

# Phishing Threat Trends Report

In the Aftermath of Scattered Spider, What Happens When You Call a Cybercriminal and the Rise (and Rise) of Legitimate Platform Hijacking



# No Rest From the Wicked

The end of 2025 is in sight – and what a year it's been!

The threat landscape continues to evolve, with cybercriminals leveraging new tactics to get through traditional email defenses and turning to multi-channel attacks to ramp up the pressure on their targets.

Our Phishing Threat Trends Reports bring you the latest insights on the evolution of phishing threats and the maturing attacks that have gained an established foothold.

In this edition, we explore how Scattered Spider has opened the door for a fresh wave of phishing after breaching a string of high-profile brands since the start of the year. We also find out who answers (and what they want) when you call back in a vishing attack and how legitimate platforms are being hijacked.

Unless otherwise stated, all statistics have been generated from [KnowBe4 Defend](#), an integrated cloud email security product. As always, please reach out if you have any questions or want to learn more about Defend.



**Jack Chapman**

SVP of Threat Intelligence, KnowBe4

# What's Inside

- 03 Most Phished Topics in 2025**
- 05 Caught in the Spider's Web**  
What Happens After Scattered Spider Breaches a Retail Giant?
- 08 Hello...? Hello...?**  
Who Answers When You Call a Cybercriminal?
- 12 A Daily Deception**  
When Do Cybercriminals Send Phishing Emails?
- 15 Is This Legit?**  
The Continued Hijacking of Legitimate Platforms
- 18 What's Getting Through Secure Email Gateways?**  
How Attacks are Engineered to Evade Traditional Defenses
- 19 By the Numbers: A Quick Round-up of Phishing Stats From 2025**  
Your Questions Answered About Phishing in 2025
- 22 A New Age for Human Risk Management**  
Email Security Is No Longer an Isolated Element in the Tech Stack
- 23 Our Contributors**

# Most Phished Topics in 2025



JANUARY

**PROMOTIONS, BENEFITS  
AND REMUNERATION**

**33%**

Of phishing emails  
featured HR-related  
topics



MARCH

**MISSED MESSAGES**

**18.4%**

Increase compared to 2024

Plus, a 245% increase in  
malicious SVG attachments

March 17th  
was the  
most-phished  
day so far



MAY

**META IMPERSONATION,  
SENT VIA APPSHEET**

**Attackers**

exploited legitimate  
platform AppSheet to send  
emails impersonating Meta

See pages  
15-17 for more  
on this topic!



FEBRUARY

**VALENTINE'S DAY**

**34.8%**

Increase in Valentine's  
related traffic vs.  
February 2024

Love definitely  
isn't in the air with  
cybercriminals  
exploiting  
seasonal  
promotions and  
carrying out  
romance scams



APRIL

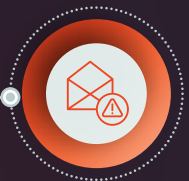
**TAX**

**22.9%**

Increase in tax-related  
attacks vs. April 2024

Top 3 terms: Tax, IRS  
and Payment

Scattered Spider  
begin campaign  
against UK  
retailers - see  
analysis on  
pages 5-7



JUNE

**MICROSOFT MAILBOX LIMIT**

**15.9%**

Of impersonation attacks  
referenced Microsoft  
mailbox storage limits

June also saw 3x more social  
engineering attacks



JULY

## COMPANY IMPERSONATION

23.4%

Of phishing attacks impersonated the recipient's company



SEPTEMBER

## START OF THE UNIVERSITY ACADEMIC YEAR

6.3%

Increase in attacks sent from compromised student accounts

Includes impersonation attacks targeting current students and alumni



NOVEMBER

## MULTI-FACTOR AUTHENTICATION

Growing

trend that uses fraudulent multi-factor authentication emails to make credential-harvesting websites seem more authentic

AUGUST

## THE US OPEN

## Cybercriminals

impersonated event vendors, including Rolex, IBM and IHG

A high proportion exploited the direct send vulnerability in Microsoft 365

## PREDICTIONS FOR THE REST OF THE YEAR

OCTOBER

## HIJACKING LEGITIMATE PAYMENT PLATFORMS

10x

Increase in phishing attacks sent using platforms such as PayPal, Strike, QuickBooks, Venmo and Cashapp

See pages 15-17 for more!

DECEMBER

## HOLIDAY CELEBRATIONS

Every year

cybercriminals exploit the religious and secular celebrations that fall in and around December



# Caught in the Spider's Web

## What Happens After Scattered Spider Breaches a Retail Giant?

In April this year, criminal gang Scattered Spider breached UK retail giants Marks and Spencer (M&S) and Co-Op. Known for its sophisticated social engineering and identity-based attacks, Scattered Spider first gained notoriety with high-profile casino hacks on MGM Resorts and Caesars Entertainment in 2023, and the 2024 Snowflake data breach.

The pace of public attack has accelerated rapidly this year, with Scattered Spider claiming involvement in breaches of UK luxury retailers Harrods, as well as Victoria Secret and Chanel. The group is also rumored to be involved in attacks on Adidas and Pandora. Away from the high street, they've been linked to attacks on UK Legal Aid Agency and Qantas Airways, with rumored links to Coinbase and Hertz.

As of Summer 2025, Scattered Spider has reportedly joined forces with ShinyHunters, who have claimed breaches on Allianz Life and Tiffany & Co, and LAPSUS\$. The loosely affiliated supergroup made from all three notorious gangs initially claimed responsibility for an attack on Jaguar Land Rover, although both state actors and other groups have also been implicated.

### How the Scattered Spider Weaves Its Web

Scattered Spider predominantly focuses on using social engineering to trick employees and third-party vendors into providing access to a company's systems and networks. Campaigns usually start with a phishing email and can escalate to vishing attacks where a cybercriminal often impersonates a panicked – sometimes high-ranking – employee who urgently needs access to an account or system.

#### Tactics include:



Email and SMS-based credential harvesting campaigns sent to a broad number of targets



SIM swapping fraud to transfer a legitimate user's phone number to the attacker's SIM card.



Multi-factor authentication (MFA) bombing that floods a target with MFA notifications to trick them into accidentally approving one



Voice phishing (vishing) to manipulate targets into revealing MFA codes



Impersonating technology providers, particularly Okta

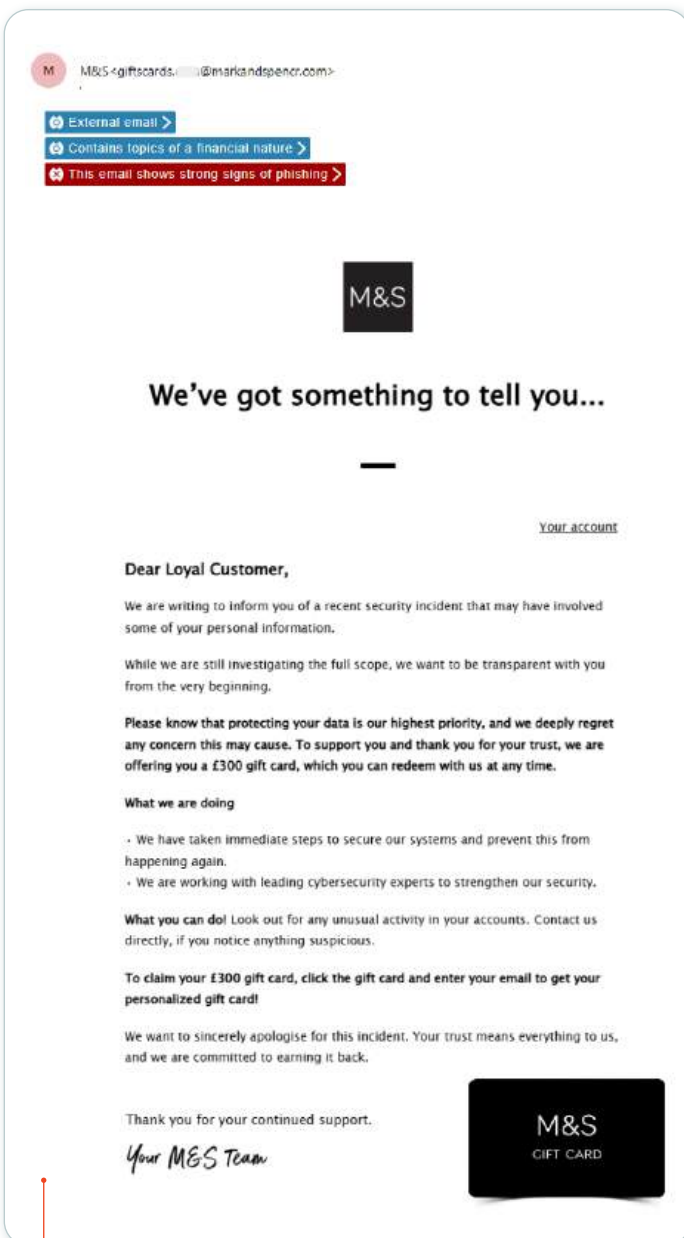
Scattered Spider has also been frequently observed using the adversary-in-the-middle (AiTM) phishing kit "Evilginx". This kit is capable of emulating a range of domains to enable attackers to target non-standard web apps, meaning attacks appear more unique and, potentially therefore, more legitimate as they're not impersonating one of the "usual suspects".

## Catching as Many Victims as Possible

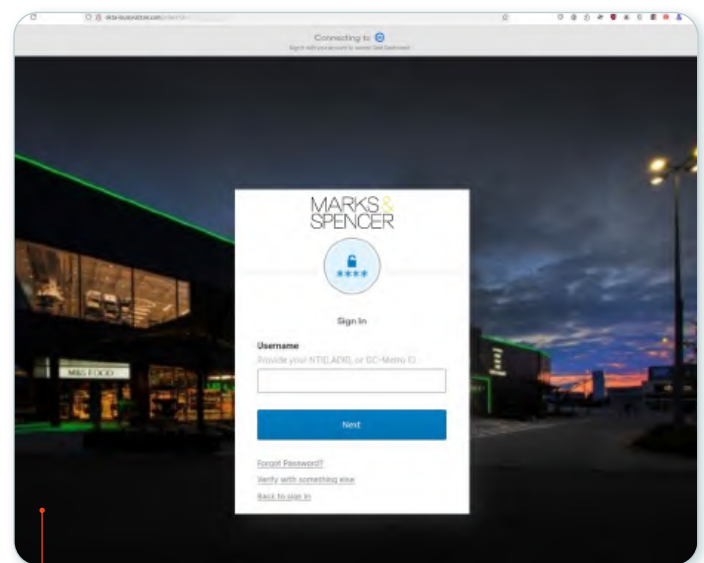
Reports have circulated of heavy losses for the brands involved. M&S has estimated a profit hit of £300M (~\$404.3M USD)<sup>1</sup> and the UK's Cyber Monitoring Centre estimates Co-Op's incident will cost between £270M - £440M (~\$363.9M - \$593M USD).<sup>2</sup>

Impacts from these incidents aren't contained to the brands alone, however, with cybercriminals using them to launch further phishing campaigns. Compromised customer data can be used to identify potential targets, while the incidents themselves provide pretext for these messages.

In the example shared below, the cybercriminals impersonate M&S through a spoofed domain ("marksandspencer.com") and using a stylized HTML template, including a gift card mockup. Targets are manipulated into believing M&S is offering some compensation for the loss of their personal data, however clicking on the link will take them to a credential harvesting website with the pretext of logging in to claim their reward.



Phishing attack impersonating M&S following cyberattack in April, with KnowBe4 Defend warning banners visible.



Credential harvesting website impersonating M&S, potentially leveraging a compromise Louis Vuitton domain.

These attacks truly stress  
test an organization's  
cybersecurity program,  
specifically how it handles  
human risk

<sup>1</sup> BBC News, <https://www.bbc.co.uk/news/articles/c931lkq4n51o>

<sup>2</sup> Computing UK, <https://www.computing.co.uk/news/2025/security/cyber-monitoring-centre-estimates-cost-uk-retail-attacks>

Below is a table summarizing the impersonation attacks our team has detected via KnowBe4 Defend since the initial incidents and the tactics they've used.

Brand	% of Attacks Impersonating Brand	Impersonation Tactics	Payloads	Breach Mentioned in Attacks	Top Three Industries Targeted
	49.9	Brand/Alias Impersonation	Hyperlinks Attachments QR codes	Yes	Finance Retail Logistics
	6.7	Brand Impersonation	Hyperlinks QR codes	Yes	Legal Government Finance
	2.1	Brand/Alias Impersonation	Hyperlinks QR codes	Yes	Health Insurance Utilities
	0.5	Brand Impersonation	Hyperlinks QR codes	No	Finance Healthcare Government
	1.8	Brand Impersonation	Hyperlinks QR codes	No	Retail Manufacturing Real Estate
	9.0	Brand Impersonation	Hyperlinks	Yes	Legal Aerospace Industrial
	9.0	Brand Impersonation	Hyperlinks	Yes	Finance Healthcare Government
	7.2	Brand Impersonation	Hyperlinks	Yes	Insurance Finance Legal
	13.8	Brand Impersonation	Hyperlinks Attachments QR codes	Yes	Insurance Legal Finance

## The Human at the Center

The person being exploited is firmly at the center of Scattered Spider's web. Their tactics are heavily designed to socially engineer their targets - whether that's by vishing or MFA bombing in the initial attack or (as we saw in the earlier phishing email example) pretending to offer free vouchers to convince someone to click.

These attacks truly stress test an organization's cybersecurity program, specifically how it handles human risk. Whether it's phishing detection to policies about sharing credentials or MFA codes over the phone, organizations need to ensure they not only have robust technical defenses but also continually support and coach employees to increase their awareness to stop gangs like Scattered Spider from gaining a foothold.

# Hello...? Hello...?

## Who Answers When You Call a Cybercriminal?

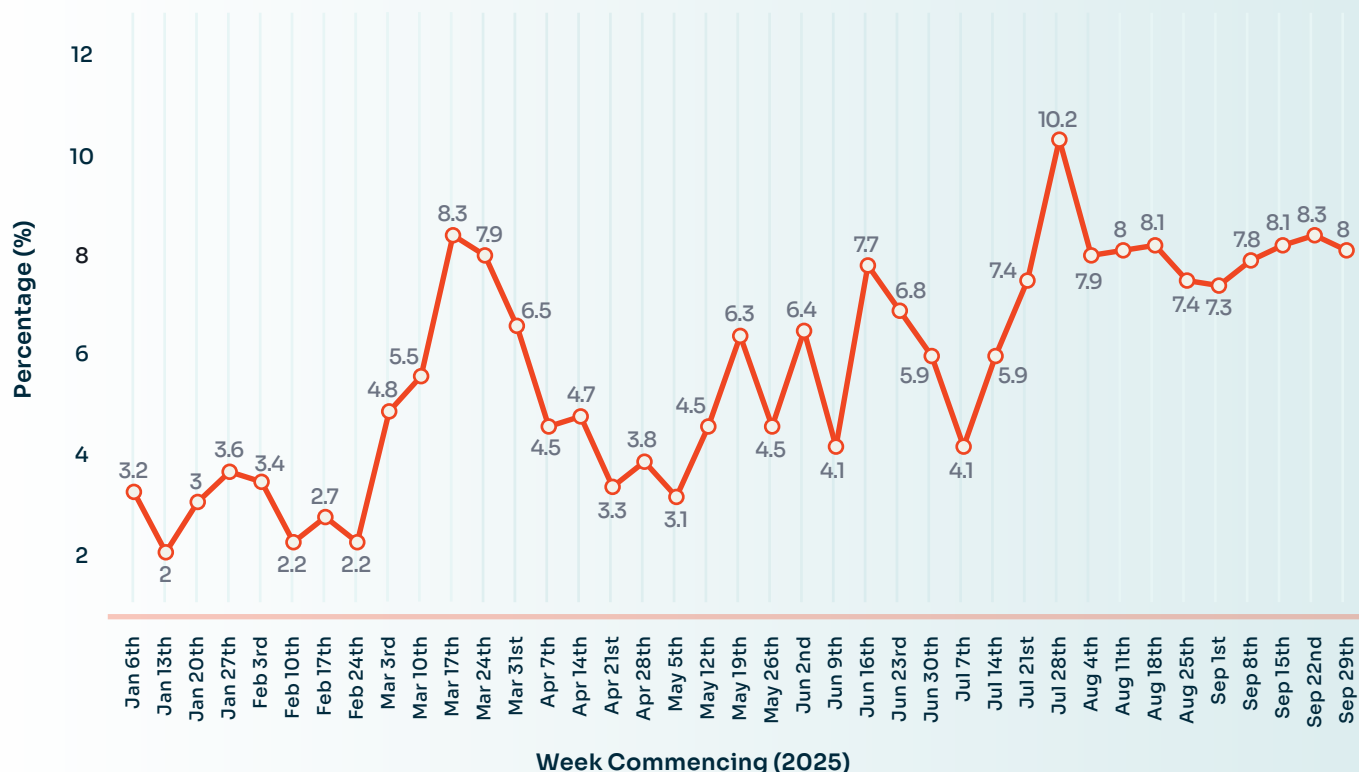
There are two reasons to include a phone number in a phishing email. First, credibility. Maybe the number was in the footer of a branded HTML template in an impersonation attack. Or it could simply be added to a signature or message body to try to reassure a target that they're communicating with a legitimate person. In these cases, the recipient isn't expected to call the phone number but will be asked to perform another action.

Alternatively - and increasingly - phone numbers are used as the payload in vishing (voice phishing) attacks, with the intention that the target calls a cybercriminal.

Between January 1st - September 30th, 2025, our threat researchers observed that on average 5.5% of phishing emails use a phone number as the sole payload. While a relatively small volume compared to other payloads, it represents a significant increase: for the whole of 2024, only 0.9% of phishing emails used phone numbers as their payload (which makes this a 449% increase so far 2025).

Overall, vishing attacks have risen throughout the year, peaking during the week commencing August 4th, when they represented 10.2% of all payloads.

Percentage of Phishing Emails That Contain a Phone Number Payload





## Ask The Expert

Dr. Martin Krämer  
CISO Advisor



### Are Phone Numbers an Effective Payload?

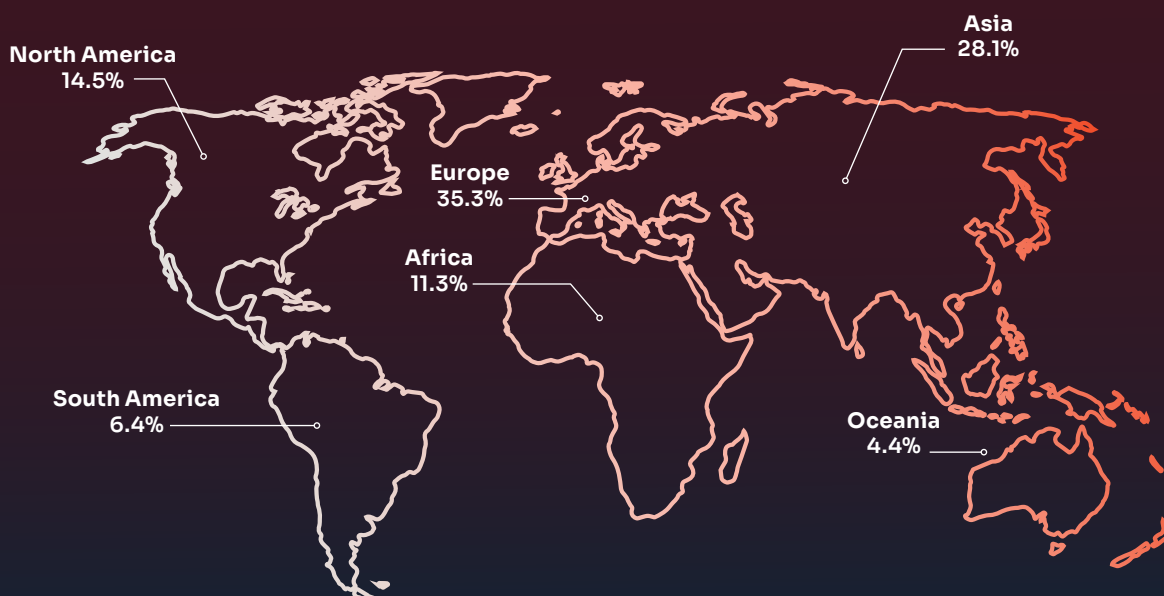
- ▶ One might think phone numbers wouldn't be great payloads, as dialing numbers on a phone requires more effort than replying to an email. While that might be true, it is also a great mechanism for self-selection, where people who make the effort to call the number have the intent of learning more and thereby have given in to their curiosity, sense of duty or self-interest.

Naturally, voice transmission over the phone is also perceived as more authentic, trustworthy and reliable. However, phone calls are also much less regulated communication channels. Attackers know that the average person who makes the call is therefore more susceptible to manipulation and less protected - and all of that before considering the effect of hearing a familiar voice on the phone that might well be AI-generated and not real.

### Who Am I Speaking To?

On analyzing the vishing payloads, our threat researchers found that just over one-third (35.3%) contained European dial codes, with those for Asian countries representing 28.1%. Russia skewed this number for European countries with 35.8% of vishing call numbers originating from there. In Asia, the top three countries were China (17.7%), Japan (15.3%) and Vietnam (10.4%).

### Where in the World Phishing Phone Numbers Are Located



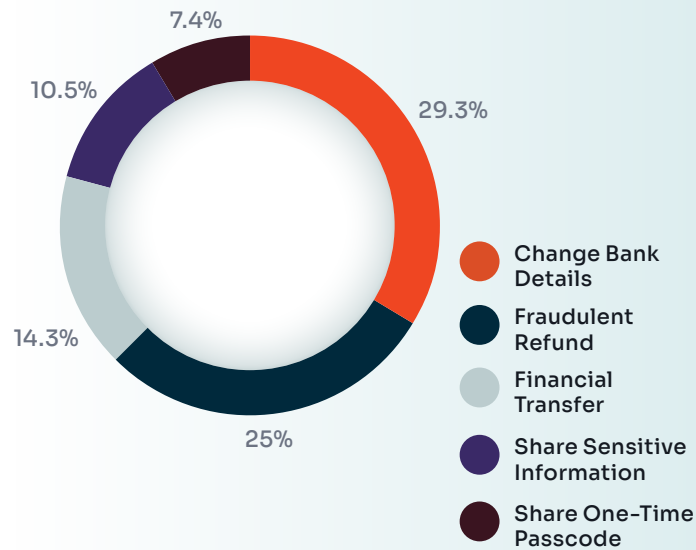
When our team rang the numbers, they found that an AI voice was used in 77.3% of attacks, while a human answered in 22.7%. Although AI voice tools theoretically enable cybercriminals to scale their attacks, this technology is still maturing and, currently, is unlikely to sound as convincing or manipulate as quickly as a skilled human.

The attacks were primarily motivated by money (68.7% made some reference to payments or financial details). In 29.3%, the cybercriminal requested an update of bank details to transfer payments from legitimate vendors to their accounts. Fraudulent refunds were next at 25.1% and financial transfers were requested in 14.3%.

### Dialing up the Pressure

Vishing attacks offer cybercriminals another avenue to carry out their aims. In the below example, an initial phishing email requests a change to bank details, with a phone number to confirm the information.

The Requests Made via Phone Number Payloads



[EXTERNAL] Correct the bank details

MB

Margarett <margarett@.com>  
To: Sandra. @.com

↩ Reply

↩ Reply All

➡ Forward

⋮

Thu 07/08/2025 01:07

Bank Details.pdf

106 KB

External email >

First time sender >

Contains topics of a financial nature >

This email shows strong signs of phishing >

CAUTION: This is an external email.

Hello Sandra,

I need to update my bank account details for my upcoming salary payment as soon as possible. My new details are attached for your reference.

If you need to confirm anything, please just give me a call on .

Thanks very much for taking care of this quickly.

Best regards,

**Margarett**  
Credit Controller

Vishing email requesting update to bank details, with KnowBe4 Defend banners applied.

Once on the line, almost every sentence out of the cybercriminal's mouth contained a pressure tactic designed to socially engineer the caller into making the requested change, as highlighted in the image below.

**Analyst:** Hi, this is Sandra. I got your email about changing your payment details.

**Phisher (posing as employee):** Yes, this is Margaret. I need to update my bank account **before the next payroll run**. Can you please switch my salary to my new account **urgently**?

**Analyst:** Why do you need this updated right away?

**Phisher:** I just got married and changed my name. I've opened a joint account with my partner, so I need my salary redirected there.

**Analyst:** Does this need to happen immediately or can it wait until the next payroll run?

**Phisher:** I really need the funds **before the first**. I've got direct debits and a mortgage due.

**Analyst:** We've already missed the payroll cutoff. We'll need to process this via BACS instead. It should be in your account by the end of the day. I just need to confirm a couple of details before making the change. Could you provide the new account information?

**Phisher:** Yes, it's in the email. Sort code [REDACTED]. Account number [REDACTED]. Do you also need an IBAN? **Please update it today, otherwise my salary payments will fail.**

**Analyst:** No, since you're based in the UK, we don't need an IBAN for local payments.

**Phisher:** Uh, I don't have that... But this is really serious. You just need to **go ahead with the change.**

**Analyst:** That's fine. For UK payments an IBAN isn't required.

**Phisher:** I'm in Europe right now, in back-to-back meetings. I can't log in myself. **Please don't delay this any longer.**

**Analyst:** Alright. I've got the information I need.

Transcript of a vishing attack, with pressure tactics highlighted

In another example, a phishing email (below) was followed up with an AI-generated recording designed to impersonate an automated message to capture a one-time passcode from the victim.

## Security Alert



Microsoft 365 Mailbox Support Team <security@account-microsoft365.com>  
To: [redacted]@[redacted].com

If there are problems with how this message is displayed, click here to view it in a web browser.

External email >

First time sender >

This email shows strong signs of phishing >

Reply Reply All Forward

Thu 07/08/2025 22:00

## Microsoft 365 Account Team



### Blocked Sign-in Attempt

Our system detected an unrecognized sign-in attempt into your Microsoft 365 Mailbox from an unfamiliar IP address. Whenever this occurs, our security protocol requires you to review your identity and complete a quick security check.

Please call the **Microsoft 365 Security Verification Line at (302) 302 6553** immediately to confirm whether this was you. If this wasn't you, we'll help you secure your account and take corrective action.

302 6553

**Do not disregard this notification, as it is very important.**

Microsoft 365 Mailbox Support Team

Vishing email requesting callback to unlock account, displaying KnowBe4 Defend banners.

Phone numbers, plus mechanisms such as video calling, play a critical role in multi-channel attacks. They move a victim from email to a typically less regulated channel, where it can be easier for cybercriminals to exploit them. As AI tools become more advanced and enable these channels to scale, it's crucial that organizations can detect the initial attack and prevent employees from calling up a cybercriminal.

# A Daily Deception

## When Do Cybercriminals Send Phishing Emails?

To succeed, not only does a phishing email need to get through technical defenses, it also needs to dupe its target into falling victim. Inevitably, the more sophisticated the threat - such as a high-quality impersonation attack - the more likely it is to appear legitimate.

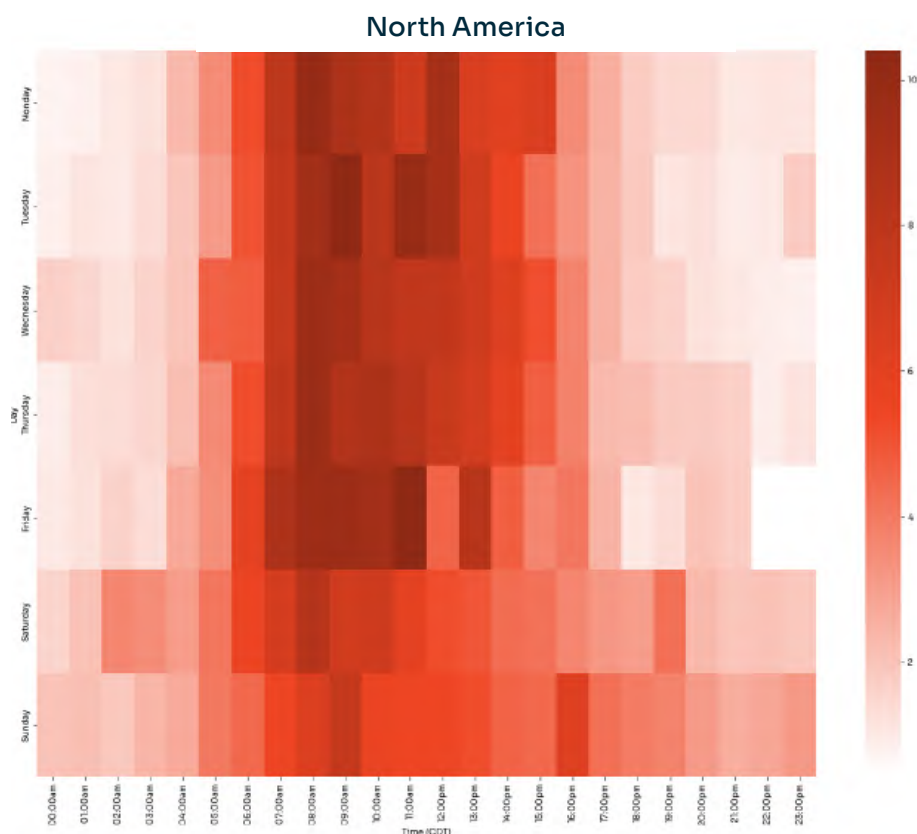
There are, however, other factors at play, including when the email is received, what device it's accessed on and a multitude of personal influences for the recipient.

Analyzing data from across [KnowBe4 Defend](#) global environments between September 1st -

September 30th, 2025, patterns emerge. Globally, cybercriminals are most likely to target organizations during working hours, Monday through Friday. Attacks peak from mid-morning until mid-afternoon, tailing off in the evenings.

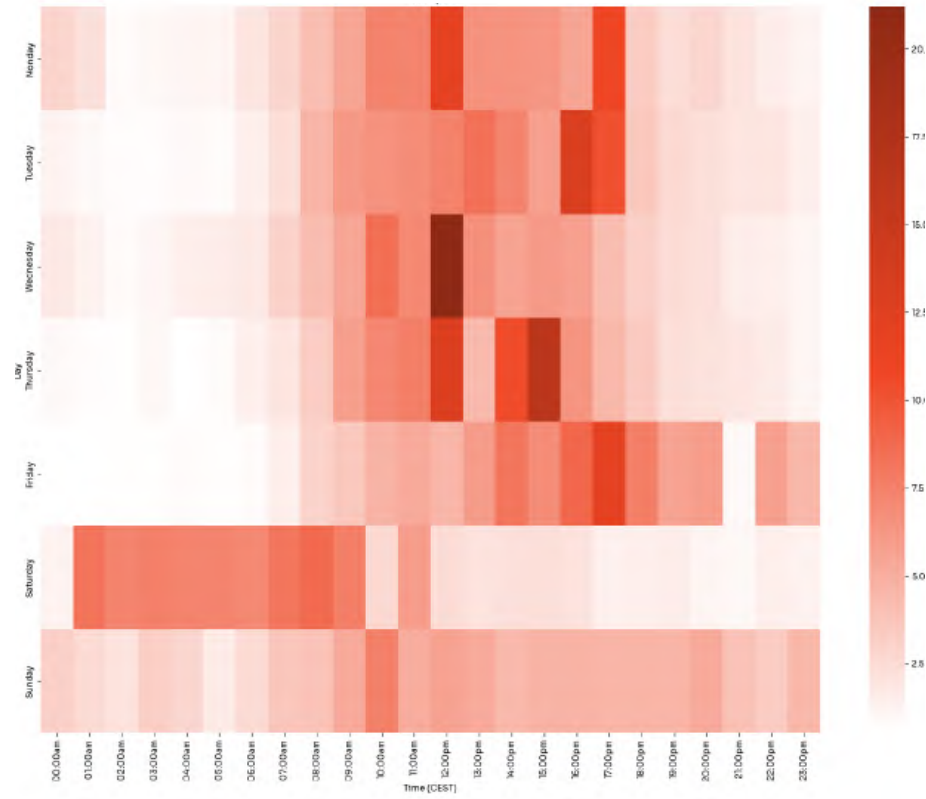
Attacks continue on the weekends, with particularly high volumes continuing in North America, as cybercriminals target always-on approaches to work, including people accessing corporate emails on mobile devices.

Heatmaps showing when cybercriminals targeted organizations with phishing emails between September 1st - September 30th, 2025.

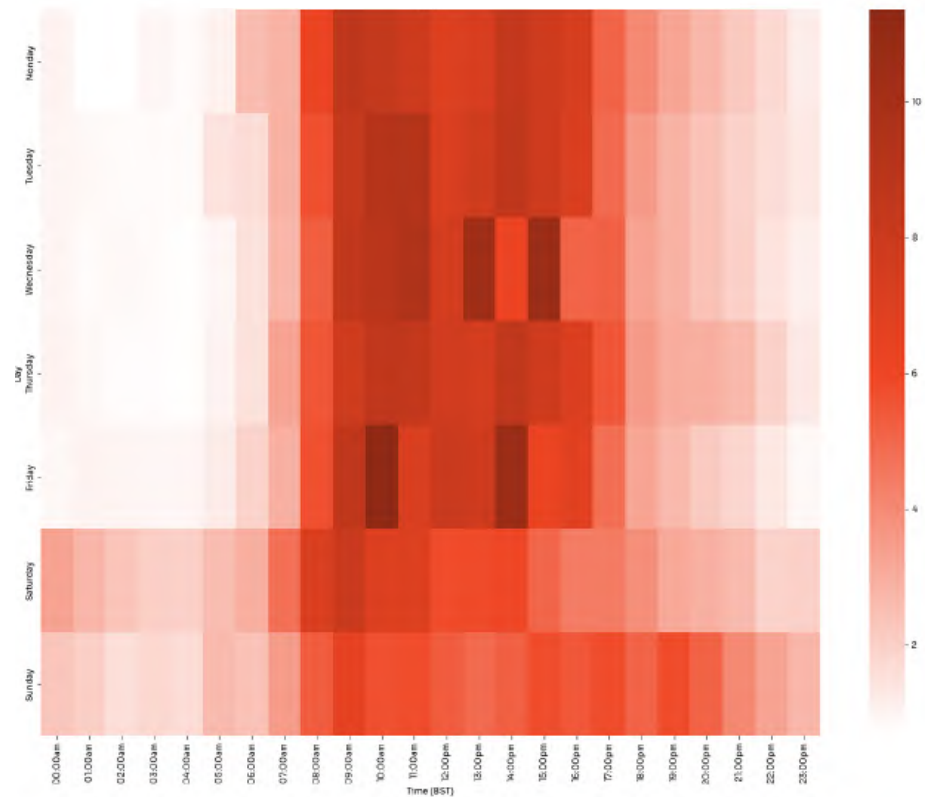




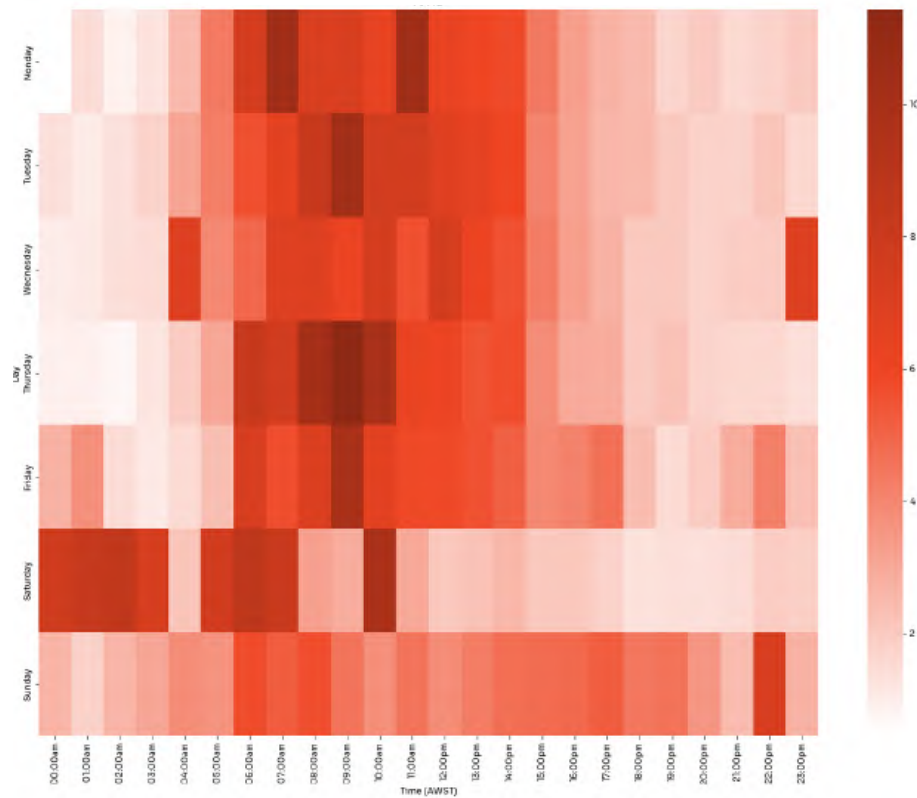
## Europe



## UK & I



## APAC



## Ask The Expert

**Dr. Martin Krämer**  
CISO Advisor



### Does Our Susceptibility to Phishing Change Based on Time and Day?

- ▶ People are more likely to fall victim to a phishing attack when they are distracted, such as in the afternoon when they might divide their attention between family duties and checking work emails. It's also true that many hit the post-lunch energy low in the afternoon and get increasingly drained from a long day at work.

While these facts are known to cybercriminals, the reason why most phishing attacks still happen during the day and not during the evening hours is because most people only check their emails during the daytime. Similarly, most attacks on businesses are launched during the workweek, as fewer people will check their email at the weekend.

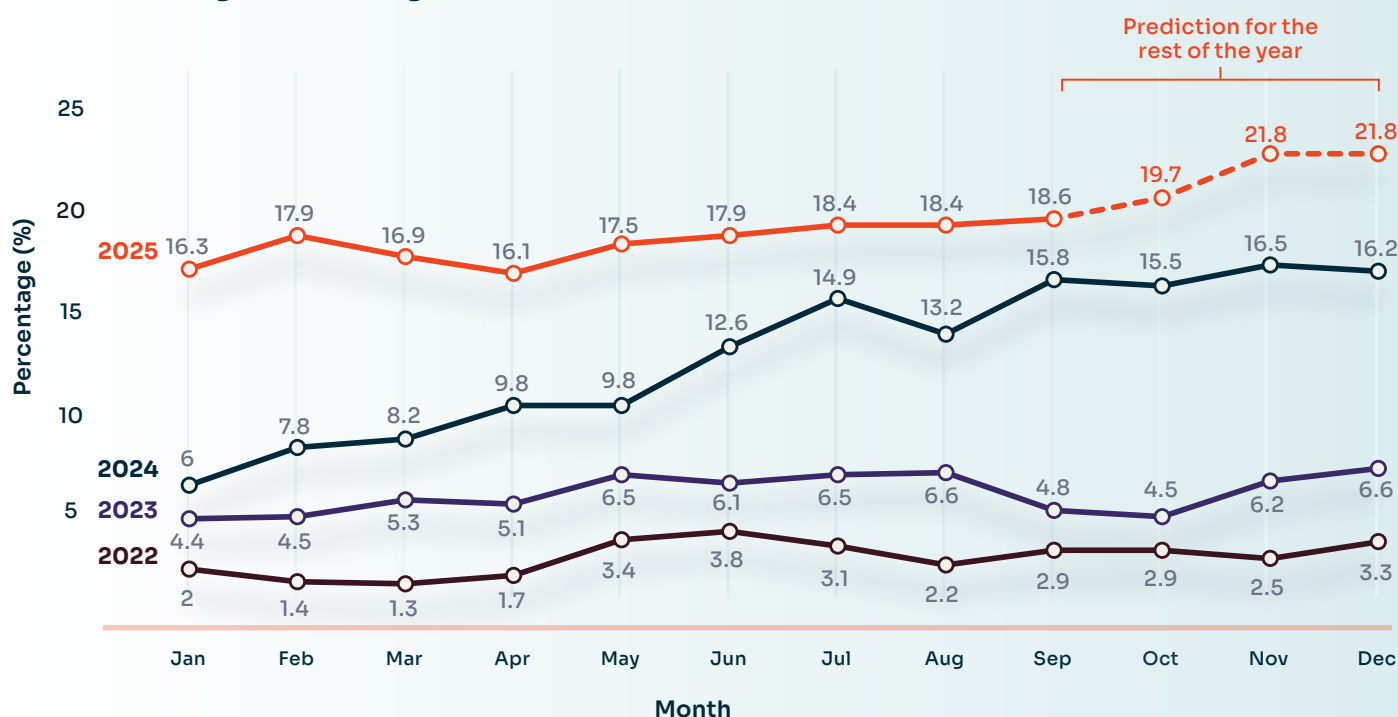
While people's susceptibility to phishing may fluctuate throughout the day and week, organizations must ensure their email security is defending them around the clock.

# Is This Legit?

## The Continued Hijacking of Legitimate Platforms

The use of legitimate platforms – such as SharePoint, DocuSign and Paypal – to send phishing emails has increased by 66.9% year to date (YTD) compared to the same period last year (January 1st – August 31st). This upward trend is even more marked when compared with previous years' data: there's been a 214.3% increase versus 2023 and 604.0% increase compared with 2022.

Volume of Phishing Attacks Sent via Legitimate Platforms as a Percentage of Phishing Mailflow in KnowBe4 Defend



100% of the attacks our Threat Lab team analyzed passed DMARC

## The 2.0 of Impersonation Attacks

The use of a legitimate platform to send a phishing email enhances an impersonation attack and, in many ways, is easier for the cybercriminal to accomplish. In these scenarios, the platforms themselves aren't actually compromised; instead, cybercriminals register for (often free) real accounts on the service. Typically, this is a simpler tactic than domain spoofing.

Cybercriminals benefit in a multitude of ways from this approach. The emails use real templates taken from the platform, meaning they're sent from a legitimate - and highly trusted - domain and contain perfectly rendered branding elements that a target would expect to see, such as logos and footers.

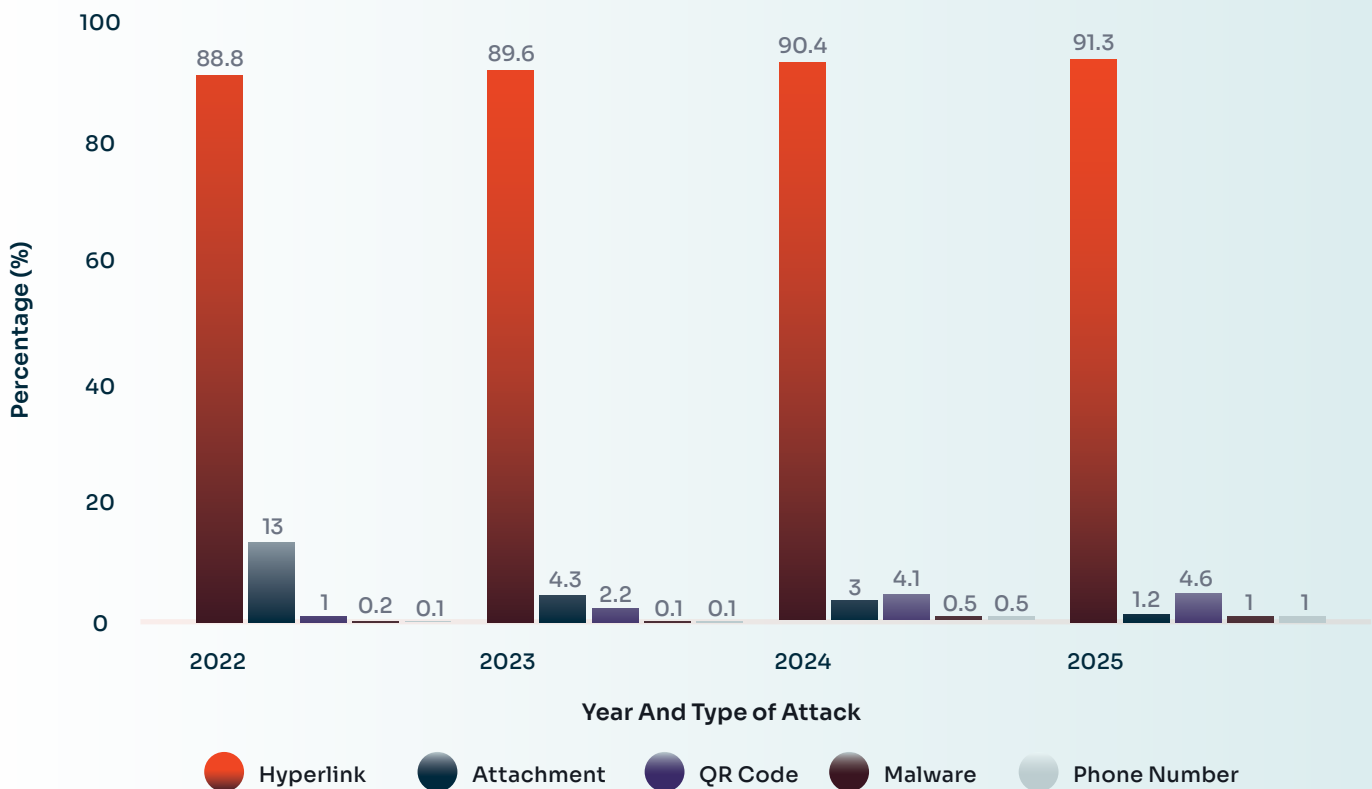
100% of the attacks our Threat Lab team analyzed passed DMARC, one of the primary authentication mechanisms used by native email security and secure email gateways (SEGs). Additionally,

59.9% of organizations had one or more of these sending domains added to their allowlists to expedite real business communications, while 89.0% of users had established relationships with these vendors. Consequently, organizations need more robust controls to detect when these platforms are being used to launch malicious attacks.

Phishing hyperlinks are the most common payload used in these attacks, with the malicious content usually hosted outside of the sending platform. As these platforms have enhanced their outbound security in efforts to protect their customers, there's been a 60.0% decrease in the use of attachments since 2024 and a 90.8% decrease since 2022.

Tying into our analysis below, the addition of a phone number has increased since 2022. While present in only 1% of attacks, this payload has technically experienced a 900% increase in the last three years.

Year-on-Year Analysis of Phishing Payloads Sent Using Legitimate Platforms














## The Most Popular Platforms in 2025 – And Who’s Being Targeted

Larger platforms are obvious targets for cybercriminals to hijack. They’re more likely to be included on an organization’s allowlist, have highly established and trusted domains, have sending relationships with individuals within an organization and are more recognizable to a target, who is inherently more likely to trust an email from a vendor they know.

In 2024, PayPal, SharePoint, Docusign and DropBox were the most commonly used platforms. The picture changed in 2025, with a two-month campaign heavily leveraging Intuit QuickBooks at the start of the year and with Zoom taking the top spot in July and August.

### The Most Popular Legitimate Being Abused by Month in 2025

<b>January</b> Intuit QuickBooks	
<b>February</b> Intuit QuickBooks	
<b>March</b> Google AppSheet	
<b>April</b> Canva	
<b>May</b> SurveyMonkey	
<b>June</b> Google Docs	
<b>July</b> Zoom	
<b>August</b> Zoom	
<b>September</b> Google Classroom	

C-level executives were the individuals most frequently targeted by these attacks. As they have greater access levels and signing authority than other employees, they’re often seen as the perfect target for phishing attacks. Next, cybercriminals target middle management and experienced non-managerial employees, who are often the individuals who have established relationships with the vendors being hijacked – meaning they might be less likely to spot a phishing email amongst legitimate communication.

Financial services firms are most likely to be targeted by DocuSign attacks (representing 11.6% of phishing attacks targeting this industry), while manufacturing and industrial companies are targeted by Microsoft Forms (11.3%), insurance and law are targeted by Docusign (11.0% and 10.9% respectively) and healthcare by PayPal (10.3%).

As noted, phishing attacks sent from hijacked legitimate platforms can easily bypass the detection used by native security and SEGs, and can be difficult for employees to spot once they land in the inbox. Consequently, organizations must implement enhanced detection that holistically analyzes all inbound emails, including subject line analysis and detection of suspicious behaviors, rather than relying on a narrow set of failsafes alone.

The use of legitimate platforms to send phishing emails has increased by 68.9% YTD

# What's Getting Through Secure Email Gateways?

## How Attacks Are Engineered to Evade Traditional Defenses

Delivery is one of the most crucial steps in the cyber kill chain. So, naturally, cybercriminals have developed a multitude of techniques to bypass the signature and reputation-based detection provided by native security and secure email gateways (SEGs).

Since the end of 2023 we've seen a 38.3% increase in phishing emails evading detection by SEGs and a 44.2% increase in attacks bypassing Microsoft's native detection. While Microsoft provides a strong foundation for email security, organizations need another layer to enhance their defenses.

### The Primary Tactics for Evading SEG Detection in 2025

As explored in pages 15-16, there's been a 66.9% increase in the use of legitimate platforms to send phishing emails. These platforms allow cybercriminals to hijack a trusted domain to bypass the authentication checks that perimeter detection relies on. Tied to this, 84.9% of phishing emails passed DMARC authentication between January 1st - September 30th, 2025.

Our threat researchers have also observed a 20.9% increase in the use of polymorphic techniques in 2025 compared to 2024. Now, 32.4% of attacks

use techniques such as randomizing subject lines, versus 26.8% in 2024 and 20.9% in 2023. Adapting emails throughout a campaign makes it harder for signature-based detection to identify them.

We've also seen a rise in technical mechanisms to evade detection, with 28.6% of attacks in 2025 displaying these mechanisms. Obfuscation techniques are also on the rise, increasing by 13.6% this year, with HTML smuggling the most common technique used to hide an encoded payload within an HTML attachment that perimeter technology won't recognize as malicious.

Hyperlinks remain the most common payload in 2025 (present in 46.7% of attacks). They're relatively quick and easy to create, meaning they can be rapidly replaced once they're added to the blocklists that perimeter detection primarily relies on.

Ultimately, signature and reputation-based technologies provide a solid foundation for filtering out the attacks they know to be bad. However, as more phishing emails evade these mechanisms over time, it's crucial that organizations layer intelligent AI-powered detection into their environments so they can stop the full spectrum of attacks.

Phishing attacks sent  
from hijacked legitimate  
platforms can easily bypass  
native security and SEGs

# By the Numbers: A Quick Round-up of Phishing Stats From 2025

## Your Questions Answered About Phishing in 2025

**Q** Is Phishing becoming more prevalent in 2025?

**A** Yes. There was a 15.2% increase in phishing email volume between March 1st - September 30th, 2025, compared to the previous six months.



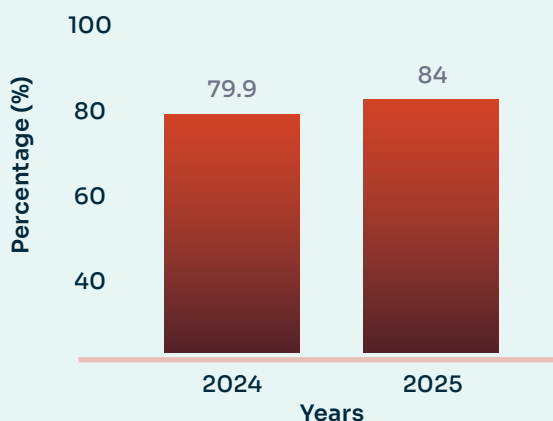
**15.2%**

Increase in phishing emails compared to the previous six months

**Q** Are more phishing emails using AI?

**A** Yes, there's been a 5.1% increase in phishing attacks using some form of AI, such as AI generated text or payloads, or using AI to automate personalization to make attacks more targeted.

Percentage Of Phishing Attacks Using AI

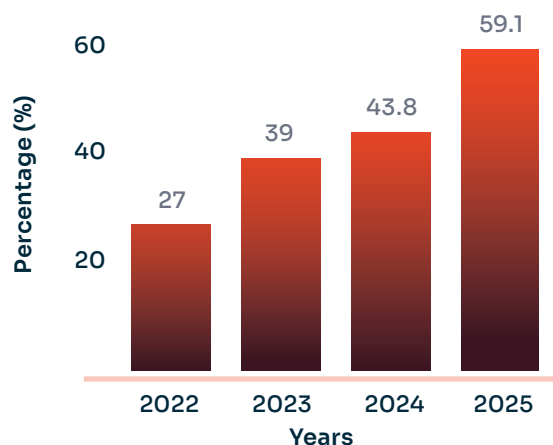


**Q** Are phishing attacks sent from compromised accounts still a problem?

**A** Unfortunately, yes. So far in 2025, we've identified that over half (59.1%) of phishing attacks have been sent from compromised accounts. That's a 34.9% increase versus 2024.

11.5% of these were sent from compromised accounts within a supply chain.

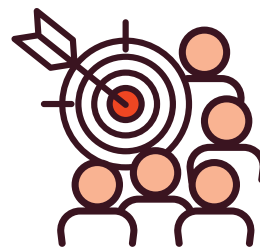
Percentage of Phishing Attacks Sent From Compromised Accounts



**Q Who are the most targeted people and departments?**

**A** Senior executives. The top five most-targeted job roles are: CEO, CFO, CPO, VP of Finance and COO.

Naturally, Exec departments are the most phished, followed by Finance, People Operations (HR), Marketing and IT.



**Top five most-targeted job roles are: CEO, CFO, CPO, VP of Finance and COO**

**Q How long is it before a new employee receives a phishing email?**

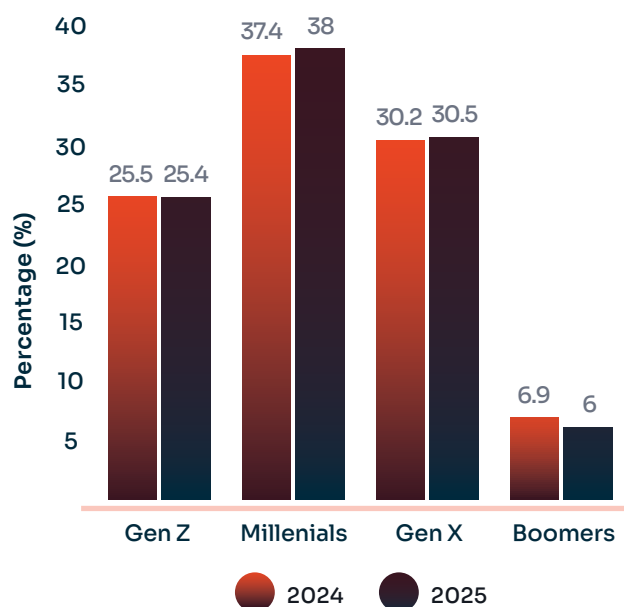
**A** On average, 3.5 weeks.



**Q What's the most phished generation?**

**A** Millennials! Followed by Gen X. As Gen Z increasingly enter the work place, they too are becoming targets.

### How Different Generations Are Targeted in the Workplace



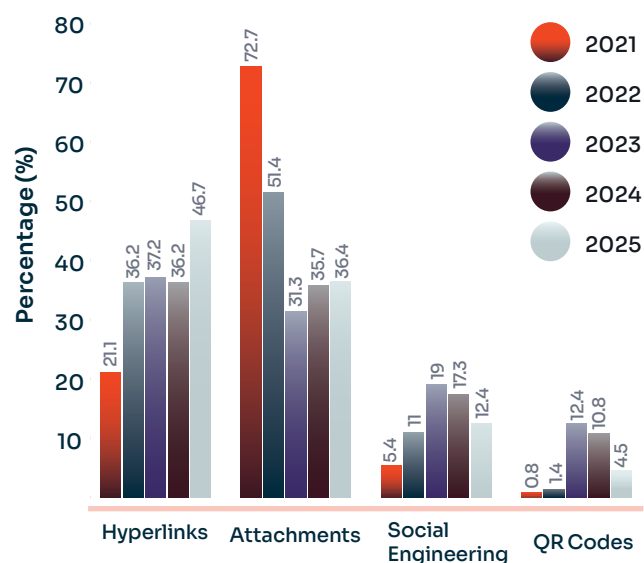


## Q What's the most common type of payload?

A Phishing hyperlinks. They take less expertise and time to create compared to other payload types (especially if the cybercriminal has purchased a templated phishing kit!) and can be rapidly recreated once they've been too widely detected as malicious.

Attachments are the next most popular payload, with an average attachment size of 150KB. The three most common attachment types are PDFs (43.0%), SVG (24.1%) and HTML (21.3%).

Percentage of Phishing Attacks Sent From Compromised Accounts Between 2021-2025



## Q How long is the average phishing email?

A 880 characters on average. The top five words used in a phishing email are: urgent, sign, review, invoice and payment.



## Q How are phishing emails using obfuscation techniques?

A There's been a steady increase in obfuscation as cybercriminals try to evade perimeter detection by native security and SEGs. In 2025, 62.7% of phishing emails used obfuscation compared to 55.2% in 2023.

Cybercriminals use HTML smuggling (hiding an encoded malicious script within an HTML attachment) most frequently, with the technique appearing in 25.9% of obfuscated attacks in 2025. Using lookalike characters is the second most popular technique, at 15.2%.

### HTML smuggling



### Lookalike characters (examples)

✓ microsoft.com	✗ mícrosoft.com (Latin í with an accent mark)
google.com	g00gle.com (Zero for letter o)
paypal.com	paypa1.com (Number 1 for letter l or capital I)



# A New Age for Human Risk Management

## Email Security Is No Longer an Isolated Element in the Tech Stack

We hope you've found this edition of the Phishing Threat Trends Report insightful. Our aim is to increase your awareness of the attacks that could target your organization so you can ensure you have the most robust defenses to protect your people, customers, data and systems.

What's been apparent throughout this edition is that organizations continue to face campaigns that, increasingly, contain technical measures to get through native security and secure email gateways (SEGs) and sophisticated social engineering tactics to manipulate their targets.

Whether it's hijacking legitimate platforms to leverage their domains and brands, using highly emotive voice phishing (vishing) attacks or obfuscating payloads, cybercriminals are simultaneously doubling down on the tactics that work while expanding their attack playbooks.

Enhanced email security is, therefore, critical – but it cannot exist in isolation. As attackers seek to move targets into less secure channels and applications, email security products must work within a holistic human risk management (HRM) ecosystem, where the latest threat intelligence and deep behavioral analytics can be used to automate continuous coaching to increase awareness of the live attacks targeting organizations and individuals.

**The KnowBe4 team would welcome the opportunity to talk about any of the findings in this report and continue the HRM conversation with you.**

# Our Contributors



**James Dyer**  
Threat Intelligence  
Lead

James spearheads the Threat Intelligence team at KnowBe4, spending his days uncovering the latest phishing threat trends, understanding emerging methodologies, and analyzing the TTPs of the crime-as-a-service ecosystem.



**Lucy Gee**  
Cyber Security  
Threat Researcher

Lucy is passionate about the intersection of psychology and cybersecurity and the use of behavioral insights to enable people to live and work securely. At KnowBe4, Lucy analyzes the latest phishing campaigns and communicates emerging trends to business stakeholders.



**Cameron Sweeney**  
Cyber Security  
Threat Researcher

Cameron specializes in understanding the technical aspects of cyberattacks. As a member of the KnowBe4 team, he reverse engineers phishing attacks and malware to identify emerging threats, using statistical analysis to track the evolving threat landscape.



**Louis Tiley**  
Cyber Security  
Threat Researcher

Louis researches diverse attack vectors, social engineering tactics and emerging threats. At KnowBe4, he analyzes phishing campaign methodologies and builds tools to automate threat intelligence gathering to identify industry trends and shape cybersecurity messaging.



**Bex Bailey**  
Director of  
Research and  
Communications  
(author)

Bex leads our research program, developing and implementing KnowBe4's global strategy with our thought leaders. Bex brings our latest insights to life in this and other reports, providing timely updates on the most critical security issues.



**Jack Chapman**  
SVP Threat  
Intelligence

Jack leverages deep insights of the cyber-threat landscape and his extensive R&D skillset to oversee threat research and AI development for KnowBe4 Defend to stop the advanced phishing attacks that defeat traditional security solutions. Jack maintains close ties with the global cyber community, particularly the UK's intelligence and cyber agency GCHQ.



**Dr. Martin J. Krämer**  
CISO Advisor

Martin is a CISO Advisor at KnowBe4. He has over 10 years of research and industry experience in cybersecurity with a focus on human-centered computing. Martin held roles in innovation, research, and technology consulting. He has worked with both public and private organizations on information security and data protection.

# About KnowBe4 Defend

An integrated cloud email security solution, Defend delivers AI-powered behavioral-based detection to eliminate the attacks that get through native security and secure email gateways. Leveraging zero-trust and pre-generative models, Defend provides the highest efficacy of detection against advanced threats, including zero-day and emerging attacks, phishing emails sent from compromised accounts, and social engineering. Using dynamic banners applied to neutralized threats, Defend provides real-time teachable moments that continually 'nudge' employees into good security behaviors to tangibly reduce risk and augment security awareness.

---

## About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk.

KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats.

The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization's biggest asset.

For more information, please visit [www.KnowBe4.com](http://www.KnowBe4.com).



KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755  
855-KNOWBE4 (566-9234) | [www.KnowBe4.com](http://www.KnowBe4.com) | [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.