KnowBe4

March 2025 | Vol.5

Phishing Threat Trends Report

The ransomware resurgence, AI-powered polymorphic phishing campaigns, and the hackers applying for the jobs at your organization.

In With The Old And In With The New...

Our Phishing Threat Trends Reports bring you the latest insights into the phishing landscape. Whether that's emerging attacks or techniques that are starting to gain traction, or new intel on established threats.

In this edition, we look at how the "old" threat of ransomware continues to grow and walk through the "new" sophisticated tactics that cybercriminals layered into an attack detected by KnowBe4 Defend. These tactics enabled it to bypass native security and a secure email gateway (SEG), and would make it virtually impossible to stop if it had launched.

Elsewhere, we continue to highlight how cybercriminals are using AI to architect polymorphic phishing campaigns; how they're injecting themselves into the hiring process to gain access to systems and data; and the attacks making it through native security and SEGs.

Unless otherwise stated, all information in this report has been generated by KnowBe4 Defend, an integrated cloud email security product. Our team would welcome the opportunity to speak with you about any of the insights in this report and how KnowBe4 can strengthen your defenses.

Jack Chapman

Jack Chapman
SVP of Threat Intelligence, KnowBe4

What's Inside

Six-Month Phishing Snapshot

17.3% increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9% were sent from compromised accounts

11.4% within the supply chain

25.9% contained attachments

20% relied solely on social engineering

54.9% contained a phishing hyperlink payload

The most phished day

16 December 2024

82.6% of phishing emails utilized AI

53.5% YoY increase!

81.9% of victims had their email addresses leaked in previous data breaches

On average, phishing emails contained

1058 characters (~188 words)

The top three words used in phishing emails:

1. Urgent
2. Review
3. Sign

New starters typically received a phishing email after 3 weeks

The top cryptocurrencies demanded during extortion are:

bitcoin MONERO XRP

5 Exclusive Insights In This Edition

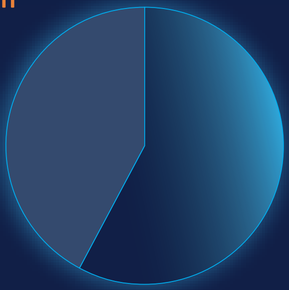
In 2024

47%

increase in **phishing emails** evading detection by **Microsoft's** native security and secure email gateways

57.9%

of business email compromise



22.6%

increase in **ransomware** delivered by phishing email since Sep 15, 2024

Cybercriminals are most likely to apply to work in **Engineering jobs**

92%

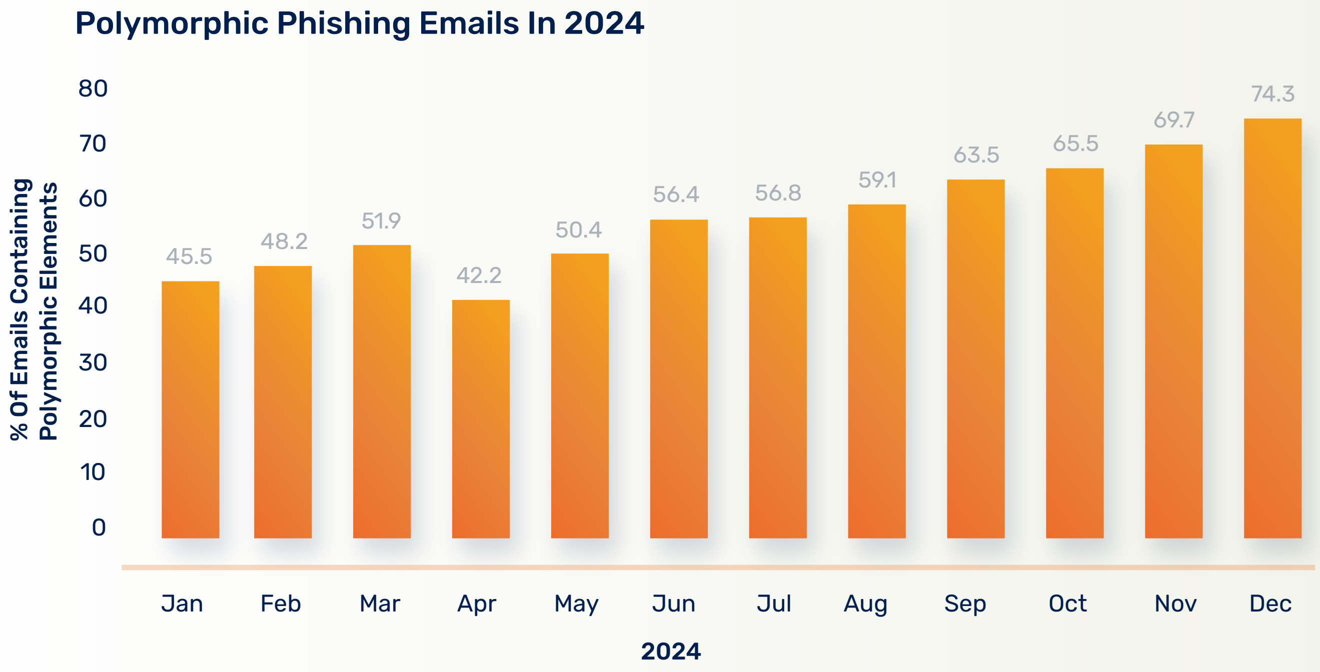
of **polymorphic attacks** utilize **AI** to achieve unprecedented scale

Keeping Up With The Changes

AI-Powered Polymorphic Phishing Is Changing The Threat Landscape For Good.

Our Threat Research team has observed polymorphic phishing campaigns being sent at a much larger scale than ever before. In 2024, at least one polymorphic feature was present in 76.4% of all phishing attacks and in 57.49% of commodity attacks (white noise phishing).

Polymorphic phishing campaigns consist of a series of almost identical emails which only differ by a small detail. These slightly altered attacks can be difficult to detect by systems that look out for 'known bad' (blocklisting of known fraudulent addresses and payloads), such as Microsoft's native security and secure email gateways (SEGs). Similarly, they can also be hard to remediate from inboxes across an organization using traditional email security technologies.



AI Threw Fuel On The Fire of Polymorphic Phishing In 2024

AI enables cybercriminals to create more personalized, more targeted, and more evasive phishing campaigns at scale, as our analysis of polymorphic campaigns shows. In 2024, 73.8% of all phishing emails we analyzed exhibited some use of AI; that increased to 90.9% when we inspected emails that also showed polymorphic elements.

Small Details That Make A Big Difference To Detection

Previously, 'grouping' phishing emails together has increased detection efficacy, as identifying commonalities — such as payloads or sending domains — makes it possible to block repeat attacks.

So, cybercriminals have adjusted to change just enough elements to 'revive' a previously successful phishing email.

They tweak the name of a known malicious attachment, amend the display name of the email sender, or tinker with email signatures, email addresses, or image metadata. The three most common alterations are replacing organization logos, the destination of a link, or the sender email address domain.

Another common tactic is to change the subject line, often by adding additional characters and symbols, and changing the lengths and patterns of the text. This makes it difficult for native security and SEGs to block phishing emails based on subject lines.

In the table below, for example, cybercriminals have used the names of three brands: United Health, Marriott, and Delta. If we take the two that reference United Health, to detect these as phishing emails based on the subject line, the hash mapping (the lookup for known bad signatures) would have to be significantly narrowed, ultimately detecting based on the brand name. This would result in any legitimate emails mentioning United Health in the subject line also being quarantined, potentially impacting business efficiency.

Examples Of Polymorphic Email Subject Lines Detected By KnowBe4 Defend

-***United Health Care #0xbar#ag6qc

United Health Care #az0vw#k8dpj

Marriott Luxury Pillows 2-piece set Department--- #n9508#vkjf7

Re: Last Chance: Unlock Ultimate Selection Box #ID:mzg

FW: --Rapid Response Needed for Limited Offer!-- ------- #5z0l6#now4i#xy6d2

FW: Solar Panel Funding #3xmo9#t4lze

Delta Airlines--#h2yii#gcpb

Putting the randomized characters towards the end of the subject lines is likely an attempt to hide them behind email preview cutoffs, so once the attack reaches the inbox, the recipient is less likely to see the "spammy" subject line in full.

As symbols are increasingly used in the subject lines of legitimate communications, this helps to disguise attacks that also use symbols within the inbox. They have the added benefit of being easy to change within a polymorphic campaign, without altering the wider theme of an attack. The five most common symbols we observed in polymorphic attacks are:

🛡️ | ⚠️ | Ô | ⛔ | 🔥

Additionally, to help them bypass domain authentication checks, most polymorphic phishing emails are sent from compromised accounts (52%), followed by phishing domains (25%), and webmail (20%).

Even AI-based approaches to detection, such as Natural Language Processing (NLP) and Natural Language Understanding (NLU), can suffer from polymorphic randomization. Attackers have become creative, with 36.9% of polymorphic attacks using invisible characters to "break" these systems.

AI-Powered Polymorphic Phishing Will Make Grouping Phishing Emails Obsolete

As we see a shift towards AI-powered polymorphic behavior in phishing emails, our Threat Research team believes the traditional approach of grouping individual attacks into campaigns to improve detection efficacy will become impossible by 2027.

As a result, organizations must find appropriate technical counter measures — such as products that can detect polymorphic campaigns, don't over-rely on blocklists, and can identify the most sophisticated attacks (e.g. those sent from compromised accounts) — in addition to employee training to protect their business.

Ransomware On The Rise (Again)

We’re On The Edge Of a Perfect Storm: Another Surge In Ransomware Attacks—But This Time, With Even More Sophisticated Tactics.

There have been several key moments within the rise of ransomware. At the start of this decade, for instance, there was a sharp increase in successful attacks, particularly against large organizations, and the size of the ransoms being paid.

Now, with a rise in both ransomware-as-a-service and GenAI lowering the barrier to entry to cybercrime, we’re standing on the edge of another key moment. One that will see an increase in the volume and sophistication of ransomware attacks.

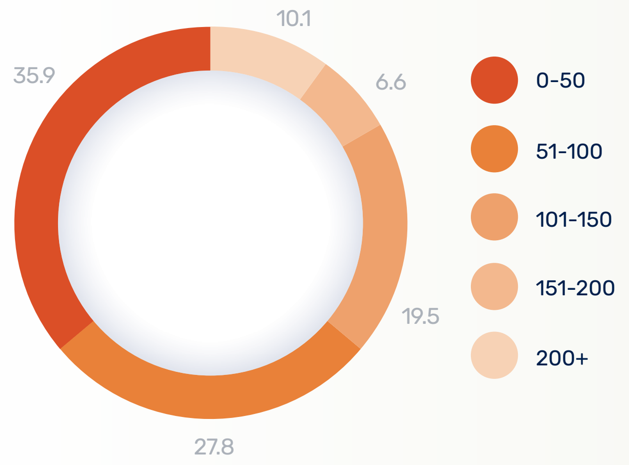
More Ransomware Is Being Delivered as Obfuscated Payloads In Phishing Emails

From September 15, 2024, until February 15, 2025, we observed a 22.6% increase in ransomware payloads in phishing attacks versus the previous six months. This trend is accelerating: between November 1, 2024, and February 15, 2025, there was a 57.5% increase compared to the previous three months.

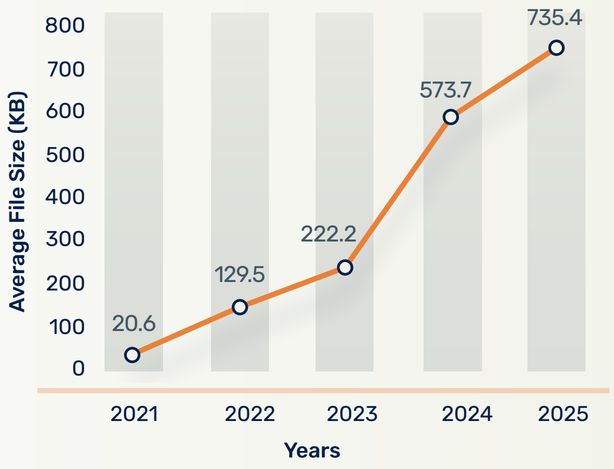
In this second time frame (November 2024 - February 2025), we also saw a 85.6% increase in HTML smuggling; currently the most popular obfuscation technique used to mask malicious payloads from file scanning AV technologies. Additionally, file sizes for both malware attachments (including ransomware) and malicious HTMLs have also increased year on year, as cybercriminals attempt to improve deliverability by maxing out email latency service-level agreements (SLAs) before an attack is detected.

Cybercriminal Can Use Large Attachments To Trigger Latency SLAs And Improve Phishing Email Deliverability

Average File Size Of Malware Attachments, Including Ransomware, Without Obfuscation (KB)



Average HTML File Size In Phishing Emails



Ask The Expert

Jack Chapman,
SVP Threat Intelligence

Will A Decline In Ransoms Being Paid Stop Ransomware Attacks?

▶ No. While a decline in ransoms being paid has been reported, it isn't enough to end ransomware. There are two main factors in play here. The cost of attacks has decreased, thanks to burgeoning crime-as-a-service marketplaces and the explosion of AI — so while cybercriminals may be being paid less frequently, they need fewer resources to launch attacks. Plus, there are currently organizations and individuals still paying ransoms, typically out of the sight of the media and governments.

Ransom Notes: Deconstructing An Advanced Ransomware Payload

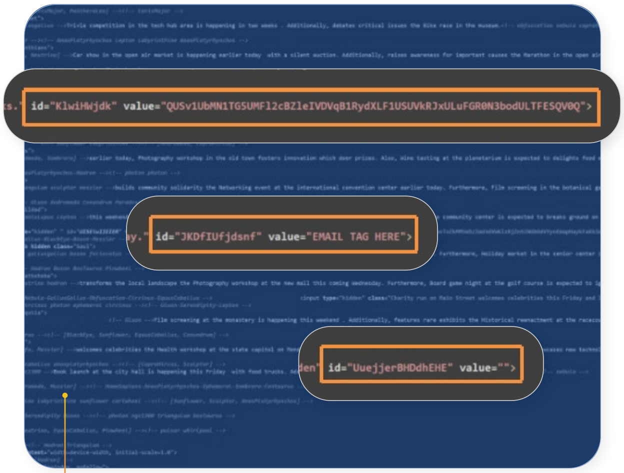
For this report, we analyzed a sophisticated INC Ransom payload attached to a phishing email detected by KnowBe4 Defend. The attack displayed numerous advanced techniques that were designed to improve its deliverability and make it harder to stop once deployed.

Advanced Techniques To Obfuscate The Payload

Multiple layers of obfuscation were applied to the JavaScript payload, including a password-protected .zip file and HTML smuggling. These techniques meant it went undetected by the signature-based detection used in the target organization's native Microsoft 365 security and its secure email gateway (SEG).

Initially, file scanning was unable to inspect the password-protected .zip file — and even if it had been able to see into it, it would have most likely classified it as a harmless HTML file. That's because, when analyzing the JavaScript, our Threat Research team noted the use of two further techniques that masked the malicious elements:

- **AI-generated obfuscation:** Randomly generated text was added to the payload to increase the time required to scan the file and potentially confuse security scanners — and analysts! Importantly, even slight changes to this filler text can change the script's hash (digital fingerprint), rendering signature-based detection ineffective for future iterations of this payload.
- **Obfuscated malicious URL:** The ransomware for this attack is automatically downloaded from a malicious website that opens when the HTML script is activated. The cybercriminal has manipulated the URL string using script reverse (backwards text) and Base64 encoding (which converts text into different characters). They then split the URL into several parts of inconsistent length and "scattered" these fragments within the HTML script. This effectively hides the URL from detection if it is present on blocklists. When activated, the script reverts all these obfuscation techniques to rebuild the original URL.



```
s." id="KlwiHWjdk" value="QUSv1UbMN1TG5UMFl2cBZleIVDVqB1RydXLF1USUVkRJxULuFGR0N3bodULTFESQV0Q">
y." id="JKDfIUfjdsnf" value="EMAIL TAG HERE">
den" id="UuejjerBHDdhEHE" value="">
```

The JavaScript payload was filled with benign AI-generated text, with a highly obfuscated malicious URL dispersed within it.

Once these obfuscation techniques are stripped from the file, the core script only comprises three lines of code that rebuilds the URL, opens a web browser, and automatically downloads an executable file containing the ransomware.

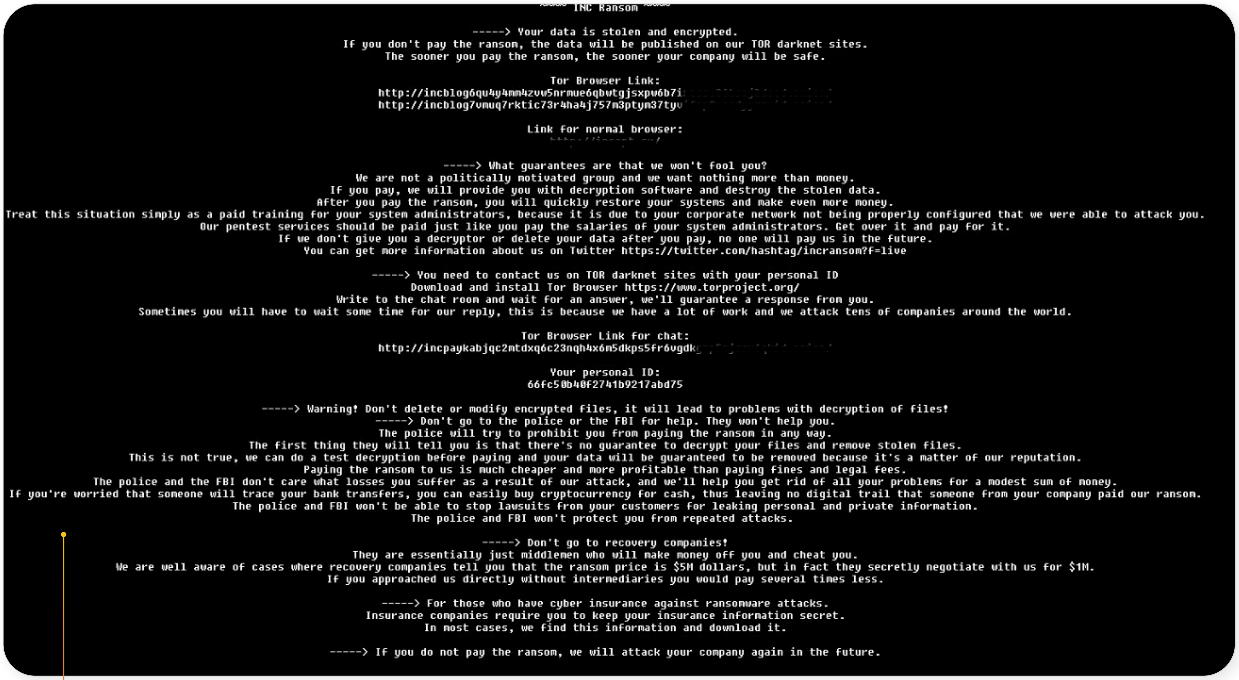
Executing a Virtually Unstoppable Ransomware Attack

Once the ransomware is downloaded, the attack requires its victim to execute the file. This is achieved through a prompt that's deceptively displayed as a false system alert or security software pop-up, so the victim is unaware of what they're actually doing.

If deployed, the malware will use several further measures to prevent the victim from stopping it:

- **Blocking right click and DevTools:** The script disables context menus and prevents F12, Ctrl+U, and Ctrl+Shift+I from working so, short of quickly holding down the power button before the file is fully executed, a user can't stop it from being deployed.
- **Debugger detection:** The script runs a looping debugger to measure delays. If a delay is detected, the script will stall the program to make it difficult to step through the code to stop the deployment.

As can be predicted, the ransomware then encrypts a victim's files, making them inaccessible. This specific script also changes the victim's desktop background (wallpaper) with text detailing the ransomware demand, payment instructions, link to dark web chatroom for negotiations, and threats for inaction.



```
INC Ransom

-----> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites.
The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Link:
http://incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7i[redacted]
http://incblog7vmuq7rktic73r4ha4j757m3ptym37tyv[redacted]

Link for normal browser:
[redacted]

-----> What guarantees are that we won't fool you?
We are not a politically motivated group and we want nothing more than money.
If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly restore your systems and make even more money.
Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.
Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.
If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future.
You can get more information about us on Twitter https://twitter.com/hashtag/incransom?f=live

-----> You need to contact us on TOR darknet sites with your personal ID
Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you.
Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tens of companies around the world.

Tor Browser Link for chat:
http://incpaykabjqc2mtdxq6c23nqh4x6m5dkps5fr6vgdk[redacted]

Your personal ID:
66fc50b40f2741b9217abd75

-----> Warning! Don't delete or modify encrypted files, it will lead to problems with decryption of files!
-----> Don't go to the police or the FBI for help. They won't help you.
The police will try to prohibit you from paying the ransom in any way.
The first thing they will tell you is that there's no guarantee to decrypt your files and remove stolen files.
This is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it's a matter of our reputation.
Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.
The police and the FBI don't care what losses you suffer as a result of our attack, and we'll help you get rid of all your problems for a modest sum of money.
If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom.
The police and FBI won't be able to stop lawsuits from your customers for leaking personal and private information.
The police and FBI won't protect you from repeated attacks.

-----> Don't go to recovery companies!
They are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is $5M dollars, but in fact they secretly negotiate with us for $1M.
If you approached us directly without intermediaries you would pay several times less.

-----> For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret.
In most cases, we find this information and download it.

-----> If you do not pay the ransom, we will attack your company again in the future.
```

The ransomware changes a victim's desktop background to include details of the attack and payment instructions.

At this point, the story is the same as almost every other ransomware attack. A target organization would either need to restore their most recent system back up and sacrifice anything new created in the interim; pay the ransom; or decrypt their files (which is highly improbable). This scenario doesn't touch on whether files are exfiltrated and then held for further ransom or dumped online.

Against a minimum of operational inefficiency to a maximum of financial losses, bad publicity, and customer churn, nothing beats stopping ransomware at delivery. As the methods used to obfuscate ransomware payloads continue to increase in sophistication and proliferation, organizations must turn to advanced detection to catch the attacks that slip through traditional products.

You’re Hired!

Engineering Roles Are A Honeypot For Cybercriminals Looking To Exploit Weaknesses Within The Hiring Process.

In 2024, KnowBe4 experienced first-hand an attack within our hiring and onboarding process. Our new employee “Kyle” attempted to install malware the minute he switched on his new laptop. We isolated his account, and he never succeeded with the installation, let alone gained access to any data.

“Kyle” had applied with a fake CV, an AI manipulated headshot, and a stolen social security number. He was not a real person but part of North Korea’s fake employee scheme which places insiders in organizations for financial gain and espionage.

Elsewhere, cybercriminals exploit job application and hiring processes to install malware on corporate machines by engaging interested parties in an application process that requires downloading documents with malicious links or software.

Engineering Roles Are The Most Targeted

We took a closer look at 512 job application-related phishing emails and registered a high number of attacks targeting engineering (64%) roles, followed by finance (12%), HR (10%), IT (10%), product (2%), and others (2%).

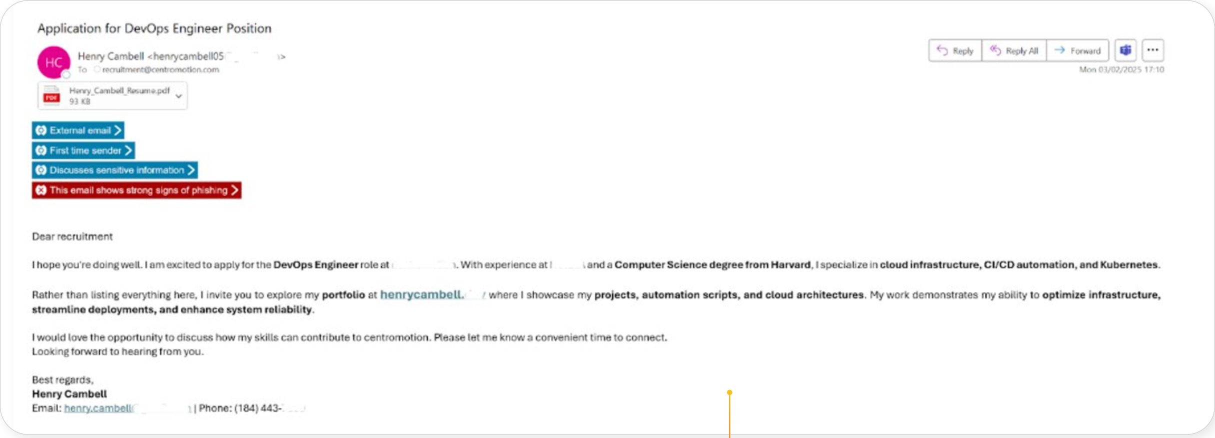
Software engineering roles are frequently targeted by cybercriminals due to their job mobility and privileged access — you may never meet someone face-to-face who has a high level of access to systems and data!

Additionally, coding challenges within the hiring process provide a unique avenue for attack.

Cybercriminals exploit this by disguising malware as coding challenges, hoping engineers will download and execute them on their current employer’s systems, leading to network infiltration or ransomware attacks. However, gaining access by tricking a software engineer into installing a malicious coding challenge requires background research and preparation time; a commitment cybercriminals don’t always want to make.

> Software engineering roles are frequently targeted by cybercriminals due to their job mobility and privileged access.

Example Of A Phishing Email And The CV Attached To It



Application for DevOps Engineer Position

HC Henry Cambell <henrycambell05[redacted]>
To recruitment@centromotion.com

Henry_Cambell_Resume.pdf
93 KB

External email >
First time sender >
Discusses sensitive information >
This email shows strong signs of phishing >

Dear recruitment

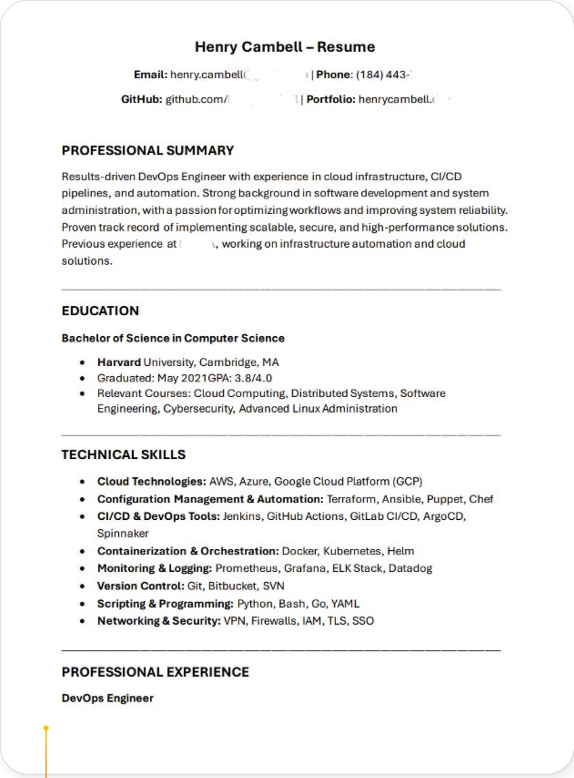
I hope you're doing well. I am excited to apply for the **DevOps Engineer** role at [redacted]. With experience at [redacted] and a **Computer Science degree from Harvard**, I specialize in **cloud infrastructure, CI/CD automation, and Kubernetes**.

Rather than listing everything here, I invite you to explore my **portfolio** at henrycambell.[redacted]/ where I showcase my **projects, automation scripts, and cloud architectures**. My work demonstrates my ability to **optimize infrastructure, streamline deployments, and enhance system reliability**.

I would love the opportunity to discuss how my skills can contribute to centromotion. Please let me know a convenient time to connect.
Looking forward to hearing from you.

Best regards,
Henry Cambell
Email: henry.cambell[redacted] | Phone: (184) 443-[redacted]

Phishing email with Defend anti-phishing banners applied.



Henry Cambell – Resume

Email: henry.cambell[redacted] | **Phone:** (184) 443-[redacted]
GitHub: github.com/[redacted] | **Portfolio:** henrycambell.[redacted]

PROFESSIONAL SUMMARY

Results-driven DevOps Engineer with experience in cloud infrastructure, CI/CD pipelines, and automation. Strong background in software development and system administration, with a passion for optimizing workflows and improving system reliability. Proven track record of implementing scalable, secure, and high-performance solutions. Previous experience at [redacted], working on infrastructure automation and cloud solutions.

EDUCATION

Bachelor of Science in Computer Science

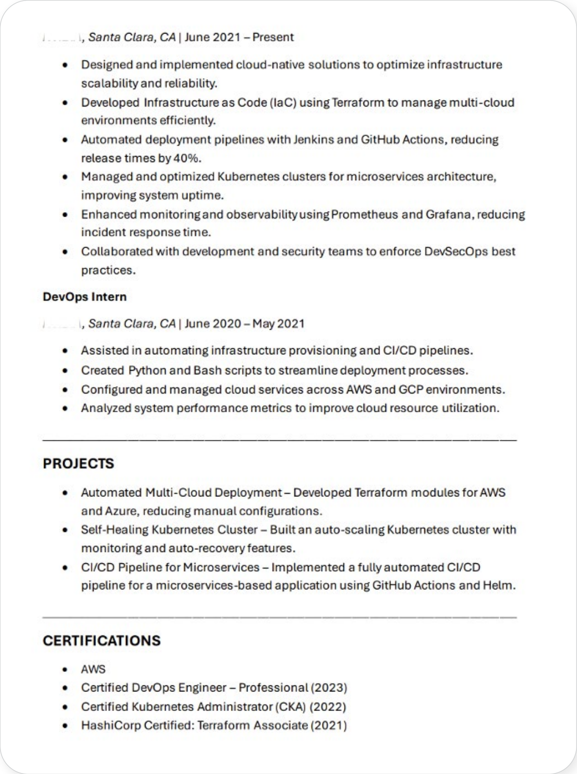
- **Harvard** University, Cambridge, MA
- Graduated: May 2021GPA: 3.8/4.0
- Relevant Courses: Cloud Computing, Distributed Systems, Software Engineering, Cybersecurity, Advanced Linux Administration

TECHNICAL SKILLS

- **Cloud Technologies:** AWS, Azure, Google Cloud Platform (GCP)
- **Configuration Management & Automation:** Terraform, Ansible, Puppet, Chef
- **CI/CD & DevOps Tools:** Jenkins, GitHub Actions, GitLab CI/CD, ArgoCD, Spinnaker
- **Containerization & Orchestration:** Docker, Kubernetes, Helm
- **Monitoring & Logging:** Prometheus, Grafana, ELK Stack, Datadog
- **Version Control:** Git, Bitbucket, SVN
- **Scripting & Programming:** Python, Bash, Go, YAML
- **Networking & Security:** VPN, Firewalls, IAM, TLS, SSO

PROFESSIONAL EXPERIENCE

DevOps Engineer



[redacted], *Santa Clara, CA* | June 2021 – Present

- Designed and implemented cloud-native solutions to optimize infrastructure scalability and reliability.
- Developed Infrastructure as Code (IaC) using Terraform to manage multi-cloud environments efficiently.
- Automated deployment pipelines with Jenkins and GitHub Actions, reducing release times by 40%.
- Managed and optimized Kubernetes clusters for microservices architecture, improving system uptime.
- Enhanced monitoring and observability using Prometheus and Grafana, reducing incident response time.
- Collaborated with development and security teams to enforce DevSecOps best practices.

DevOps Intern

[redacted], *Santa Clara, CA* | June 2020 – May 2021

- Assisted in automating infrastructure provisioning and CI/CD pipelines.
- Created Python and Bash scripts to streamline deployment processes.
- Configured and managed cloud services across AWS and GCP environments.
- Analyzed system performance metrics to improve cloud resource utilization.

PROJECTS

- Automated Multi-Cloud Deployment – Developed Terraform modules for AWS and Azure, reducing manual configurations.
- Self-Healing Kubernetes Cluster – Built an auto-scaling Kubernetes cluster with monitoring and auto-recovery features.
- CI/CD Pipeline for Microservices – Implemented a fully automated CI/CD pipeline for a microservices-based application using GitHub Actions and Helm.

CERTIFICATIONS

- AWS
- Certified DevOps Engineer – Professional (2023)
- Certified Kubernetes Administrator (CKA) (2022)
- HashiCorp Certified: Terraform Associate (2021)

CV attached to the phishing email.

Targeting Shared Inboxes For More Susceptible Victims

To increase the victim pool, job application-related attacks are not only sent to individual accounts (24%) but also shared mailboxes (52%) and individual inboxes with activated delegate functions (21%) (e.g. a personal assistant has access to an executive's inbox). An email sent to a shared account might be picked up by the person who is most intrigued and interested in it, allowing cybercriminals to target more susceptible social engineering victims.

Engineering roles are the most targeted through user accounts and shared inboxes, as criminals use phishing and spear phishing attacks alike. IT roles, on the other hand, are most targeted through individual user accounts, suggesting criminals favor spear phishing over general phishing tactics. This makes sense: IT workers often also have privileged access to systems and data, and criminals are willing to invest their time.

Interestingly, we find that Finance and HR roles are mainly targeted through shared inboxes, suggesting that criminals have not yet taken towards spear phishing employees from these departments in job application scams.

Given that finance and HR professionals are frequently targeted in other social engineering scams (and fall victim to them, as publicized in the media), the lack of spear phishing tactics should not invoke a false sense of security. It's, rather, a question of time before cybercriminals target finance and HR workers with fake job offers as well.

Types of Jobs They're Applying For	**Accounts That Are Receiving These Emails**			
	User Accounts	Shared Mailboxes	Linked Users	Other
Engineering	140 (27.3%)	171 (33.4%)	16 (3.1%)	3 (0.6%)
Finance	5 (1.0%)	56 (10.9%)	0	0
HR	1 (0.2%)	30 (5.9%)	20 (3.9%)	0
IT	32 (6.3%)	10 (2.0%)	6 (1.2%)	1 (0.2%)
Product	8 (1.6%)	0	0	0
Other	12 (2.4%)	0	0	0

We categorized 512 emails according to the job role they targeted and the type of account they were sent to.

To increase the victim pool,
52% of job application-related attacks
are sent to shared mailboxes.

Attachments Are Crafted To Fit Different Attack Goals

Cybercriminals either use attachments to deliver their payload or direct their victims to phishing websites. We observed 47% PDFs, 11% ZIP, 11% DOCX and DOCM, 14% ODT, and 5% SVG attachments.

Attachment types frequently change with changing technical requirements and countermeasures. Naturally, most emails include PDF, DOCX, ODT, or DOCM attachments, such as CVs or application letters. Malicious code can be deployed as JavaScript in PDFs but also as macro in DOCM files. Text-based document types (DOCX and ODT) likely include links to malicious software, and SVGs are used as links themselves. It's likely that ZIP archives might hold malicious payloads or even a coding challenge.

Whether the target is a specific software engineer or the threat actor prefers to send a phishing email to a shared inbox, cybercriminals can customize the content and payload of the emails.

Cybercriminals Leverage AI

Deepfakes are frequently used to create fake profile pictures, just like "Kyle" did. We also find that AI is used to create pictures for fake LinkedIn accounts and generate fake information for online platforms such as GitHub, personal blogs, portfolio websites, and even to fake professional certificates.

As deepfake video technology for online meetings is rapidly advancing, organizations and individuals will soon be faced with the challenge of fake attendants in online meetings. In May 2024, British engineering firm Arup hit the headlines with a story of an online meeting in which senior finance officials were impersonated by pre-recorded deepfake videos. This social engineering attack cost the organization about GBP 20M. The invitation to the online meeting and as well as payment instructions after the meeting were, of course, received by email.

Protecting The Hiring Process From External Attacks

Criminals know how to leverage the intricacies of job application processes in phishing and spear phishing campaigns. Whether individuals are targeted or emails are sent to shared inboxes, attackers exploit business processes and the people who bring these processes to life to further their needs.

While there is a lot of attention on fake employees and fake job offerings in the IT and engineering sectors, we should not forget about influential roles in HR and finance departments. Detecting these attacks at their entry point — which, so often, is phishing — is crucial to stopping external threat actors literally becoming privileged insiders, who might be much harder to detect and root out.

> Whether the target is a specific software engineer or a shared inbox, cybercriminals can customize the content and payload of their phishing emails.

What's Getting Through Your Traditional Email Security Defenses?

Find Out How Cybercriminals Are Engineering Their Attacks To Get Through Microsoft And Secure Email Gateways.

It's simply the cost of doing business for cybercriminals to get through traditional signature-based and reputation-based phishing detection. Naturally, we therefore see attackers consistently doubling down on the tactics that get their emails one step closer to their targets.

In fact, in 2024, our Threat Researchers observed a 47.3% increase in attacks evading detection by Microsoft and secure email gateways (SEGs).

Analyzing The Attacks That Bypass Signature-Based and Reputation-Based Detection

When the team compared phishing emails sent between September 15, 2024, and February 15, 2025, with the previous six months, three payload types had experienced significant increases in bypassing Microsoft and SEG detection:

36.8%+
phishing hyperlinks

20.0%+
malware

14.2%+
social engineering only

As cybercriminals can quickly set up new phishing websites (particularly if they purchase phishing kits from crime-as-a-service (CaaS) marketplaces) it's relatively easy for them to replace blocklisted hyperlinks.

Additionally, URL redirects can obfuscate hyperlink payloads and, on average, redirected hyperlinks would contain three "hops" between sites. Another technique to mask phishing links is hijacking legitimate domains. The top domains we observed being used were:

- google.com
- sharepoint.com
- dropbox.com
- youtube.com
- docusign.com
- tiktok.com
- kahoot.com

In particular, there was a 201.5% increase in Google Slide links and a 154.5% increase in Kahoot links.

While malware payloads and emails that solely rely on social engineering previously required more resources and expertise to create, again CaaS and GenAI has lowered the barrier for entry and likely contributed to the increase in these attacks evading traditional detection mechanisms.

Sending from trusted domains is another proven tactic for getting through reputation-based detection and, in the timeframe, we observed:

49.9%+
emails sent from compromised accounts

67.4%+
in third-party platforms

11.1%+
sent from compromised email addresses within the supply chain

3,829
days average domain age for attacks getting through

The most common third-party platforms used were:

- sendgrid.com
- salesforce.com
- amazonaws.com
- sendlayer.com
- mailgun.com
- marketo.com

Finally, there was 22.7% increase in the use of technical measures to obfuscate attacks and payloads. In particular, as vendors layer newer detection mechanisms such as large language models (LLMs (natural language processing (NLP) and natural language understanding (NLU)) into their detection capabilities, we saw an increase in the following tactics known to bypass these:

Image-based emails
The body of the email is an image, with no text written into the email to scan.

Invisible characters
Addition of special characters or disguising characters through font color. While invisible to the human eye these characters are still read by detection software and are used to separate words or phrases or manipulate hyperlinks.

Homoglyph UNIcode characters
A form of spoofing that uses UNIcode to mimic Latin characters.

Left-to-right override
Spoofing technique used to disguise attachment types or trick NLP detection within body copy.

As our research shows, it's never been more crucial for organizations to determine what phishing emails make it through their existing defenses and layer an advanced anti-phishing product into their tech stack to protect their people, customers, and data from these attacks.

Ask The Expert

Jack Chapman,
SVP Threat Intelligence

How Does KnowBe4 Defend Detect The Attacks That Get Through Microsoft And SEGs?

▶ Signature-based and reputation-based detection provides a solid email security foundation — but, on its own, it's no longer enough to hold back the tide of phishing attacks targeting organizations. Success in phishing equals a payday for cybercriminals — and these email security platforms are the first hurdle for cybercriminals to jump.

That's why our customers layer KnowBe4 Defend into their environments. We architected our product to use AI-powered detection from the start (rather than bolting it on at a later date) and take a zero-trust approach to detection. All aspects of every email — including technical elements and the message itself — are analyzed separately and together using advanced techniques to determine whether or not an email can be trusted.

By The Numbers: How You're Being Phished in 2025

Your Questions Answered With A Round-Up of Phishing Statistics.

Q **Is phishing becoming more prevalent?**

A Yes. We've observed a 17.3% increase in phishing emails between September 15, 2024, and February 14, 2025, versus the previous six months.

17.3%

increase in phishing emails

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

A There's been a 57.9% increase in attacks being sent from compromised accounts between September 15, 2024, and February 14, 2025, versus the previous six months. 11.4% of these were sent from trusted accounts within an organization's supply chain.

57.9%

increase in attacks being sent from compromised accounts

11.4%

sent within the supply chain

Q **Do cybercriminals use legitimate platforms to send phishing emails?**

A Yes. The top five we've observed being used currently are: Docusign, Paypal, Microsoft, Google Drive, and Salesforce.

PayPal

docusign

salesforce

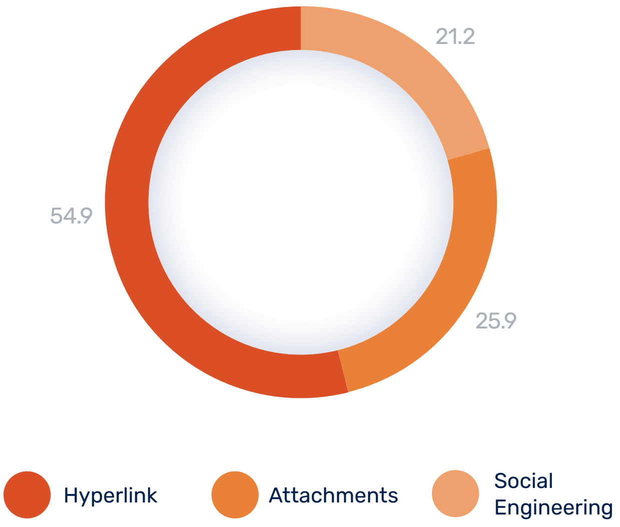
Microsoft

Google Drive

Q What’s the most common type of payload?

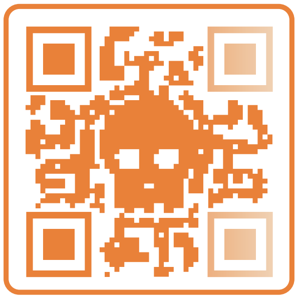
A Links to phishing websites, with an average of 3.9 hyperlinks per email.

3.9 hyperlinks per email



Q How are QR code payloads being delivered?

A When inserted into the email body, the vast majority (67.6%) are images, with one-third (32.4%) built using unicode characters. We’re also observing an increase of malicious QR codes delivered within obfuscated file attachments, however this can increase a target’s suspicion and decrease the likelihood of interaction.



Q What are the most impersonated brands?

A Currently it’s Microsoft, Docusign, Adobe, Paypal, and LinkedIn.

Microsoft

docusign

Adobe

LinkedIn

PayPal

It’s Time To Change Or Be Left Behind

We’re Firmly In A New Age Of Phishing Threats — One Of Unprecedented Scale And Advancements Powered By AI And Cybercriminal Collaboration.

Innovation in both phishing threats and anti-phishing defenses is moving at a sprinting pace. In the next 18 months, both the attack landscape and the defensive tech stack will have evolved more quickly than ever before.

In this edition of our Phishing Threat Trends Report — and in the insights we generate more widely — we’re seeing cybercriminals revive old attacks, such as ransomware and polymorphic campaigns, with new tactics. This helps them evade detection by traditional signature-based and reputation-based technologies and even some newer mechanisms, like natural language processing (NLP) and natural language understanding (NLU).

As we progress through 2025, these efforts will continue and entirely new attacks will be created. Our defenses will also change radically. Yes, we’ll continue to look at email security within the technical layer, but it’s now an established part of a broader conversation: human risk management (HRM).

It’s now possible to understand the ways in which individuals are targeted by phishing attacks. This is no longer a discussion solely about the efficacy of detection, but one also about the ways in which your organization can prepare its people to be your best defense through technical controls, in-the-moment coaching, and education and awareness.

This is the most effective way organizations can defend against not only a rising tide of sophisticated phishing threats, but also the many other ways that people create risk — each unique to the individual and whether they mean to or not!

It really is time to advance or be left exposed.

We look forward to going on this journey with you. Please use the button below if you’d like to find out how KnowBe4 Defend can protect your organization from advanced phishing attacks or to discuss our wider HRM+ platform.

Learn more about what KnowBe4 can do for your organization.

Get In Touch →

Our Contributors

Jack Chapman, SVP Threat Intelligence

- Jack is tasked with deeply understanding the cyber-threat landscape to help KnowBe4's customers remain one step ahead of cybercriminals. Leveraging these insights and his extensive R&D skillset, Jack oversees threat research and AI development for KnowBe4 Defend, an inbound threat detection and prevention solution that mitigates zero-day phishing attacks that defeat traditional security solutions. Jack maintains close ties with the global cyber community — particularly with the UK's intelligence and cyber agency GCHQ.

Dr. Martin J. Kraemer, Security Awareness Advocate

- Martin is a Security Awareness Advocate 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.

James Dyer, Threat Intelligence Lead

- James spearheads the Threat Intelligence team, spending his days uncovering the latest phishing threat trends, understanding emerging methodologies, and analyzing the TTPs of the crime-as-a-service ecosystem. Some of his primary research areas include the use of AI in cyberattacks, social engineering, OSINT, and understanding human risk in organizations.

Bex Bailey, Director of Research and Communications

- Bex heads up our research program, working with KnowBe4's thought leaders to develop and implement our global strategy. Bex brings our latest insights to life in this and other reports, ensuring our audience benefits from timely updates on the issues that matter most.

About KnowBe4 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.

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

KnowBe4

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