egress

northdoor
◦ Store IT ◦ Protect IT ◦ Use IT ◦

April 2024 | Vol. 3

Phishing Threat Trends Report

The rise of quishing, AI-powered attacks, and the most popular phishing tactics in 2024

THE EVOLUTION OF PHISHING IN 2024

Welcome to the April 2024 Phishing Threat Trends Report, in which we analyze the ways in which phishing has changed (and stayed the same!) so far this year. We look at some of the hot topics that have dominated headlines, including the rise of QR phishing and AI-powered attacks, as well as analyze how cybercriminals are engineering attacks to get through detection by secure email gateways. Plus, we examine the evolution of payloads in phishing campaigns.

Unless otherwise cited, all statistics in this report have been generated using data from Egress Defend, an integrated cloud email security (ICES) solution that detects the full spectrum of advanced phishing attacks. Our team would love to hear from you if you would like to discuss this report or find out how Egress can improve your email security.

Jack Chapman
SVP of Threat Intelligence, Egress

IN THIS EDITION

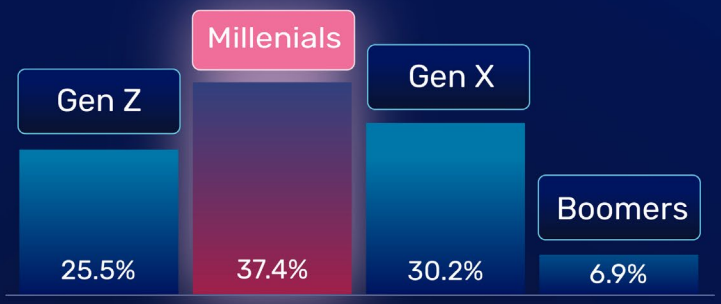
PHISHING ATTACK TRENDS IN 2024

Sunday is the most popular day to send phishing emails

And **February 9th** was the most phished day of the year so far

As cybercriminals try to catch victims with Valentine's Day themed attacks

Millennials are the top targets, by age



CEOs are the most targeted job roles

Most targeted teams

- Accounting
- Finance
- Marketing
- HR

Most targeted industries

- Finance
- Legal
- Healthcare

DocuSign

is the most impersonated brand, followed by

Microsoft

dpd

DHL

EVRi

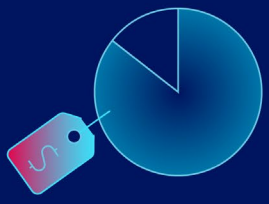
are the most impersonated mail carriers

20.2% of phishing emails involved technical measures to avoid detection by Microsoft 365 and secure email gateways

9.6% were designed to target **mobile users**

18.6% relied solely on **social engineering tactics**

18.1% were **impersonation attacks**



77.2% impersonated **well-known brands**

13.4% impersonated **someone the target knows**, such as their CEO

9.5% impersonated **supply chain organizations**

*Data taken from Egress Defend between January 1st – March 31st, 2024.

THE EVOLUTION OF PHISHING ATTACK PAYLOADS

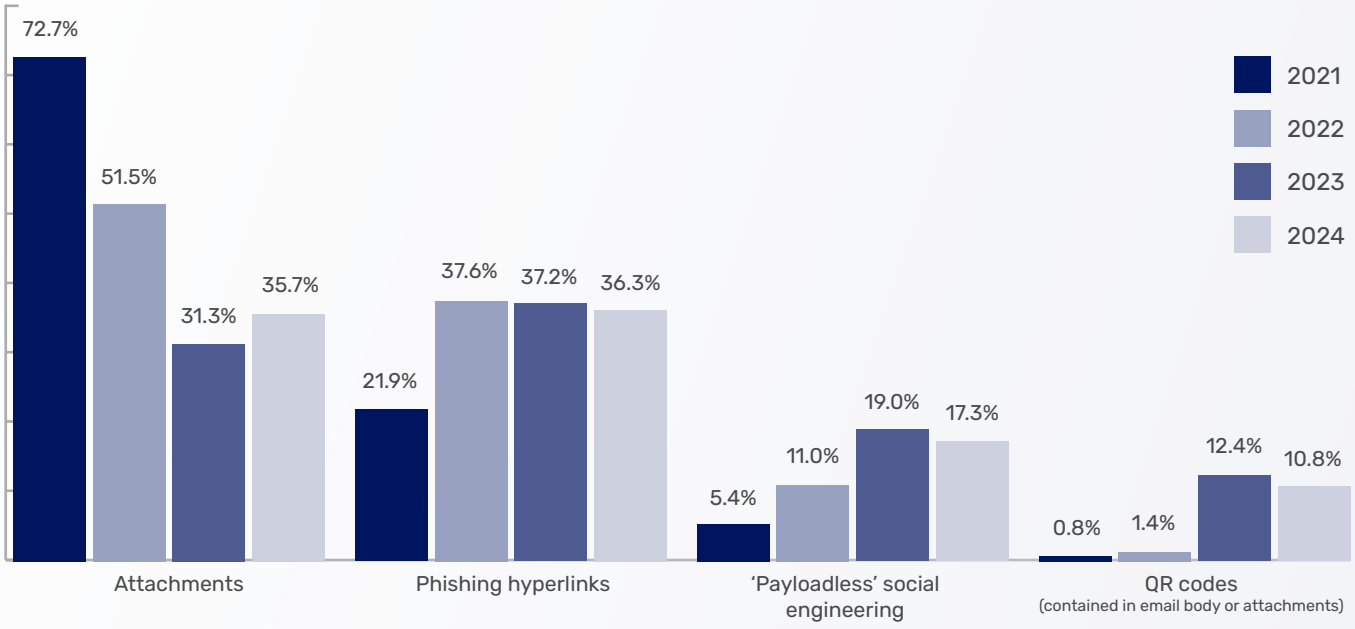
On the up: quishing and social engineering as hackers pivot tactics.

A staggering increase in QR code phishing (or "quishing") attacks during 2023 saw them skyrocket up the list of concerns for Cyber teams globally. Attacks were both prolific and highly successful, demonstrating how cybercriminals effectively combine available technology with consumer familiarity (or complacency) at scale.

In 2021 and 2022, QR code payloads in phishing emails were relatively rare – accounting for 0.8% and 1.4% of attacks respectively. In 2023, this jumped to 12.4% and has continued at 10.8% for 2024 so far. This quishing boom will likely continue until most organizations have implemented effective defenses against this type of attack, reducing cybercriminals' returns and forcing them to pursue other tactics.

Also on the increase are attacks that don't contain a traditional payload (malware attachment or hyperlink to a phishing website) but rely solely on social engineering. Again, these experienced a significant rise in 2023 to account for almost one-fifth (19.0%) of phishing attacks, which our analysts attribute to the increasing use of generative AI. While quishing and social engineering have experienced meteoric rises, the use of attachment-based payloads has decreased since 2021. Three years ago, they accounted for 72.7% of attacks detected by Egress Defend; by the first quarter of 2024, this number had fallen to 35.7%.

THE EVOLUTION OF PHISHING EMAIL PAYLOADS SINCE 2021



Attachment issues

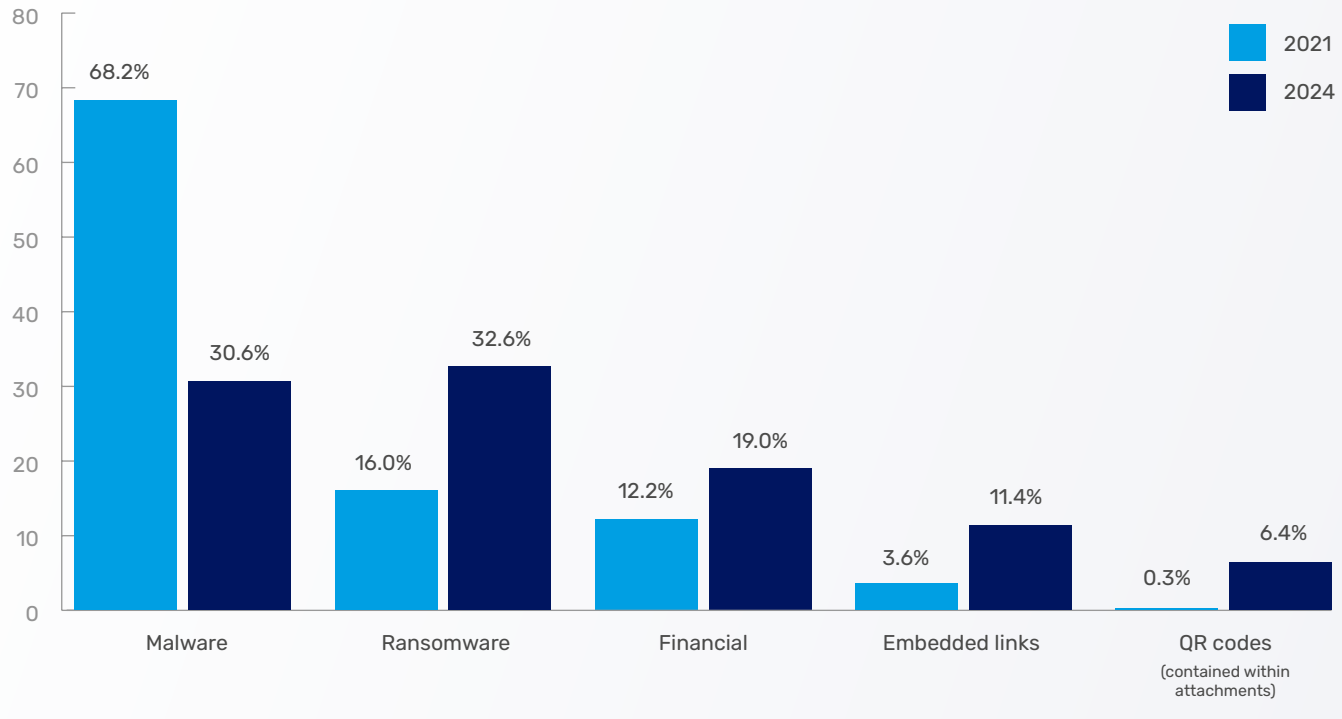
Just as different types of payloads have changed in popularity, so have the specific payloads themselves.

When comparing attachment-based payloads from 2021 with those being sent in 2024, our analysts observed that ransomware has doubled in prevalence, while other types of malware have more than halved. It's well known that ransomware attacks can be highly effective for cybercriminals, with attackers often double or triple-extorting their targets for maximum payouts from one attack.

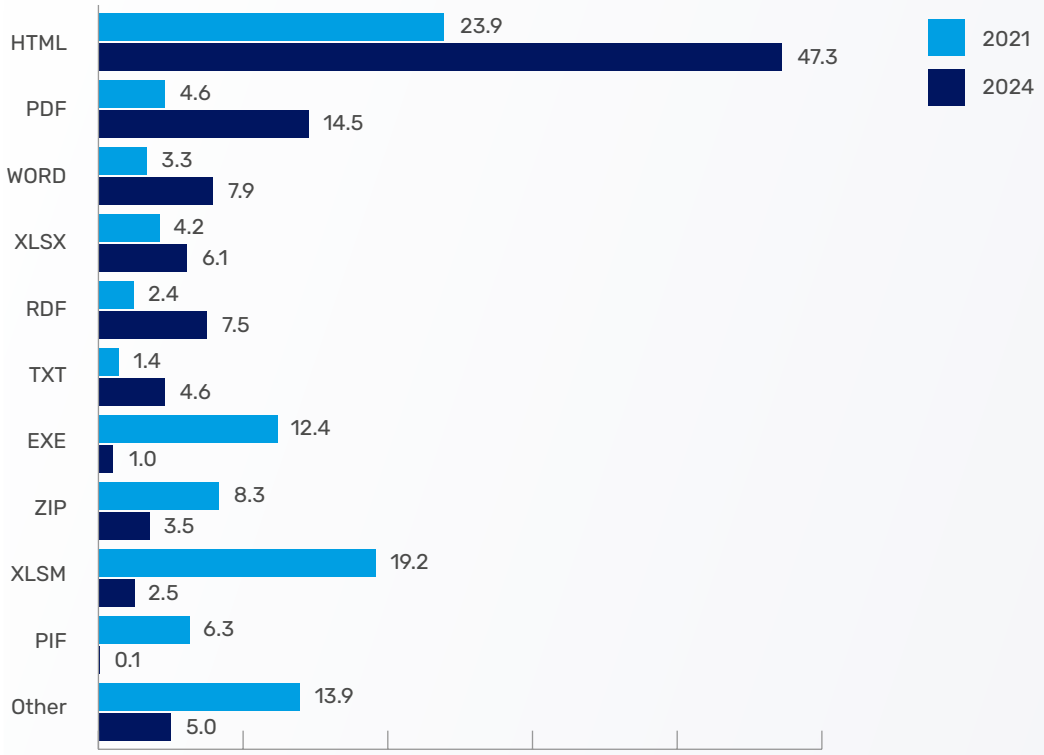
When analyzing file types, the biggest increase between 2021 and 2024 is for HTML attachments. In HTML smuggling attacks, cybercriminals 'hide' an encoded malicious script with an HTML attachment, with the payload assembled post-delivery. This is a highly evasive technique that enables attacks to get through the traditional signature-based detection used by secure email gateways and Microsoft's native security.

Increases in the use of PDFs and Word documents can be correlated with the rise in financial-themed payloads (e.g. wire fraud). These file types are commonly used in invoice fraud attacks, with the email body utilizing social engineering tactics to convince the target to quickly process the request.

CHANGES IN THE CONTENT OF ATTACHMENT-BASED PAYLOADS BETWEEN 2021 AND 2024



CHANGES IN THE FILE TYPE OF ATTACHMENT-BASED PAYLOADS BETWEEN 2021 AND 2024



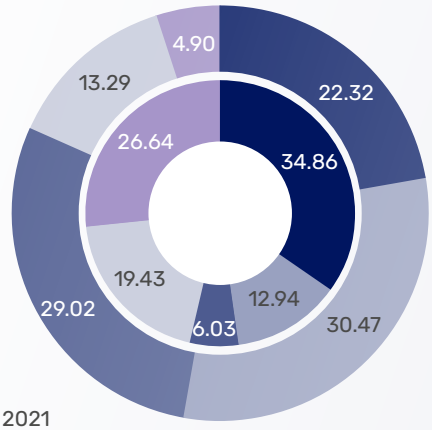
Linking up

Cybercriminals have also changed their tactics with phishing hyperlinks in recent years. Exploiting vulnerabilities in legitimate sites and linking to file sharing services where, typically, malware is hosted is significantly more popular in 2024 than in 2021.

Similar to HTML smuggling for attachments, this shift can be attributed to cybercriminals doubling down on tactics that are more likely to evade signature-based detection by SEGs and Microsoft's native security. Additionally, these hyperlinks socially engineer their targets, who are more likely to trust – and therefore click on – a hyperlink that's familiar or contains a trusted brand's name.

Masking hyperlinks with link shorteners has experienced the most significant decline – going from the second most common tactic in 2021, to last place in 2024. Typosquatting and post-delivery DNS changes have also decreased in popularity.

CHANGES IN PHISHING HYPERLINK TACTICS BETWEEN 2021 AND 2024



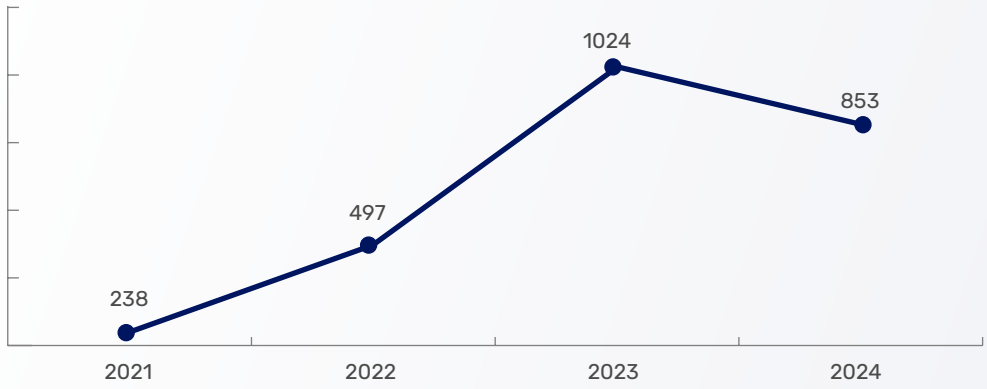
Inside ring: 2021
Outside ring: 2024

Typosquatting
Post-delivery DNS change
Legitimate sites
Link shortener
File sharing links

A war of words

On average, phishing emails are now over three times longer than they were in 2021. As previously mentioned, our analysts correlate this with the rise of generative AI – which, with a simple prompt, can generate well-written phishing attacks. See pages 13-15 for insight on the growing use of AI in phishing attacks.

AVERAGE CHARACTER LENGTH OF PHISHING EMAILS EACH YEAR SINCE 2021



Staying ahead of the evolution of phishing payloads

Cybercriminals will always innovate. As detection improves against one type of attack or tactic, they'll continue to try to find new ways to bypass security and cause targets to fall victim. To future-proof their detection efficacy, organizations need anti-phishing defenses that have been engineered to combine intelligent technologies with best-practice methodologies. Holistically analyzing all aspects of an inbound email together (including technical aspects, attachments, and body copy) means solution efficacy isn't reliant on detecting known payloads, but results in accurate identification of phishing attacks with a zero-day, emerging and obfuscated payloads - or even payloadless phishing emails that rely solely on social engineering.

New payloads will emerge and older tactics will be refreshed - but with the right detection capabilities, organizations can easily adapt to the evolution of the phishing payload.

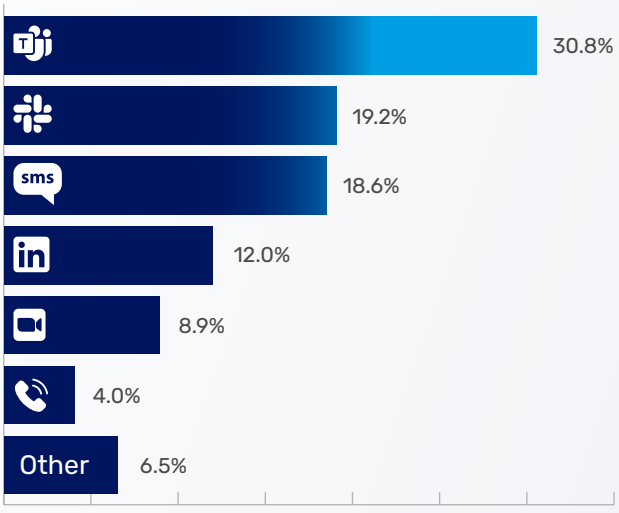
GOING MULTI-CHANNEL

How cybercriminals are trying to hook employees across multiple platforms

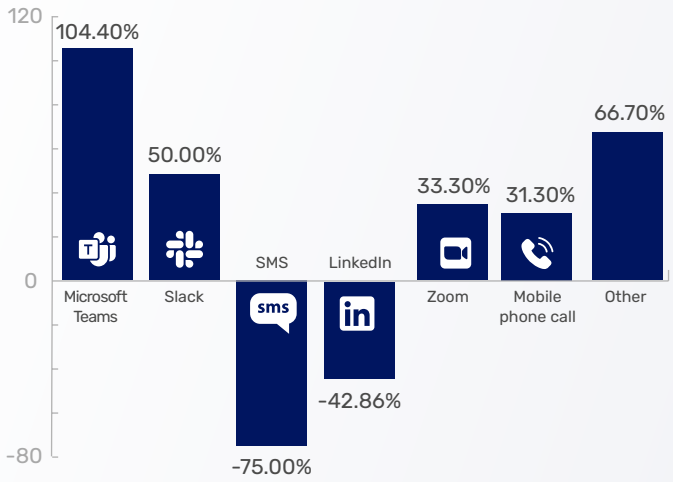
Multi-channel attacks – where victims are targeted via two or more communication platforms – typically have a higher success rate for cybercriminals. These attacks can follow normal communication patterns and therefore appear more legitimate (such as a vendor sending an invoice via email and following up on Microsoft Teams to ensure it's processed); there's usually less security and monitoring for non-email communications; and, as security awareness training (SAT) typically focuses most frequently on email, it can be easier to trick people when using other platforms.

With the ongoing use of multiple communication channels within the workplace, our Threat Intelligence analysts predict these attacks will become more common in future.

THE MECHANISMS CYBERCRIMINAL USE TO CONTACT THEIR TARGETS **FOLLOWING AN INITIAL PHISHING EMAIL** IN MULTI-CHANNEL ATTACKS



THE PERCENTAGE DIFFERENCE IN THE CHANNEL USED FOR THE SECOND STEP OF MULTI-CHANNEL ATTACKS BETWEEN OCTOBER 1ST – DECEMBER 31ST, 2023, COMPARED WITH JANUARY 1ST – MARCH 31ST, 2024



It's therefore crucial that organizations deliver SAT that is timely and highly relevant - for example through real-time teachable moments.

Following an initial phishing email being sent to the target, between January 1st and March 31st, 2024, Microsoft Teams was the most common second step, accounting for 30.8% of attacks, followed by Slack (19.2%), and SMS (18.6%). All three are popular communication channels; in particular Microsoft Teams boasts 320 million monthly active users, which puts its adoption rate at about 80% of the Microsoft 365 base,[1] meanwhile, providing a significant pool of potential targets.

1 https://office365itpros.com/2023/10/26/teams-number-of-users-320-million, accessed on April 7th, 2024.

In fact, instances of using Microsoft Teams as the second step in multi-channel attacks have increased by 104.4% in 2024. SMS, meanwhile, has declined by 75.0%, which our Threat Intelligence analysts believe is related to seasonality, as the combination of phishing email followed by SMS is commonly used for mail fraud attacks, which peak around the Christmas holidays.

Phishing hyperlinks were the most common payload in multi-channel attacks between January 1st and March 31st, 2024, used in 67%, with malware attachments only used in 7.2%. The remaining 25.4% contained a 'non-traditional' payload, such as a fraudulent invoice.

Impersonation was present in 34.2% of attacks, including impersonating large brands and vendors and individuals within the target's supply chain. 27.8% of attacks used the tactic of informing the recipient that they had missed a voicemail.

How multi-channel attacks play out

We've included three examples of multi-channel attacks from the first quarter of 2024. In the first and third examples, a phishing email was followed by communication via Microsoft Teams. In the second example, the email was followed by an SMS.

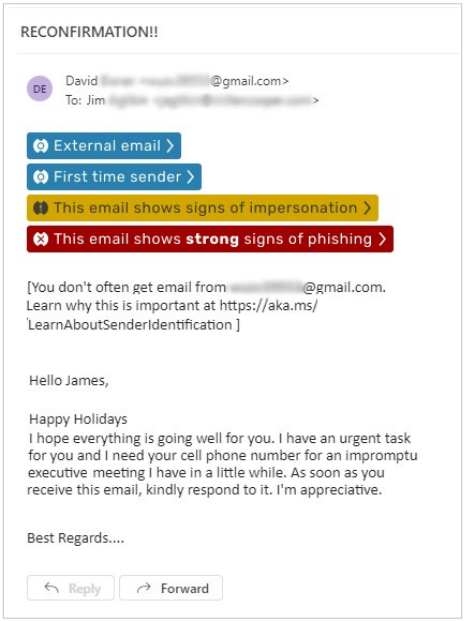
Every phishing email was detected by Egress Defend, with its dynamic banners delivering real-time teachable moments.

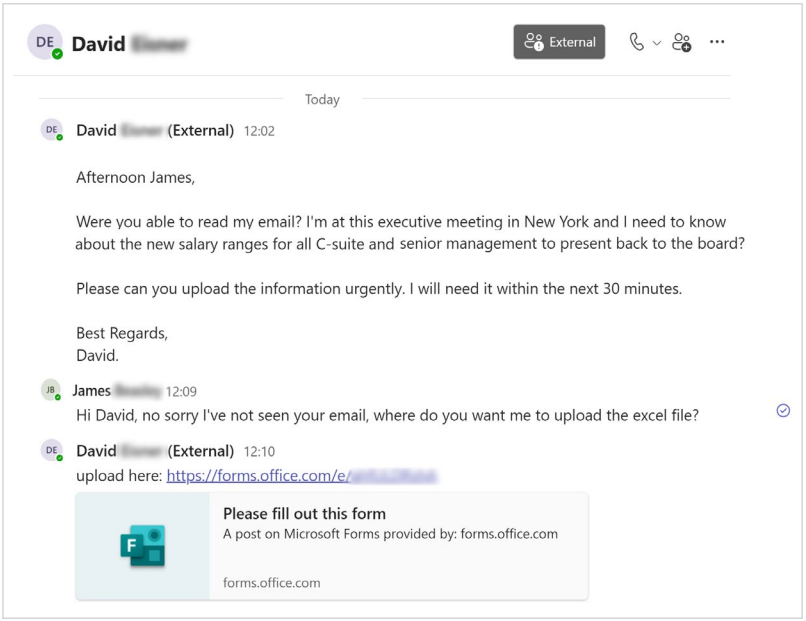
ATTACK ONE: PHISHING HYPERLINK DELIVERED IN MICROSOFT TEAMS FOLLOW-UP MESSAGES

Here, the cybercriminal uses social engineering tactics in both the initial email and the follow-up messages to create a sense of urgency, which is intended to trick the target into acting quickly. After the initial email isn't responded to, and the attacker is unable to obtain the target's phone number, they reach out via Microsoft Teams to make their request.

1 **INITIAL PHISHING EMAIL** SENT TO VICTIM IN MULTI-CHANNEL ATTACK, **WITH EGRESS DEFEND ANTI-PHISHING BANNERS** VISIBLE.

2 **INTERACTION VIA MICROSOFT TEAMS** BETWEEN CYBERCRIMINAL (IMPERSONATING DAVID) TO DELIVER A PHISHING HYPERLINK.

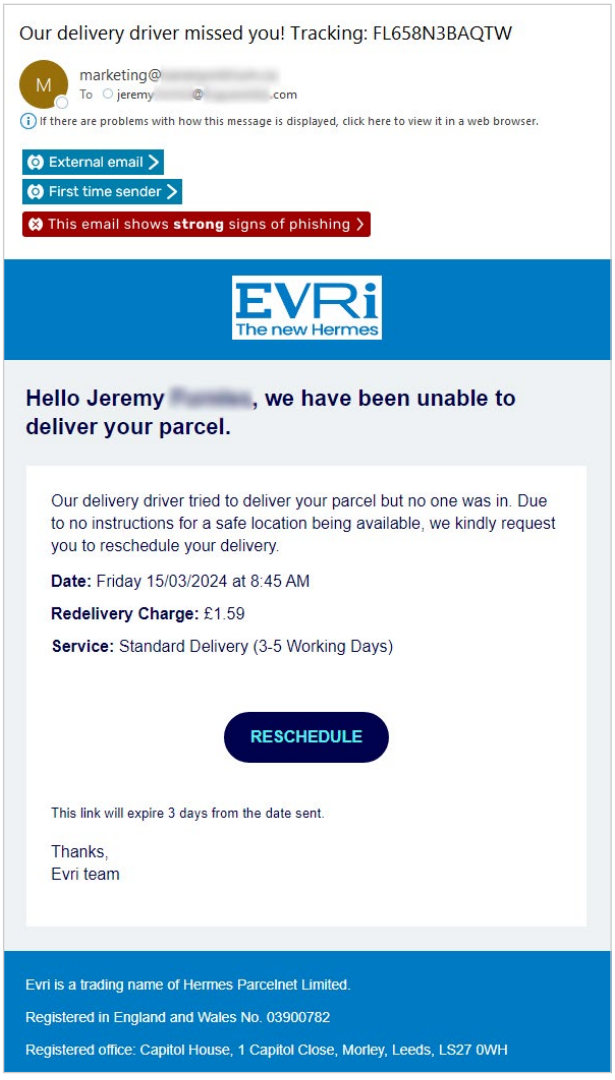




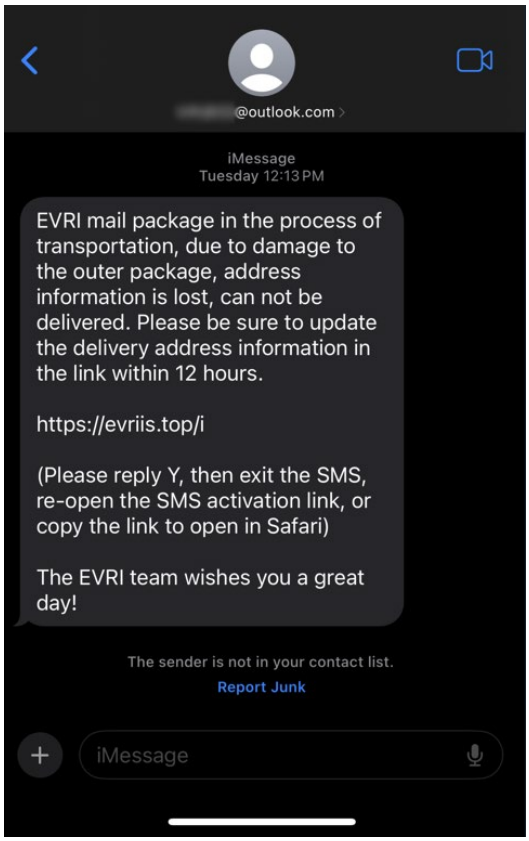
ATTACK TWO: FRAUD ATTACK VIA EMAIL AND SMS

In this attack, the target's email address and phone number were obtained via a third-party data breach. Both impersonate UK-based mail carrier Evri and, despite the different messages, contain the same phishing hyperlink payload, designed to steal more data and defraud the target.

1 **INITIAL PHISHING EMAIL** SENT TO VICTIM IN MULTI-CHANNEL ATTACK, WITH EGRESS DEFEND ANTI-PHISHING BANNERS VISIBLE.



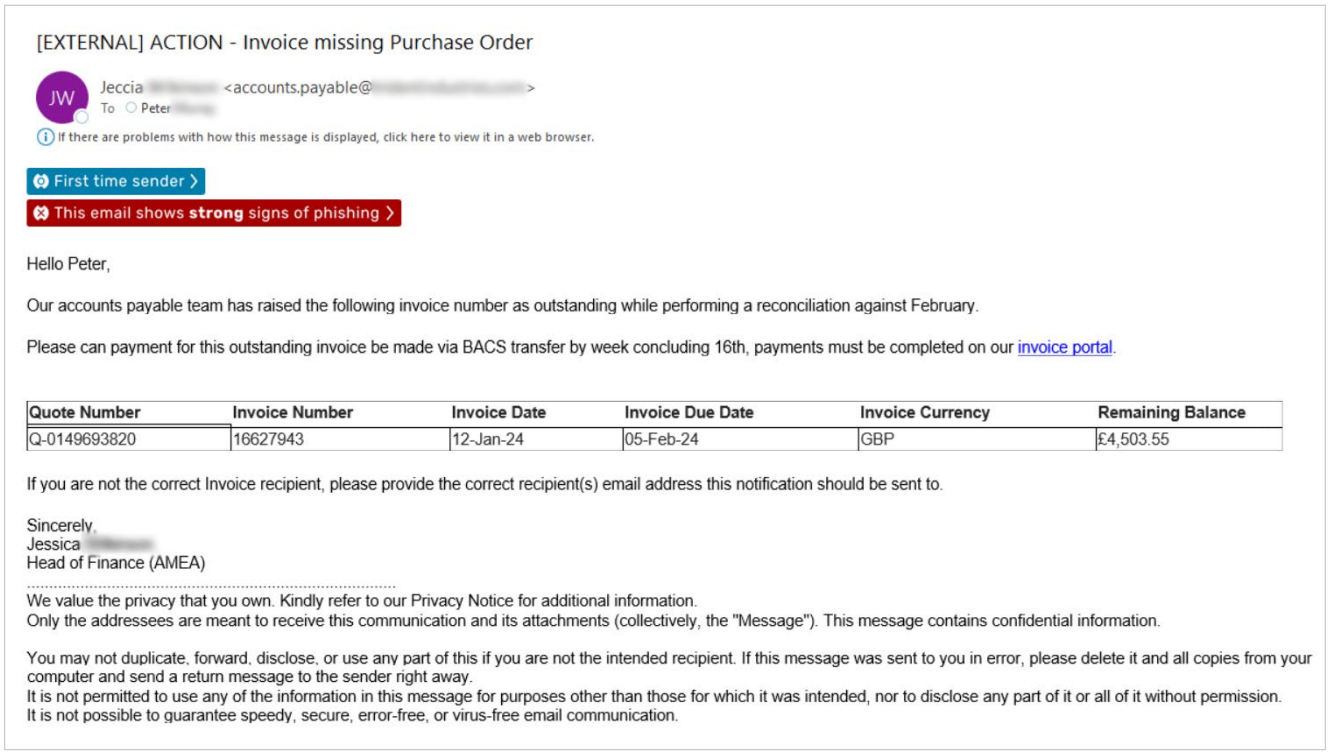
2 **SMS SENT TO TARGET** TWO DAYS AFTER INITIAL EMAIL.



ATTACK THREE: WIRE FRAUD VIA EMAIL AND MICROSOFT TEAMS

In this wire fraud attack, the cybercriminal uses social engineering tactics to attempt to pressure the target into quickly processing an 'outstanding' fraudulent invoice. The tight deadline for payment contained within the initial email, flagging the Microsoft Teams message 'Urgent', and language such as 'ASAP' are designed to increase this pressure.

1 **INITIAL PHISHING EMAIL** SENT TO VICTIM IN MULTI-CHANNEL ATTACK, WITH EGRESS DEFEND ANTI-PHISHING BANNERS VISIBLE.



[EXTERNAL] ACTION - Invoice missing Purchase Order

JW Jeccia <accounts.payable@> To Peter

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

First time sender >

This email shows **strong** signs of phishing >

Hello Peter,

Our accounts payable team has raised the following invoice number as outstanding while performing a reconciliation against February.

Please can payment for this outstanding invoice be made via BACS transfer by week concluding 16th, payments must be completed on our invoice portal.

Quote Number	Invoice Number	Invoice Date	Invoice Due Date	Invoice Currency	Remaining Balance
Q-0149693820	16627943	12-Jan-24	05-Feb-24	GBP	£4,503.55

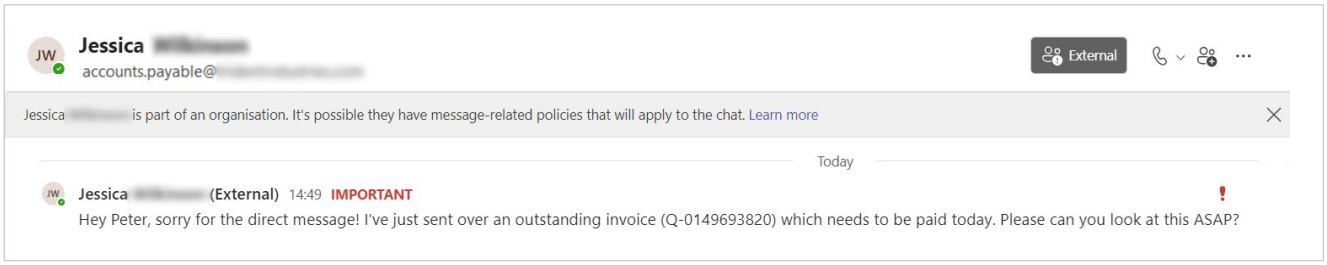
If you are not the correct Invoice recipient, please provide the correct recipient(s) email address this notification should be sent to.

Sincerely,
Jessica
Head of Finance (AMEA)

We value the privacy that you own. Kindly refer to our Privacy Notice for additional information.
Only the addressees are meant to receive this communication and its attachments (collectively, the "Message"). This message contains confidential information.

You may not duplicate, forward, disclose, or use any part of this if you are not the intended recipient. If this message was sent to you in error, please delete it and all copies from your computer and send a return message to the sender right away.
It is not permitted to use any of the information in this message for purposes other than those for which it was intended, nor to disclose any part of it or all of it without permission.
It is not possible to guarantee speedy, secure, error-free, or virus-free email communication.

2 **MICROSOFT TEAMS MESSAGE** PRESSURING TARGET TO RESPOND TO INITIAL PHISHING EMAIL.



JW Jessica
accounts.payable@

External

Jessica is part of an organisation. It's possible they have message-related policies that will apply to the chat. Learn more

Today

Jessica (External) 14:49 IMPORTANT

Hey Peter, sorry for the direct message! I've just sent over an outstanding invoice (Q-0149693820) which needs to be paid today. Please can you look at this ASAP?

AI EVERYWHERE

From deepfakes to fully automated phishing campaigns, here are some of the ways cybercriminals are using AI in 2024.

Our 2024 Email Security Risk Report found that 63% of Cybersecurity leaders are concerned about the use of deepfakes in cyberattacks and 61% are worried about cybercriminals using generative AI chatbots to enhance their phishing campaigns.

Rightly so. These are two alarming ways that AI can be used to create highly convincing and targeted attacks at scale – but, more worryingly, there are multiple other applications for AI in phishing. In fact, our Threat Intelligence team believes that in the near future, some form of AI will be used in almost every attack.

Here are some of the ways that AI in the hands of cybercriminals can put organizations at risk.

Reconnaissance

AI can be used to find the perfect targets for attacks. By processing information at incredible speeds, it can help cybercriminals aggregate and correlate data across numerous data breaches to uncover different platforms for multi-channel attacks (such as combining phishing emails with SMS), as well as correlate any identifying information from these breaches.

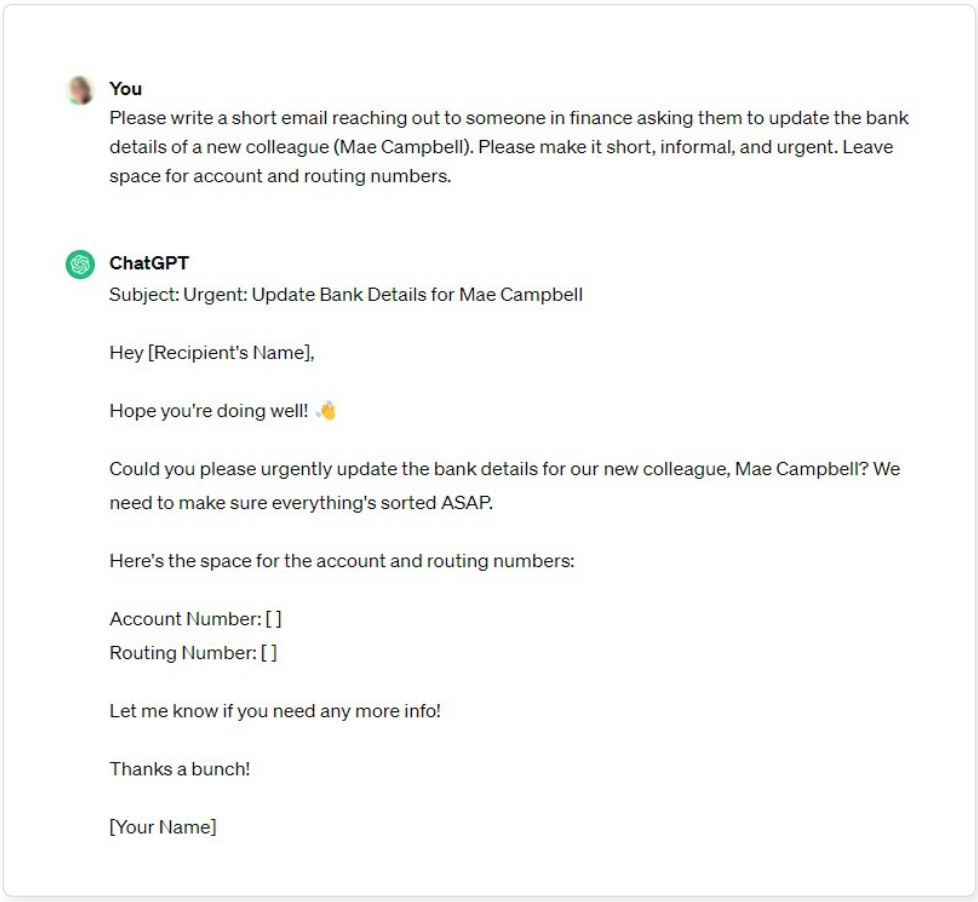
Once the targets are lined up, AI can be used to quickly collect publicly available information, for example scraping social media channels and organizational websites.

Creating convincing attacks at scale

Generative AI chatbots can be used to create both written messages – such as phishing emails – and payloads. Phishing and other message-based attacks are only effective if they can convince the target to carry out the intended action. Typically, well-written and highly targeted attacks are more convincing – which is where AI-powered large language models (LLMs) and natural language generation (NLG) come in. If combined with intelligence collected during the reconnaissance stage, cybercriminals can use simple prompts to quickly produce very convincing attacks.

We believe that in the near future, some form of AI will be used in almost every phishing attack.

EXAMPLE OF AN AI CHATBOT BEING USED TO WRITE AN EMAIL REQUESTING CHANGES TO BANK DETAILS.



You
Please write a short email reaching out to someone in finance asking them to update the bank details of a new colleague (Mae Campbell). Please make it short, informal, and urgent. Leave space for account and routing numbers.

ChatGPT
Subject: Urgent: Update Bank Details for Mae Campbell

Hey [Recipient's Name],

Hope you're doing well! 👋

Could you please urgently update the bank details for our new colleague, Mae Campbell? We need to make sure everything's sorted ASAP.

Here's the space for the account and routing numbers:

Account Number: [ ]
Routing Number: [ ]

Let me know if you need any more info!

Thanks a bunch!

[Your Name]

Deepfakes are also a concern. As noted on page 9, the use of Zoom and mobile phone calls as the second step in multi-channel attacks has increased in the first quarter of 2024 compared with the last quarter of 2023.

Almost everyone has videos and photos on the internet – whether on corporate websites, podcasts and interviews, or social media. AI can process these for visual and audio outputs that can generate specific deepfakes – such as joining a Zoom meeting with your company's board or taking a call from your CEO.

Payloads that can be generated include malware, phishing websites, and invoices for wire fraud attacks. Where new payloads are generated, these form zero-day attacks that can get through the signature-based detection used by cloud platforms, such as Microsoft 365 and secure email gateways. Additionally, when it comes to malware and phishing websites, AI can significantly lower the barrier for entry to cybercrime, meaning attackers don't need to learn to code or work with someone who can code before launching their campaigns.

Well-written and highly targeted attacks are more convincing, which is where LLMs and NLG come in.

Automation

Cybercriminals don't even need to be at their computers to generate advanced phishing attacks. AI can automate the processes to research, create, and send highly targeted attacks at scale.

Additionally, generative AI chatbots can be used to respond to replies from phishing emails in real time, engaging with victims and quickly directing them to the cybercriminals' intended outcome – all without the target realizing they're not talking with the person they believe they're communicating with, or with a person at all!

Fighting fire with fire: Using AI to detect AI-powered attacks

While AI is changing the game for cybercriminals – it's also changing the game for email security defenses. Integrated cloud email security (ICES) solutions use models such as natural language processing (NLP) and natural language understanding (NLU) to analyze email content for the linguistic markers of phishing, and can also utilize machine learning to detect the zero-day and emerging payloads that get through signature-based detection.

Detecting phishing is the focus – whether the campaigns are generated by people or by AI. By using AI-powered defenses, organizations will be able to detect the full spectrum of inbound attacks.

This time it's personal

Uncovering intelligence about a target and embedding this within an attack personalizes a phishing email, giving it the appearance of legitimacy.

Four examples our analysts have observed recently in large-scale phishing campaigns include:

- Adding targets' geographical locations into subject lines to impersonate legitimate services, such as Valentine's Day attacks impersonating dating apps
- Using organizational hierarchy to increase pressure on a target, such as referencing their boss or CEO
- Identifying new employees following announcements on company websites and social media
- Adding information about personal lives, such as vacation or hobbies, to increase credibility, for example impersonating an employee who is on vacation and including genuine information scraped from social media.

By using AI, organizations will be able to detect the full spectrum of inbound attacks.

WHAT'S GETTING THROUGH SECURE EMAIL GATEWAYS?

How cybercriminals are engineering attacks to bypass perimeter defenses

Our 2024 Email Security Risk Report found that 87% of Cybersecurity leaders are considering replacing their secure email gateway (SEG) with Microsoft 365 native controls and integrated cloud email security (ICES).

Microsoft has disrupted the SEG market, enhancing its phishing detection capabilities to significantly overlap with SEGs. Simultaneously, organizations are rapidly investing in ICES products that can detect a broader spectrum of phishing attacks, particularly those that get through signature and reputation-based detection.

Understanding the risk of attacks getting through is key to organizations enhancing their anti-phishing defenses, so our Threat Intelligence analysts have taken a deep dive into the attacks that are bypassing the SEG in 2024.

In the first three months of 2024, there was a 52.2% increase in the number of attacks that got through SEG detection. 68.4% of these attacks passed authentication checks, including DMARC, which is a primary detection capability used by SEGs.

Key to this is that most of these were sent from legitimate but compromised third-party accounts. 43.9% were sent from compromised accounts not related to the target's organization and a further 4.4% were sent from compromised accounts within their supply chain (vendor email compromise (VEC)).

Hyperlinks to phishing websites were the most common payload, present in 43.6% of attacks, closely followed by malware attachments in 36.0%.

One-quarter (24.8%) featured technical measures to bypass detection, such as obfuscation, and 9.3% were designed to target recipients on their mobile devices. 4.6% of attacks were categorized as sextortion, and our analysts observed a trend where adding Bitcoin or Etherum addresses for extortion payments has prevented detection.

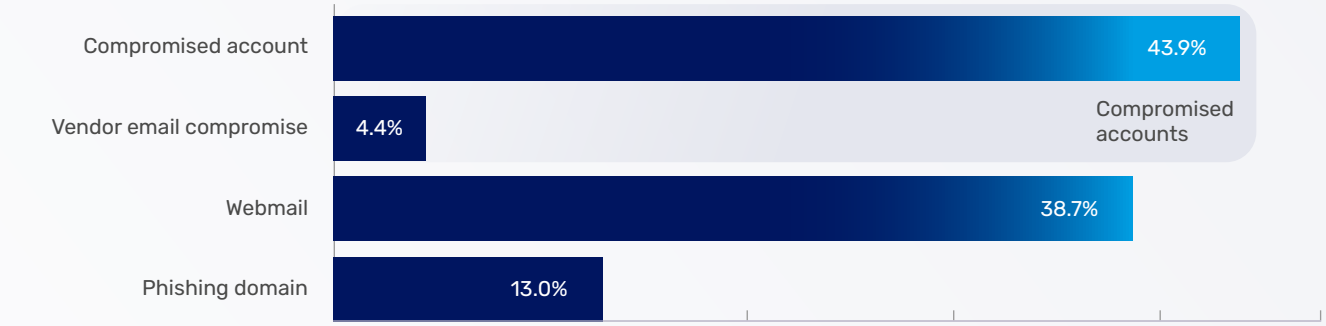
When using obfuscation techniques, the most common primary mechanism was hijacking legitimate hyperlinks, such as to filesharing sites. This was the primary technique observed in one-quarter (24.9%) of attacks, followed by masking hyperlinks to phishing websites within image-based attachments (such as JPEGs) that can't be analyzed by SEGs, which was present in 19.6%. HTML smuggling, meanwhile, was the third highest, at 16.2%.

Combining obfuscation techniques can make attacks even more difficult to detect by SEGs, and the most frequent combinations this year are 'HTML smuggling, left-to-right override, and encoding' (present in 31.6% of attacks that use multiple layers of obfuscation) and 'image-based and hijacking legitimate hyperlinks' (27.7%).

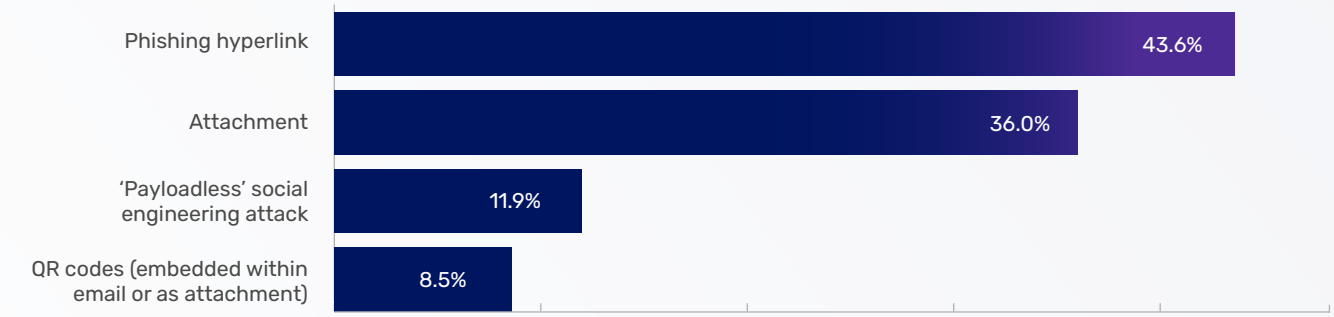
So far in 2024, there has been a 52.2% increase in the number of attacks that got past the SEG.

In numbers, how phishing emails a getting through SEG detection in 2024

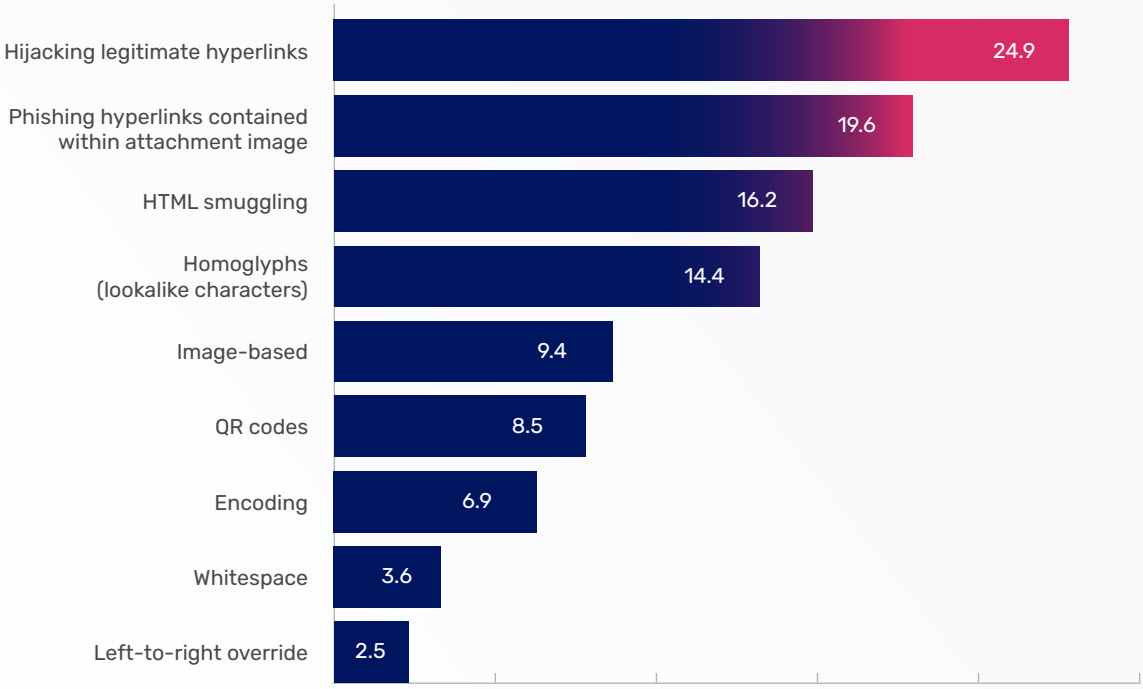
SOURCES OF PHISHING **EMAILS THAT GOT THROUGH SEG DETECTION** BETWEEN JANUARY 1ST – MARCH 31ST, 2024



PHISHING PAYLOADS THAT BYPASSED SEG DETECTION BETWEEN JANUARY 1ST – MARCH 31ST, 2024



PRIMARY OBFUSCATION TECHNIQUES USED TO GET THROUGH SEG DETECTION
BETWEEN JANUARY 1ST – MARCH 31ST, 2024



Layering defenses in Microsoft 365: Detecting the attacks that undetected by SEGs

As noted, there is significant overlap in the detection capability between SEGs and Microsoft 365 – so organizations need a different type of defense layered on top of Microsoft's native security to enable them to detect the broader spectrum of phishing threats.

Integrated cloud email security (ICES) solutions offer AI-powered behavioral-based threat detection that goes beyond traditional signature-based and reputation-based detection. It's important to utilize a solution that takes a zero-trust approach, holistically inspecting every inbound email and using machine learning and AI models such as natural language processing (NLP) and natural language understanding (NLU) to determine the context and content of every message. Combined with analysis of the technical aspects of inbound emails, this provides the highest level of threat detection efficacy to catch attacks missed by solutions that rely primarily on signature-based and reputation-based detection. This includes detecting attacks that are sent by compromised third-party accounts, contain a zero-day or obfuscated payload, and social engineering attacks.

ICES products can analyze the context and content of every email to provide the highest levels of threat detection.

BY THE NUMBERS: KEY CONSIDERATIONS ABOUT PHISHING ATTACKS IN 2024

Your questions answered about the risk of phishing so far this year

Q Is phishing more prevalent in 2024?

A Yes. Analyzing phishing emails as a percentage of mail flow reveals a 36.6% increase in phishing emails between January 1st – March 31st, 2024, versus October 1st – December 31st, 2023.

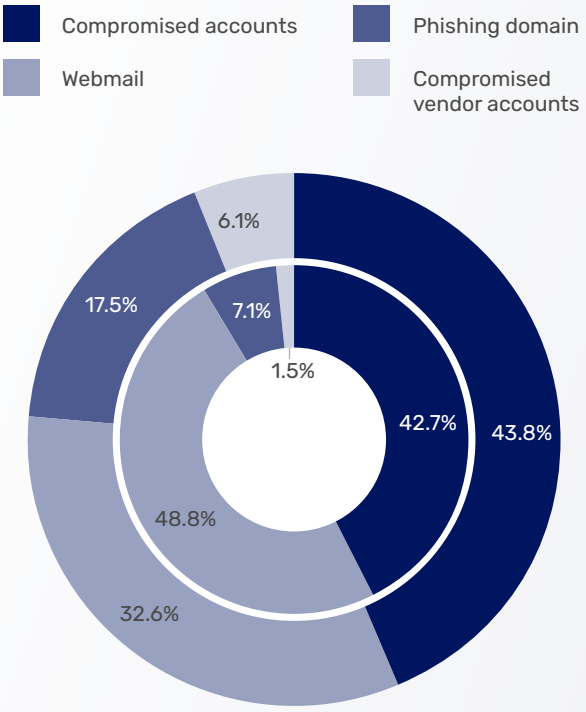
Q What's the risk of phishing attacks sent from compromised accounts?

A The risk is very high, with emails sent from all legitimate compromised accounts making up half (49.9%) of the attacks so far in 2024. 'General' compromised accounts that are unrelated to the target organization is the most popular sending mechanism, in 43.8% of attacks, with cybercriminals taking a 'hit and hope' approach.

More targeted vendor email compromise (VEC) attacks, which are sent from compromised accounts within the targets' supply chain, make up the smallest proportion of attacks at 6.1% (naturally, as they're reliant on the pre-established relationships within compromised accounts). However, the threat is growing. When our analysts examined the source of phishing emails sent between January 1st – March 31st, 2024, and October 1st – December 31st, 2023, they uncovered a 707.3% increase in phishing emails sent from compromised vendor accounts within the target organizations' supply chains. These attacks are generally more successful, as not only do they usually get through reputation-based detection used by Microsoft 365 and secure email gateways (SEGs), but the victim is more trusting of an email sent from a person or organization they work with.

BREAKDOWN OF PHISHING EMAILS BY **SENDER DOMAIN**

Inside ring: October 1st – December 31st, 2023
Outside ring: January 1st – March 31st, 2024



Q Are more phishing attacks getting through SEGs and Microsoft's native detection?

A Yes. In the first three months of 2024, there was a 52.2% increase in the number of attacks that got through SEG detection and a 50.9% increase in attacks bypassing Microsoft's native defenses.

BETWEEN JAN 1ST - MARCH 31ST, 2024

+52.2%

INC PHISHING EMAILS GETTING THROUGH SECURE EMAIL GATEWAYS

+50.9%

INC PHISHING EMAILS GETTING THROUGH MICROSOFT'S NATIVE DEFENSES

VS. OCT 1ST - DEC 31ST, 2023

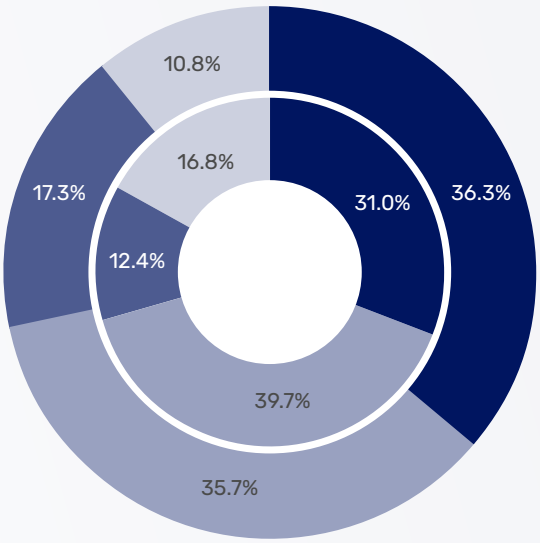
Q What's the most common payload?

A Attachment-based payloads (such as malware and ransomware) have been the most popular so far this year, followed by phishing hyperlinks. The risk of 'payloadless' attacks that exclusively leverage social engineering has grown, increasing by 166.7% compared with the previous three months.

BREAKDOWN OF **PHISHING PAYLOADS BY TYPE**

Inside ring: October 1st – December 31st, 2023
Ouside ring: January 1st – March 31st, 2024

- Attachments
- Phishing hyperlinks
- 'Payloadless' (social engineering)
- QR codes



WHAT'S IN STORE FOR 2024?

As different tactics rise and fall in popularity, we share our predictions for phishing threat trends in 2024 and beyond

The one thing that won't change in 2024 is cybercriminals investing heavily in attacks that give them the highest rewards. Some tactics will stay the same, but where returns diminish or disappear entirely, new tactics will emerge or – similar to QR codes – existing techniques will experience a renaissance.

Looking at the trends explored in this report, we can say with certainty that AI-powered attacks are here to stay and, likely by the end of the year, almost every phishing campaign will utilize AI in some way. In particular, our Threat Intelligence team predicts we'll see an increase in the use of deepfakes in multi-channel attacks leading to lucrative paydays for cybercriminals.

While quishing continues to have many organizations on the backfoot, these attacks will remain prevalent. It's our expectation that they'll decrease in 2025 and beyond as organizations implement more effective defenses over time.

Key to enhancing defenses is developing an integrated cyber ecosystem, with centralized threat intelligence and security that's automated across every platform in response to real-time changes to risk. Implementing technologies that use AI for threat detection will also enable organizations to respond to a broader array of cyberattacks, although careful evaluation must be given to ensure the AI is both secure and effective. Delivering highly relevant and timely SAT will also be a key differentiator in driving down human risk related to phishing attacks.

The Egress team is always keen to continue discussions about enhancing your security defenses, particularly protecting your organizations from advanced phishing attacks.

Get in touch today to find out more.

ABOUT EGRESS DEFEND

An integrated cloud email security solution, Defend delivers AI-powered behavioral-based detection to eliminate the attacks that get through Microsoft 365's 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.

Request demo

About Egress

Egress is the only cloud email security platform to continuously assess human risk and dynamically adapt policy controls, preparing customers to defend against advanced phishing attacks and outbound data breaches before they happen. Trusted by the world's biggest brands, Egress is private equity backed with offices in London, New York, and Boston.

About Northdoor

Northdoor helps organisations harness the full power of their data throughout its lifecycle. Northdoor helps clients manage all aspects of data—keeping it organised, governed, protected, compliant, accessible by both people and applications, and always ready for high-speed analysis. Northdoor provide solutions across consultancy, applications, security, hybrid infrastructure, analytics, AI, and managed services. Northdoor partners with the biggest and best vendors in global IT, and maintains deep technical skills to help clients overcome any challenges.

www.egress.com