FORTRA

2025 Email Threat Intelligence Report

Executive Summary

This report describes how the email threat landscape evolved in 2024 and forecasts what defenders should expect in 2025. Fortra analyzed more than 1 million email threats in 2024, many of which bypassed traditional email security measures. The observations and predictions in this report are based on this data as well as the expertise of Fortra analysts and researchers. Readers will gain valuable insights into the threats plaguing emails, a deeper understanding of how adversaries exploit email to compromise targeted organizations, and the knowledge required to strengthen defenses against these continuously evolving attacks.

Critical Trends and Predictions

Trend 1: 99% of email threats reaching corporate user inboxes in 2024 were response-based social engineering attacks or contained phishing links, without delivering malware.

Prediction: Use of generative AI to craft convincing messages will be more prevalent, driving growth in social engineering attack volume and sophistication.

Trend 2: Scammers are exploiting leaked personal data, such as home addresses, to craft highly personalized attacks and extortion schemes.

Prediction: The 1+ billion records breached in 2024 will be used to further personalize attack campaigns with leaked information.

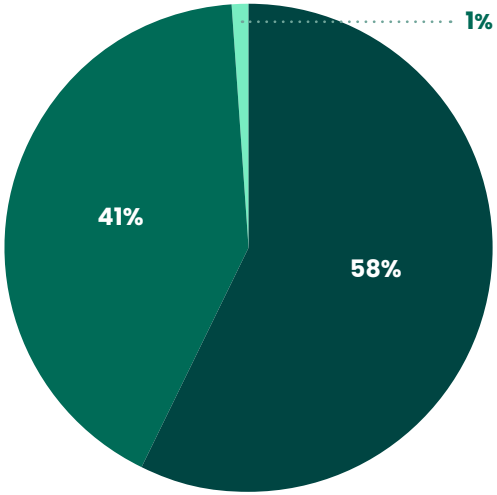
Trend 3: Legitimate services are being heavily abused to get malicious emails into user inboxes. Misuse of developer tools grew sharply, increasing more than 200% in 2024.

Prediction: Abuse of developer tools will grow as cybercriminals further integrate these tools into their illicit operations.

Trend 4: Multichannel attacks are luring victims out of secure email environments. Methods include malicious QR codes and hybrid vishing, which surged in Q4 2024 to account for 40% of response-based email threats.

Prediction: The rise of AI voice generation will lead to more convincing vishing scams that impersonate accents, dialects, and known individuals.

Top Inbox Threats Are Credential Theft Attacks and Social Engineering

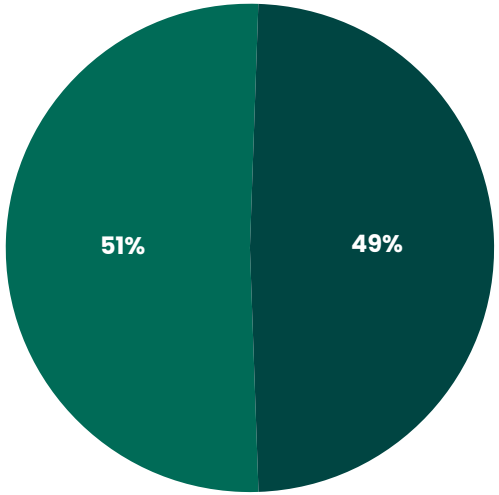


Threats that Reached Inboxes in Q4 2024

58% Credential Theft **41%** Social Engineering **1%** Malware

Nearly all threats observed reaching user inboxes are credential theft attacks and response-based social engineering. In Q4, this trend continued with 99% of attacks being in these categories. Only 1% of malicious emails delivered malware.

Anti-malware scanning, sandboxing, and other pre-delivery security processes are increasingly common and make it more difficult for emails containing malware payloads to reach user inboxes. However, these methods are ineffective for detecting social engineering and credential theft attacks, which lack payloads.



Credentials Targeted in Q4 2024

49% Microsoft 365 **51%** Other Credentials

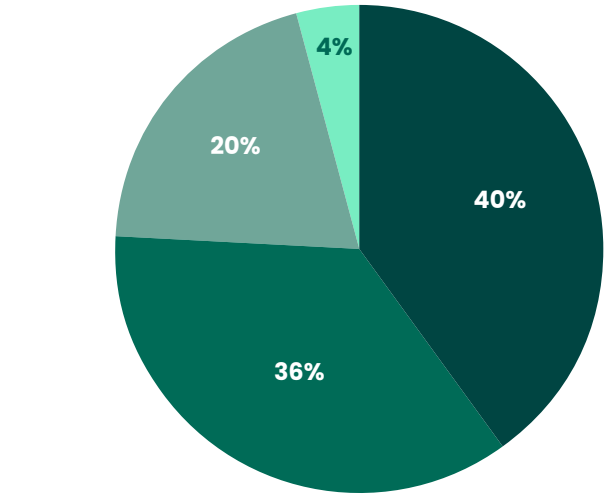
Credential theft email attacks trick victims into submitting user credentials on phishing sites. 49% of the Q4 attacks targeted Microsoft 365 credentials as they can provide access to a wide range of organizational data and services. They also enable account takeover (ATO) attacks where malicious communications are sent from the account of a trusted internal user.

Top Inbox Threats Are Credential Theft Attacks and Social Engineering

Fortra also observed a growing trend of docuphishing, where phishing links are delivered via email attachments. Nearly one-third of phishing links observed in Q4 were delivered using this technique. The growth in docuphishing indicates a relatively high success rate despite victims needing to take the additional step of opening the attachment. Users may be less suspicious of links in attachments as most phishing awareness training scrutinizes the email itself.

More than 40% of email threats that reached corporate user inboxes in Q4 were social engineering attacks. These attacks lack malicious links or attachments and rely solely on social engineering to convince victims to take actions such as disclosing sensitive information, transferring funds, or engaging in other fraudulent activity. Hybrid vishing, explored in greater detail later in this report, was the most prevalent response-based attack observed in Q4 followed by 419 and BEC scams.

Although BEC only made up 20% of observed attacks, the consequences of this type of attack to organizations can be severe as they may include regulatory fines, data leaks, financial losses, and even the loss of intellectual property.



Q4 Response-Based Threats

40% Vishing **36%** 419 Scam **20%** BEC **4%** Job Scam

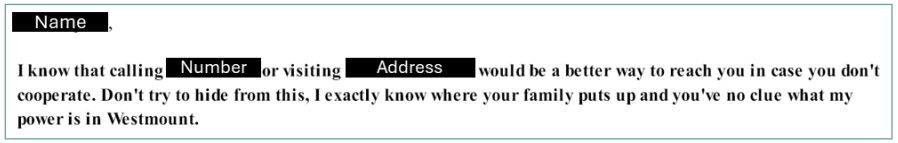
Prediction

Social engineering email threats will quickly grow in quality and sophistication, presenting defenders with a difficult challenge. As generative AI becomes more common, there will be a “rising-tide” effect on social engineering emails. Even the least sophisticated actors will be able to craft messages free of awkward translations and basic grammatical errors. More advanced cybercriminals will use generative AI to streamline steps required to launch phishing campaigns.

The volume of attacks that bypass spam filters and cannot be easily dismissed by users will grow. Defenders should expect more convincing social engineering attacks to reach user inboxes.

Email Threats Are Getting Personal

Fortra observed a growing trend of phishing attacks that incorporate personal information about the targeted user. In these attacks, personal information pulled from public sources or leaked data is used to lend credibility to the scam. One example of this tactic is using a victim's leaked home address from a data breach to include images of their home, sourced from services like Google Street View. This is done to create a sense of fear and make the scam feel more convincing, rather than relying on a generic email.


[Name],

I know that calling [Number] or visiting [Address] would be a better way to reach you in case you don't cooperate. Don't try to hide from this, I exactly know where your family puts up and you've no clue what my power is in Westmount.

Example of an extortion scam using public data to lend credibility

This tactic is frequently observed in extortion scams that seek to create urgency, panic, and a sense of being trapped. These attacks confront victims with a wide range of threats unless they send bitcoin payment.

Prediction

The volume of personal information available on open sources and the dark web is immense, with more than 1 billion records breached in 2024 alone. Cybercriminal data brokers aggregate and organize stolen data into bulk packages to anyone willing to pay the price. Email addresses are associated with a wide range of stolen information such as government identification numbers, employers, and service providers.

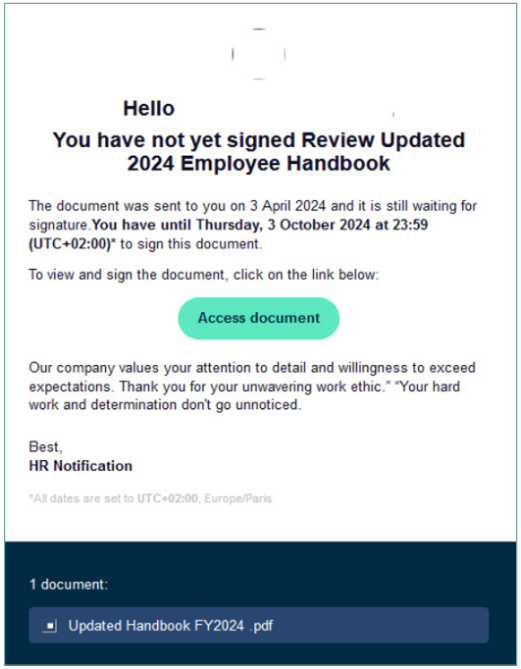
Fortra expects cybercriminals to use this data to personalize attacks even further, utilizing information about individuals, their families, their co-workers, etc. Cybercriminals who specialize in whaling will use the data to profile high value victims and find weaknesses to exploit. Email threats of all kinds will become more personalized, making them harder to ignore and more convincing.

Legitimate Service Abuse Is Growing Unabated

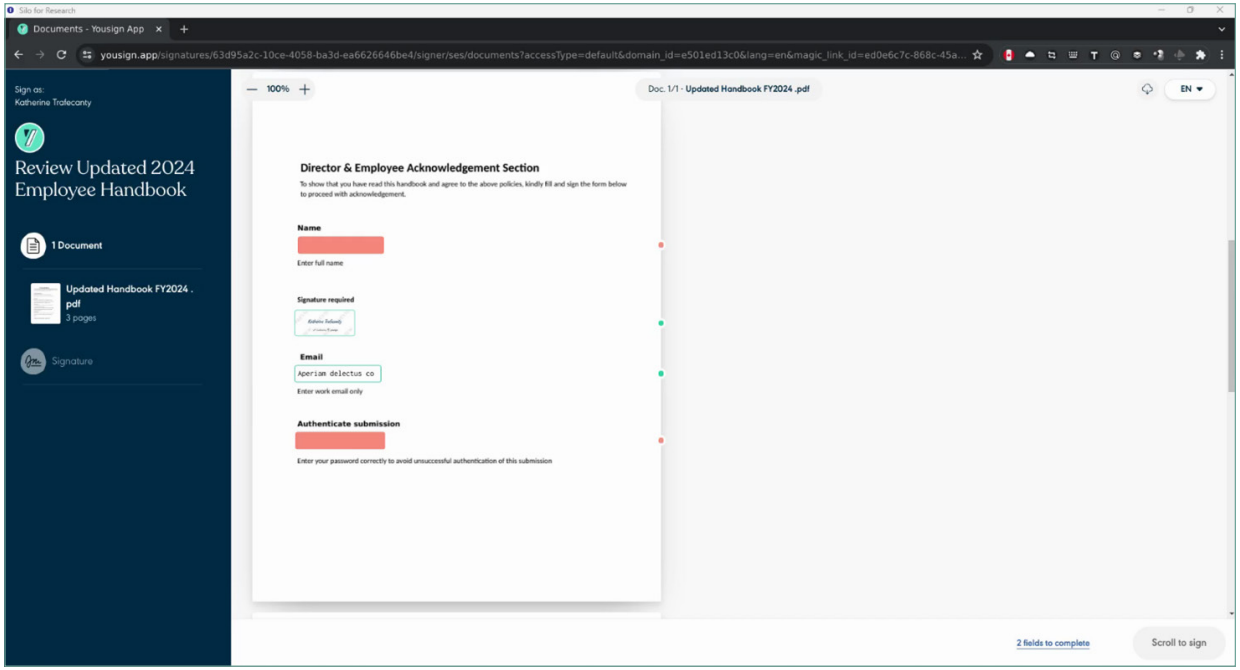
Tools for development, email, business services, etc., provide cybercriminals with infrastructure at zero cost. These services are typically “freemium” versions that have basic features compared to the full premium versions. However, basic is all cybercriminals need to launch attacks.

Abuse of legitimate services surged in 2024. E-signature platforms were the most abused kind of legitimate service, with DocuSign being the most heavily abused e-signature service in 2024. A high volume of email threats using DocuSign were used to send malicious email and attachments.

However, Fortra also observed scams using e-signature platforms end-to-end. In this example, attackers exploited the YouSign platform for every major step of the attack from sending phishing emails to harvesting credentials.



The “Access document” button links to a URL in the YouSign web application that presented a fraudulent employee handbook document for signature.



The signature form requested the victim’s name, work email, and work password to “sign” and acknowledge the fraudulent employee handbook.

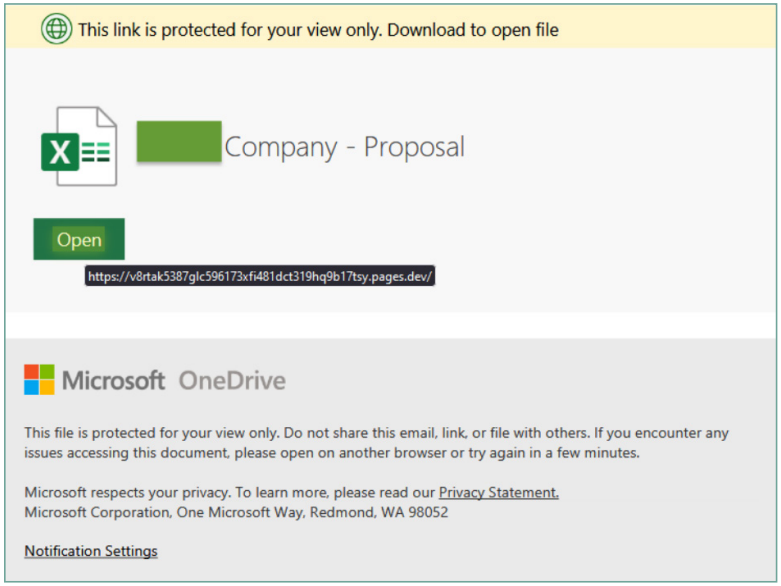
Legitimate Service Abuse Is Growing Unabated

In 2024, Fortra also continued to see significant abuse of free developer tools. Many of these tools allow code to be quickly published to publicly accessible domains. This is great for developers who want to rapidly test and deploy code, but also makes these tools prone to abuse by cybercriminals. These tools also provide automation and application programming interface (API) features that enable more advanced cybercriminals to integrate them into kits for managing and orchestrating attack campaigns.

In 2024, Cloudflare was the most abused provider of free developer tools. Domains from Cloudflare Pages and Workers services were constantly observed being used in phishing attacks for redirects and destination URLs.

Cloudflare's global content distribution network (CDN) ensures phishing sites load quickly and reliably across regions, which increases the effectiveness and reach of attack campaigns. Additionally, the service provider offers free and easy-to-use hosting, enabling cybercriminals to quickly deploy phishing sites with minimal resources or technical skills. Cloudflare's automatic SSL/TLS encryption also adds a layer of legitimacy to these phishing sites, as users are more likely to trust sites with secure HTTPS connections. Finally, attackers can leverage custom domains and URL masking to increase the authenticity of phishing sites, while Cloudflare's reverse proxying renders it difficult for security controls to trace the origin of malicious content.

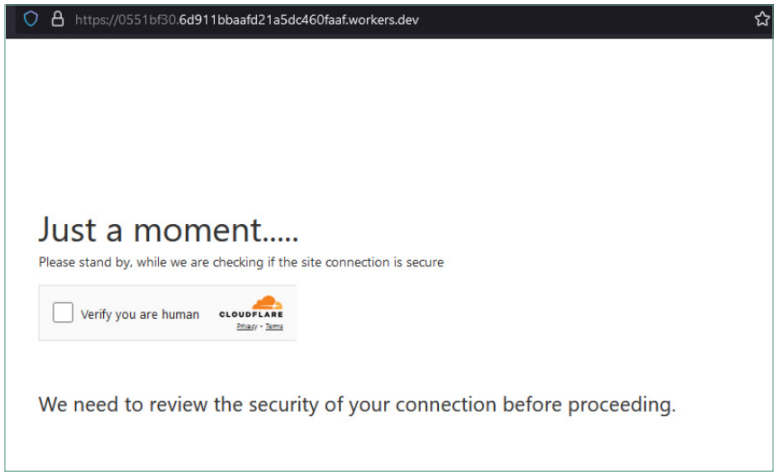
Cloudflare Pages is a platform used to deploy websites directly from code repositories (such as GitHub and GitLab). For cybercriminals, this makes it easy to quickly create phishing sites and redirects.



Example of a URL from Cloudflare Pages being used to redirect a victim to a Microsoft 365 phishing site.

Legitimate Service Abuse Is Growing Unabated

Cloudflare Workers is a serverless computing platform that allows deployment of code directly at the edge of Cloudflare's CDN. This enables code execution on the client-side, which reduces latency and improves performance for web applications. It has been observed as being abused to deploy phishing sites and redirects, inject harmful scripts, and conduct distributed denial of service (DDoS) attacks.



Workers was used to create a human verification page before redirecting the victim to a phishing site. This step makes phishing sites seem more legitimate and can make victims lower their guard.

Prediction

For cybercriminals, abusing legitimate services delivers efficiency gains and trusted infrastructure. The benefits are too attractive to not take advantage of them.

Companies that offer free services are reluctant to introduce stronger verification measures prior to usage. Doing so would introduce friction and get in the way of the instant gratification customers want. Instead, they rely on abuse reports and other reactive measures to clean up abuse after it happens.

Absent stronger regulatory or market incentives to encourage proactive anti-abuse measures by legitimate service providers, we predict this abuse will continue to grow. Cybercriminals will seek to exploit as much trusted infrastructure as they can, using that infrastructure to bypass security controls and present victims with more convincing phishing attacks.

We expect to see the most growth in abuse of developer tools. Freemium is the predominant business model for these kinds of tools and in general, these tools are designed to make it easier and more efficient to deploy code to publicly accessible sites. Developer tools also tend to have features that support programmatic integrations, allowing cybercriminals to further automate and streamline processes to craft, stage, and launch attacks.

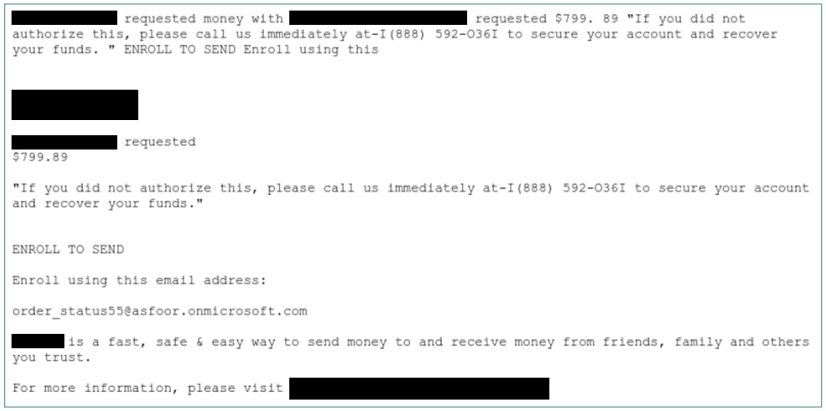
Multichannel Threats Continue to Rise

Multichannel threats are attacks initiated via email that lead victims to other environments. Attackers use simple emails that are unlikely to be flagged by email filters to move victims to less secure environments where exploitation occurs.

The most common multichannel threat in 2024 was hybrid vishing, which begins with a phishing email that tricks the victim to call a phone number where the scam is executed. As aforementioned, hybrid vishing was also the highest volume social engineering threat observed. Hybrid vishing is so effective because the varying nature of phishing emails prevents pattern recognition and hinders the development of filters, allowing the scam to bypass email security undetected. When victims call the phone number, the attack essentially moved from a corporate IT environment, with multiple layers of security, to a relatively unprotected voice channel.

The content of hybrid vishing emails varies. Fortra's analysis identified multiple hybrid vishing campaigns that were commonly used by attackers in 2024. For example, PayPal hybrid vishing scams typically begin with an email alerting the user of a financial charge on their account and instructing them to call the phone number to cancel this transaction. When the user calls the fake PayPal call center, they are tricked into revealing sensitive financial information that can be used to conduct even more financial fraud and theft. One in three hybrid vishing attacks in Q4 impersonated PayPal.

Another hybrid vishing campaign from 2024 involved using Twilio's SendGrid to send phishing emails impersonating well-known brands such as Walmart, Amazon, Apple, and Microsoft. These emails claim the recipient made a purchase and to call a phone number to dispute these charges. The call directs them to a fake call center where the attackers trick victims into sharing personal identifiable information (PII), which Fortra observed being sold on the dark web.



[redacted] requested money with [redacted] requested $799. 89 "If you did not authorize this, please call us immediately at-I(888) 592-036I to secure your account and recover your funds. " ENROLL TO SEND Enroll using this

[redacted]

[redacted] requested
$799.89

"If you did not authorize this, please call us immediately at-I(888) 592-036I to secure your account and recover your funds."

ENROLL TO SEND

Enroll using this email address:

order_status55@asfoor.onmicrosoft.com

[redacted] is a fast, safe & easy way to send money to and receive money from friends, family and others you trust.

For more information, please visit [redacted]

Example hybrid vishing P2P payments phishing email

You don't often get email from angelisantimakleyer256@gmail.com. Learn why this is important

MPORTANT NOTICE - This message sourced from an external mail server outside of the Company.

Walmart

Your order is on the way.[redacted]
We appreciate your recent order .

Order Identification: LMXBDG4154HF
Product: Canon Printer S Series (S47840)
Amount Charged: $524.85
Your order is scheduled for delivery by 07/05/2024.

If this order was not placed by you, please contact us immediately to report and block this transaction.

Thank you
18142801492

Angela
AS, Phoenix,
Unsubscribe - Unsubscribe Preferences

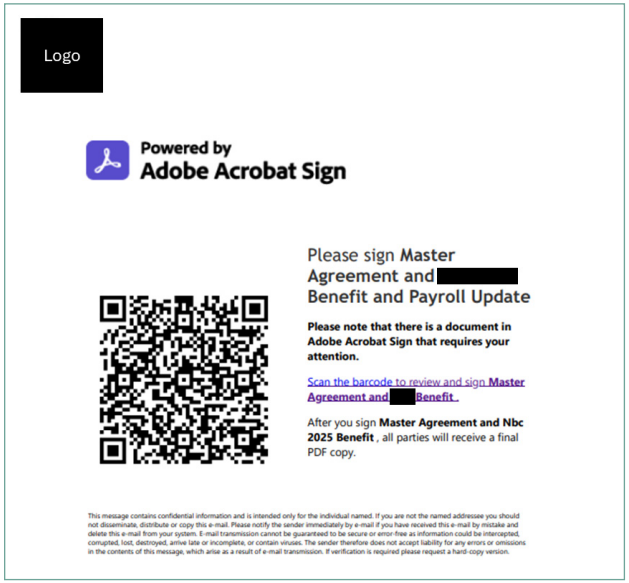
Example from 2024 hybrid vishing campaign sent via Twilio SendGrid

Multichannel Threats Continue to Rise

Another multichannel threat trend in 2024 was delivering malicious URLs via QR codes in message body content or attachments. This method allowed cybercriminals to slip malicious URLs past email filters lacking the ability to extract and analyze content stored in QR codes. It can also lead the user to a less protected environment, where the likelihood of exploitation is higher, as scanning a QR code with a smartphone is the most common and easiest method. If a user encounters a malicious QR code on their work PC, they will most likely scan it and open the malicious link on a less secure smartphone, which is beyond the reach of the organization's IT security controls.

The email lure on the right is an example of a QR code multichannel campaign targeting employees of a financial institution, featuring a PDF attachment instructing them to scan a QR code to sign a benefit and payroll update.

This led to a Microsoft 365 phishing site customized with the organization's logo to imitate single sign-on (SSO), which would not be unexpected when signing into an organization's HR platform.



Example of QR code multichannel phishing lure

Prediction

Exploitation is more likely to succeed in less secure environments, which makes methods that move victims out of their corporate email environment attractive to cybercriminals. The growth in hybrid vishing and QR code phishing attacks are prime examples of this dynamic at work. We predict these two methods will continue to grow.

Cybercriminals will pursue additional methods of initiating multichannel attacks via email, increasing pressure on defenders to detect these attacks before victims are moved to environments beyond their control.

We also expect hybrid vishing attacks to become much more sophisticated as generative AI is used to produce more realistic dialogue and voices. Fewer attacks will have obvious red flags such as odd background noise and robotic voices. Cybercriminals will be able to convincingly mimic accents and dialects, no matter their location, making vishing attacks significantly more believable.

Conclusion

In 2024, corporate email threats evolved as cybercriminals took advantage of defensive weaknesses and new resources. Credential theft and social engineering attacks continued to bypass email filters and land in user inboxes. Cybercriminals used the abundance of private data available online to craft personalized scams, heavily abusing legitimate services to enable campaigns with trusted infrastructure. And they used multichannel hybrid vishing and QR code attacks to slip past email defenses and move victims to less secure environments for exploitation.

In 2025, social engineering and vishing attacks will become more sophisticated with the use of generative AI to create error-free dialogue. Language will be less of a barrier, opening the door to more clever and convincing lures.

Cybercriminals will expand their utilization of data brokers and datasets comprised of stolen information to further personalize attacks. Personalization has always been an effective tactic, but the effort required to collect personal details on an individual limited attacks to smaller targeted campaigns. This is no longer the case as cybercriminals now have the tools and abundance of personal data needed to launch large-scale attacks tailored to individual targets.

Legitimate services including e-signature, file sharing, and developer tools will be heavily abused in 2025. The pressure on defenders to disrupt these attacks without interrupting legitimate web and email communications will increase. Developer tools will experience the highest abuse growth in 2025, as they provide the most versatility and the greatest potential for integration into cybercrime kits.

Throughout 2025, organizations can stay ahead of the shifting landscape by strategically approaching email security as a stack of defensive layers capable of analyzing and disrupting email threats before and after they are delivered to user inboxes. It will become increasingly difficult to stop malicious emails without analyzing them by using various techniques at multiple points in the attack chain.

Moreover, it will not be enough to train users to spot basic red flags in phishing emails. Generative AI will be used to craft messages without obvious mistakes in subject lines and body content. Trusted services will be abused to deliver malicious emails with trusted sender domains and legitimate URLs. Security awareness training efforts must evolve beyond basic awareness, focusing on helping users recognize risky scenarios and report suspicious activity.

FORTRA®

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the attack chain at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.

fta-gd-0325-vm