Phishing Activity Trends Report

4th Quarter 2025

APWG

Unifying the
Global Response
To Cybercrime

Activity October-December 2025

Published 18 February 2026

Phishing Report Scope

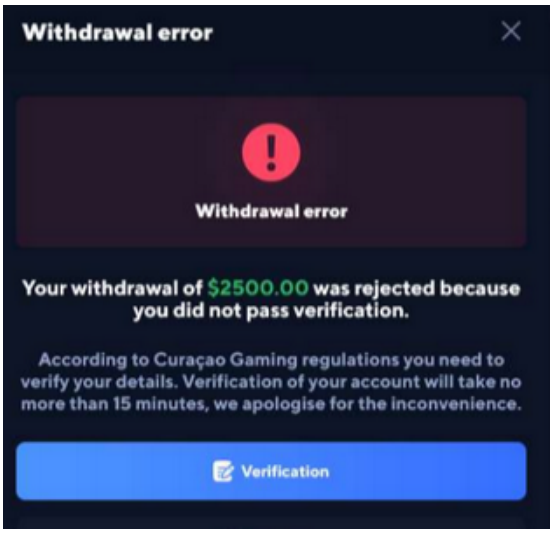
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG measures the evolution, proliferation, and propagation of identity theft methods by drawing from the research of our member companies and industry experts.

Phishing Defined

Phishing is a crime employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and messages, bogus web sites, and deceptive domain names. These are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept consumers' account usernames and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

2025 in Review: Scams Explode via Social Media, SMS, Email, QR Codes



Phishing Activity Trends Summary

- In the fourth quarter of 2025, APWG observed 853,244 phishing attacks, down 4% from Q3. [pp. 3-4]
- During 2025, the volume of scams, impersonations, and other threats increased on every social media platform, and increased across threat types in every quarter, according to ZeroFox. [pp. 5-7]
- Phishers targeted the Social Media and SaaS/Webmail sectors most frequently. [pp. 4-5]
- The total number of wire transfer BEC attacks observed in Q4 2025 increased by 136% compared to Q3. [pp. 11-12]
- During Q4 2025, the use of SMS for phishing rose [p. 4], while the use of QR codes for phishing decreased by 9%. [pp. 8-9]

Statistical Highlights for the 4th Quarter 2025

APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same destination.) Thus, APWG measures reported phishing *sites*, which is a more relevant metric than URLs. A synonym for sites is *attacks*.
- **Unique phishing e-mails subjects**. This counts email lures that have different email subject lines. Some phishing campaigns may use the same subject line but advertise different phishing sites. This metric is a general measure of the variety of phishing attacks, and can be a rough proxy for the amount of phishing taking place.
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

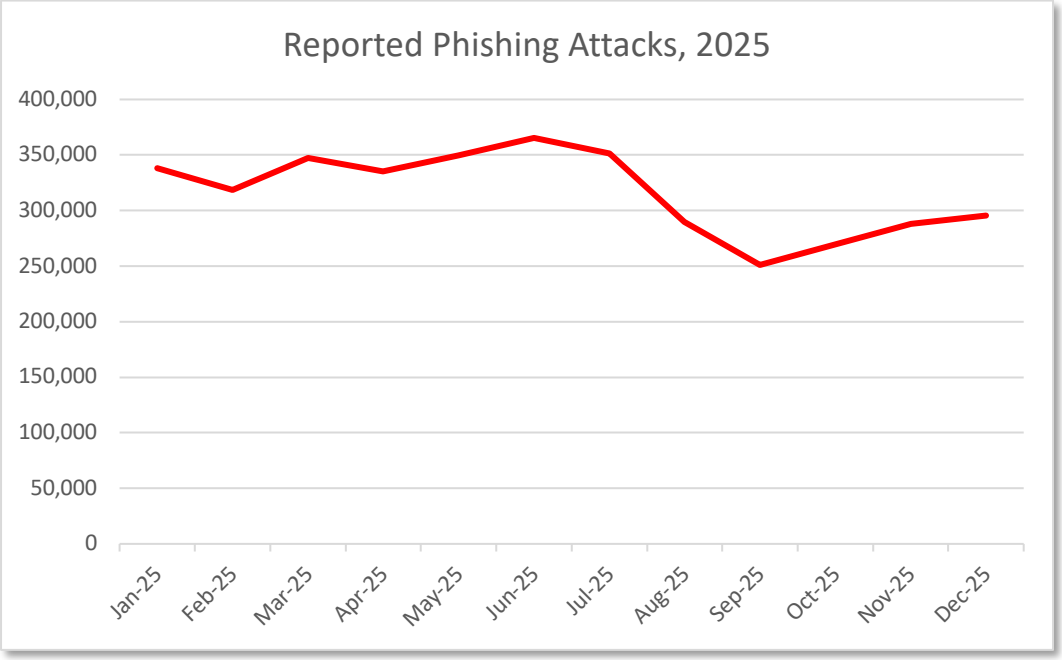
	October	November	December
Number of unique phishing Web sites (attacks) reported	269,558	287,995	295,691
Unique phishing email campaigns	16,284	14,980	14,091
Number of brands targeted by phishing campaigns	457	461	496

Phishing attacks occurred at a high but steady pace in 2025. During 2025, APWG observed 3.8 million phishing attacks, which was up slightly from 3.76 million in 2024. In the fourth quarter of 2025, APWG observed 853,244 phishing attacks. That was down 4 percent from 892,494 attacks in Q3 2025, and down from 1,130,393 attacks in Q2 2025, which was largest quarterly total seen since Q2 2023.

The number of spam campaigns that APWG recorded dropped dramatically, from 81,710 in Q3 2025 to 45,355 in Q4 2025 – a 45 percent decrease. Email systems are preventing users from forwarding phishing lure emails and sending phishing URLs to APWG and similar organizations, because the mail systems

perceive those as harmful. This cuts into the number of successful reports to *reportphishing@apwg.org*, one of APWG's main collection methods.

A total of 866 unique brands were identified in the reports across the quarter.

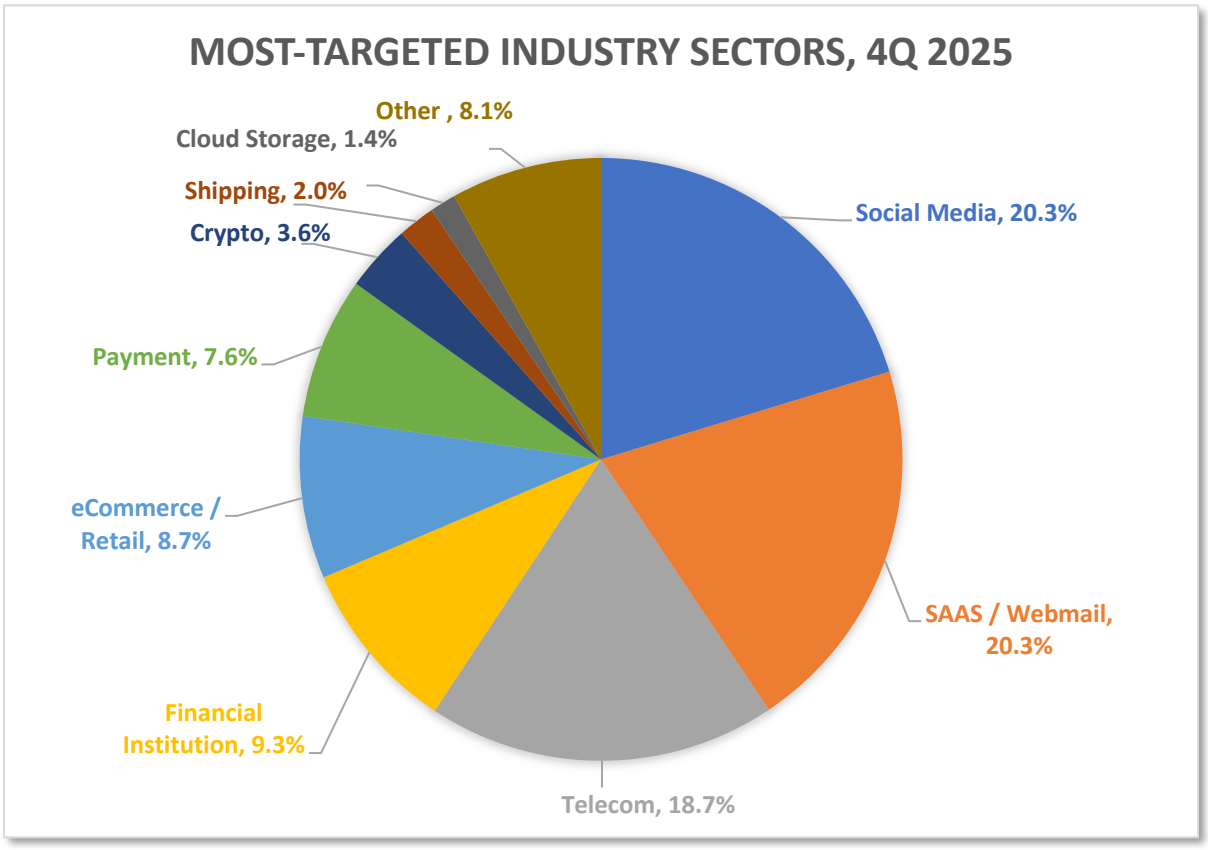


Most-Targeted Industry Sectors

In the fourth quarter of 2025, APWG founding member Crane Authentication recorded that the Social Media and SAAS/Webmail categories were the sectors most attacked by phishing, each suffering 20.3 percent of all phishing attacks. Attacks against telecom providers rose from 5.9 percent in Q3 to 18.7 percent in Q4, while attacks against Financial Institutions dropped.

Crane Authentication detected a slight decrease in overall URL phishing volumes in Q4 2025 as compared to Q3 2025. But smishing (text message phishing) volumes continued to rise. "SMS-based fraud detections have shown steady 30 to 40 percent growth quarter-over-quarter. Text communications are effective – they allow fraudsters to bypass email filters and reach out to potential victims directly, said Matthew Harris, Senior Product Manager, Fraud at Crane Authentication.

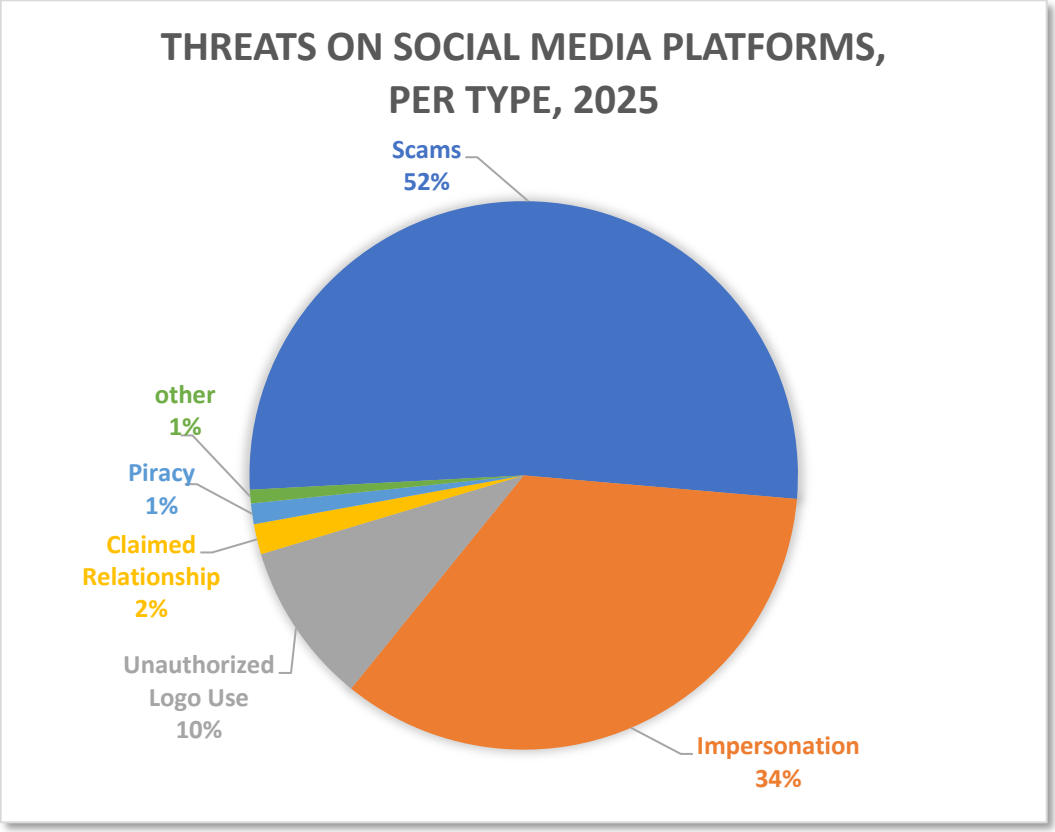
Crane Authentication offers expertise and cutting-edge innovations that protect and enhance products, secure identities, and safeguard revenues.



Social Media Threats

APWG member ZeroFox detects and remediates targeted phishing attacks, credential compromises, brand hijacking, and other threats. ZeroFox monitors the entire Internet, the domains space, and major social media platforms for its customers, finding threats that affect organizations, individuals, or assets.

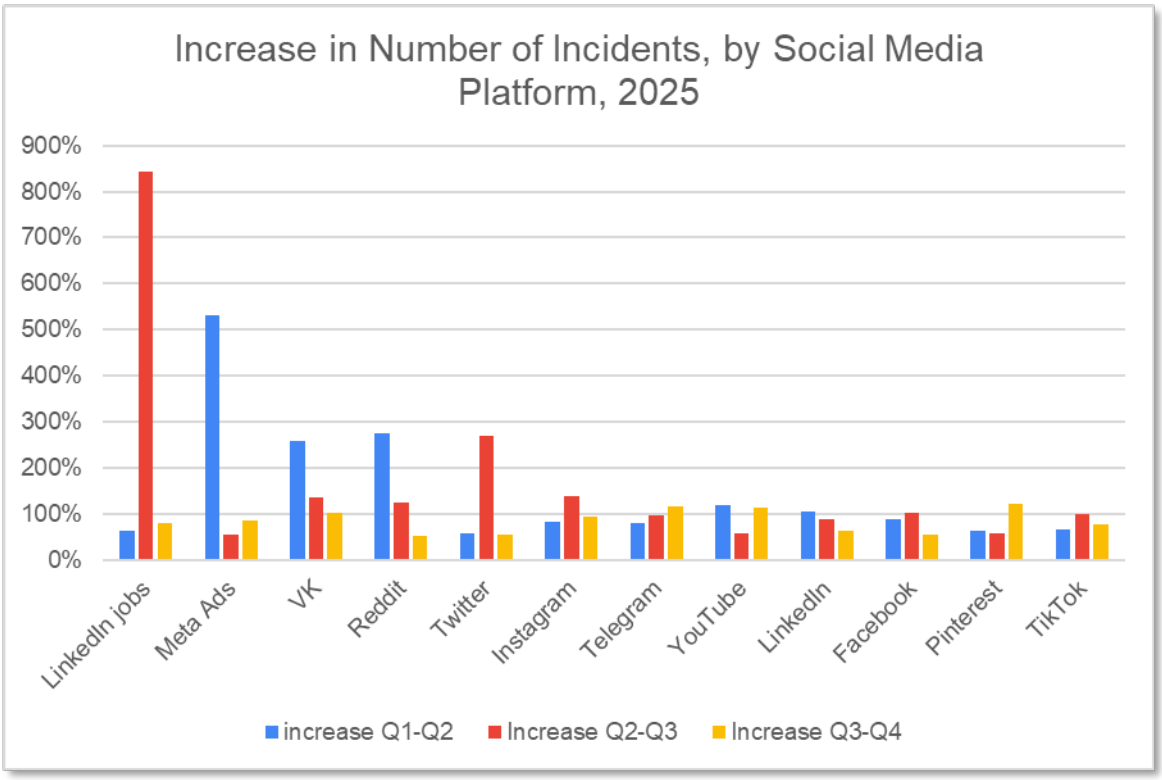
ZeroFox found that threats on social media in 2025 were predominantly of two types: Scams and Impersonation. Together, these two threat types accounted for 86 percent of all confirmed threats. Other threat categories, including piracy, counterfeit goods, phishing, and physical threats, collectively made up the other 14 percent.



Definitions:

- Scams: content uses deceptive tactics to defraud users of money or personal information.
- Impersonation: content falsely claims to be from a real person, brand, or organization.
- Unauthorized logo use: use of an organization's logo by a threat actor posing as that organization, with a malicious purpose.
- Claimed relationship: content falsely claims affiliation or endorsement in order to mislead users.
- Piracy: the practice of downloading and distributing copyright protected content digitally without permission, such as music, movies, or software.
- Other categories: Malvertising, Phishing, Doxxing, Physical threats to employees. unauthorized data disclosures.

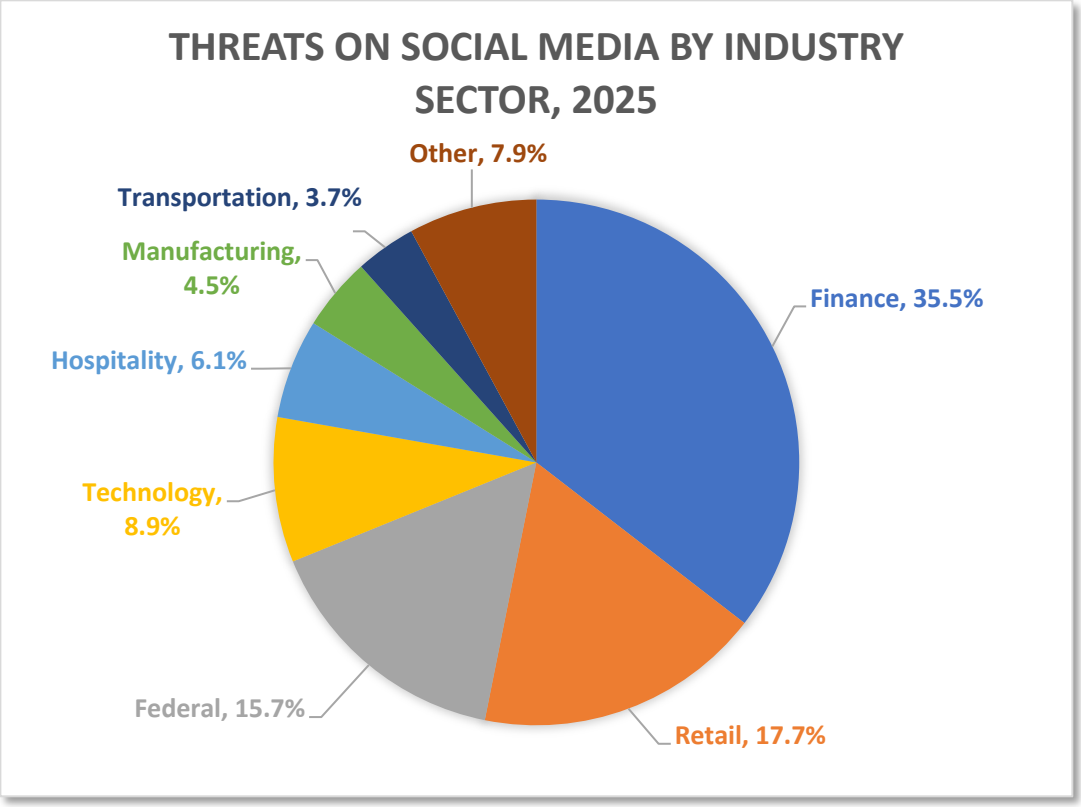
During 2025, ZeroFox found that threat volume increased on every social media platform, and increased across threat types, in every quarter. Threat volume growth ranged from 51 percent up to 843 percent from quarter to quarter. "This widespread, significant growth on all major social media platforms simultaneously demonstrates that threat actors are successfully scaling their operations across the entire social media ecosystem," said Carlos Alvarez, Disruption Partnerships Lead at ZeroFox.



Definitions:

- LinkedIn Jobs: malicious postings in the Job section of LinkedIn, made for purposes such identity theft, fraud, fake job postings, etc. These are separate from user-created posts made elsewhere on LinkedIn.
- Meta Ads: advertisements across all Meta platforms (such as on Facebook and Instagram) that are identified as being malicious. These are separate from posts made on Facebook and Instagram.

Analysis of the confirmed threats across 2025 reveals that three sectors—Finance, Retail, and Federal—collectively accounted for nearly 70 percent of all confirmed threats on social media. The Finance sector was the primary target, 35.5 percent of the time, followed by the Retail sector at 17.7 percent, and the Federal sector at 15.7 percent, indicating where threat actors are directing the majority of their attention and resources. Conversely, sectors like Healthcare were rarely targeted.



QR Code Attacks

Some criminals send QR codes in the emails they send to potential victims. When scanned by a mobile phone, these malicious QR codes take users to phishing web sites, or trick users into downloading malware. These QR codes are not caught by traditional email filtering. APWG member Mimecast is a leading email security platform, and has developed tools to find and stop emails containing malicious QR codes. Below, Mimecast presents data about the QR code-based attacks it found within email attachments. The analysis below looks at QR codes that Mimecast found pointing to phishing pages, brand impersonation

Some criminals send QR codes in the emails they send to potential victims. When scanned by a mobile phone, these malicious QR codes take users to phishing web sites, or trick users into downloading malware. These QR codes are not caught by traditional email filtering. APWG member Mimecast is a leading email security platform, and has developed tools to find and stop emails containing malicious QR codes. Below, Mimecast presents data about the QR code-based attacks it found within email attachments. The analysis below looks at QR codes that Mimecast found pointing to phishing pages, brand impersonation pages, and other fraudulent scam-promoting websites.

During Q4 2025, Mimecast detected 655,673 unique malicious QR codes, down 9 percent from 716,306 in Q3. Phishers timed some QR code-based attacks during November's Black Friday week, when users may place heightened trust in order, delivery, and payment notifications.

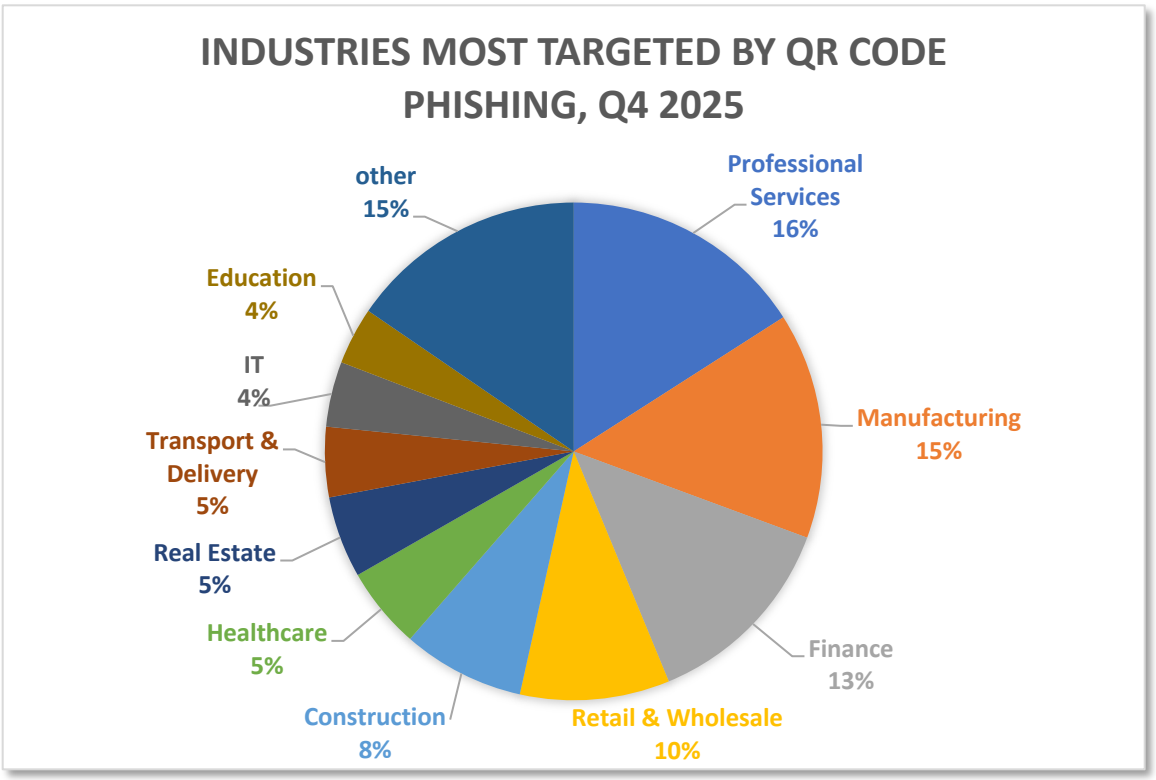
To create QR codes, people use QR code generators. These are commercially available, online services. All kinds of legitimate companies and organizations use them to generate QR codes for their advertising and events. Criminals also use these generators. QR code generators offer various features, and these features can be leveraged by criminals:

- While some QR code generators require a subscription, others are free. Free services naturally tend to devote fewer resources to preventing and shutting down malicious use.
- Many QR generators offer tracking—they allow their customers to see how many times a QR code has been scanned and when, and the general locations of the Internet users who scan the codes. Criminals use the tracking to optimize their campaigns.
- Some QR code generators allow their customers to change a QR code's destination URL after the QR code's been generated. This is a handy feature that criminals leverage as they try to fool security companies and keep ahead of detection.
- Criminals also pointed QR codes to URL shortening services, which then redirected users on to different destination URLs. This is a tool to obscure the malicious nature of the QR codes.

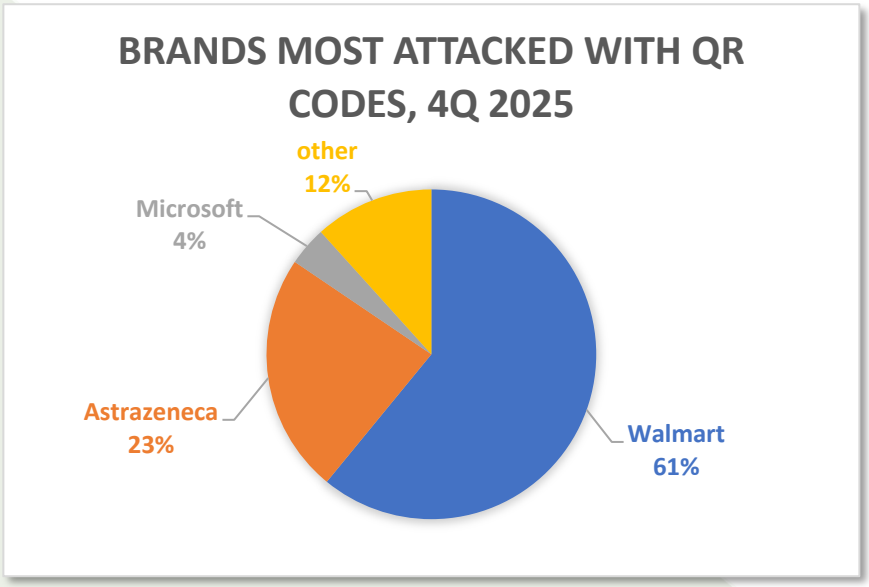
In Q3 2025, the domain JSJ[.]TOP was the most prolific attack source, generating 1,149,088 detected attacks. But in Q4, use of JSJ[.]TOP dropped 64 percent to 415,345 attacks. Q3's other most-used QR platforms were used to generate zero attacks in Q4: QRTO[.]ORG, QR[.]PRO, ME-TEAM[.]ORG, and BIO[.]LINK all disappeared from Mimecast detections. Either those QR platforms implemented better defenses against abuse, or security vendors implemented better blocking of these threats, and/or the threat actors moved on to using other resources.

Instead, in Q4 threat actors moved to using new QR infrastructure: SCAN[.]PAGE dominated with 61.1 percent of Q4 detections, followed by VIEW[.]PAGE (38.6%), QR.SCANNED[.]PAGE (36.6%), and QRFY[.]IO (18.3%). In Q4, attackers notably redirected attacks through URL shortener TINYURL.COM.

No single industry stood out as particularly vulnerable during this time period—criminals attacked multiple sectors. Professional Services became the most-often-attacked sector, driven by year-end consulting engagements, contract renewals, and heightened email volumes as tax, legal, and accounting firms navigated critical deadlines. Manufacturing fell to the #2 spot.



Walmart was most-impersonated brand again in Q4. Pharmaceutical company AstraZeneca was the second-most-targeted company, but was not attacked at all via QR codes in Q3 2025. Delivery company DHL was the most-attacked brand in Q2 2025, but was the target in only 0.7 percent of attacks in 4Q 2025. The AstraZeneca and DHL examples show how phishers can pivot to new targets.

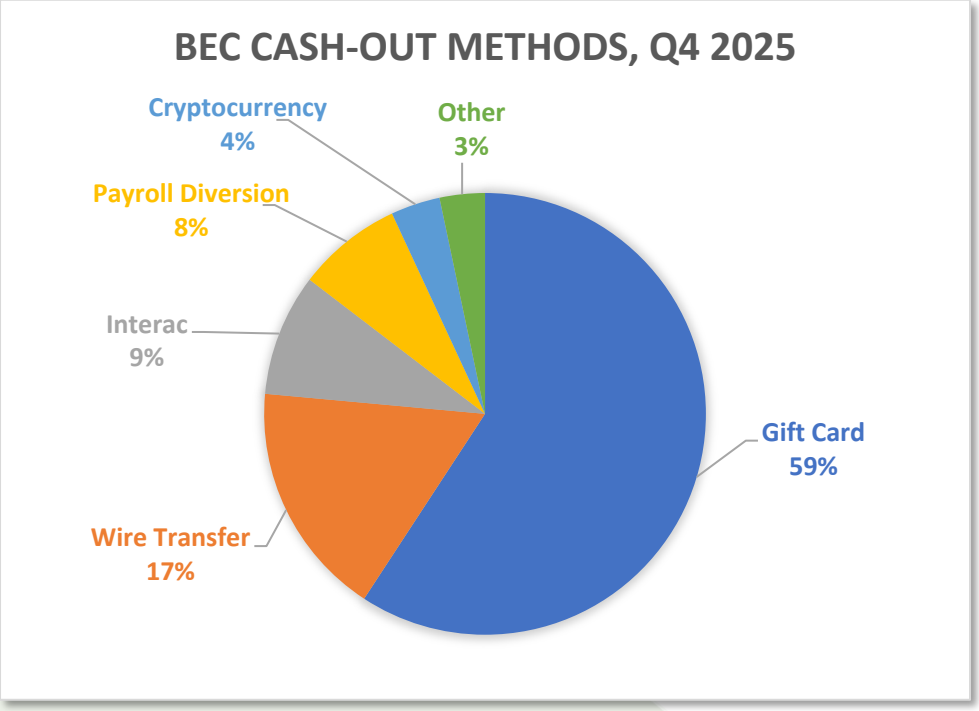


Business e-Mail Compromise (BEC)

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.8 billion dollars in *reported* losses in the U.S. in 2024 according to the FBI's Internet Crime Complaint Center (IC3). (Many more losses go unreported.) In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q4 2025. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

Fortra found that the average amount requested in wire transfer BEC attacks in Q4 2025 was $50,297, a 4.5 percent increase from the prior quarter's average of $48,115. The total number of wire transfer BEC attacks observed by Fortra in Q4 2025 increased by 136 percent compared to the previous quarter.

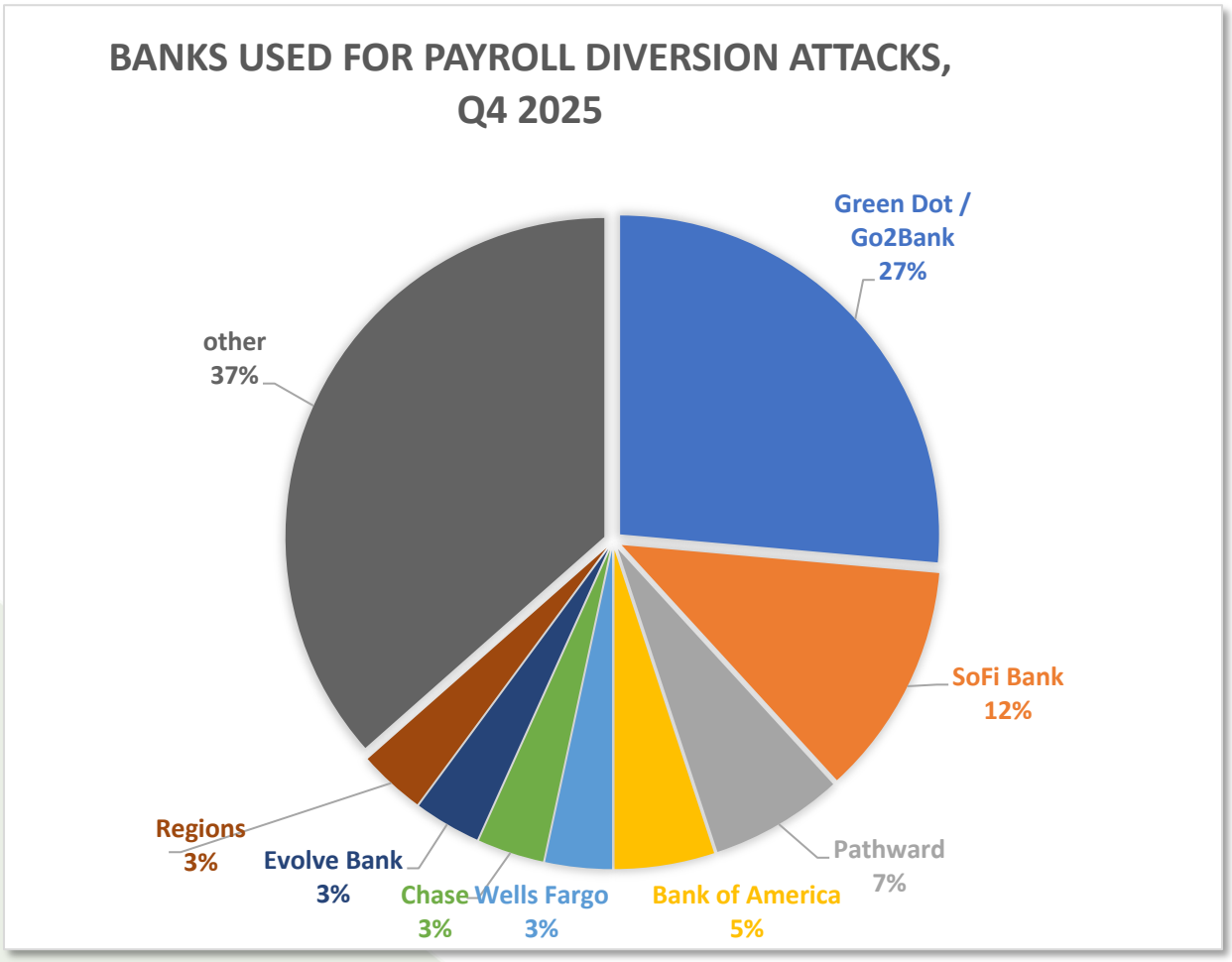
Fortra attributes the increase in attack volume to Scripted Sparrow, a threat group first observed in June 2024. The group is currently the world's most prolific BEC gang. Fortra estimates that the group sends as many as 6 million highly targeted emails monthly, targeting Accounts Payable teams with bogus executive coaching invoices. The group, whose members hail from South Africa, Nigeria, the U.S., and Turkey, uses a spoofed reply chain designed to trick the recipient into believing the expense was approved by a company executive.



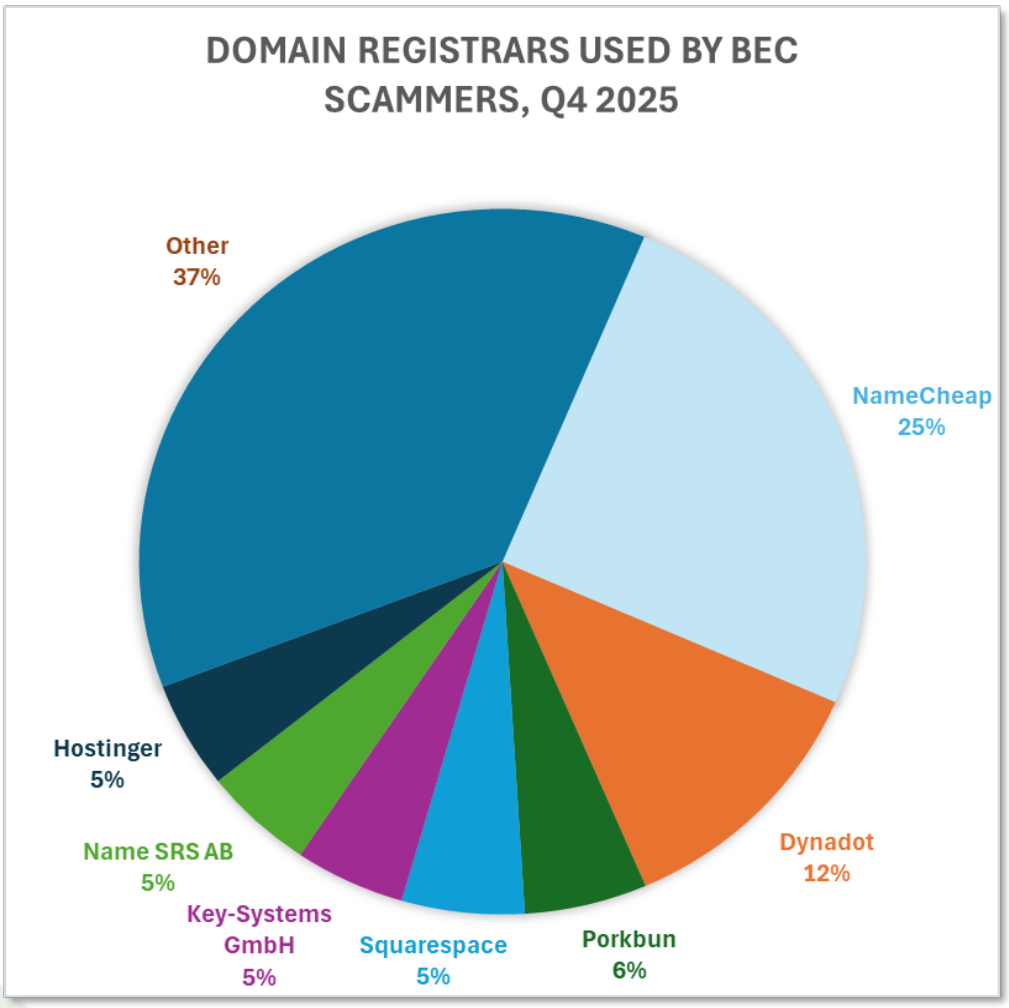
During the fourth quarter of 2025, gift card scams were once again the most popular scam type, making up 59 percent of the total. Seventeen percent of attackers requesting a wire transfer payment. Interac (9%)

and payroll diversion (8%) were also popular cashout methods in the last quarter of 2025. Fortra ascribes the continued growth in wire transfer attempts to Scripted Sparrow.

Green Dot was once again the preferred bank of payroll diversion scammers, with 27 percent of payroll diversion attempts directed towards accounts held at one of Green Dot's brands. SoFi was the second most popular bank for payroll diversion scammers, followed by Pathward.



Domain registrar NameCheap continued to be the domain registrar used most often by BEC scammers. Registrar GoDaddy dropped out of the top listings, after being the second-most-popular registrar with BEC scammers in Q3 2025.



Fortra observed that 69 percent of BEC attacks in Q4 2025 were launched using a free webmail domain, down from 74 percent in Q3 2025. The remaining 31 percent of BEC attacks in Q4 2025 utilized non-webmail domains.

APWG Phishing Activity Trends Report Contributors

Crane Authentication is the leading provider of integrated online protection and on-product authentication solutions for brands and governments.
www.craneauthentication.com/

Forta's mission is to help organizations increase security maturity while decreasing operational burden. Forta's brands include PhishLabs and Agari.
www.fortra.com

Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.
www.illumintel.com

Mimecast's AI-powered, Human Risk Management platform is purpose-built to protect organizations from the spectrum of cyber threats.
www.mimecast.com

ZeroFox provides cyber + physical threat intelligence to discover, validate, and disrupt threats, neutralizing adversaries before they harm brands, domains, people, and assets.
www.zerofox.com

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to financial institutions, online retailers, ISPs, solutions providers, the law enforcement community, government agencies, multilateral treaty organizations, and NGOs. There are more than 2,200 enterprises worldwide participating in the APWG.

Operationally, the APWG conducts its core missions through: APWG, a US-based 501(c)6 organization and curator of the eCrime eXchange, the apex clearinghouse for cybercrime event data; the STOP. THINK. CONNECT. Messaging Convention, Inc., a US-based non-profit 501(c)3 corporation; APWG Applied Research the APWG's applied research secretariat <http://www.ecrimeresearch.org> and EU-based research chapter, APWG.eu.

APWG's directors, managers and research fellows advise: national governments; global governance bodies such as the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a founding member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

APWG's clearinghouse for cybercrime-related data sends more than two billion data elements per month to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of users, software clients, and devices worldwide.

APWG's STOP. THINK. CONNECT. cybersecurity awareness campaign has officially engaged campaign curators from 26 nations, 13 of which are deployed by cabinet-level ministries, government CERTs and national-scope NGOs.