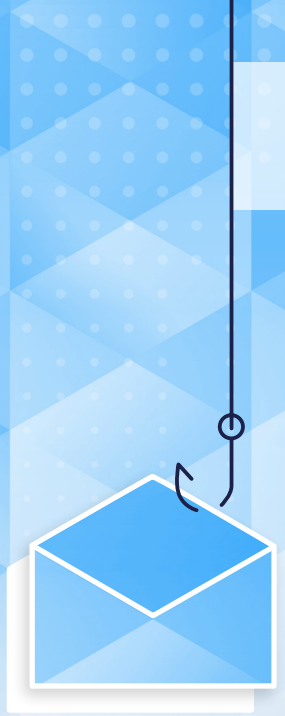
VIPRE SECURITY GROUP



Email Threat Trends Report: 2025: Q2

An Expert Look at Email-Based Threats

Contents

Executive Introduction

We have seen it coming for a while. And now it's crystal clear. The trend towards human-centered attacks is established, and we are seeing the data to prove it.

Attackers are very much favoring social engineering schemes as their tactics evolve, using technology to deceive us rather than dupe our technological defenses.

From diversified forms of phishing to mining the ever-giving BEC cash cow, adversaries are just getting started when it comes to using technology in new and human-proof ways. Employees are faced with a difficult choice every time they open their inbox – to click or not to click – and hold the well-being of their organizations at the tips of their fingers.

It is important to define these human-centric trends so that organizations know which way to invest and how to adjust their strategy. There may be a lot of hype in the news about sophisticated new forms of attack, advanced ransomware, and more. But when we look at the vast majority of threats and how they are getting in, the smart money says invest in what will give you the biggest bang for your buck. In other words, categorize the risks, and prioritize accordingly.

Right now, those are email-centered attacks, and specifically ones that slide past traditional signature-based defenses with apparent ease. You can't train your employees enough to keep up with AI-based dupes at scale. But by understanding the types of social engineering scams out there, you can know where to act next and with what solutions.

Every quarter, VIPRE sounds the alarm with data-driven anomalies we see in our customer landscape. With over 25 years of experience and insights gained from round-the-clock detection worldwide, we make it our mission to share with the community what we've found. And once again, the VIPRE Email Threat Trends Report is published to inform global cybersecurity professionals of the trends, techniques, and attacks only someone with our vantage point can see.

We encourage you to review this report and take the action you see fit.

5 Biggest Takeaways From Q2 2025

We track trends to see where attackers are heading. Our Q2 2025 data leads us to emphasize some significant happenings that represent a departure from this time last year and even last quarter. And, just as interesting, certain pieces that refuse to move.

1. Manufacturing and Retail – Still Top Targets for the Second Year in a Row

Last year in Q1, Manufacturing overtook Finance in an upset no one saw coming. Unfortunately for the world's manufacturers, they have stayed in the lead ever since. The trend continues to this day, six consecutive quarters later.

Last year, attacks against Manufacturing increased by a staggering 71%. This year, our data show that the Manufacturing sector suffered the most email attacks in Q2 (26%) across a range of vectors, including BEC, phishing, and malspam – you name it. Close behind (as in last year and the last quarter) was Retail (20%), followed by Healthcare (19%).

The fact that Manufacturing received the highest number of email-based attacks aligns perfectly with its current landslide of cyberattacks in general. When we look at the latest Verizon 2025 Data Breach Investigations Report, we note that phishing was the initial access vector in 16% of all cases; credential theft came in with the most at 22% with vulnerability exploitation taking second at 20%.

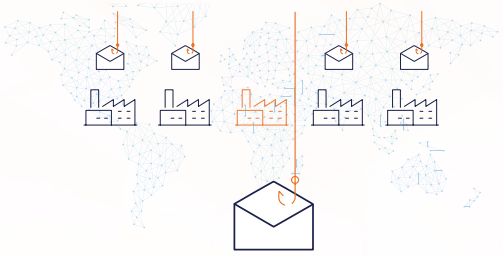
This would indicate that phishing is a significant, but not the largest, issue. However, when you consider that phishing is a major factor in threat actors obtaining stolen credentials in the first place, you see how much of a problem it really is.

By tamping down on email-based threats, the manufacturing sector could drastically reduce its number of cyber compromises overall.

2024 / 2025

MANUFACTURING

sector hit hard with attacks



Attacks increased by

71% last year

MANUFACTURING SUFFERED THE MOST ATTACKS IN Q2

EMAIL ATTACK BREAKDOWN

Credential Theft	Vulnerability Exploitation	Phishing Emails
22%	20%	16%

2. Phishing Kits are Out. Customized Deployments are In

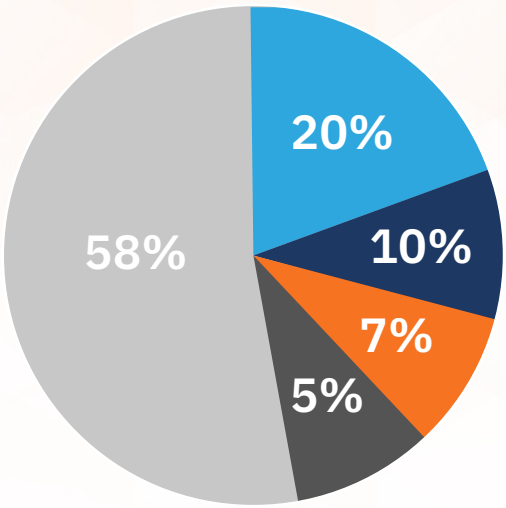
For digital "ages," phishing kits have been a powerful way to propagate malicious campaigns at scale. This quarter, it's no surprise that we continue to see them, underpinning a substantial number of phishing sites.

- **Evilginx (20%)**
- **Tycoon 2FA (10%)**
- **16shop (7%)**
- **Other generic kits (5%)**

However, what was surprising was that more than half (58%) of the phishing sites we analyzed this quarter did not use identifiable phishing kits. Indicating a trend towards custom-made or obfuscated deployments, this shift is something we anticipate seeing more of in the future.

Phishing-as-a-Service tools have their pros and cons; while a great way for low-level hackers to launch spray-and-pray campaigns at low cost, they are also established pieces of software that can be reverse-engineered, tracked, and caught. A bespoke phishing deployment doesn't run the same risks, and thanks to AI, even those are affordable, too.

Phishing Kits Breakdown



58% Did not use identifiable phishing kits

20% Evilginx

10% Tycoon 2FA

7% 16shop

5% Other generic kits

3. Call Me Maybe: Callback Phishing

Callback phishing scams are a dark horse that first appeared in our crosshairs only last quarter. Sighted in the wild since 2021, callback scams had yet to make our "list" of top phishing vectors.

In Q1 2025, that changed, with this once-obscure method rising to take responsibility for 16% of phishing attacks overall. For context, malicious attachments took the first spot at 50% and links accounted for 32%.

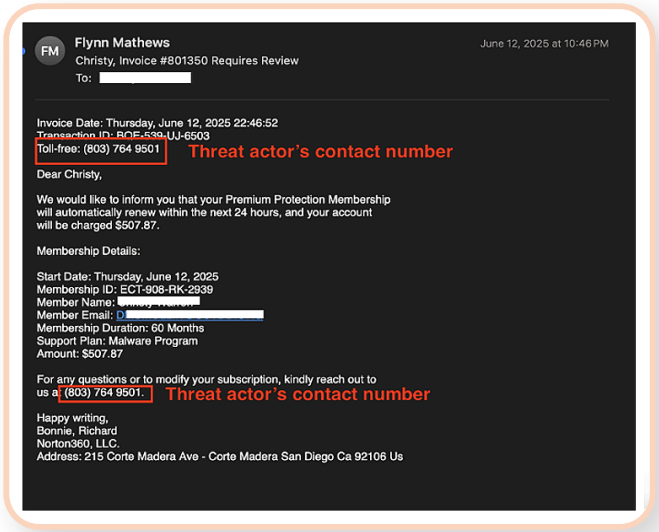
This quarter, the trend continues. Callback scams keep their spot as the third most prevalent phishing type in Q2 2025.

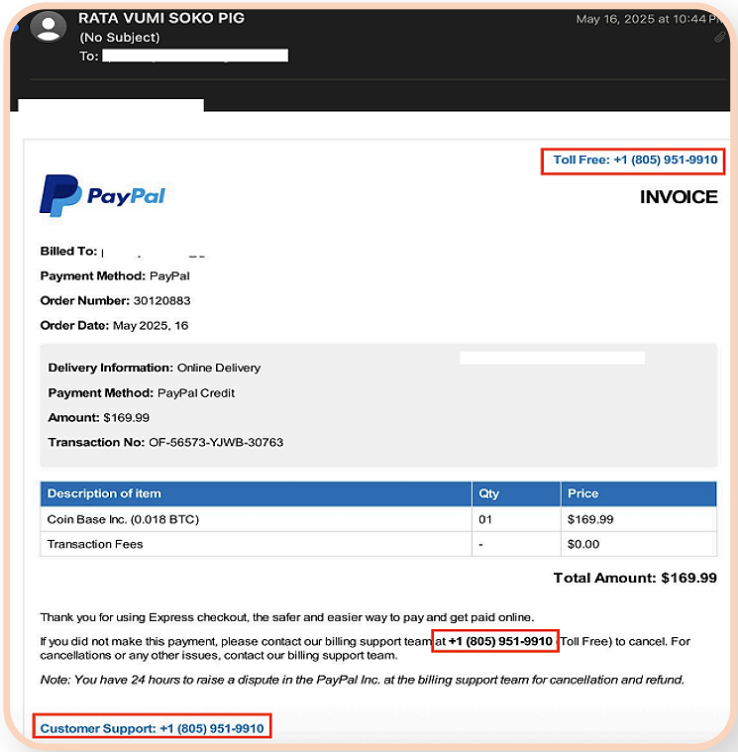
For the uninitiated, callback scams "[are] a social engineering attack that tricks the recipient into calling a phone number included in a deceptive email," to quote our last report. Also referred to as TOAD attacks ("telephone-oriented attack delivery"), these ploys lean on lies like:

- **You bought something, sending a fake confirmation for a payment never received**
- **You didn't buy something, because your payment didn't go through**
- **Your subscription is due for renewal, along with a handy link to renew it**

As in all phishing scams, they rely on a sense of urgency and seek to pique the user's curiosity, fear of missing out, or sense of panic. The trick here is that they get you to call them, thereby evading the need to send a malicious link or attachment (that could get caught). Instead, once they have you on the phone, they can help you navigate to a site where they can "resolve the issue," or take personal details upfront so they can do it themselves.

Check out these callback scams in action:





4. BEC Targets Scandinavia

Executives Are Always a Top Target

Cited often for its high yield (adjusted losses over $2.9 billion, compared to ransomware's paltry $59.6 million), BEC scams are high on attackers' priority lists for the damage they can do and the rewards they can bring.

In this quarter's report, BEC accounted for 42% of scam emails overall, leaving all other forms (Diversion, Email Hijacking, Account Takeover) to account for the remaining 58% combined.

Like last quarter, the majority of BEC scams were launched via impersonation attacks — nearly eight out of ten BEC emails (78%) were an impersonation attempt. And, like last quarter, executives are still the favorite to impersonate.

In Q2, the "impersonation breakdown" looked like:

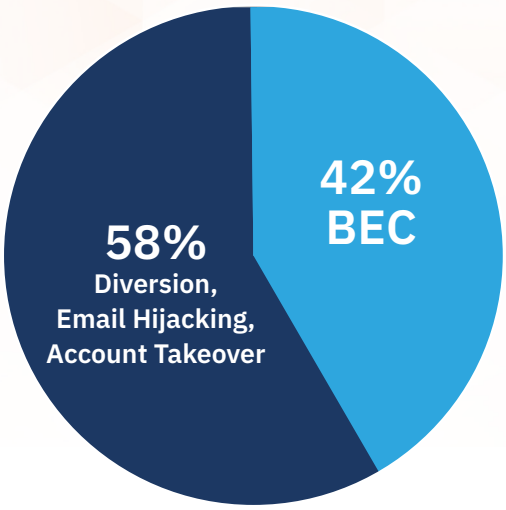
- **CEO/Executive: 82%**
- **Director/Manager: 9%**
- **Human Resource: 4%**
- **IT Personnel: 3%**
- **School Head: 2%**

BEC Scams Target English, Danish, Swedish, and Norwegian Speakers

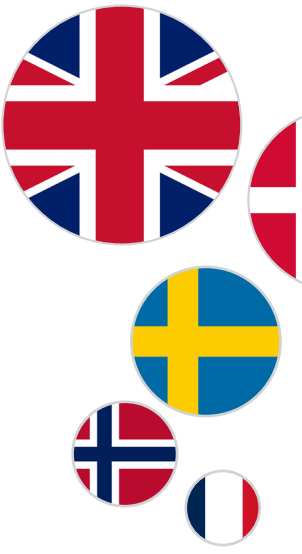
On closer examination, we see that executives in a few select countries were targeted the most.

- **English accounts for 42% of BEC samples**
- **Danish takes home 38%**
- **Swedish and Norwegian BEC scams make up 19% collectively**

Type of scams this Quarter



The percentage of BEC scams is so prevalent that these figures likely had the power to sway the whole. Overall, our figures indicated that the top five languages targeted the most by any type of email spam this quarter were:



72.3% English
11.9% Danish
3.8% Swedish
1.5% Norwegian
0.7% French

The notable use of Danish, Swedish, and Norwegian in BEC emails reflects a strategic shift by threat actors towards regional targeting and language localization.

While users in these regions are often proficient in English, corporate communication, especially within HR, finance, and executive teams, is often conducted in the native language. Leveraging this, attackers craft emails that closely resemble internal correspondence, boosting credibility and dramatically increasing the chance that someone will click.

We also have to consider the financial and digital maturity of Scandinavian nations. Scandinavia is home to some of the world's most digitized and economically stable economies, making them highly attractive targets for threat actors looking to exfiltrate wire transfers or sensitive financial information.

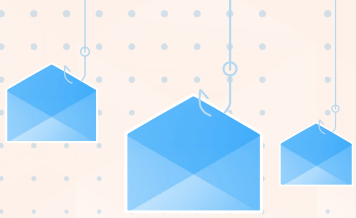
This deeply informed targeting demonstrates how adversaries are evolving their methods and combining cultural context, industry relevance, and linguistic familiarity to bypass traditional security measures and dupe employees on the front lines.

BEC Pick Up Lines: Don't Fall for Them

Lastly, with so many warnings about BEC scams, why are we still falling for them? Maybe because these little phrases know how to hit us where it hurts. Check out these BEC subject lines we saw trending last quarter:

- **Account change**
- **Are you available now?**
- **Fwd: need a response**
- **Immediate attention required**
- **Office task details**
- **Outstanding invoices report**
- **Payroll adjustment**
- **Please treat as urgent!**
- **Quick availability check for brief discussion**
- **Quick response**

Note the use of the words "quick," "immediate," and "available," not to mention anything having to do with payroll and invoicing reports. Needless to say, when you see these seemingly benign tag lines, watch out. Attackers are often subtle and can be best hidden in plain view. Thankfully, today, advanced email solutions can also help you spot tell-tale language signs of BEC and phishing – but we'll cover that in our Concluding Thoughts.



5. Malware Family of the Quarter: Lumma Stealer

Our telemetry and malicious spam campaign analysis indicated that Lumma Stealer was the most encountered malware family found in the wild during Q2. This infostealer continues to evolve rapidly, frequently seen distributed through emails containing malicious attachments or download links.

Here are our key observations:.

Primary Delivery Method

Lumma Stealer is often delivered via malicious .docx, .html, or .pdf attachments, or through phishing links hosted on compromised or legitimate-looking cloud services (eg, OneDrive, Google Drive).

Data Theft Capabilities

- Browser-stored credentials
- Cryptocurrency wallets
- System information
- Saved passwords and autofill data

Frequent Campaign Themes

- Fake invoice or payment notifications
- Account suspension alerts
- Software updates or security warnings

Attribution and Access

- **Highly distributable MaaS**
  Lumma Stealer is sold as Malware-as-a-Service (MaaS), making it accessible to a broad range of threat actors.
- **Affordable for low-level attackers**
  Its low cost and active developer support make it attractive for both novice and experienced cybercriminals.

Evasion and Obfuscation

- **Packers and encrypted payloads**
  Often uses packers or encrypted payloads to evade antivirus and EDR detection.
- **Anti-VM and anti-analysis**
  Includes anti-VM and anti-analysis techniques to avoid sandbox detection.

On May 21, Microsoft announced that it had successfully taken down Lumma Stealer with the help of law enforcement. Their digital crimes unit had uncovered more than 394,000 Windows computers infected within the two-month period from March 16 to May 16, 2025.

Thanks to a court order from the US District Court for the Northern District of Georgia, the tech company was able to remove five malicious web domains underpinning the malware. The US Department of Justice followed up by commandeering control of Lumma's central command structure and eliminating the digital marketplaces where the infostealer was sold.

Feature:

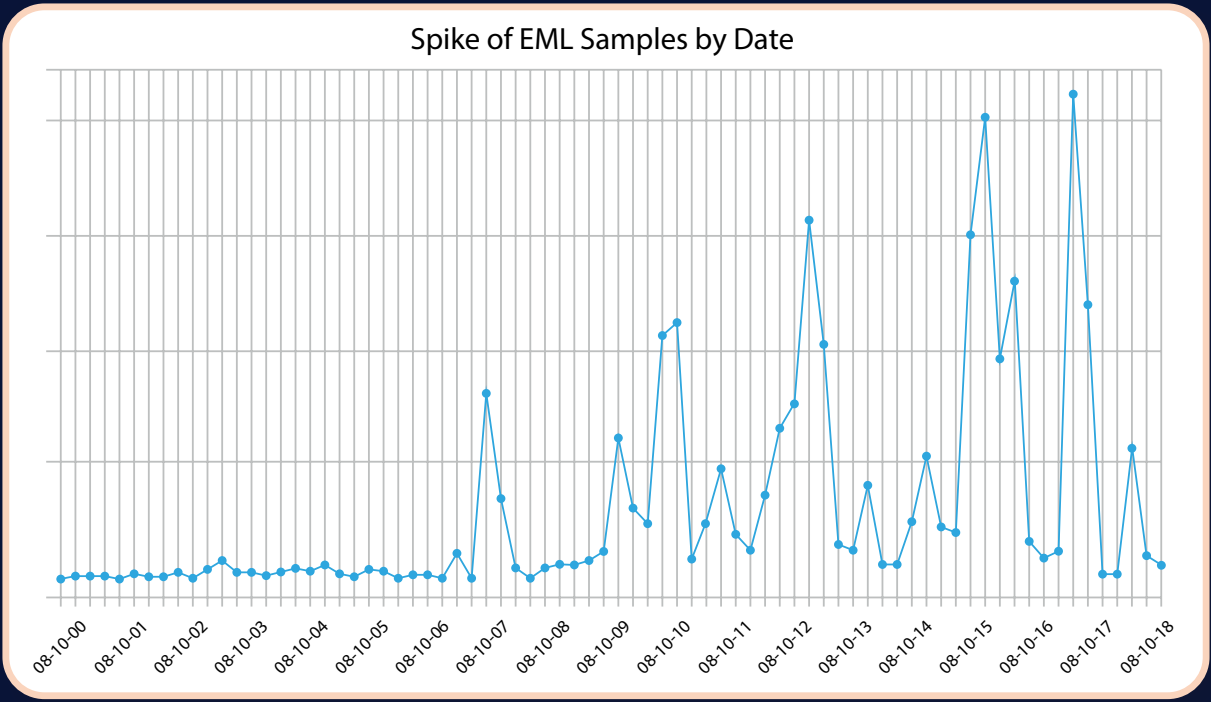
Malicious Emails Spike Worldwide in June

Spam levels remained consistent throughout Q2, but there were two concentrated incidents that sent numbers off the charts.

Between June 9 and June 12, there was a pronounced spike in the number of spam emails. This denotes a sustained spam operation over multiple days and intentional, organized activity. Another sharp increase occurred four days later on June 16th (see chart).

So what was going on? The timing of the spikes corresponds with critical end-of-quarter (Q2 in this case) financial closing activity such as budget reviews, invoicing, and reporting deadlines. This is particularly true in sectors like manufacturing.

Threat actors exploit the increased urgency during these periods to boost the likelihood that phishing emails disguised as invoices or payment notifications will be opened. The observed campaigns were mainly phishing emails, many impersonating trusted services and using compromised domains for redirection.



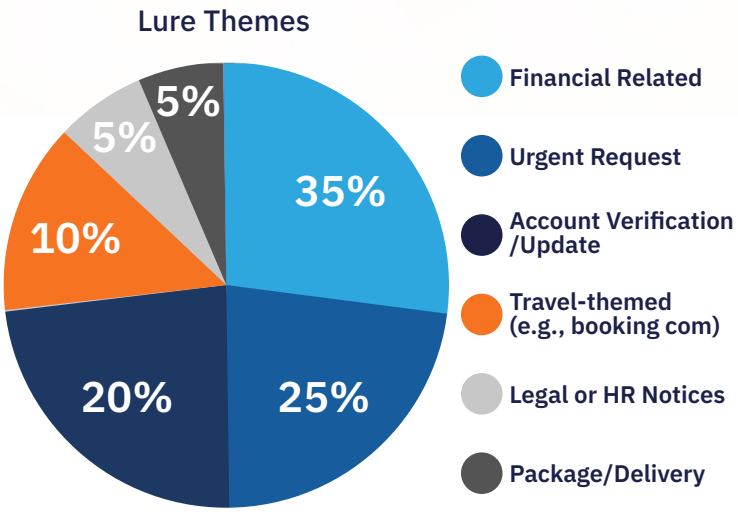
The ability to see global phishing volume in real-time is a high-value asset for clients that need to be ahead of international cybersecurity threats. Our ability to spot these trends and warn our customers allows them to be on high alert for the duration of unexpected spam email emergencies.

New Trends in The Anatomy of An Attack: From Start to Finish

It always helps to get the "big picture" view of how attackers are doing what they are doing. From baiting the hook to reeling us in, these are the tactics that sadly got the better of users in Q2.

1. The Bait. How Attackers Lure Us In?

Motivated by money themselves, attackers know human nature doesn't change much on the "other side."



Financial lures – emails regarding money, financial errors, fiduciary imperatives – were the number one ploy used to get users to open malicious emails. And it worked. Impersonating banks, payment services, or other financial institutions, these phishing emails threaten to hit us where it hurts – our pocketbooks — and they often do.

Next, urgency-based messages were the second most tried approach. Seeing alarm bells often causes panic, putting us in fight-or-flight mode, which circumvents our usual logical thought processes. The risk of missing a deadline or disappointing a boss can loom large, leading to a lot of "just in case" clicks and subsequent regrets.

Following these top two were account verification/updates (20%), travel (10%) (as people book summer accommodations in the spring), and package delivery (5%).

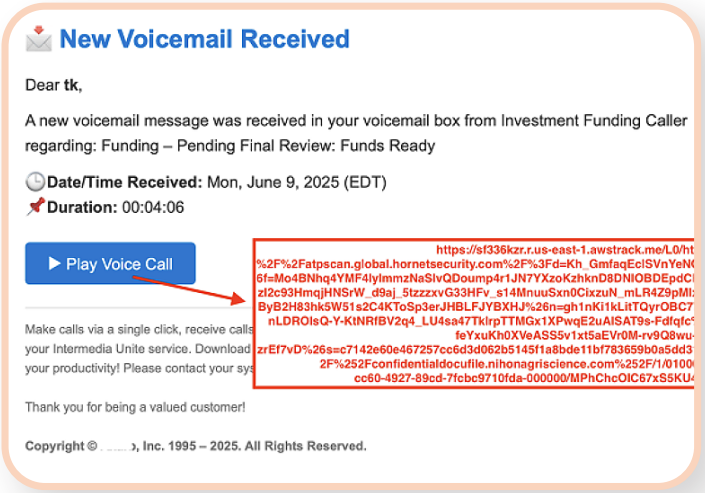
2. Closing the Trap: Links and Attachments

Once they've "hooked us," how do they get us to the actual point of compromise? Links and attachments are perennial choices, and even those are developing increased nuances as the quarters roll by.

Among phishing link delivery types, the majority (54%) utilized open redirect mechanisms. Threat actors leverage open redirect links hosted on marketing services, email tracking systems, and even security platforms to mask the true malicious destination. These links appear trustworthy due to their origin domains, making users more likely to click. Examples include:

- https://sf336kzr.r.us-east-1.awstrack.me/L0/
- https://www.googleadservices.com/pagead/aclk
- https://nam12.safelinks.protection.outlook.com/
- http://trk-mkt.tason.com/CheckNew.html

These links typically redirect to credential harvesting pages or malware-hosting sites after encoding user-related information. Check out this example of an open redirect phishing scam caught in the wild:



Following open redirects, the next most prevalent link delivery mechanism was compromised websites (30%). These can evade detection by blacklisting the IPs used in email security solutions to scan websites, leveraging legitimate services like Google Drive to make them seem safe to secure email gateways (SEGs), or changing their content frequently to outsmart automated scanners (dynamic content injection).

The third most popular link delivery technique was the use of URL shorteners, or tools that abbreviate sketchy-looking web addresses into more believable, shorter links. These came in at 7%.

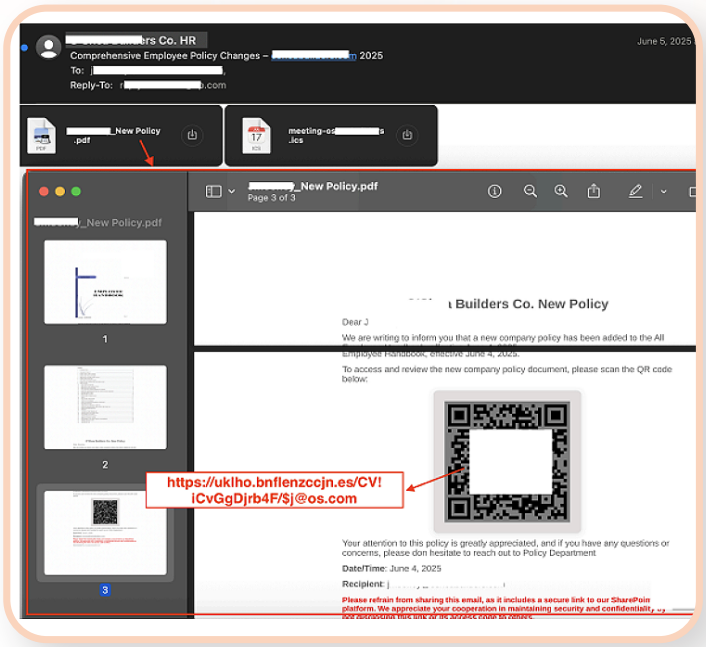
When it comes to attachments, PDFs are still a top contender in malicious campaigns. The numbers shook out as follows:

- **PDFs (64%)** - The majority of these contained QR codes.
- **HTML (14%)** - Used for fake login forms embedded in the file.
- **DOCX (13%)** - Frequently containing malicious content such as QR codes or macros.
- **SVG (9%) -** These graphic files were all the rage last quarter but have since plummeted from 34% to the 9% we observed in Q2.

Note that QR codes popped up prominently in PDFs and DOCX files this quarter, with the majority of those files containing them in some form. These malicious QR codes:

- **Redirect users to phishing websites, often Microsoft or banking impersonations.**
- **Bypass email filtering solutions that primarily scan text-based content or traditional URLs.**
- **Would be found embedded in business-themed documents such as “invoice”, “payment due”, or “2FA reauthentication” notices.**

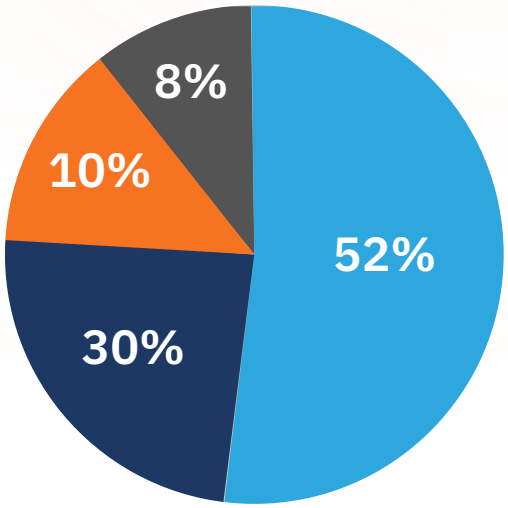
Take a look at this real-world example:



3. Where the Rubber Hits the Road: Exfiltration Methods

Lastly, after baiting their victims with financially based lures and reeling them in with trusted PDFs, attackers finish the last leg of the race with various exploitation mechanisms.

This quarter, they favored:



- 52% **HTTP POST To Remove Server**
- 30% **Email Exfiltration**
- 10% **Telegram Bots/Webhooks**
- 8% **Unknown/Obfuscated**

Most phishing pages exfiltrate credentials via direct HTTP POST requests to attacker-controlled servers. A significant portion still used legacy methods like sending stolen data to attacker emails, but the use of Telegram — the popular messaging app — bot exfiltration is now growing in popularity due to its ease of setup and anonymity.

With Telegram, attackers can easily target anyone from anywhere. Given that these scams are social engineering attacks, attackers with open communication channels have a clear advantage if they can hook people via text: think bitcoin schemes, romance scams, and other group messages that draw in dozens of strangers for unsolicited reasons.

In other words, it may no longer be the "hacker in the basement with the laptop." Now, it could be the woman on the subway with the cellphone. The most worrying part about the rising Telegram tide is that it is extremely hard to police. In May of this year, Telegram purged all of its most dangerous Chinese crypto scam markets that provided "money laundering, stolen data, and a variety of other illicit wares" to investment scams in Southeast Asia; then "watched impassively as those black marketeers rebranded, rebuilt, and returned to business as usual," as reported in WIRED.

Feature:

Attackers Use Legit Login Pages to Throw Us Off the Trail

Another interesting trend is appearing on the horizon as attackers continue to find new ways to make it look like they were never there.

This is next-level planning; we are accustomed to threat actors muddying the waters to evade initial detection, but this most recent tactic ensures we don't even suspect foul play.

Our analysis of Q2 data reveals that no less than 60% of all credential harvesting pages redirect to an actual, legitimate Microsoft login page. When the victim has to enter their account credentials twice, it will seem like the page is just reloading, or that double authentication was required (for security purposes, of course).

The scheme is brilliant because there is nothing to arouse suspicion when you can ultimately – and legitimately – access your Microsoft account. Perhaps due to login fatigue, users are less prone to notice differences in authentication requirements upfront. Or, it could be because companies are changing their identity and access management (IAM) practices with more regularity.

This tactic not only evades human detection but also delivers an edge against security solutions designed to spot anomalies in the flow. When the flow ends on a trusted site like login.microsoft.com, it all "checks out."

Concluding Thoughts: Personalization Is Public Enemy #1 in Phishing

Every attacker knows that customizable is better when you're outsmarting humans.

It is exactly those (creepy?) little touches that make us doubt our doubts and let down our defenses. They know our name. They know our hometown. They know which school our children attend. And they just referenced an email we sent to our boss last week.

It must be genuine.

By scraping social media sites and other publicly available domains, vast amounts of personal data can be gleaned with the click of a well-trained AI model button.

Thanks to AI, in all its forms, malicious hackers can take powerful and personalized spear-phishing techniques that target high-value individuals over time and apply those same customizable tactics to...well, everyone.

Spear phishing campaigns boast incredible click-through rates of over 53%, while regular phishing emails hover around 18%. The amount of work it took to track someone down over months, building a profile on their personal facts, was prohibitive and therefore saved for "big game" only, like executives.

The force-multiplying capability of AI means that the devastating personal power of spear phishing attacks can be leveled at any unsuspecting victim. And again, these highly customized (and convincing) attacks can be sent out at a scale unimaginable before. Here's a depressing statistic to prove it:

Since the release of ChatGPT, phishing has increased by 4,151%.

The takeaway? If employees can't catch these phishing ploys at scale (or at all), organizations need to turn to the technology that can. Integrated cloud email security (ICES) solutions like VIPRE Integrated Email Security (IES) are built to do what no other advanced email platform has been able to do before: catch behavioral patterns, giveaways in semantics, and red flags in attacker language and tone to spot social engineering threats that otherwise evade detection.

- **Behavioral detection**
- **Threat correlation across channels**
- **Intelligence in prevention strategies**

One thing is certain: As attackers continually improve social engineering techniques, something in the way organizations address their typical email security problems is going to have to change. Because attackers aren't leaning into 'typical' anymore. Now it's personal.

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

Email Threat Trends of 2025

To learn more about VIPRE Email Security and what we do for organizations, schedule a demo today.

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