Phishing Activity Trends Report

1st Quarter 2025

APWG

Unifying the Global Response To Cybercrime

Activity January-March 2025

Published 2 July 2025

Phishing Report Scope

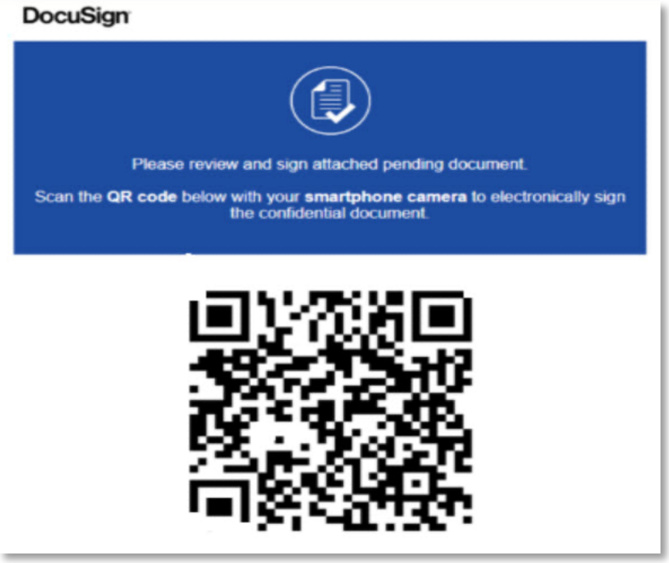
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG 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

Millions of Malicious QR Codes Lead to Phishing



DocuSign

Please review and sign attached pending document.

Scan the **QR code** below with your **smartphone camera** to electronically sign the confidential document.

Phishing Activity Trends Summary

- In the first quarter of 2024, APWG observed 1,003,924 phishing attacks, This was the largest number since late 2023. [pp. 3-4]
- Criminals are sending millions of emails each day that containing QR codes. The QR codes lead consumers to phishing sites and malware. (pp.5-7)
- Attacks against the online payment and financial (banking) sectors grew in 1Q 2025, together totaling 30.9 percent of all attacks [pp. 4-5]
- The total number of wire transfer BEC attacks observed in Q1 2025 increased by 33 percent compared to the previous quarter. [pp. 8-10]

Statistical Highlights for the 1st Quarter 2025

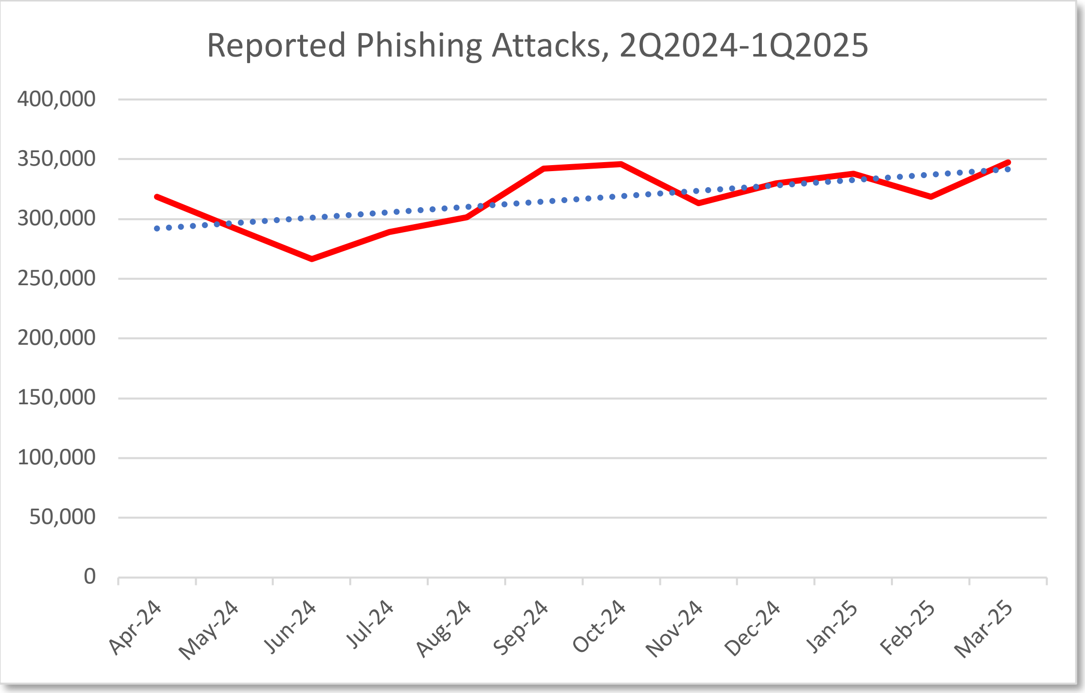
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

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.

	January	February	March
Number of unique phishing Web sites (attacks) detected	337,998	318,513	347,413
Unique phishing email campaigns	35,279	28,296	23,550
Number of brands targeted by phishing campaigns	328	312	328

In the first quarter of 2025, APWG observed 1,003,924 phishing attacks. This was the largest quarterly total since 1.07 million were observed in Q4 2023. The number has climbed steadily over the last year: from 877,536 in Q2 2024, to 932,923 in Q3, to 989,123 in Q4.

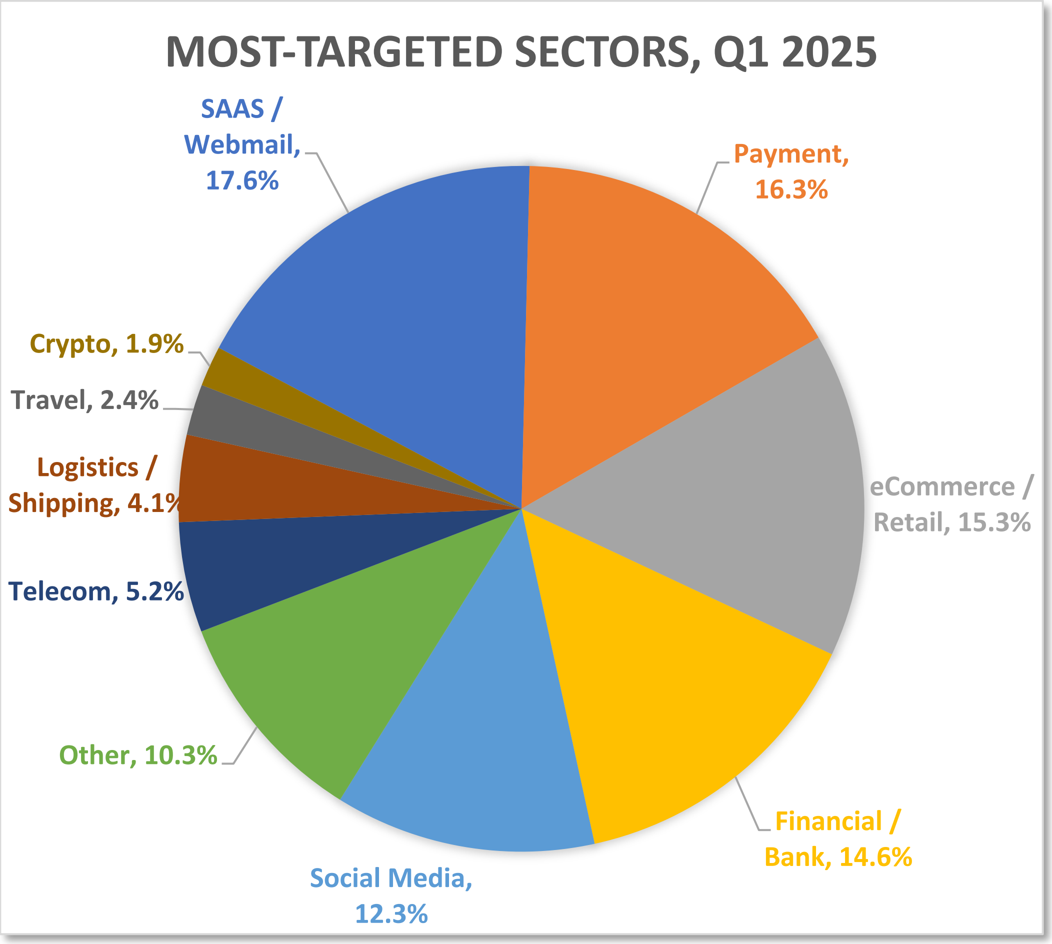


Most-Targeted Industry Sectors – 1st Quarter 2025

In the first quarter of 2025, APWG founding member OpSec Security recorded that the SAAS/Webmail category was the most-attacked sector, with 17.6 percent of all phishing attacks. That was down from 23.3 percent of all attacks in Q4 2024. Attacks against online payment companies and the financial (banking) sectors grew in 1Q 2205, together totaling 30.9 percent of all attacks.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, reported: “We are continuing to see scammers branching out in the types of companies and industries they are impersonating, such as public utilities, car parking meters, bridge toll collection systems, and financial institutions.” Harris also noted that OpSec Security observed an increase in vishing/smishing volumes in the first quarter, and saw more unique brands targeted—”this might be an indication that scammers are continuing to look for better ROIs by expanding the companies they target and impersonate.”

.



OpSec Security offers world-class brand protection solutions.

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, in Q4 2024 and Q1 2025 (October 1, 2024 through March 31, 2025).

During the six-month period, Mimecast detected more than 1.7 million unique malicious QR codes, and found an average of 2.7 million emails with QR codes attached daily. The analysis below looks at QR codes that Mimecast found pointing to phishing pages, brand impersonation pages, and other fraudulent scam-promoting websites.

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:

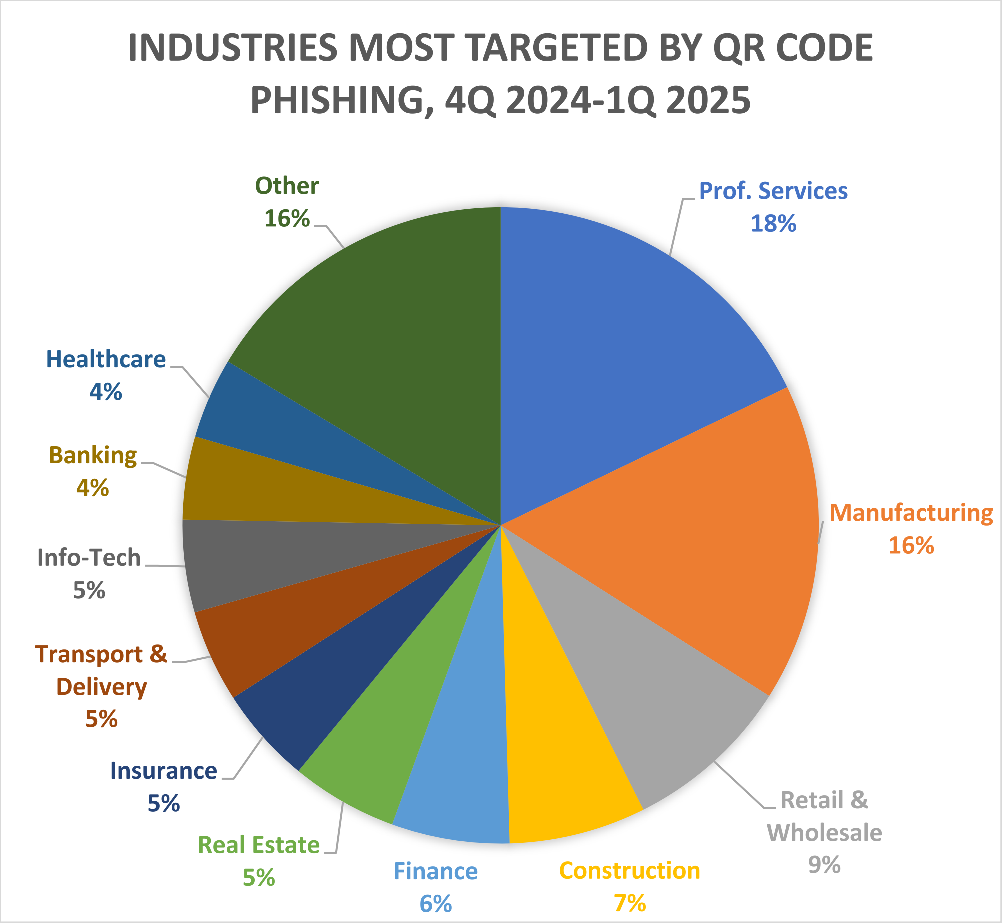
- While some QR code generators require a subscription, others are free. Free services naturally tend to devote fewer resources to preventing and shutting down malicious use.
- Many QR generators offer tracking—they allow their customers to see how many times a QR code has been scanned and when, and 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.

Mimecast identified which QR code generators were used by criminals most often:

1. **QRCC**[.]**IO** was the most-used QR code generator, used to create 189,011 unique malicious QR codes. While this service offers legitimate business operations, threat actors have consistently exploited its infrastructure for phishing and fraud campaigns.
2. **QRCO**[.]**DE** was used to generate 177,909 malicious QR codes. This provider was used to enable multiple kinds of attacks, including malware distribution and phishing campaigns.
3. **ME-QR**[.]**COM** was used to generate 148,004 malicious QR codes, yet positions itself as a security-conscious service. This provider's dynamic QR code feature and tracking capabilities are attractive to criminals.

Most-Targeted Industries

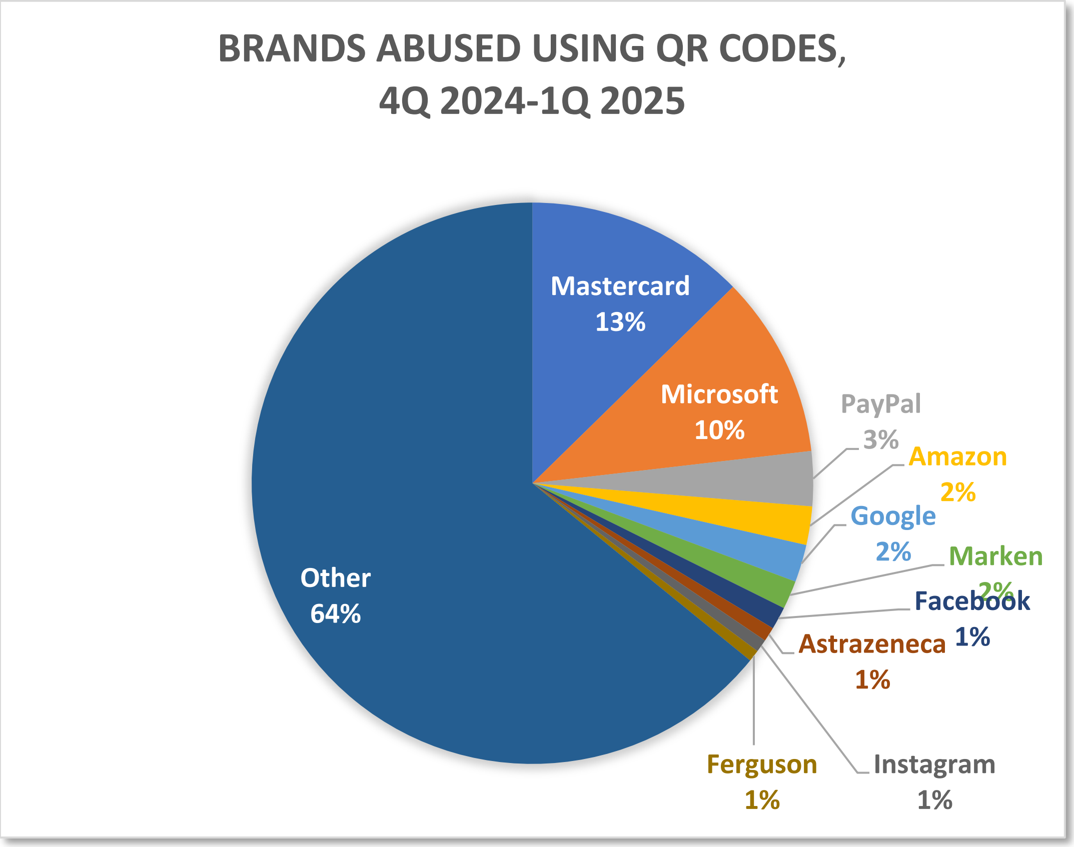
No single industry stood out as particularly vulnerable during this time period—criminals attacked multiple sectors relatively evenly. However, the Retail & Wholesale sector recorded 148,596 detections, Manufacturing suffered 132,242 detections, and Construction had 123,322 detections. These industries are likely targeted often because consumers regularly access retail services through mobile apps (such as Amazon and Walmart), and these sectors have widely adopted QR codes to relay information about products and services.



Brands Most Targeted By Malicious QR Code Phishing

Mastercard was targeted most, with 14,233 QR codes, while Microsoft had 11,796. A large number of other brands were attacked, but using far fewer QR codes each, suggesting the criminals were performing focused attacks rather than opportunistic attacks. The attacks against Mastercard highlight attackers' desire for credentials they can turn into cash, such as by buying physical goods with stolen credit card data. Payment processing platforms faced ongoing attacks—PayPal was attacked with 3,546 QR codes, and banking institutions suffered noticeable attack volumes.

Mimecast also identified sophisticated regional targeting patterns. Consumers in the Asia-Pacific region tended to receive emails that targeted banks. Those in Europe saw more attacks against payment processors and government services, Email recipients in North America saw more attacks against enterprise cloud services and financial platforms.



Attackers also demonstrated expertise at exploiting subdomain providers. Phishers often used Google services. Attackers pointed 27,017 QR codes to URLs on content.googleapis.com, and pointed 15,891 QR codes to URLs on ep2.adtrafficquality.google. These attacks demonstrate advanced understanding of enterprise trust relationships.

The combination of these techniques with legitimate service abuse creates significant challenges for traditional security controls.

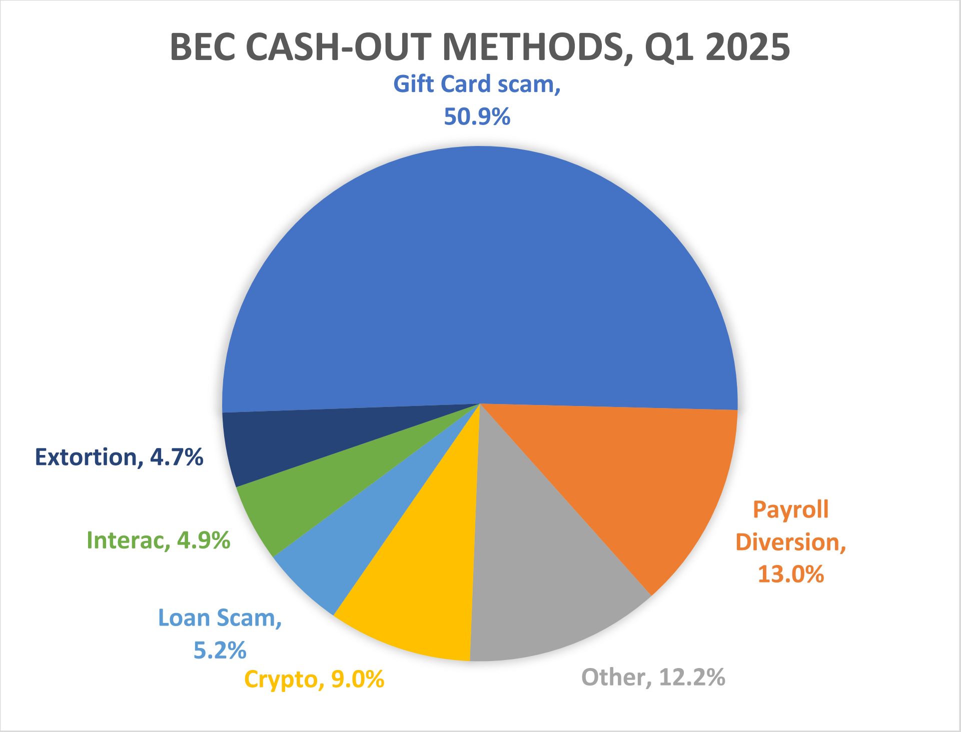
Business e-Mail Compromise (BEC), 1st Quarter 2025

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 Q1 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 Q1 2025 was $42,236, a 67 percent decrease from the prior quarter's average of $128,980. The total number of wire transfer BEC attacks observed by Fortra in Q1 2025 increased by 33 percent compared to the previous quarter.

Fortra categorizes each corporate email attack as either Credential Theft, Malware Delivery, or Response-based. Response-based attacks reaching corporate inboxes edged up slightly to 43 percent of all attacks, compared to 41 percent in the previous quarter. On the malware front, the Remcos RAT was the most common payload Fortra observed in the first quarter of 2025.

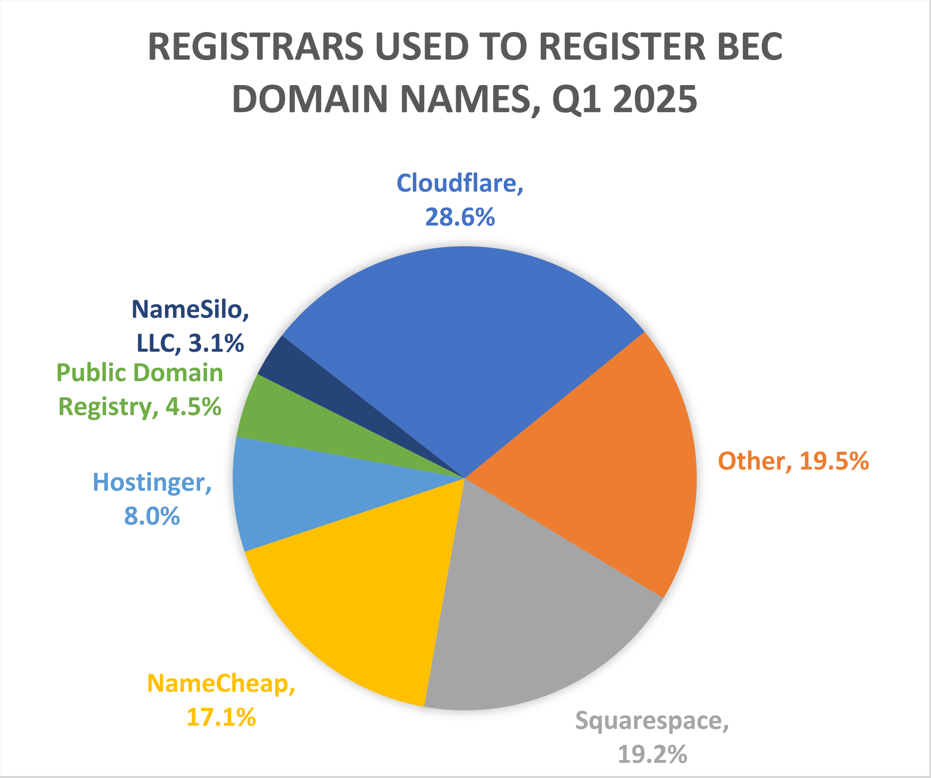
During the first quarter of 2025, gift card scams were once again the most popular scam type, making up 51 percent of the total, About 13 percent of attackers attempted to conduct a payroll diversion scam. Cryptocurrency scams remained a popular attack type, making up 9.2 percent of Forta's cases.



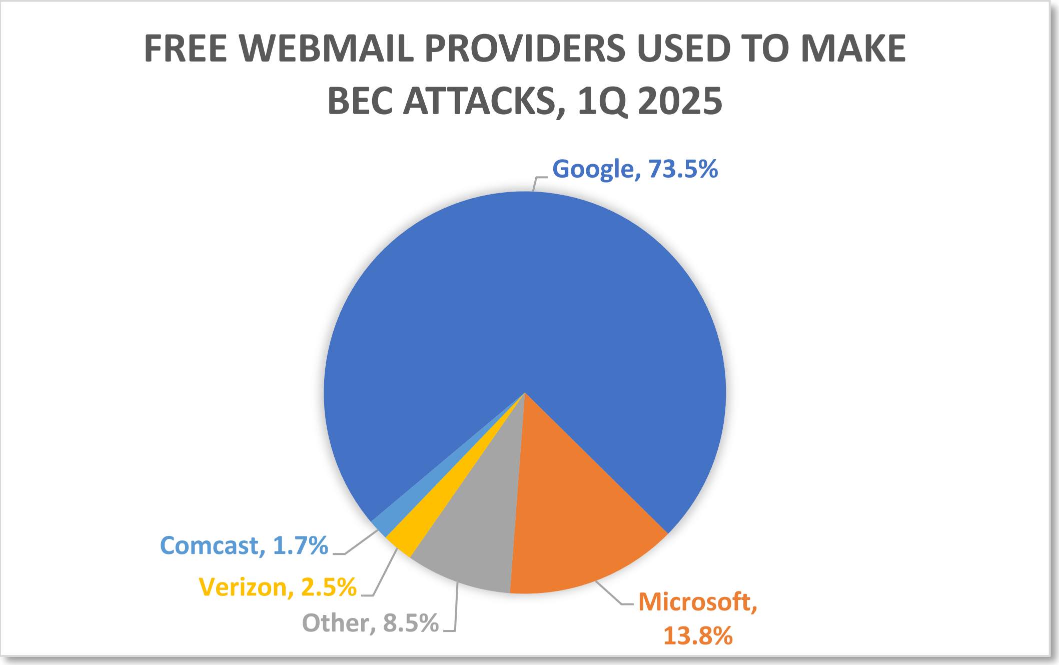
Fortra found that 72 percent of BEC attacks in Q1 2025 were launched using a free webmail domain. This is back to Q3 2024 levels, after a dip to just 63 percent in Q4 2024. The remaining 28 percent of BEC attacks in Q1 2025 utilized non-webmail domains.

Twenty-nine percent of the non-webmail BEC domains Fortra observed in Q1 2025 were registered at Cloudflare, making it the most popular registrar utilized by BEC scammers. At 19 percent, Squarespace was the second most popular registrar for BEC scammers.

John Wilson, Senior Fellow, Threat Research at Forta, remarked: “Fortra notes that Cloudflare was the most popular registrar for BEC scammers in Q1 2025. Q4 2024 was the first time Cloudflare broke our top ten, coming in at #3. This data suggests that BEC scammers feel protected when they hide behind Cloudflare's service offerings.”



Google’s Gmail was by far the most popular free webmail provider used by BEC scammers — Gmail was used for 73.5 percent free webmail accounts that scammers set up for BEC scams. Far below that at #2 were Microsoft’s webmail properties, which were used for 13.8 percent.



APWG Phishing Activity Trends Report Contributors

FORTRA Forta's mission is to help organizations increase security maturity while decreasing operational burden. Forta's brands include PhishLabs and Agari. www.fortra.com	mimecast Mimecast's AI-powered, Human Risk Management platform is purpose-built to protect organizations from the spectrum of cyber threats. www.mimecast.com
OP SEC OpSec Security is the leading provider of integrated online protection and on-product authentication solutions for brands and governments. www.opsecsecurity.com	ILLUMINTEL Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce. www.illumintel.com

The *APWG Phishing Activity Trends Report* is published by and is © the APWG. For info about the APWG, please contact info@apwg.org. For media inquiries related to company-provided content in this report, please contact: APWG Secretary General Peter Cassidy (pcassidy@apwg.org, +1.617.669.1123); Stefanie Wood Ellis of OpSec Security (sellis@opsecsecurityonline.com); Rachel Woodford of Fortra (Agari and PhishLabs) (Rachel.Woodford@fortra.com); Tim Hamilton of Mimecast (thamilton@mimecast.com).
Analysis and editing by Greg Aaron, Illumintel Inc., illumintel.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.

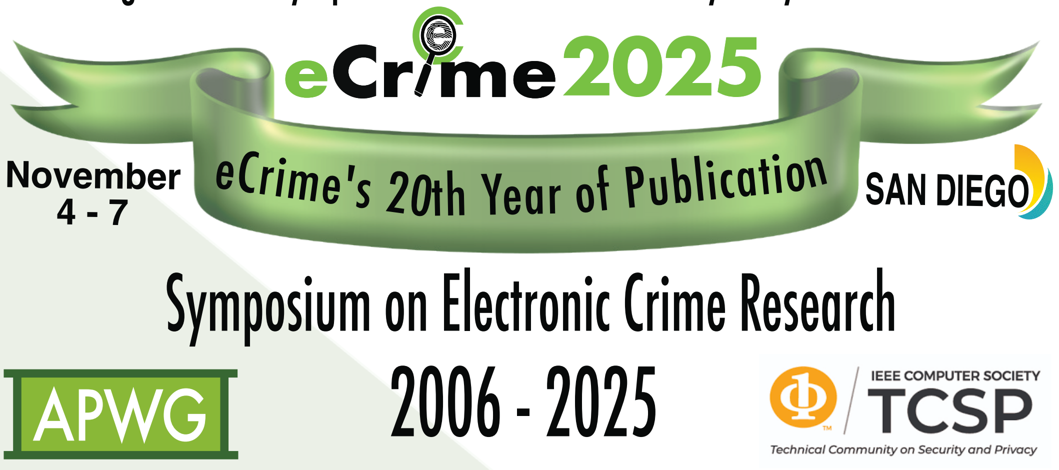
APWG eCrimeX

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.

The annual APWG Symposium on Electronic Crime Research, proceedings of which are published by the IEEE, attracts scores of papers from leading scientific investigators worldwide. The conference, founded in 2006 by APWG, is the only peer-reviewed, published (IEEE Digital Xplore since 2008) conference dedicated exclusively to cybercrime studies.

Come Celebrate APWG eCrime's 20th Anniversary: World's Only Peer-Reviewed Publishing Research Symposium Dedicated Exclusively to Cybercrime Research


eCrime2025
November
4 - 7
eCrime's 20th Year of Publication
SAN DIEGO
Symposium on Electronic Crime Research
APWG
2006 - 2025
IEEE COMPUTER SOCIETY
TCSP
Technical Community on Security and Privacy