VIPRE SECURITY GROUP

Email Security in 2025

What to Expect from the Evolving Email Threat Landscape

Contents

Introduction 03

What VIPRE Caught in 2024 04

Let's Talk Spam: You're Going to Need a Bigger Folder 05

Top Targets of 2024 08

Feature: The Most Dysfunctional Malware Family of the Year 10

What's Worse Than Spam? Malspam 11

Phishing: A Host of Slippery Tactics 13

Feature: Cracking the QR Code 15

Looking at Business Email Compromise (BEC) 16

Feature: VIPRE Vs. BEC 17

Vipre Predictions and Recommendations for 2025 18

Conclusion 21

Introduction

Email Security in 2025: What to Expect from the Evolving Email Threat Landscape.

For those of us on the front lines of the email threat battleground, last year was full of ingenious new tactics that keep us all on our toes.

From innocuous QR codes hiding suspicious-looking domains to artificial intelligence doing what we knew it was capable of all along, this year's threats not only demand attention but potentially some changes in our email security methodologies as well. Organizations unable to address email threats that bypass defenses and reach the inbox face heightened vulnerability. Now, more than ever, users can fall prey to word-perfect AI-created phishing campaigns, subtle BEC messages that sound remarkably like the sender, and highly convincing ploys from trusted vendors with legitimate-looking websites and clean domains.

It's a trickier world than ever for email defenders, and we at VIPRE make it our mission to deliver the intelligence needed to help organizations know the enemy and come out on top. That is why this year we are releasing the findings of our year-long global research.

We invite you to scour our findings, and consider our projected trends for 2025.

What VIPRE Caught in 2024

It was a remarkably busy year in 2024, and we have the numbers to prove it. In the past twelve months, we've been chasing cybercriminals through inboxes around the globe, flagging bad behavior and using their tactics to build profiles against them. All in all, we've been pretty successful. As we've "hunted the hunter," here's how our efforts have played out.

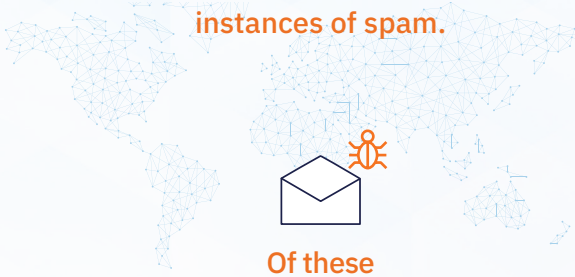
VIPRE has:

- **Detected 858 million instances of spam.**
  - 437 million were flagged due to content.
  - 411.62 million were flagged due to links.
  - 8.3 million were flagged due to attachments.
  - 609,000 were caught via attachment sandboxing.

- **Protected over 51 million links via Link Isolation.**
  Of those, 443,000 were detected at click time, meaning that by the time these malicious emails managed to make it past other defenses and into an inbox. Without click-time detection, millions of unsuspecting users (who obviously already clicked) would have been face-to-face with malware or a malicious site. And, according to one industry report, in a simulated phishing test of nearly 600 organizations "6 out of every 10 end users who clicked on [a] simulation email link ended up compromising their credentials." The ability to detect suspicious exploits at click-time is a necessary capability in today's email threat environment.

2024 - WE DETECTED

858 MILLION
instances of spam.



Of these
437 MILLION
were flagged due to content

The good news?

VIPRE Email Security Link Isolation, one of our features, detected and protected over 51 million links clicked by users.

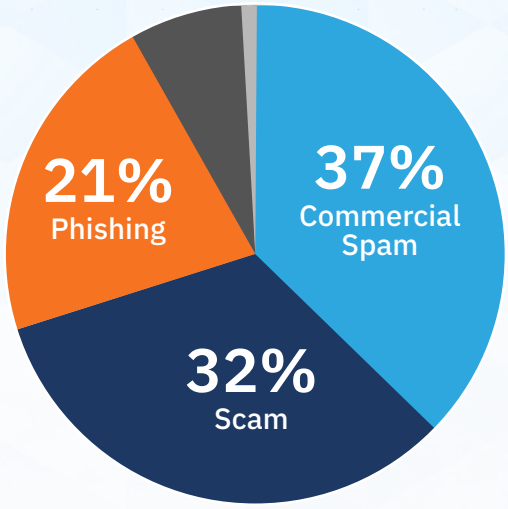
We're pretty proud of that.

Let's Talk Spam: You're Going to Need a Bigger Folder

The fact that we discovered that over nine out of ten emails received last year were categorized as spam will come as little surprise to anyone who's ever opened their inbox.

Spam comprises of emails that are unsolicited, unwanted, and potentially used for marketing purposes or with malicious intent. In other words, anything from the everyday "junk mail" clutter to the notorious "Nigerian prince" fraud attempts.

Organizations are so desperate to eliminate this constant nuisance that the Global Email Spam Filter market is estimated to grow by $10.35 billion in the next six years, boasting a CAGR of 13.6%. Not only are excess (and useless) emails a drain on productivity, but they are also the vehicle for a high level of cybersecurity risk.



Prevalent Spam Types of 2024

In 2024, we analyzed 118,557 never-seen-before spam emails. They fell into the following distinct categories:

- Commercial | 37%
- Scam | 32%
- Phishing | 21%
- Malware | 9%
- Others | 1%

Where Did It Come From, Where Did It Go?

A quick look at aggregated Q1-Q4 2024 numbers will reveal that much of the world's spam is coming from the US and going to the US.

They must be busy! It is also possible that the numbers may be skewed simply because the United States is home to many of the world's servers. This allows cybercriminals in foreign countries to make their emails look like they are coming from the US, when in reality, they are not.

Other countries that made the 'top spam senders' list in 2024 include:

Q1: [US], UK, Ireland, Japan, France, India

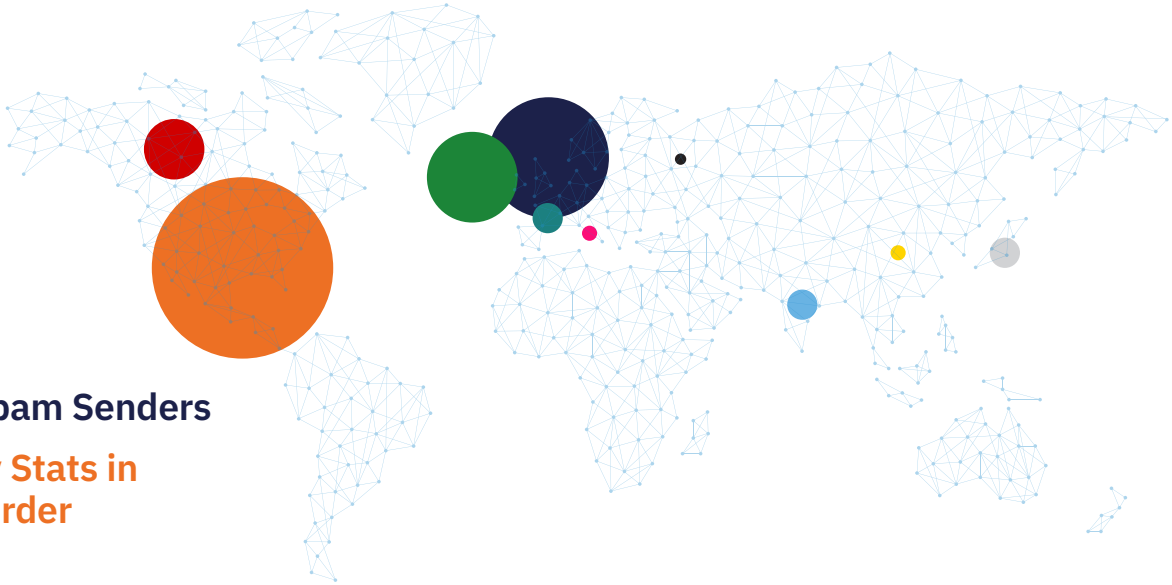
Q2: [US], UK, Ireland, India, Canada, France

Q3: [US], UK, Ireland, China, Italy, Russia

Q4: [US], UK, Canada, Ireland, France, Japan

Successful social engineering is all about trust. It is interesting to note that many of the countries that sent the most spam also ranked high on a global survey of the most trusted countries in the world. Note the appearance of the following countries on that recent 'most trusted' list:

1 Switzerland
2 Sweden
3 Norway
4 Denmark
5 Canada
6 Finland
7 New Zealand
8 Austria
8 Australia
10 Netherlands



One thing can't be faked, however, and that's the amount of spam a country takes in. With nearly two-thirds of global spam barraging the US, American employees (and employers) need to take extra precautions to avoid falling prey to these schemes. The danger is that with so many of these types of emails coming in, users will get email fatigue and miss a malicious message sooner or later.

Other countries getting an (unwanted) notable mention for the amount of spam received last year include:

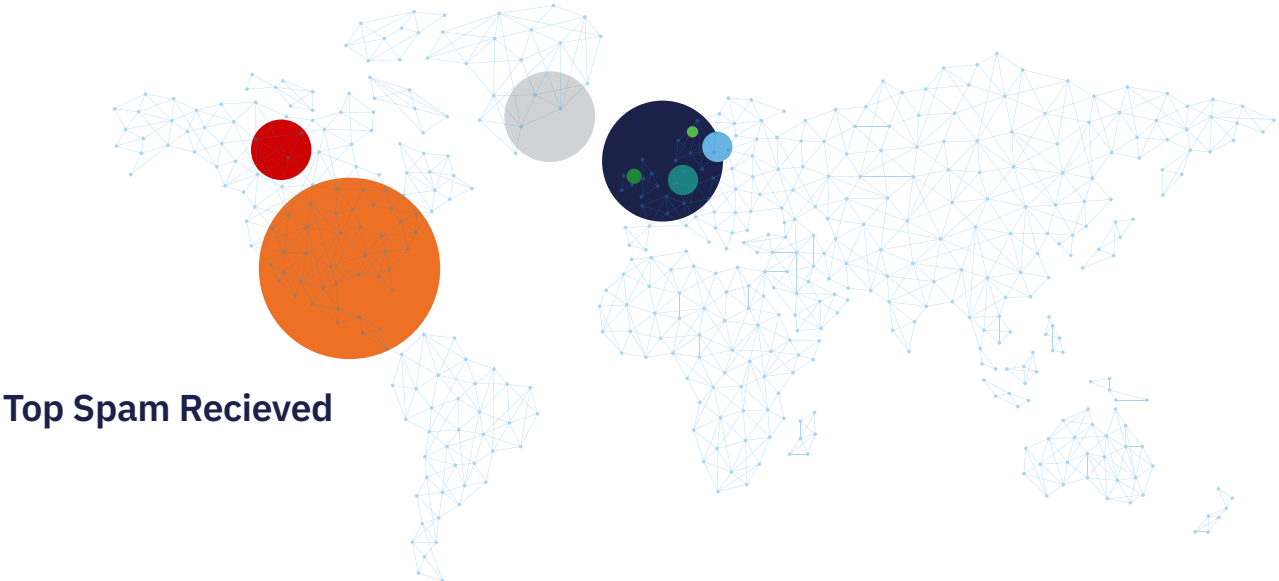
Q1: [US], UK, Canada, Iceland, Denmark, Ireland

Q2: [US], UK, Canada, Sweden, Iceland, Denmark

Q3: [US], UK, Canada, Sweden, Ireland, Norway

Q4: [US], UK, Iceland, Canada, Sweden, Denmark

It may appear from these findings that many of the world's most trusted countries are actively flooding their own networks with unsafe, unwanted junk mail, but this is unlikely to be the case. It's remarkably easy to block traffic coming from countries flagged as significant cyber threats, like Russia or China, so hackers from these countries tend to send their emails from more trusted countries, like the UK. Essentially, attackers deliberately obfuscate their locations to bypass defenses, which can skew results.



Top Targets of 2024

Top-targeted Sectors of 2024

In 2024, phishing and malspam threat actors took a liking to the following industries, listed here by the top three per quarter:

Q1
- Manufacturing (43%)
- Government (15%)
- IT (11%)

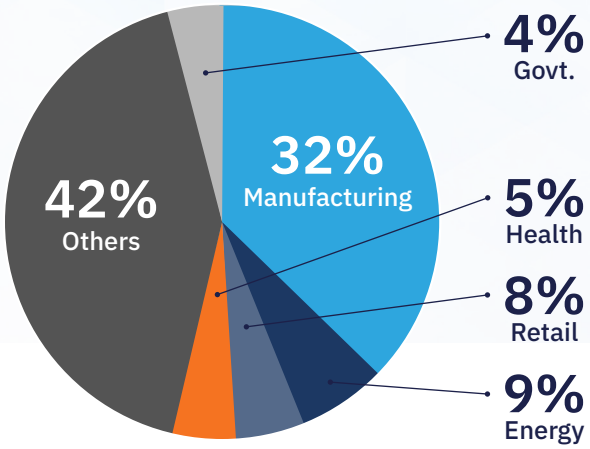
Q2
- Manufacturing (25%)
- Retail (20%)
- Real estate (11%)

Q3
- Manufacturing (27%)
- Energy (23%)
- Retail (10%)

Q4
- Manufacturing (31%)
- Health (18%)
- Energy (11%)

The top five most-targeted sectors of 2024 are:

1. Manufacturing (32%)
2. Energy (9%)
3. Retail (8%)
4. Health (5%)
5. Government (4%)



Other sectors (Tourism, Transportation, Finance, Real Estate, and more) account for the remaining 42%.

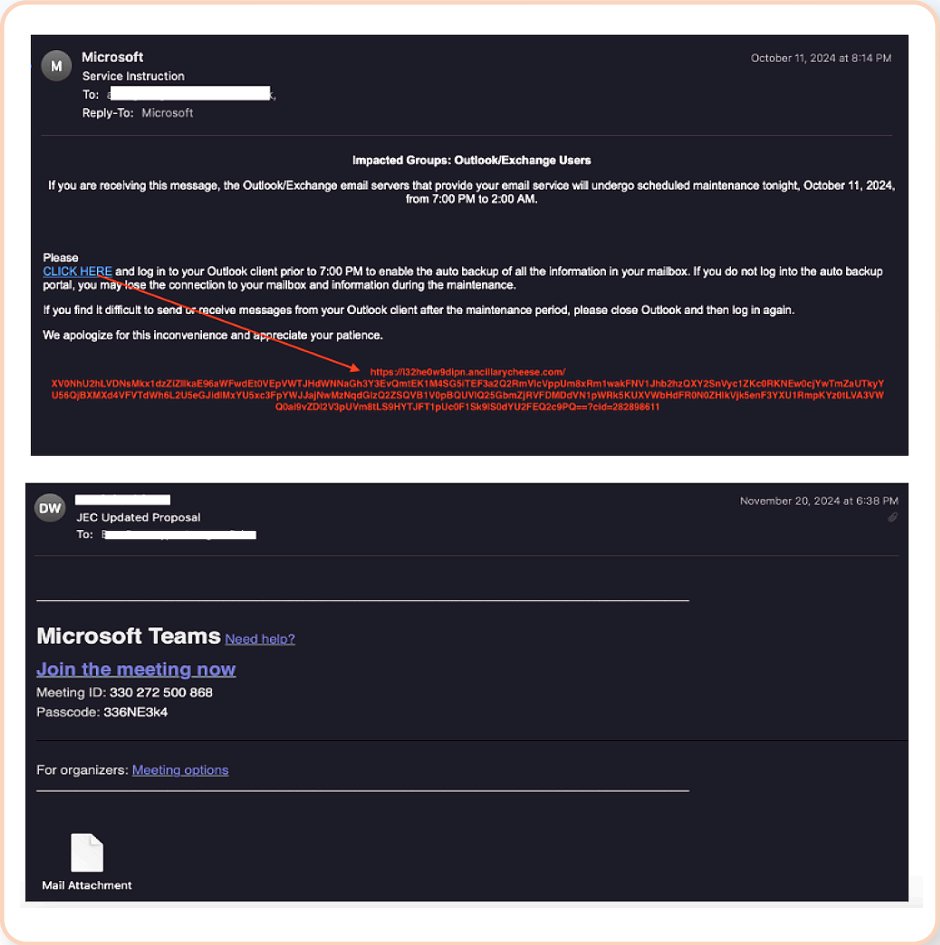
Despite suffering a slight dip between the first and fourth quarters, the sector most targeted in 2024 remained consistent across the quarters, with manufacturing being the clear favorite for email-based attacks.

The Most Spoofed of 2024

Once again, it's no surprise that Microsoft retains its title as the most spoofed brand.

After all, it's the price of creating a name that commands such widespread trust. The last thing cybercriminals want to look is suspicious, and the software behemoth has long been the favorite big name to hide behind. It also helps that over one billion people (an eighth of the world's population) use some sort of MS product, increasing threat actors' ability to spread a single, well-crafted email campaign to the greatest number of users.

Below are a couple of examples of Microsoft-spoofed phishing emails we caught last year:



While Microsoft has remained a constant, the number two and three spots for 'most spoofed' have been mercurial at best through the quarters. These can reveal digital undercurrents that attackers watch and try to use to their advantage. The quarterly 'top 3' lists are as follows:

Q1: Microsoft, DocuSign, eFax
Q2: Microsoft, Apple, DocuSign
Q3: Microsoft, DocuSign, Google
Q4: Microsoft, Apple, Dropbox

The fourth quarter saw Apple take the number two spot, potentially due to the following factors: Apple's iPhone 16 was released at the end of September, and it's likely that a large number Q4 scams rode that wave, pushing new deals and capitalizing on the chance to get a new iPhone for the holidays. Apple has long since been among the top consumer brands, and with the company posting over $93 billion in revenue for the fiscal 2024 fourth quarter, attackers likely felt confident hiding behind yet another large (and seasonally popular) brand.

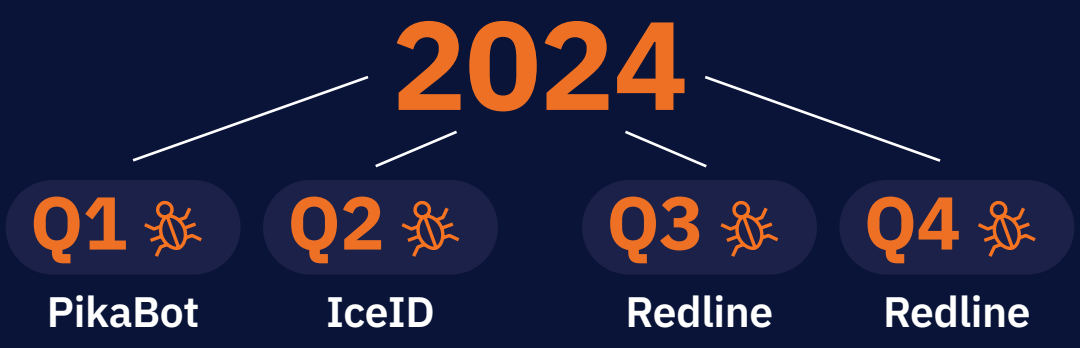
Feature: The Most Dysfunctional Malware Families of the Year

In the yearly "race to the bottom," these four malware strains stood out for the wrong reasons.

Individually, they all proved their ability to compromise the highest number of systems, steal the most data, take the most money that wasn't theirs, disrupt lives, and generally make a nuisance of themselves.

- In Q1, it was PikaBot, a malicious backdoor active since early 2023.
- In Q2, it was IceID (AKA BokBot), a banking trojan and Remote Access Trojan (RAT).
- And in both Q3 and Q4, Redline took the top spot. This malware is designed to swipe sensitive information from web browsers.

Interestingly, all the malware we encountered in Q4 appeared to be Windows-based (Stealc, Lumma, AgentTesla, etc.). We also observed that most of the malware received were infostealers and RATs, which can spy on the victim's machine and deliver additional threats, such as ransomware.



What's the Worst Part of Spam? Malspam.

We've addressed spam, a general catch-all of junk mail ranging from commercial annoyances to downright malicious messages.

Now, we are going to zero-in on only those malicious messages, otherwise known as malspam.

When a malicious email is sent, it delivers its payload in one of two ways: links or attachments. Which one will be used more often depends on the quarter, it seems.

Here's the breakdown:

- Q1: **22% links, 78% attachments |** In Q1, only 22% of all malspam leveraged links, while 78% hid malware and other ills in attachments.

- Q2: **86% links, 14% attachments |** In Q2, it was the near opposite; 86% links and 14% attachments. This could be due to URL redirection, a technique that employs a clean link which then redirects users to a compromised site.

- Q3: **36% links, 64% attachments |** The pendulum swung back as Q3 saw 36% of all malspam using links with the remaining 64% using attachments. This could be attributed to more caution on the side of users or cybercriminals targeting newly discovered vulnerabilities in file formats and document processing software.

- Q4: **33% links, 67% attachments |** In Q4, things stayed fairly level; 33% used malicious links while 67% delivered malware via unsafe attachments.

Malspam Links

As traditional email threat detection tools improve, it becomes harder for cybercriminals to get away with leveraging bad links that could (more and more easily) be flagged. Nevertheless, they try.

These are the main types of links used this year, by quarter:

- Q1: **Compromised website**
- Q2: **Cloud-based software development platform**
- Q3: **Compromised website**
- Q4: **Compromised website**

Compromised websites are legitimate-looking web pages that are actually spoofed versions of a trusted site. When the unsuspecting user clicks through, nothing looks suspicious (if the attacker's done their job right) and it is only a matter of time before the victim 'authenticates' and compromises their credentials on the site. The more trusted and well-known the target site in these cases, the better.

This is where our Link Isolation tool shines. It scans websites at access time to identify newly compromised sites based on their behavior; this means we can protect users in real time, discovering new threats as they happen instead of relying on known signatures and a "patient zero" or first infection.

Malspam Attachments

If links are becoming less reliable malspam vehicles, attachments are rising as a way to provide attackers with a leg-up.

During Q4, malicious attachments appeared in 67% of all malspam, and in an average of 56% for the year. And there are reasons, current email security software being one of them.

As noted by Paul Apostolescu, VIPRE's Chief Technology Officer, "Reactive, signature-based detection isn't sufficient to protect organizations from malicious attachments - email security solutions must also employ proactive, behavior-based detections. VIPRE's Advanced Threat Protection solution identifies and blocks never-seen-before malicious attachments by analyzing their behavior to determine what they will actually do when a user opens them."

But that doesn't mean users can let their guard down: email threat actors spoof some of the most widely used file types to deliver malware. These file types, including PDF and DOCX files, not only lull users into a false sense of security but are also often the only attachments companies allow; typically, companies block all other binary attachments, such as executables, as a matter of policy.

With this in mind, the malicious malspam attachment types we spotted the most in 2024, and the file types users should be most wary of in 2025, include:

- Q1: PDF, DOCX, HTML
- Q2: ZIP, DOCX, HTML
- Q3: PDF, DOCX, HTML
- Q4: XLSX, DOCX, PDF

Q4

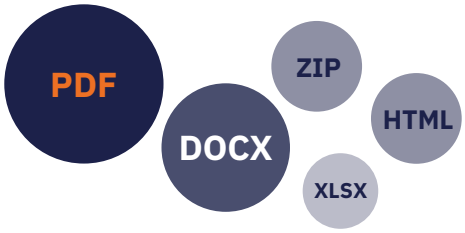
MALICIOUS ATTACHMENTS

67%

of all malspam.

"Reactive, signature-based detection isn't sufficient to protect organizations from malicious attachments - email security solutions must also employ proactive, behavior-based detections."

MALSPAM ATTACHMENT TYPES IN 2024



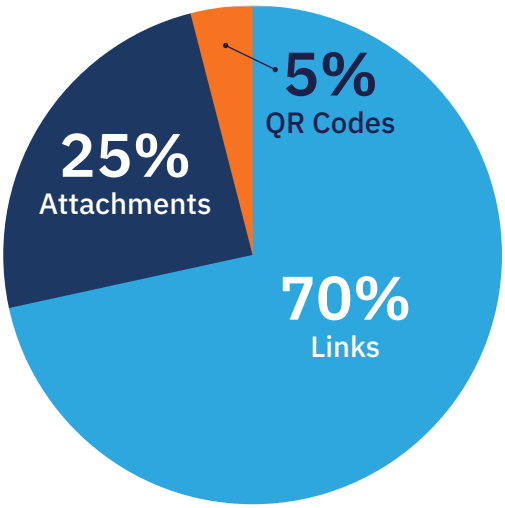
Phishing: A Host of Slippery Tactics

Links, Attachments, and QR Codes, Oh My

If malspam uses links and attachments, phishing uses the same, with one other weapon thrown in: QR codes.

In Q4, QR codes appeared in 12% of phishing scams, attachments almost doubled at 23%, and links in the lion's share, popping up in a whopping 65% of all phishing attempts. These numbers are echoed in 2024's overall figures, with phishers using:

- 70% Links
- 25% Attachments
- 5% QR codes (up from 1% in Q1 and peaking at 12% in Q4)



Now, let's dive into each.

Phishing Links: Choosing the Right Bait

While 65% of all phishing emails use malicious links, not all links are created equally.

Last year, those links broke down into several categories. URL Redirection was the most-employed phishing link tactic across all four quarters, with the yearly averages as follows:

- URL Redirection: 51%
- Compromised Websites: 19%
- Newly Created Domains: 7%
- File-hosting Services: 4%
- Other: 12%

Because URL Redirection can employ trusted sites with a clean bill of health, it is a favorite among email attackers. Once the user clicks, they are forced onto a compromised site where they are likely to enter sensitive information or give up their credentials. VIPRE's Link Isolation is like URL sandboxing for your inbox, opening the link as a user would to analyze its behavior, determine whether it's malicious, neutralize any threats, and warn the user.

It's also worth mentioning that to detect many of these tactics - including URL redirection, compromised websites, and file sharing services - dynamic link analysis is essential. VIPRE's dynamic link analysis capability analyzes a link's behavior in real-time, identifying any hidden redirects, malicious destinations, and potential threats that static analysis might miss.

Phishing's Favorite Phrases of 2024

If you're looking for more ways to spot a fake email, keep an eye out for these commonly used phrases we've collected from our phishing samples over the past twelve months.

Red flag any emails that use the following language, and think twice before clicking, downloading, or scanning:

- CLICK HERE to upgrade
- Please Access Your Account to review it
- Sign-in activity review
- New voicemail received!
- Your subscription is about to expire!
- Revoke your session and update password immediately
- To prevent any data or email loss
- You have received a new secure email
- Your password for "victim's email address" is set to expire on...
- 2FA Authentication is outdated
- Clear your cache to free up space
- Changes for upcoming payroll enrollment

Most Used Top-Level Domains (TLDs) of 2024

The phishing ruse runs deep, and threat actors are careful to carry the trust factor as far as they can.

In addition to padding their chances with trusted names like Microsoft and Apple, using well-known phrases like the ones above, and carefully choosing a delivery method most likely to slip under the radar, they also place high value on selecting a top-level domain that looks trustworthy. Or, at the very least, might go unnoticed as they spoof a popular domain name. That explains why ".com" was the most used TLD in phishing campaigns during 2024 and .org (largely used by nonprofits) was the second-most.

For a breakdown by quarter, we have the top TLDs coming in at:

- Q1: .com, .org, .uk
- Q2: .com, .org, .uk
- Q3: .com, .uk, .net
- Q4: .com, .net, .fr

It is likely that ".fr", the TLD of France, was still being widely exploited in connection with a range of lingering Olympics-based phishing scams this year.

Feature: Cracking the QR Code

While QR codes are relatively new to the phishing game and have yet to corner a significant portion of the criminal market, they are rapidly rising in popularity among the criminal underground.

Our 2024 data revealed an increase in nefarious QR code usage from the start of the year until now, rising from 1% in Q1 to 12% by the end of the year.

1. Users are getting better at spotting dubious links in emails, so criminals are hiding those links in the form of QR codes.

2. Many traditional email defenses are not capable of scanning images, allowing malicious QR codes to slip through.

3. Personal mobile devices are the tool of choice for scanning QR codes, and those devices often lack the stringent security precautions of work devices.

VIPRE's Advanced Threat Protection solution uses Deep Link, the dynamic URL analysis sandbox that powers our Link Isolation tool. It scans links that are embedded in QR codes to protect users from QR code phishing.

For extra protection against QR code phishing, warn staff against using their personal cell phones to scan any QR code originating from a work-related email. For that matter, threat actors are getting more adept at finding any inroad into a company's network, and even a personal email to a corporate employee can open the door if a malicious site is visited. Warn them of the dangers and advise wariness on all fronts.

Looking at Business Email Compromise (BEC)

Last but not least is the behemoth of email spam known as Business Email Compromise (BEC).

BEC tactics center around an employee being tricked into divulging sensitive company information or authorizing a fraudulent payment from their business to a scammer. One of the most lucrative of all email scam types, BEC accounted for over $2.9 billion in losses, roughly 49 times that of ransomware ($59.6 million), per the latest FBI IC3 Report. Perhaps that large monetary draw is why Q4 saw BEC account for a landslide 70% of all scam emails.

How do BEC Scammers Work?

BEC scams are, at their heart, well-crafted social engineering ploys.

Our second-half data revealed their primary tactic was Impersonation, which they leveraged in an average of 88% of all cases. Following was Diversion, Email Hijacking, and Account Takeover, in that order. This could be attributed to the fact that today's email defenses do a decent job of preventing technically based attacks. It's a cliche, but attackers know that as security software gets better, people are increasingly the weakest link.

Most Likely to Get Impersonated

Who do BEC scammers impersonate?

Our most recent quarterly data reveals that CEOs and executives are the most likely roles within the business chain to be compromised, to a tune of 74% of the time. Executive spoofing is a serious threat, exacerbated by the rise of artificial intelligence. Using AI, cybercriminals can weaponize even an individual's writing style, illicitly scraping and analyzing data from their sent mail once they've compromised access.

They feed that data into an AI model which not only crafts a word-perfect email but does so in the same tone and style as the "sender," even down to their usual sign-offs and greetings. In Q2, 40% of all our collected BEC samples were AI-generated.

Feature: VIPRE vs. BEC

We've established the two major factors allowing BEC to run rampant this year: people falling for impersonations, and impersonations (thanks to AI) being incredibly easy to fall for. Here is how VIPRE helps to solve those problems.

What Happens If You Click?

With VIPRE's advanced click-time detection and attachment sandboxing capabilities, users can interact with potentially deceptive content without worrying.

Even in cases where mistakes occur, such as clicking, downloading, or scanning malicious files, VIPRE provides robust solutions to address these scenarios. This unwavering commitment to comprehensive protection is precisely what distinguishes VIPRE from the rest.

Using VIPRE's three-tiered approach, organizations can work around even these clever obstacles. VIPRE can flag users when something seems "off" besides just the text. It takes into account not only the style of the email (for those non-profiled cases), but the time the email was sent, the location from which it was sent, and other metrics that provide multi-point proof of authenticity. Without tools of this sort, combatting scams like BEC – especially when powered by AI – will be next to impossible in the coming year.

VIPRE Predictions and Recommendations for 2025

As this report demonstrates, the VIPRE research team has worked tirelessly to ensure that the facts about this past year's email threats are available.

They uncover knowledge about attackers' techniques, and we seek to leverage every drop of that knowledge for the good of the community going forward. Based on twelve months of extensive observation and continuous research, we need to raise a warning voice regarding some of the most notable trends we see threatening global email security in 2025.

Predictions

1. QR Codes for Phishing and Malware Delivery.

Threat actors will continue to use QR codes not only for phishing purposes but also to deliver malicious files or links to compromised systems. While QR codes are typically seen as a safe way to share links or information, attackers are increasingly embedding them in phishing emails and malicious documents. Scanning these QR codes can direct users to malicious websites or trigger the download of malware.

Tip:

Be cautious when encountering QR codes in email attachments, especially in documents like RTF, DOC, or PowerPoint files. These files may not just contain phishing links but could also be designed to exploit vulnerabilities or download harmful files.

2. Infostealers as a Persistent Threat.

Infostealers, such as Redline, Stealc, AgentTesla, and Remcos, will remain a persistent threat in 2025. These malware types, often delivered via email, are designed to steal sensitive information, including login credentials, browser data, and financial information.

Infostealers continue to be a favorite among cybercriminals due to their effectiveness in collecting valuable data. These malware variants are often used in conjunction with Remote Access Trojans (RATs) to maintain long-term access to compromised systems, enabling attackers to conduct espionage or further infiltration. The growing sophistication of these tools makes them harder to detect.

Tip:

Expect a rise in targeted attacks using infostealers, particularly those focusing on high-value individuals within organizations. These attacks may often involve email attachments like EXE files, scripts, or compressed archives that contain the malware payload. Additionally, watch for infostealers hidden in unusual file formats such as RTF, DOC, or PowerPoint files, rather than the more commonly associated PDF or ZIP files.

Predictions

3. Deepfakes and Synthetic Media in Email Attacks.

The use of deepfake technology and synthetic media (including manipulated images, audio, and video) will become more common in email-based attacks. Deepfakes can be used to create highly convincing impersonations of individuals in BEC or spear-phishing attacks, increasing the effectiveness of social engineering tactics.

Tip:

Expect a rise in email attacks that use synthetic media to impersonate high-profile targets, such as CEOs, and to manipulate recipients into taking harmful actions.

4. Business Email Compromise (BEC) Attacks.

BEC will remain a significant concern in 2025. This type of attack often involves impersonating a trusted person or entity (such as a company executive or vendor) to manipulate recipients into transferring funds or sensitive data. Advances in artificial intelligence (AI) will make it easier for attackers to craft convincing messages, mimicking the tone and style of trusted individuals. In particular, the use of deepfake technology could further enhance the realism of these attacks.

Tip:

Stay vigilant for more sophisticated BEC campaigns targeting specific departments like finance or HR, and for those using AI to automate and personalize phishing attempts.

5. AI-Driven Phishing and Social Engineering

Cybercriminals will increasingly use AI to generate highly personalized and convincing phishing emails. AI allows for the automation of social engineering tactics, enabling attackers to analyze target behavior and deliver more tailored, convincing emails. This makes phishing attacks harder to detect and easier to execute at scale.

Tip:

Look for phishing emails that adapt to the recipient's actions in real-time, or that pull information from social media and other sources to appear more authentic.

Recommendations

Our recommendations for shoring up email defenses in the coming year include employing the following technologies in your security stack:

Email Authentication
Ensure the use of SPF, DKIM, and DMARC to combat spoofing and impersonation.

AI-Powered Detection
Invest in advanced email security solutions that leverage AI to identify emerging threats in real-time.

Multi-Factor Authentication (MFA)
Enforce MFA for all users to add an extra layer of protection against credential theft and account takeovers.

Security Awareness
Continuously educate users on identifying phishing attempts, particularly those that leverage new tactics like deepfakes, QR codes, synthetic media, and infostealers.

Behavioral Analysis
Deploy email filters that integrate threat intelligence feeds and advanced behavior analytics to detect and block suspicious messages.

Endpoint Protection
Ensure that endpoint protection systems are configured to detect and block infostealers and RATs, particularly those targeting high-value employees.

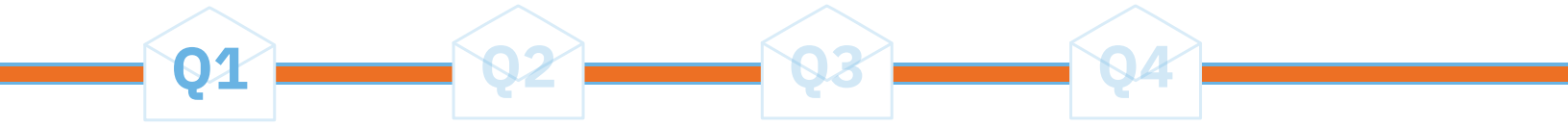
Although the outlook may appear bleak, it is not surprising, and it is not insurmountable. By staying vigilant and proactive, organizations can better protect themselves from the growing email-based threats expected in 2025, including the continuing risk posed by infostealers and other evolving malware types.

Conclusion

Phishing is on the rise thanks to new tactics, links and attachments are getting harder to spot as attacks evade traditional technology, and there is still little one can do to prevent an employee from reading, believing, and clicking. So, what is to be done?

As the adage goes, only worry about what you can control. And thanks to VIPRE's three-part email security approach, organizations can control a lot more than they think when it comes to email security.

Stay up to date and look out for the next installment of the VIPRE Email Threat Trends Report.



Email Threat Trends of 2025

Sign up today for your FREE 30 day VIPRE Email Security Trial.

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223