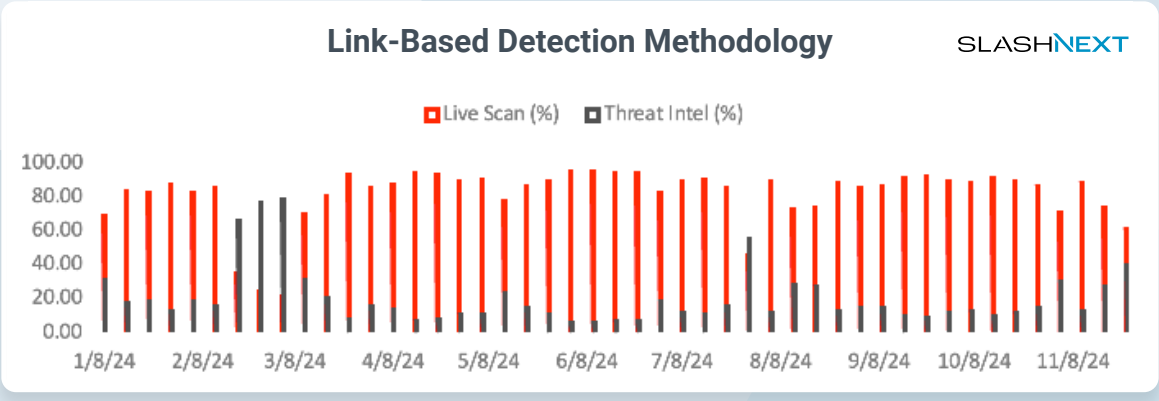


Figure 6. Comparison of Malicious Link Identification: Live Scan (unknown) vs. Threat Intel (known bad)

Throughout the year, the data reveals that relying on threat intelligence alone is ineffective against modern attacks. Most malicious links sent in email are zero-day URLs, created and deployed moments before the attack using AI and machine learning tools available on the dark web. These tools can generate thousands of unique pages through neural networks and phishing kits.

The key finding from this data is that traditional signature-based detection methods, which require 24-48 hours to develop signatures for malicious URLs, are no longer sufficient. The graph demonstrates why real-time scanning capabilities are essential for detecting these zero-day threats as they're being deployed.

80% of the links in email link-based threats are unknown

Non-email Attack Vectors

URL and Browser Threats

The data shows links that bypassed traditional network security layers and DNS-based detection mechanisms that users clicked on but were mitigated by SlashNext using AI embedded in the browser extension. This graph in Figure 7 is key to understanding the bigger trend: **phishing attacks have evolved beyond email-only delivery channels.**

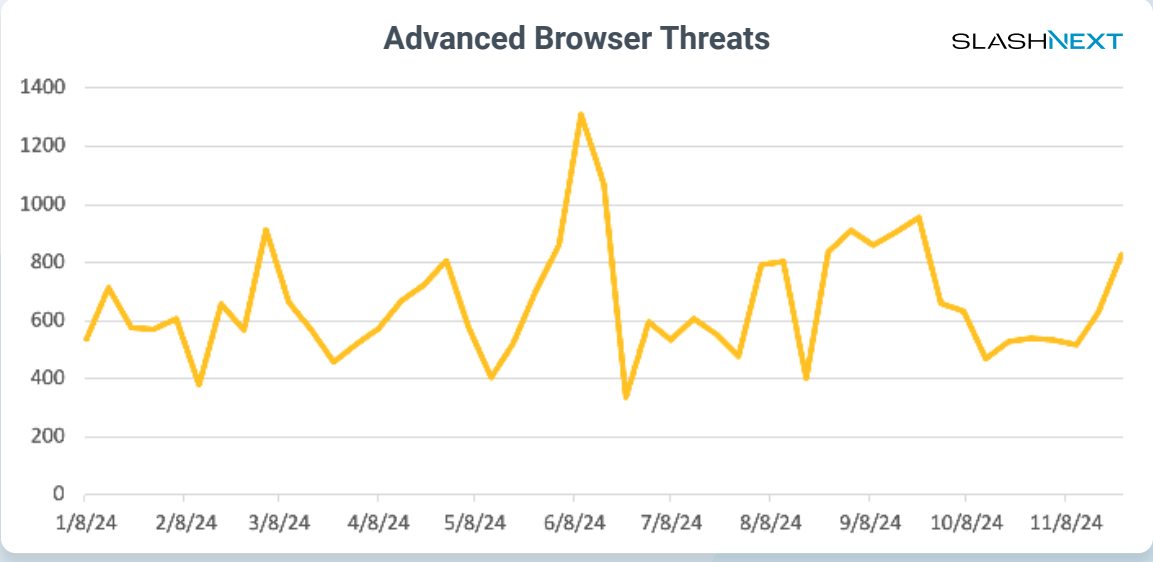


Figure 7. Advanced Browser Threats getting through advanced network security reaching users through multiple alternative channels such as: Browser-based messaging apps, Teams/Slack communications, LinkedIn messages, Personal Gmail accounts, and CRM forms.

Notable examples in the data include Operation Dream Job from Lazarus and Midnight Blizzard's Teams-based attacks. Even organizations with multiple network layers and browser protections are vulnerable because of these attacks:

- Utilize brand-new, previously unseen threats
- Bypass categorization due to their novelty
- Can be hosted on legitimate, trusted infrastructure (notably DocuSign, OneDrive, and Sharepoint)
- Pierce through organizational controls before detection systems can update

Users Get Advanced Phishing Every Week!

We take this all-encompassing approach because spot protection for individual applications isn't scalable. We've found the browser-based messaging phishing protection approach through browser extensions is crucial to mitigate these threats. Each link shown in the graph successfully circumvented existing security controls, highlighting how attackers are adapting their delivery methods as email security hardens.

Mobile Threats

Understanding the mobile threat landscape requires examining multiple attack vectors targeting mobile devices. The data we track here consists of two combined categories of mobile threats. The first category consists of malicious SMS messages that were identified and blocked before reaching users. The second encompasses malicious links delivered across various mobile platforms—from encrypted messaging apps like WhatsApp, Signal, and iMessage to business communication tools like Teams and Slack, as well as other mobile applications. The graph below illustrates mobile threat patterns tracked over the year, measuring two specific types of mobile threats per 1,000 users.

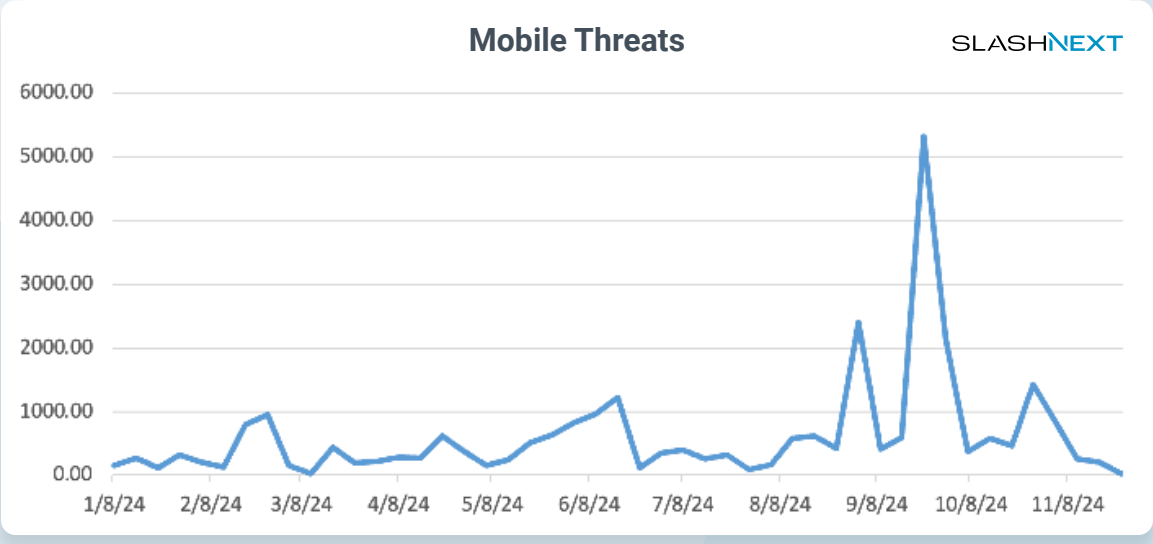


Figure 8. Mobile Threats over 2024, both SMiShing and Mobile Web threats

The data in Figure 8 reveals consistent threat activity throughout most of the year, with a notable spike in late September/early October.

Looking at the numbers:

- Users encounter at least one mobile threat weekly on average
- During peak periods, users faced 3-6 threats per week
- Annually, individual users may encounter anywhere from 50 to 600 mobile threats

Up to 600 threats annually on average

This volume of threats is particularly concerning because most users lack dedicated security controls on their mobile devices. The Twilio breach serves as a real-world example, originating from SMS phishing. While user awareness continues to improve, the sheer volume of threats means that even a single successful attack can lead to significant organizational impact.

Next Steps

As the phishing threat landscape continues to evolve, staying proactive in your defense strategy is crucial. The data in this report highlights both the scale and sophistication of emerging threats, underscoring the importance of advanced solutions to protect your organization. By leveraging this information, you can better anticipate risks and take the necessary steps to safeguard your systems and users.

If you have any questions about the data in this report or how to prevent these advanced attacks, please visit us at www.slashnext.com. To discover how many threats may be bypassing your current defenses, try our free observability mode trial. It takes less than 10 minutes to set up and provides valuable insights to help you plan your defenses.

Start your free trial here

slashnext.com/free-trial-request/

SLASHNEXT

NEXT GEN AI EMAIL+ SECURITY

SlashNext, Inc.
6701 Koll Center Parkway
Suite 250
Pleasanton CA 94566
800.930.8643
info@slashnext.com
www.slashnext.com