VIPRE SECURITY GROUP

Email Threat Trends Report: 2025: Q3

An Expert Look at Email-Based Threats

Contents

Executive Summary

Some offer annual reviews of the industry; we think email threats move too fast. For that reason, VIPRE publishes its Email Threat Trends Report quarterly.

We process almost 2 billion emails every three months and analyze millions of malicious messages. If we've learned one thing, it's that attacker tactics are always changing. Your email security needs to adapt just as fast.

For over 25 years, we have been securing our clients' data worldwide. We've protected over 20 million endpoints and currently process over 1 million unique malware samples per day. Few companies have the depth or breadth of expertise that we do, and every quarter we share our findings with the global cybersecurity community.

In this Q3 report, we note a deepening of trends that have been evident for some time. As technical (but traditional) barriers stand strong, attackers strategize increasingly clever ways of using everyday methods to get around them.

The attacks that succeed in the inbox are not always the ones that carry the most sophisticated malware; they are the ones that use simple, available tactics in the most sophisticated ways.

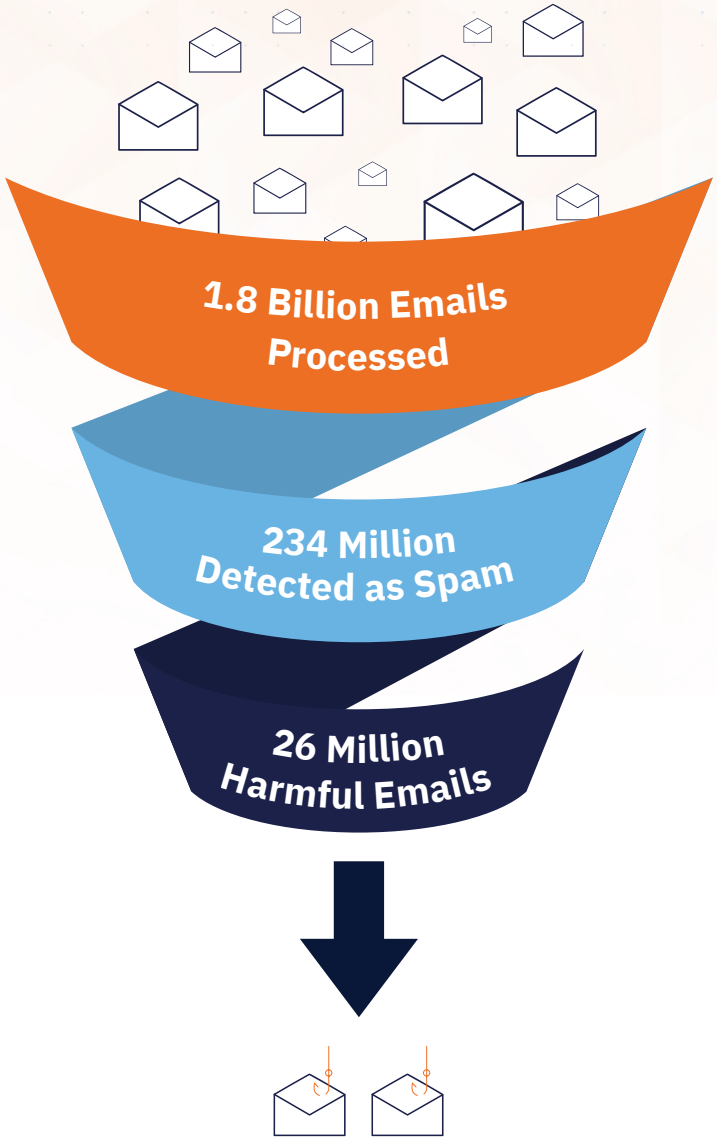
As the Q3 figures show, these tactics have become laser-focused on duping us and our traditional techniques.

Key Trends From Q3 2025

Malicious Emails Up 13%

This quarter, we processed 1.8 billion emails, detecting about 234 million as spam. Compared with the same period last year, that's the same number processed but 26 million more harmful emails, an increase of 13%.

On average, the VIPRE network processed around 2.6 million spam emails a day throughout the quarter. The good news is that this volume gives us the best vantage point in the industry. We see – again and again – what attackers over the past twelve weeks have been doing, how they have been doing it, and who they have been doing it to.



An Even Split Between Content and Link Detection

It's always interesting to see the ratio between the number of malicious emails caught due to content (infected or suspicious files, social engineering language patterns, header anomalies, and so on) and the number detected due to links. In our Q2 Email Threat Trends Report, content won by a full 16% (a 58%/42% split). However, in Q3, numbers were back to nearly even, with content taking 52% and malicious links 48%.

150k Caught by Sandboxing

Another important metric is the number of emails that slip through the cracks. These ploys leave no trace and evade discovery by both content-catching mechanisms and methods of sniffing out bad links. The only way to find out what they are is to click the link or download the attachment, and then it's too late. But VIPRE catches these never-before-seen new malicious attachments with sandboxing.

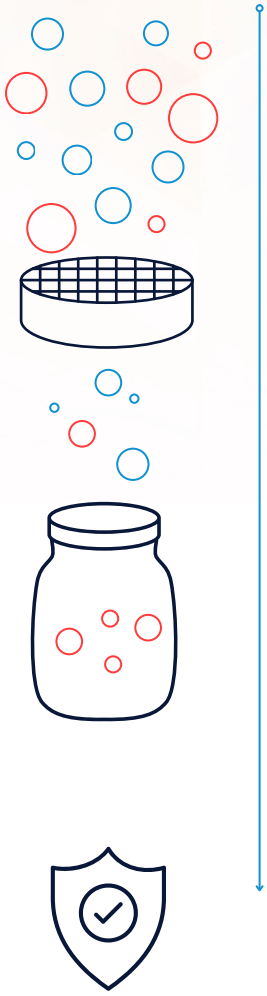
This quarter, VIPRE caught 148k malicious attachments with sandboxing. That's nearly 150k newly discovered malicious files, which could have resulted in successful attacks if opened by users. These may be less than 0.1% of the total, but they are potentially the most dangerous.

Along the same lines, links can also fail to show their true colors on the first pass. VIPRE detected over 67k malicious links that had never been seen before at click time:

- **89% were flagged due to content**
- **11% were flagged due to webpage behavior**

Sandboxing links mitigates widespread threats like URL redirects, which bypass email filters using a clean link but then redirect users to a compromised site when clicked. Advanced features like dynamic analysis are essential to protect against email threats that require real-time action.

These numbers hold consistent with last year's, showing that attackers are not slowing their use of these techniques and underscoring the need for companies to get ahead of them.



1.8 Billion

Emails Processed

Standard Filters

Link & Content Analysis

Sandbox

148k new malicious attachments caught

Threats Neutralized

Only <0.1% of total emails, but highest risk avoided

Expert Rules Detect Nearly 3 Million

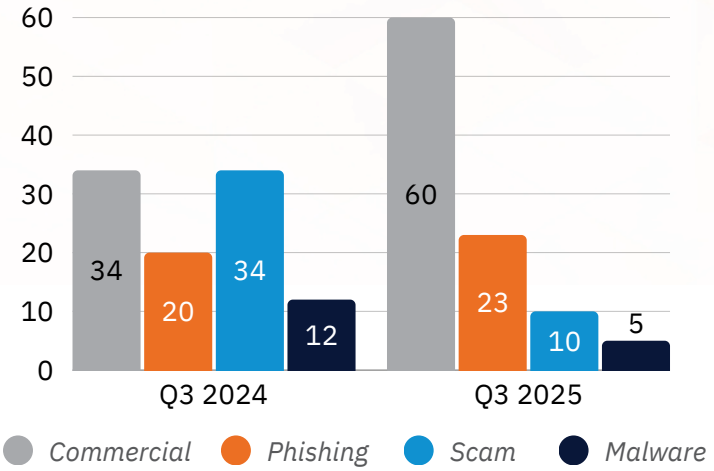
Speaking of the ones that get away: VIPRE Labs constantly curates new heuristics, and these proprietary rules were responsible for detecting a total of 2.8 million spam emails in Q3.

Generalized tools and rules can only do so much. Increasingly, it takes the in-house expertise and specialization that only dedicated teams can provide to go beyond the basics.

VIPRE's team of cybersecurity experts, malware researchers, software developers, and engineers is constantly innovating in unexpected ways to catch Advanced Persistent Threats, sophisticated malware, and zero-day exploits. As a result, VIPRE customers were protected from 2.8 million attacks they would have otherwise been exposed to this quarter.

The number of legitimate (but still "spammy") messages this quarter was significant: 60% were classified as Commercial. The top 3 types breakdown as follows:

- **Commercial 60% (up from 34% YoY)**
- **Phishing 23% (up from 20% YoY)**
- **Scam 10% (down from 34% YoY)**



**Percentages rounded; total may not equal 100%.*

Commercial Emails Crowd Out Phishing, Scams, and Malware

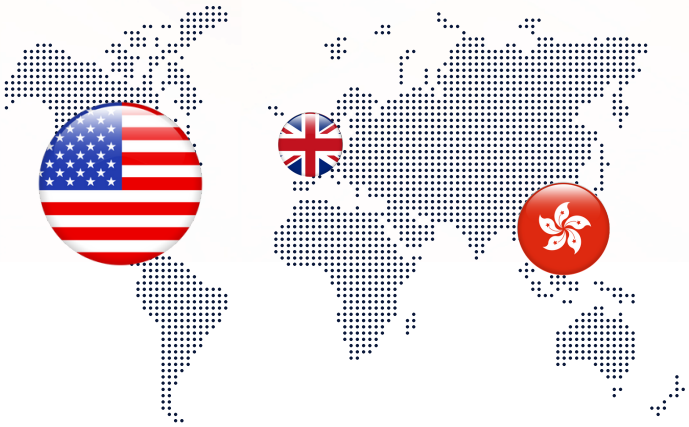
It's no wonder people click. Even if they're uninterested in the content, the sheer volume of mundane messages that come through could be enough to desensitize even the savviest user.

Last year's Q3 report cited Scam as the top category with over a third of the total volume. However, that number has dropped to a mere one in ten. Phishing is dangerously higher at nearly one in four commercial spam emails, up from one in five.

However, when you look at it from a broader perspective, the combined 38% of Phishing (23%), Scams (10%), and Malware (5%) is actively malicious and designed to harm, and accounts for more than 1 in 3 spam emails overall.

Distributed Geographies Make Malware Hard to Block

Q3 figures show that over 60% of spam emails are still coming from the United States. Other advanced economies continue to dominate the spam-sending market, with Hong Kong (9%) and Great Britain (6%) ranking a far second and third among geographies.



The dominance of the US may be primarily explained by its hosting the world's largest concentration of data centers and cloud servers. Attackers deliberately rent or compromise US-based servers because they offer fast, reliable performance. More importantly, emails originating from US IP addresses carry significantly better reputation scores and are far less likely to be blocked by security filters.

While perennially the top contender, the US continues to decline in this category, down from 74% last year (though up from Q2's 57%). Hong Kong is the relative upstart, taking home none of the pie last year but coming out swinging with an impressive 5% growth in Q1 2025, rising to 8% in the following quarter. This will be an interesting trend to watch.

Reiterating our comment on the US, the point we make most often is that spam follows the data centers and doesn't necessarily come from those locales—but it's hard to tell, and that's the point. A lot of crucial, business-imperative communications originate from those countries as well, so blocking geographic IPs from those locations en masse is unwise at best. Attackers count on this.

The Whac-a-Mole game continues with the other 25% or so being from such a smattering of (mainly) first-world countries that blocking by IP becomes futile; Ireland, the Netherlands, Japan, France, Canada, and Germany.

The Whac-a-Mole game continues with the other 25% or so being from such a smattering of (mainly) first-world countries that blocking by IP becomes futile; Ireland, the Netherlands, Japan, France, Canada, and Germany.

Wealthy Nations "Target" Wealthy Nations

As we've pointed out before, the discrepancy doesn't pass the smell test. All the top targets are wealthy nations (which, incidentally, appear to be the originators of said spam in the first place):

- **USA 60% (down from 73% in Q2)**
- **UK 12% (down from 15% in Q2)**
- **Canada 6% (up from 4% in Q2)**
- **Sweden 4% (up from 3% in Q2)**
- **Denmark 3%**

If it were true that most spam (and let's talk phishing and malware) messages came from English-speaking countries to English-speaking countries, why would grammatical errors have historically been such a dead giveaway? Again, we posit that the prevalence of regional datacenters has a significant impact on these figures.

What Language Reveals About Attacker Technique

Dominance of English

The analysis of Q3 spam reveals an overwhelming focus on English, which accounts for 87.61% of all observed samples. This pronounced dominance suggests that threat actors are primarily engaged in high-volume campaigns aimed at:

- **Global Audiences:**
  - Leveraging the status of English as the lingua franca of business and technology to maximize reach.
- **Major Target Markets:**
  - Concentrating efforts on North American and English-speaking European regions, where high-value targets and well-known brands are prevalent.
- **Efficiency:**
  - Utilizing English for widespread, less-localized attacks, which typically offer a higher return on investment for broad spam distribution.

Secondary Regional Targeting

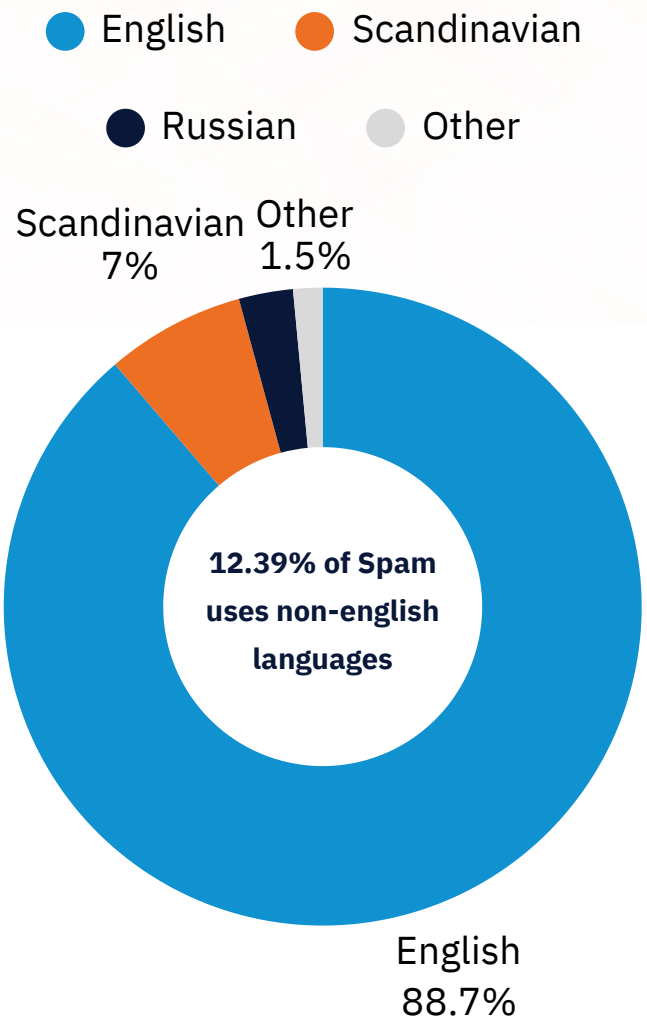
Languages other than English collectively account for approximately 12.39% of the threat landscape, highlighting specific regional targeting efforts:

- **Northern European Focus:**
  - The Scandinavian languages—Swedish (3.67%), Danish (2.78%), and Norwegian (0.51%)—represent a significant secondary cluster (6.96% combined). This suggests sustained regional campaigns, often associated with phishing, tax scams, or localized banking fraud, which rely on language accuracy to appear legitimate to local victims.
- **Eastern European/Russian Campaigns:**
  - Russian (2.71%) is a prominent secondary language, indicating a major campaign focus on Eastern European countries or global Russian-speaking populations. This volume suggests dedicated, high-effort campaigns rather than sporadic test runs.

Low-Volume and Test Distributions

The findings also reveal something about the 1.47% denoted as “Others.” This category typically includes numerous low-volume languages (eg, various Asian, African, and smaller European languages) that do not meet the threshold for individual tracking. Their presence often indicates:

- **Testbeds:**
  - Threat actors using small distributions to test the efficacy of new malware or social engineering lures before a large-scale launch.
- **Highly Localized Attacks:**
  - Targeting specific expatriate communities or high-value individuals with tailored spear-phishing attempts.



Feature:
What Sender Sources Can Tell Us

When we look at the distribution of sender sources in Q3, we notice a plethora of creative techniques being used to evade detection and maximize delivery. Here are some insights into what those sources revealed:

33%
Compromised accounts

32%
Free Email Services / Free Relay Providers

25%
Third-party Senders

7%
Newly Registered Domains

3%
Others

Compromised accounts (33%):
These are hijacked but legitimate accounts. Attackers exploit trusted domains to bypass reputation checks. This allows them to slip through filters even when email authentication (SPF/DKIM) shows anomalies.

Free email services / Free relay providers (32%):
Nearly one-third of campaigns abused free services, and not only popular ones like Gmail, Yahoo, and Outlook, but also lesser-known free relays such as GMX, ProtonMail, Zoho, and Yandex.

These providers are attractive to attackers because they are widely trusted, easy to register, and harder to block without disrupting legitimate business traffic. What's more, free relay infrastructure gives adversaries the ability to quickly rotate accounts, lowering their operational costs while maintaining high deliverability.

Third-party senders (25%):
Bulk mailing services like SendGrid, Mailgun, and Amazon SES continue to be misused, either through fake sign-ups or compromised customer accounts. The reason is simple: their strong IP reputations make malicious campaigns more challenging to distinguish from legitimate business mailings.

Newly registered domains (7%):
Although they account for less volume, these domains are tactically effective. They represent disposable infrastructure built for short-lived campaigns that rely on speed before security teams denylist them.

Others (3%): The smallest portion of campaigns originated from botnets, misconfigured mail servers, or niche infrastructure.

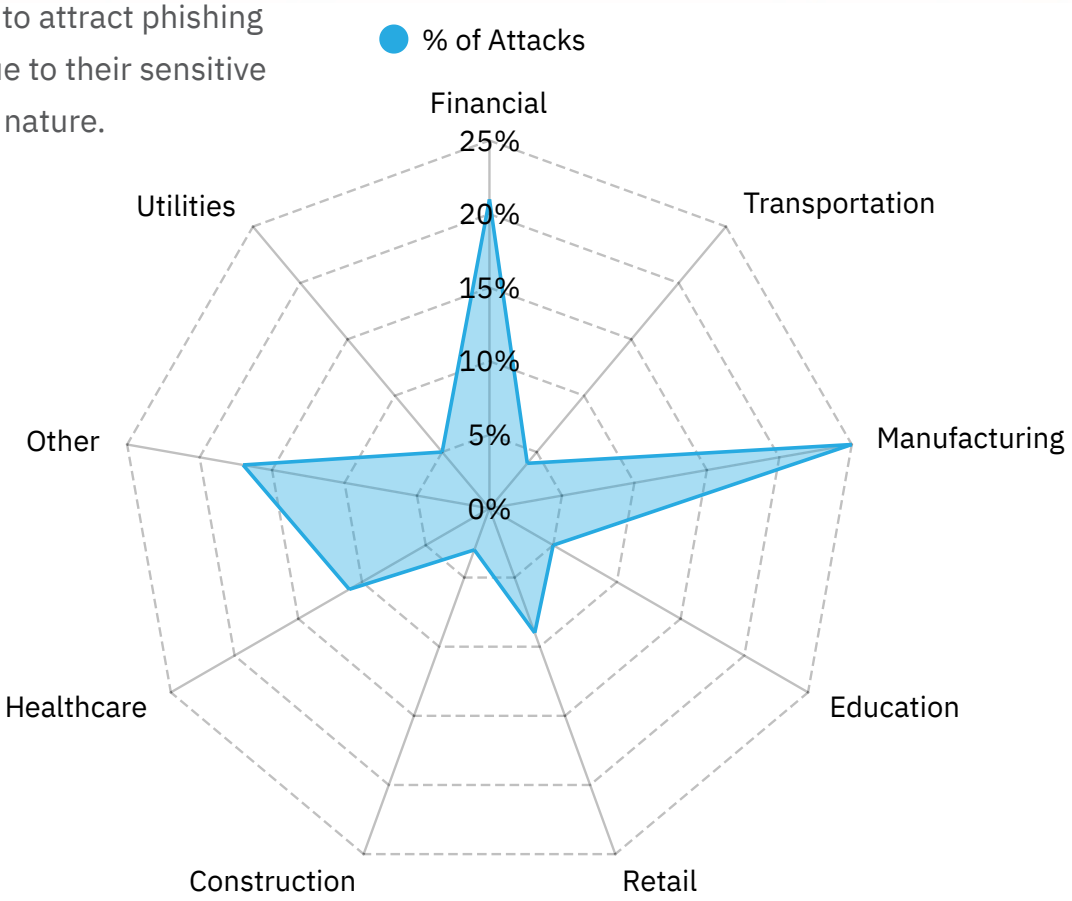
Top Targeted Sectors in Q3 2025

Which sectors were hardest hit by BEC, phishing, and malspam this quarter?

- **The Manufacturing sector (25%)** remained the most targeted, as it has been every quarter since our Q3 2024 report. Its continued vulnerability is attributable to complex supply chains and a necessary reliance on third-party vendors.
- **The Financial sector (21%)** followed closely, driven by attackers' focus on credential theft and fraudulent transactions.
- **Sectors such as Healthcare (11%) and Retail (9%)** continued to attract phishing and BEC campaigns due to their sensitive data and transactional nature.

Meanwhile, Utilities (5%), Education (5%), Transportation (4%), and Construction (3%) were also targeted, though at lower volumes. While seemingly insignificant, the fact that these are still making the list highlights the fact that critical services and industries of all sizes remain within threat actors' scope.

Additionally, a notable 17% of attacks fell into "Others", showing that adversaries aren't limiting themselves to the top targeted sectors—they're still opportunists at heart.



Feature:

Commercial Spam: Cold Outreach and List Bombing

While not inherently malicious, commercial spam took such a large share of the reported spam pie in Q3 (60%) that it deserves a closer look.

VIPRE analysis showed that cold outreach marketing emails dominated the category, accounting for 72% of observed cases. Second to that was a tactic known as list bombing, which took home another 16%.

Insights into Cold Outreach:

- **What is cold outreach?**
  A cold outreach marketing spam email is an unsolicited email sent to recipients who have had no prior interaction, relationship, or expressed interest with the sender.
- **How does it work?**
  The goal is usually to promote a product, service, or business opportunity, often in bulk campaigns. These emails often bypass opt-in requirements, ignore unsubscribe mechanisms, and target harvested or purchased email lists.
- **Why is it a problem?**
  Legitimate cold outreach (eg, sales or networking) can exist, but when it is sent at scale without consent, it crosses into spam. As we'll see with list bombing, even that can be a security concern.

Characteristics of Cold Outreach Marketing Spam Emails

Sent to large volumes of recipients without permission

- Mass distribution
- No prior relationship
- Unsolicited

Overly generic (not personalized to the recipient)

- Lack of name/company
- Vague language
- Irrelevant content

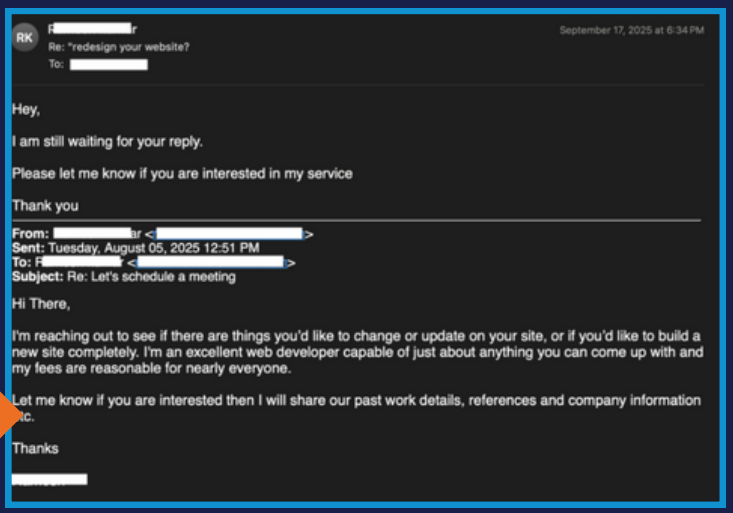
Focus on sales pitches, product promotion, or lead generation

- Direct selling
- "Buy Now"
- Sign up here

Often disguised as "business opportunity" or "professional networking"

- "Unlock potential"
- Exclusive invite
- Connect with us

Here's one example of a cold outreach marketing email VIPRE caught in the wild.



What You Need to Know About List Bombing

What is list bombing? This happens when a victim's email address is maliciously (or automatically) subscribed to hundreds or thousands of mailing lists, newsletters, or promotional sign-ups at once.

- **A Shotgun Approach:**
  Instead of one cold outreach spam message, the victim's inbox is "bombed" with marketing emails from legitimate companies they never signed up for.
- **How It Works:**
  Attackers usually abuse automated newsletter signup forms or "refer-a-friend" systems that don't require proper verification (weak or missing CAPTCHA, no double opt-in).
- **Malicious Intent:**
  Often used as a smokescreen to hide important messages (eg, a password reset or fraudulent account activity alert gets buried under the flood of spam)

Although commercial spam in and of itself doesn't log as inherently "bad," the way attackers are leveraging it definitely puts it in that category. It's like a DDoS for the brain; when humans are inundated with so many spammy commercial emails, important things (that attackers are trying to hide) get missed as we eventually "shut down" or fail to see.

Words to Watch

Cold Outreach	List Bombing
"Exclusive offer"	"Confirm your subscription"
"Special promotion"	"Verify your email"
"Let me introduce myself"	"You are now subscribed"
"increase your revenue"	"Weekly Digest"
"Boost your sales"	"Thank you for registering"
"Trusted by industry leaders"	"Your account has been created"
"Act now!"	"Unsubscribe here"
"Lead List/Contact Database"	"Manage subscription"

How Does List Bombing Affect a Business Email Setup?

Inbox Overload

- Employees (especially executives or finance teams) may be flooded with irrelevant emails, securing missed or delayed.
- Important business emails (e.g., invoices, contracts, securities) missed or delayed.

Security Risks

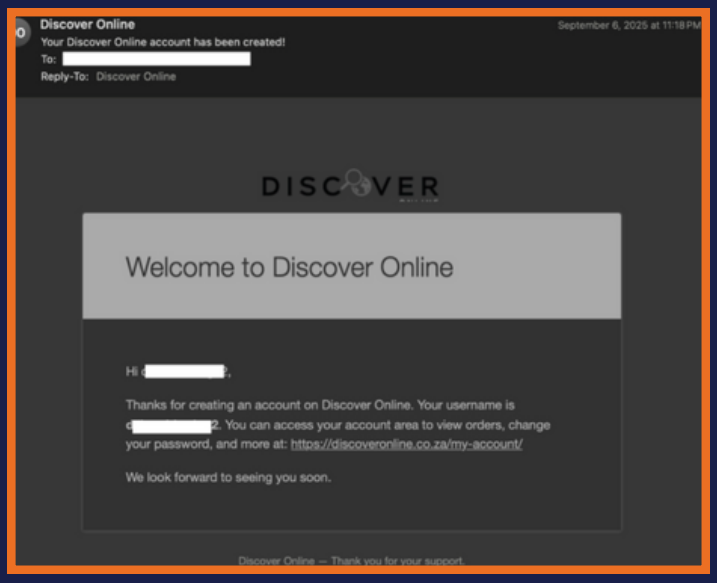
- Attackers may use listbombing to distract the true target while carrying fraud or account takeover.
- Example: A victim's inbox gets spammed, hiding a bank alert email about unauthorized transfers.

Reputation Damage

- If a business's web forms are abused to send listbomb spam, its domain/IP may get flagged by spam filters, lowering deliverability of legitimate business emails.

Resource Drain

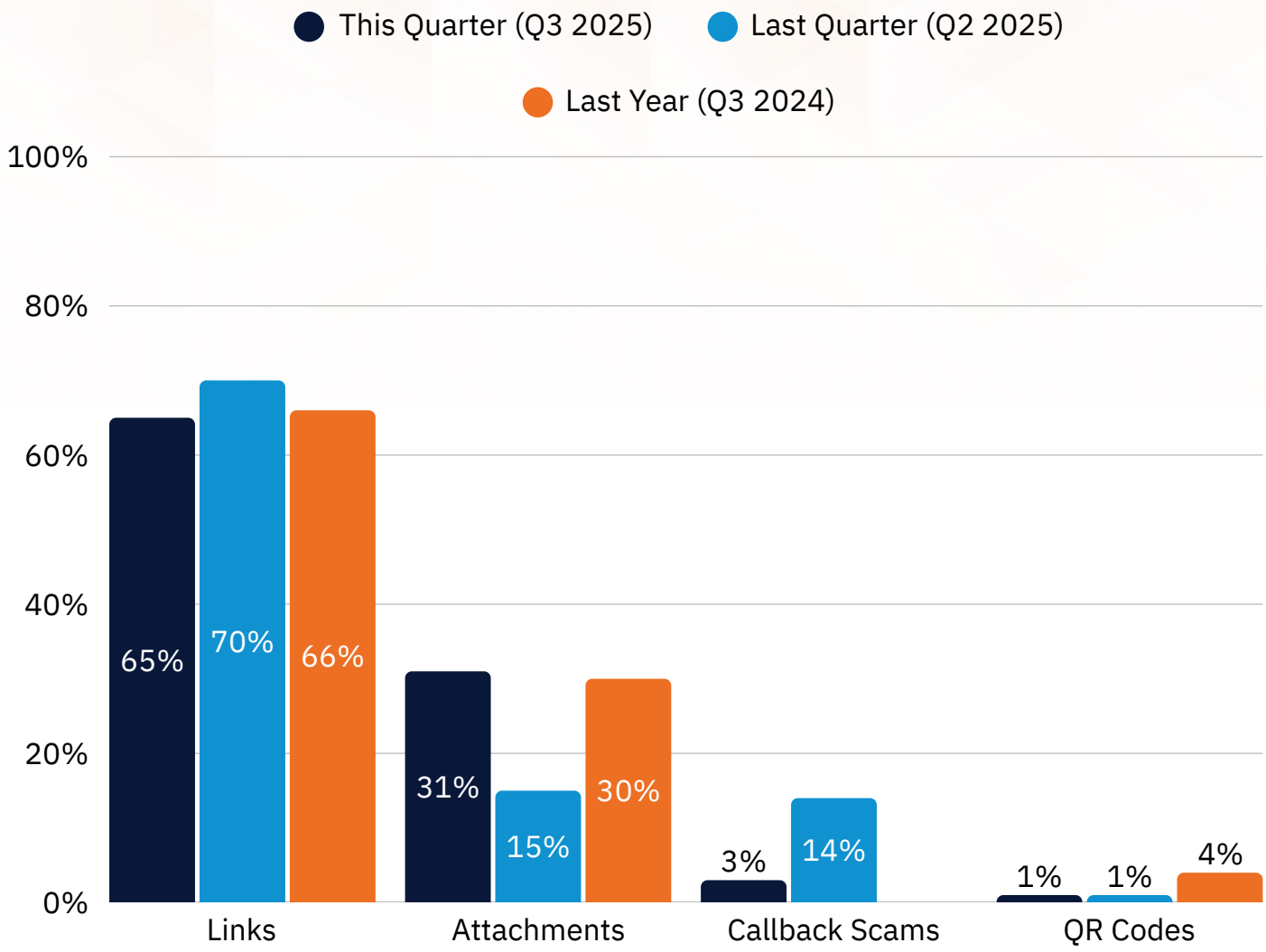
- Email servers must process a sudden spike in traffic.
- Email servers must handle surges in traffic, which affect performance.
- Employees waste time sorting through junk emails.



Phishing

A side-by-side comparison best illustrates the trends in the key phishing metrics we track every quarter. Keeping an eye on the moving target helps us predict what and where attacks will strike next.

Phishing Types



In Q3, malicious links continue to be the primary delivery mechanism for credential harvesting and malicious redirection. But the presence of callback schemes is not to be ignored; though usage has dipped sharply since last quarter, they are still used in brand spoofing attacks as trusted names get users on the phone.

Spoofed Brands

Trend: Most Spoofed Brand	This Quarter (Q3 2025)	Last Quarter (Q2 2025)	Last Year (Q3 2024)
#1	Microsoft	Microsoft	Microsoft
#2	McAfee	Google	Docusign
#3	PayPal	Amazon	Google

Attackers continue to exploit **Microsoft's** popularity and trust to trick victims into giving up credentials or access— especially around cloud services and authentication.

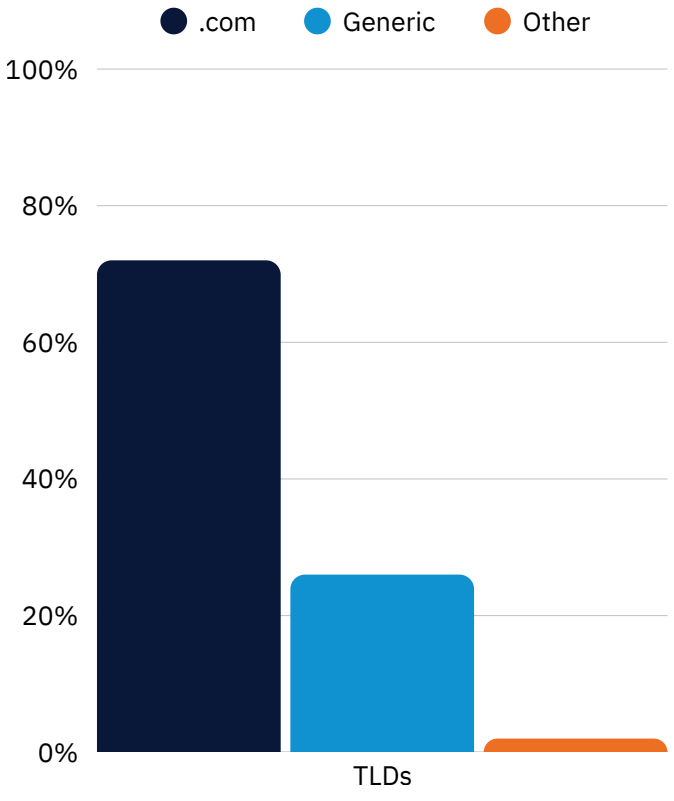
Notably, both **McAfee** and **PayPal** were heavily abused in callback phishing campaigns, where victims are tricked into calling fake customer support numbers that ultimately lead to credential harvesting or financial fraud.

The **other spoofed brands**—like Facebook, Netflix, Spotify, GeekSquad, eBay, Norton, Adobe, Apple, DocuSign, Twitter, and Zoom—are typically selected because of their widespread global user bases and high levels of user trust, making them effective lures across a variety of phishing campaigns.

Top-Level Domains (TLDs)

Attackers are diversifying their domain choices, making use of both country-code domains and a wider pool of miscellaneous TLDs.

- **.com – 72%** Still the most abused TLD in phishing due to its global recognition, trust among users, and ease of availability. Its strong dominance underscores how attackers exploit user familiarity with .com to make malicious links appear legitimate.
- **Generic Country-Code TLDs (ccTLDs) – 26%** Includes domains such as .uk, .fr, .se, .cn, .de, .it, .ie, .ca, .nz, .dk, .us, etc. These are commonly used in geographically targeted phishing campaigns or to impersonate local companies and institutions.
- **Other TLDs – 2%** Encompasses low-cost or less regulated TLDs like .info, .site, .online, .live, .tech, .pro, .cloud, and .ai. While smaller in volume, they remain noteworthy due to frequent abuse in short-lived campaigns



How Phishing Slips Under the Radar

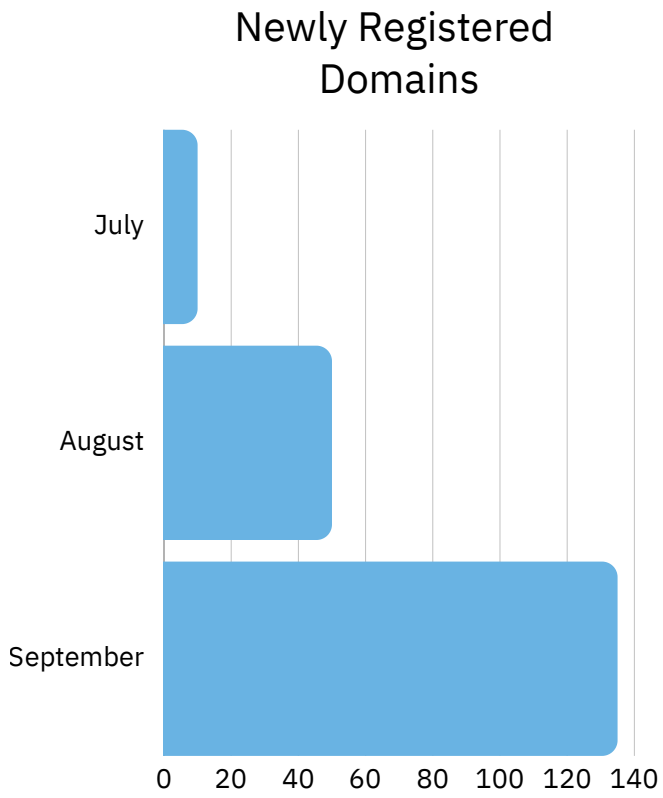
Using Q3's top TLDs as a jumping-off point, the consistent prevalence of ".com" says something: attackers stick with what users trust most. And it works.

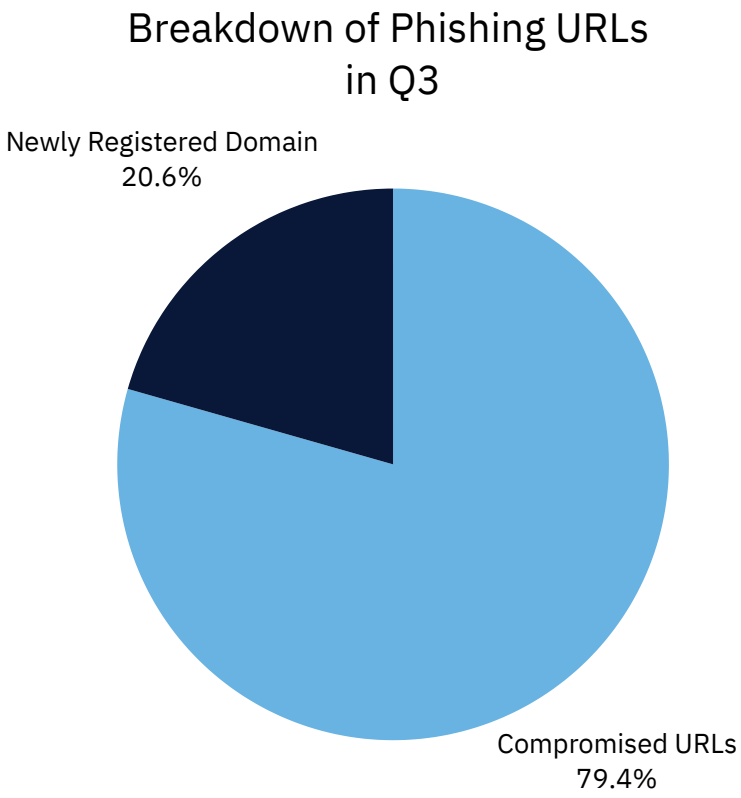
Top-line themes from our subsequent domain analysis reveal that traditional defenses based on deny listing and reputation are increasingly inadequate. This underscores the fact that modern phishing defenses require real-time behavioral analysis, user education, and mandatory MFA to prevent credential compromise from leading to account takeover.

In other words, today's enterprises need a new radar to catch increasingly slippery phish.

A Clean Bill of Health: NRDs and Open Redirects

Newly Registered Domains (NRDs): We witnessed a threefold increase in NRD creation between July and August, and then again between August and September. Threat actors are registering large numbers of these domains to launch temporary phishing sites, then quickly deactivating them once discovered to evade detection and denylisting.





Compromised URLs (Open Redirects): Despite the viability and success of NRDs, attackers still favored Compromised URLs to do their phishing dirty work nearly 80% of the time; NRDs were used for the other 20%.

Why are compromised accounts so successful?

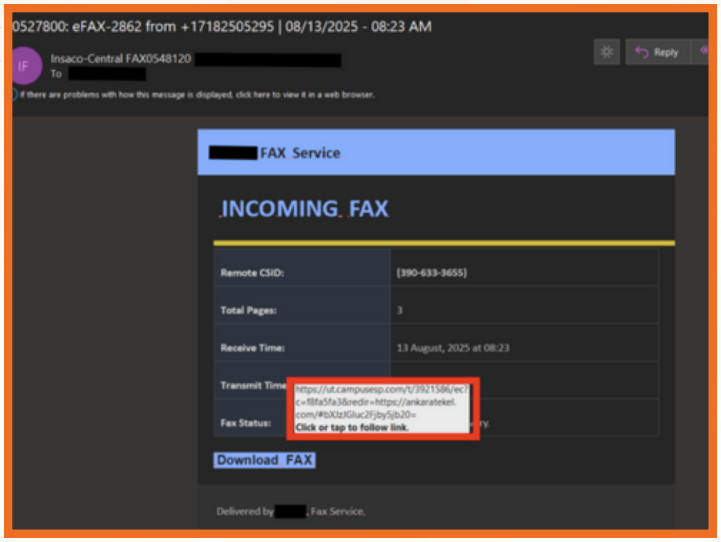
1. **They leave no trace as these URLs refer to legitimate web addresses** (that have been co-opted for nefarious purposes).
2. **An open redirect attack involves a mostly clean URL** that starts with the legitimate domain but appends a parameter that instructs the server to redirect the user to a different, malicious destination.
3. **This method uses the trusted domain's reputation** to trick users into clicking what they believe is a safe link.

Typo Squatting: This tried-and-true method still takes home a sliver of the pie. It relies on common misspellings or variations of popular, legitimate websites. The goal is to capture traffic from users who make typing errors when entering a URL into their browser.

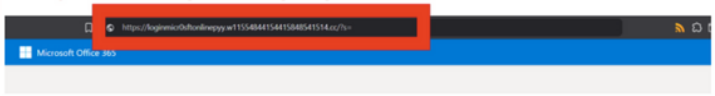
These under-the-radar forms of phishing can all evade typical detection mechanisms that scan only the top URL, don't sandbox all links, or fail to recognize malicious behavior. This is why they are so widely used.

Direct malicious links are easily caught by standard email security tools. Without more advanced protections, however, most phishing links would slip through undetected.

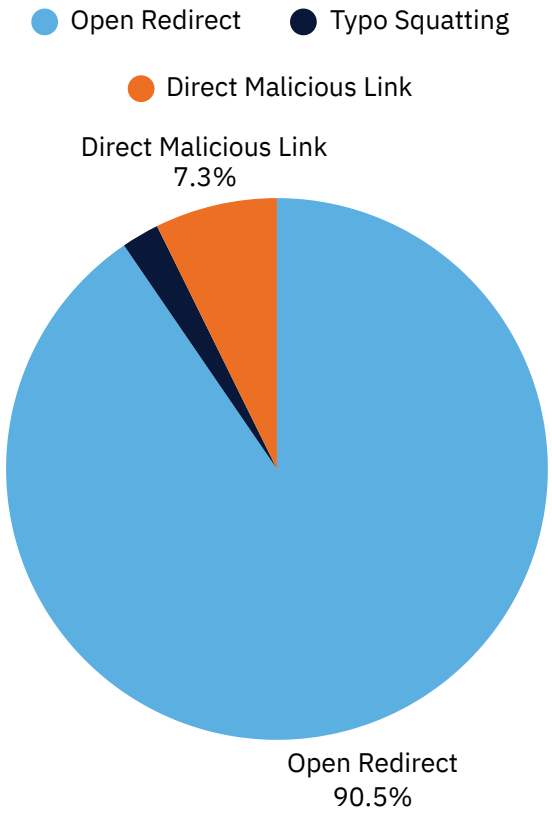
Example of Open Redirect Phishing Link



Example of a Typo Squatting Phishing Page



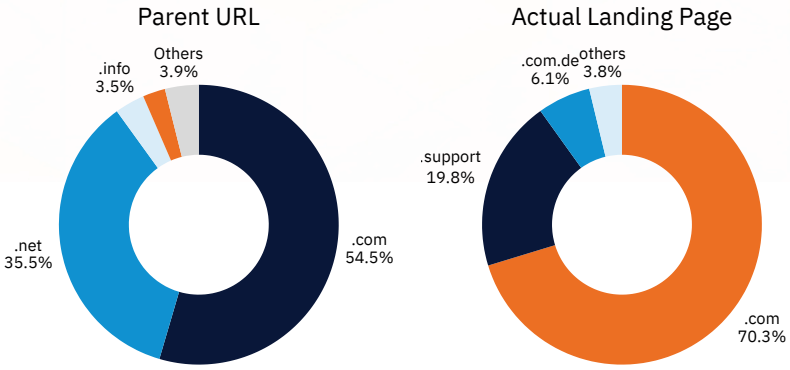
Phishing Link Delivery



Burying the Lead

Attackers also see success with a variation of the process described above. By splitting the Parent URL from the Landing Page in a multi-step process, attackers hide the malicious Landing Page from both users and security scanners.

By the time a scanner analyzes the Parent URL, the user may have already been passed along to the actual phishing site.

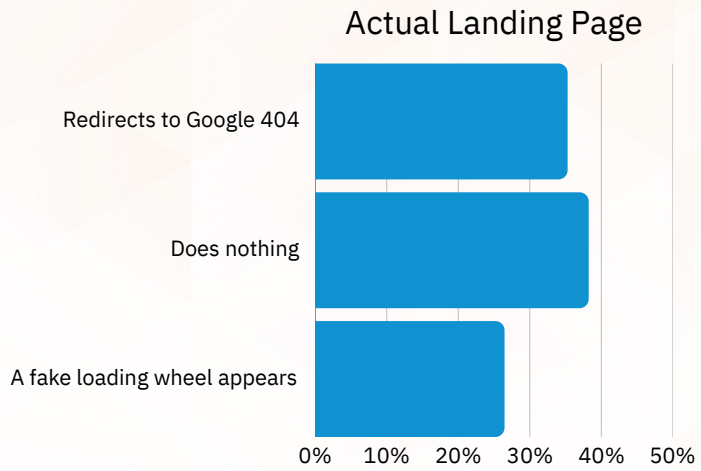


Cut and Run

What happens after a phishing attack? After a phishing page steals your credentials, its main goal is to get rid of you without raising suspicion. Our analysis revealed a fairly even split between 3 malicious actions this quarter:

- **Redirect to a Google "404 error", making you think it was a broken link**
- **Show a fake loading wheel, making you think the network is slow**
- **Do nothing, making you think the site is frozen**

These tactics cause users to blame a simple tech problem rather than a scam, giving the attacker time to use their stolen password.

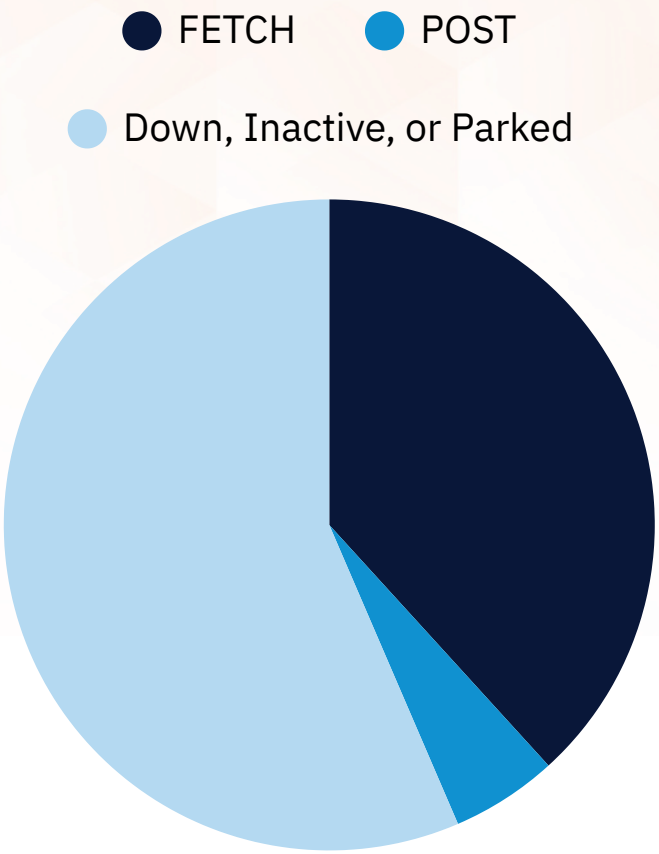


The (Literal) Takeaway: Credential Harvesting

The goal of every phishing campaign is to attain data not previously in the attacker's possession: data exfiltration. To maximize returns, attackers must be strategic. When it came to taking the data home this quarter,

- **One-third used Fetch API:** A modern, powerful, and flexible JavaScript interface for making network requests. While it can execute POST requests, its capabilities are far more extensive, making it a preferred tool for sophisticated attacks.
- **Under 10% used POST:** A standard HTTP request type designed to send data to a server, typically to create or update a resource. In malicious applications, such as phishing or form-grabbing malware, POST is the fundamental mechanism for data exfiltration.

Credential Harvest Method



And 90% targeted either Outlook or Google mailboxes. Our Q3 data showed Outlook and Google being targeted in over 90% of phishing attacks, with each one absorbing slightly less than half. This indicates that attackers are prioritizing access to the two largest business and personal email ecosystems and hoping to save time in the process.

Fewer targets mean less research and customization.

Phishing Attachments

Analysis of the Q3 2025 phishing attachments reveals a strategic balance between reliability and evasion, with attackers using trusted file types while simultaneously experimenting with alternatives to bypass security filters.

PDFs overwhelmingly dominate, with three out of four of all malicious attachments. Attackers favor them because they're universally trusted as legitimate "business documents".

The remaining attachments are spread across eight file types (EML, HEIF, HTML, GIF, SVG, ICS, PPTX, BMP). This serves two purposes: evading security systems that don't thoroughly scan uncommon formats, and using files like .eml and .html as secondary delivery mechanisms that launch phishing pages rather than directly containing malware.

Unsurprisingly, attachment names cluster around high-urgency business scenarios:

- **Financial: "ACH_Deposit_Form.pdf", "EmployeePayrollCompensation.pdf"**
- **HR/Benefits: "Benefits Enrollment.pdf", "Employee Records.eml"**
- **Confidential: "Confidential_HR_Report.pdf", "Company Alert.pdf"**

Callback Phishing Evolves to Attachments

All in all, Phishing defenses require real-time behavioral analysis, user education, and mandatory MFA to prevent credential compromise from leading to account takeover.

Spotting Callback Phishing Emails: A Guide

Sender Indicators

- Suspicious sender address (ee, free we webmail)
- Lookalike/spoofed domains (ee, mcafee-support@secure-mail.com)
- Compromised accounts (SPF/DKIM/DMARC failures)

Email Content Indicators

- Urgency/Scare tactics (“Immediate” action)
- Generic greetings (“Dear Customer”)
- Callback instructions (Phone#/attachments, vague details to services)

Email Content Indicators (duplicate title, different box)

- Callback instructions (Phone # in order # body #, unknown services)

Attachment & Link Indicators

- Attachents containing phone numbers
- Unisual file types to “support” sites (Malicious URLS)

Attachment & Link Indicators (duplicate title, different box)

- Attachents containing phone numbers (PDFs, images, .ics)
- Links leading to “support” sites

Technical Red Flags

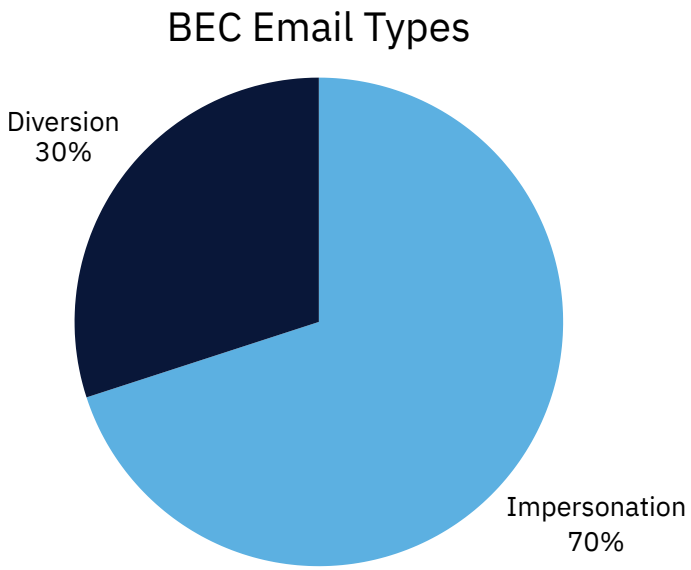
- Mismatched headers (“From” vs. “Return-Path”)
- Abnormal sending infrastruter services
- Recent domain registration (Newly created)

Top BEC Trends

In Q3, the majority of scams reported to VIPRE were verified as BEC, comprising 51% of all malicious emails observed. This majority has held up as a trend since last year.

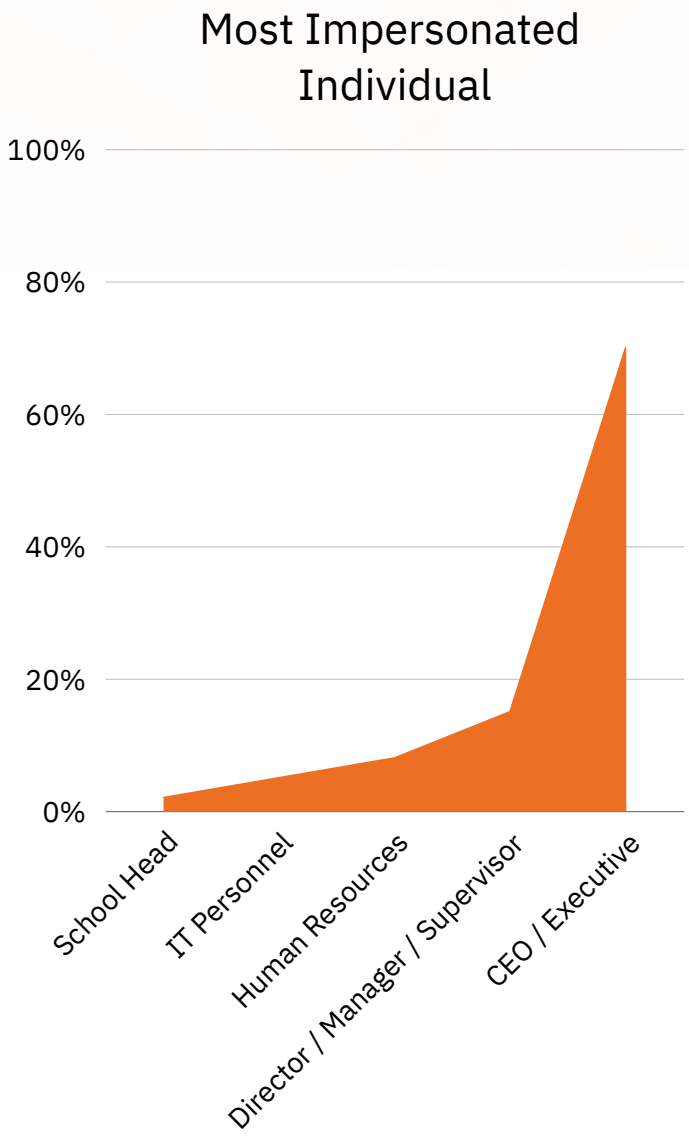
Impersonation Over Diversion

Impersonation remains the tactic of choice in Q3, with 63% of all BEC attempts attributed to it. This demonstrates threat actors' continued preference for social engineering tactics over technical exploitation, as they rely on trust and authority to manipulate victims. Increasingly, they attempt to take the conversation off email to non-monitored channels such as WhatsApp.



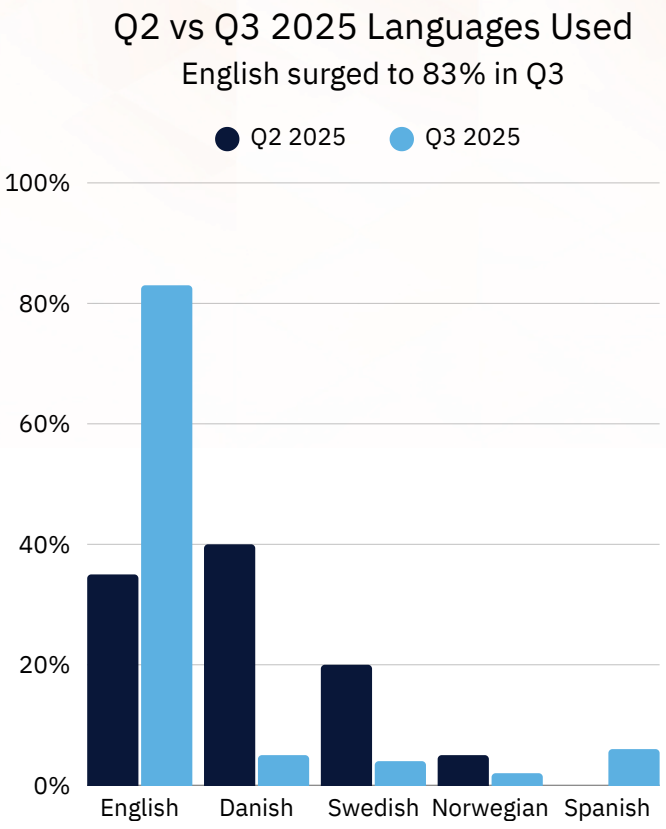
CEOs Remain Most Impersonated

Impersonation remains the tactic of choice in Q3, with 63% of all BEC attempts attributed to it. This demonstrates threat actors' continued preference for social engineering tactics over technical exploitation, as they rely on trust and authority to manipulate victims. Increasingly, they attempt to take the conversation off email to non-monitored channels such as WhatsApp.



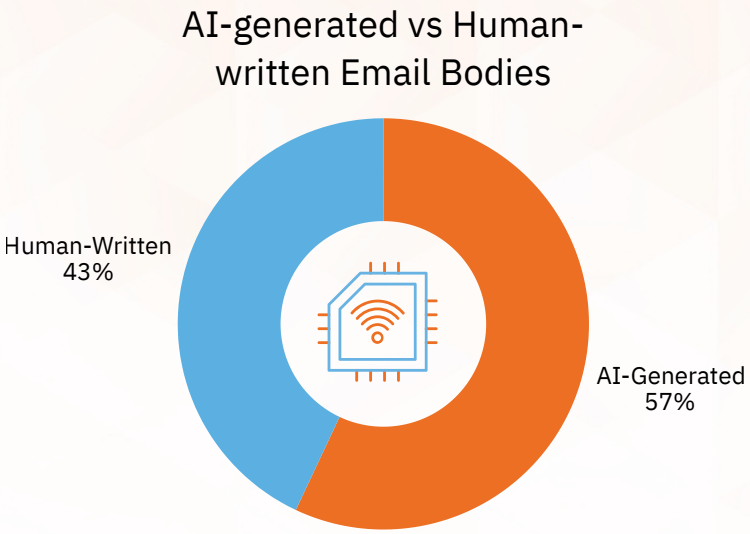
English is Still the Weapon of Choice

In our Q3 BEC samples, English overwhelmingly dominated, accounting for 83% of the total share—an interesting leap from Q2, in which it accounted for less than half.



While these figures reinforce English as the primary global business language and therefore offer attackers the best reach, the presence of other languages offers insights as well.

- **Spanish (8%)** – Attackers target organizations in Spanish speaking regions, particularly in financial and retail sectors.



- **Swedish (6%) and Danish (3%)** – This points to a small but continued focus on Nordic enterprises, where attackers may exploit local business norms, fiscal deadlines, or supplier relationships.

This shows attackers are tailoring campaigns to specific geographies to appear more legitimate.

AI-Written vs. Human-Written BEC

A significant portion of the analyzed emails were AI-generated, indicating that threat actors are increasingly using automated content creation to make spam and phishing messages more convincing. This reflects a shift toward more scalable and sophisticated email threats.

Malicious Emails

In Q3, 100% of all malspam used links instead of attachments. This reflects the ongoing shift by threat actors to bypass email gateway defenses.

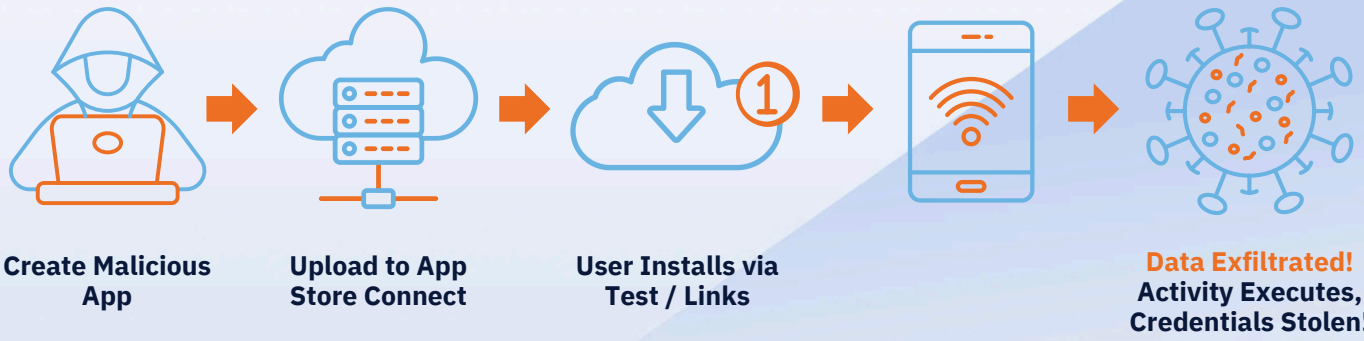
While phishing and BEC emails bode no good thing, malware spam (malspam) emails are openly and aggressively malicious. Though malspam only accounted for 2% of all spam types observed, it remains a significant threat due to its payload delivery methods.

Apple TestFlight Co-opted to Distribute Malware

What We Observed: Threat actors are leveraging Apple's TestFlight beta distribution platform to deliver malicious iOS builds to targeted users.

How It Works: Since TestFlight is designed for pre-release testing and operates via invite links (or public TestFlight links), attackers can sidestep the standard App Store review process and distribute apps outside of Apple's typical security controls.

Apple TestFlight Attack Flow



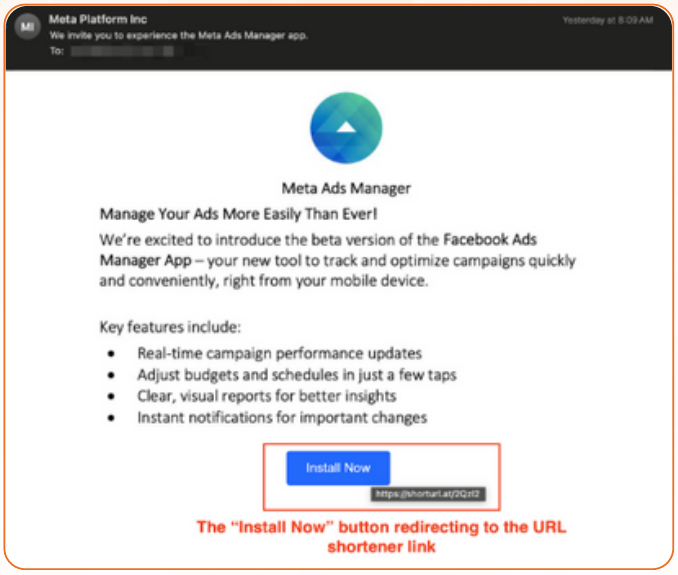
As Seen in the Real World

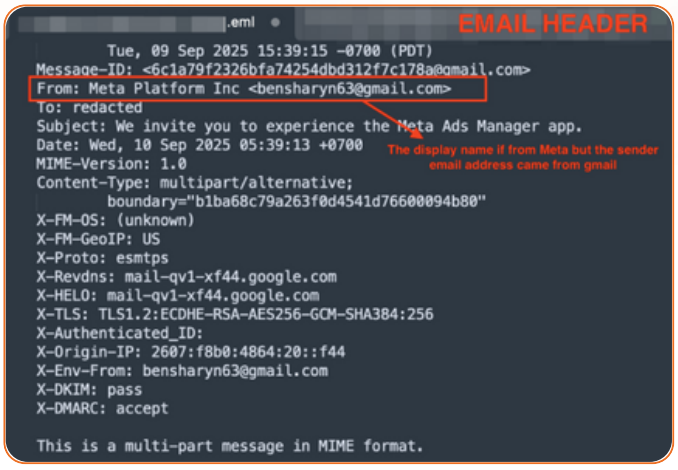
- **Malicious iOS apps were distributed** via TestFlight by sending convincing invitation emails impersonating legitimate vendors—in this case, Meta Platforms Inc.
- **Attackers utilized legitimate mail infrastructure** (such as personal Gmail accounts or bulk-mail services), URL shorteners, and TestFlight invite links (https://testflight.apple.com/join/...) to evade basic email filters.
- **Threat actors socially engineered victims** into installing harmful beta builds.

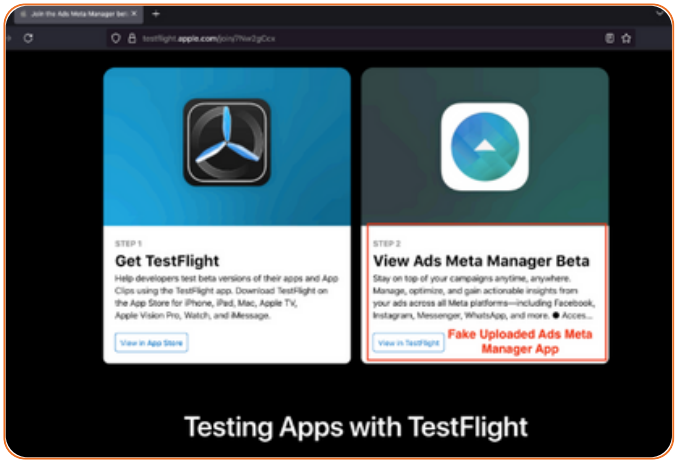
The Impact: These builds can steal data, deliver secondary social-engineering payloads (eg, malicious MDM profiles), or act as iOS trojans exfiltrating sensitive information, including biometric data and banking credentials.

Who Is Responsible: This technique has been attributed to sophisticated threat groups, including Chinese-speaking actors.

What to watch out for:







The PDQ RAT

What We Observed: Links leading to downloads of PDQ RAT, a Remote Access Trojan that enables attackers to remotely control infected machines and exfiltrate sensitive information.

How It Works: Basic social engineering tactics like creating urgency and sending from legitimate-looking sources to get users to click embedded links and download custom installers.

As Seen in the Real World:

- **Malicious spam emails** attempted to lure victims with themes such as payroll updates, UKVI (United Kingdom Visas and Immigration) notices, and “secure document” reviews.
- **The links redirected users to download installers** tailored to their environment—typically MSI files for Windows systems and PKG files for macOS systems. This adaptive delivery method demonstrates the attackers’ efforts to increase infection success rates across platforms.

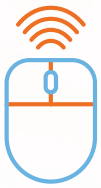
The Impact: The PDQ RAT was responsible for stealing sensitive user information, spying on victim machines, and providing attackers with remote control capabilities.

Step 1

Delivery - Malicious Spam Email

Step 2

Deception - Legit-looking link + Urgency



Step 3

Execution - Download of MSI / PKG Installer

Step 4

PDQ RAT Control & Data Theft

The Final Say

Q3 2025 reveals a threat landscape defined by strategic sophistication rather than technical complexity. The 13% year-over-year increase in malicious emails tells only part of the story. What matters most is how these attacks succeed.

Attackers have mastered the art of blending in. They're combining multiple tactics into single, cohesive attack chains:

- **Trusted Parent URLs mask compromised Landing Pages**
- **Newly Registered Domains bypass reputation filters**
- **Legitimate platforms like TestFlight distribute malware under the guise of beta software.**

Meanwhile, the 60% surge in commercial spam creates the perfect smokescreen, desensitizing users to malicious messages hidden among the noise.

BEC remains the dominant threat at 51% of all scams, precisely because it exploits human psychology rather than technical vulnerabilities. When attackers impersonate your CEO and move conversations to WhatsApp, traditional email defenses become irrelevant.

The lesson is clear: signature-based detection and static denylists are no longer sufficient. Organizations need layered defenses that combine behavioral analysis, real-time sandboxing, and AI-driven detection to identify threats that traditional tools miss.

As attackers continue experimenting with new evasion techniques, the question is not whether your defenses can catch known threats. It's whether they can adapt fast enough to catch the ones being invented right now.

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

Email Threat Trends of 2025