Phishing Activity Trends Report

2nd Quarter 2025

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2025

Published 28 August 2025

Phishing Report Scope

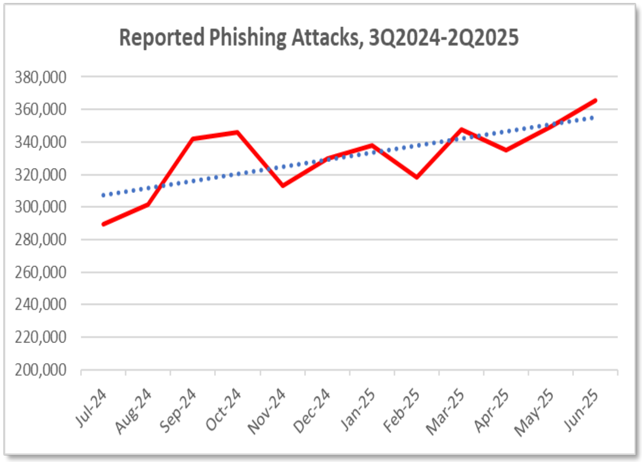
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG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

Phishing and Business e-Mail Compromise Attacks Rise in Q2 2025



Phishing Activity Trends Summary

- In the second quarter of 2025, APWG observed 1,130,393 phishing attacks, up from 1,003,924 attacks in Q1 2025. The number of phishing attacks has risen steadily over the last year. [pp. 3-4]
- The average amount requested in wire transfer BEC attacks in Q2 2025 was $83,099, a 97 percent increase from the prior quarter. The total number of wire transfer BEC attacks observed in Q2 2025 increased by 27 percent compared to Q1 2025. [pp. 8-10]
- 1,642 brands were targeted by criminals using QR codes. Delivery company DHL was attacked most often, followed closely by Microsoft. [pp. 5-7]
- Phishing attacks targeted the Financial/Payment, SaaS/Webmail, and the e-commerce sectors most frequently in Q2 2025. [pp. 4-5]

Statistical Highlights for the 2nd Quarter 2025

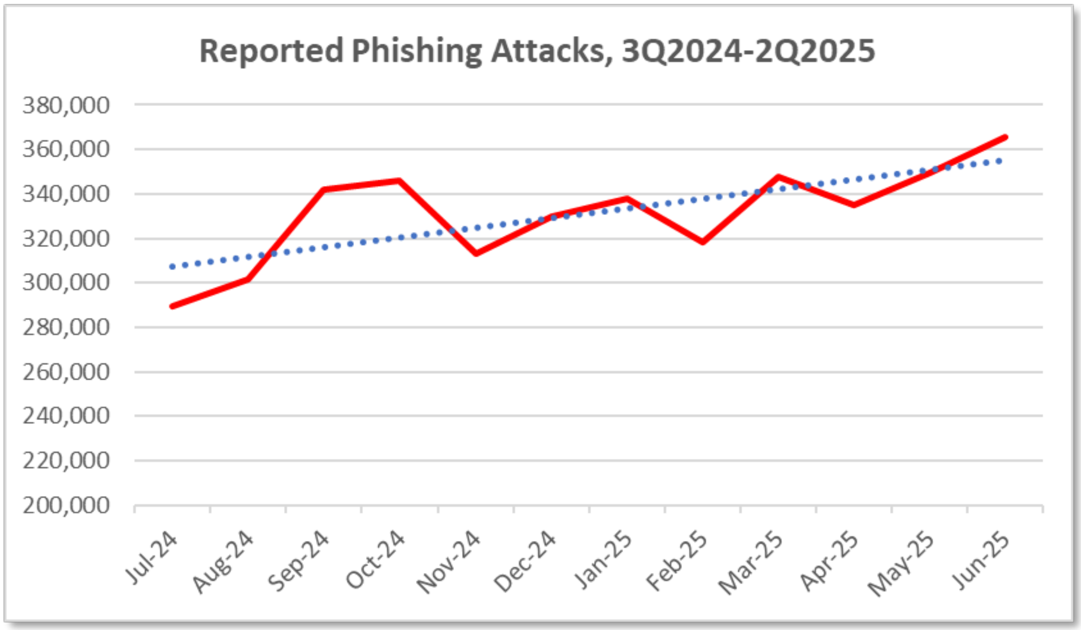
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

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.

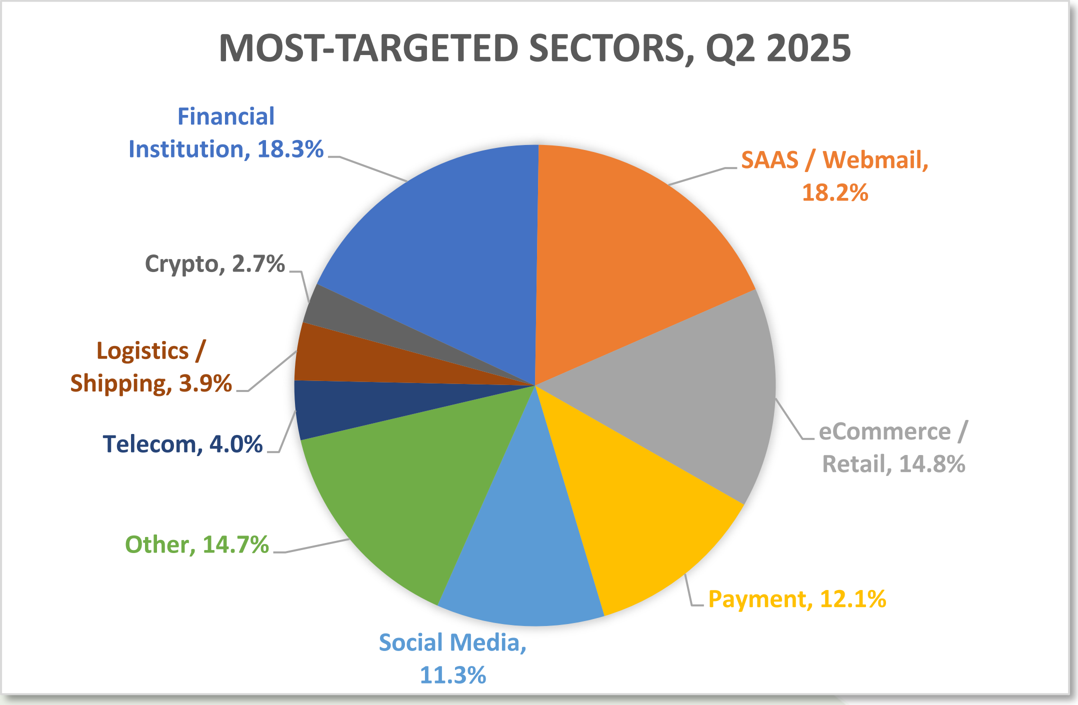
	April	May	June
Number of unique phishing Web sites (attacks) detected	335,139	349,511	365,381
Unique phishing email campaigns	23,288	21,729	35,345
Number of brands targeted by phishing campaigns	333	341	345

In the second quarter of 2025, APWG observed 1,130,393 phishing attacks, up 13 percent from 1,003,924 attacks in Q1 2025. This is the largest quarterly total since 1.28 million were observed in Q2 2023. The number has climbed steadily over the last year, from 932,923 in Q3 2024.



Most-Targeted Industry Sectors – 2nd Quarter 2025

In the second quarter of 2025, APWG founding member Crane Authentication/OpSec Security recorded that the Financial Institution category was the most-attacked sector, with 18.3 percent of all phishing attacks. The SAAS/Webmail category was close behind, with 18.2 percent of all phishing attacks.



Matthew Harris, Senior Product Manager, Fraud at Crane Authentication/OpSec Security, reported: "We are seeing a rise in the volume of phishing located on free hosting platforms and on domains where the network and hosting infrastructure is behind third-party protection services. We also saw an increase in vishing/smishing volumes, similar to Q1."

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

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 pages, and other fraudulent scam-promoting websites.

During Q2 2025, Mimecast detected 635,672 unique malicious QR codes. Over the six-month period covering Q4 2024 and Q1 2025, Mimecast detected more than 1.7 million unique malicious QR codes.

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:

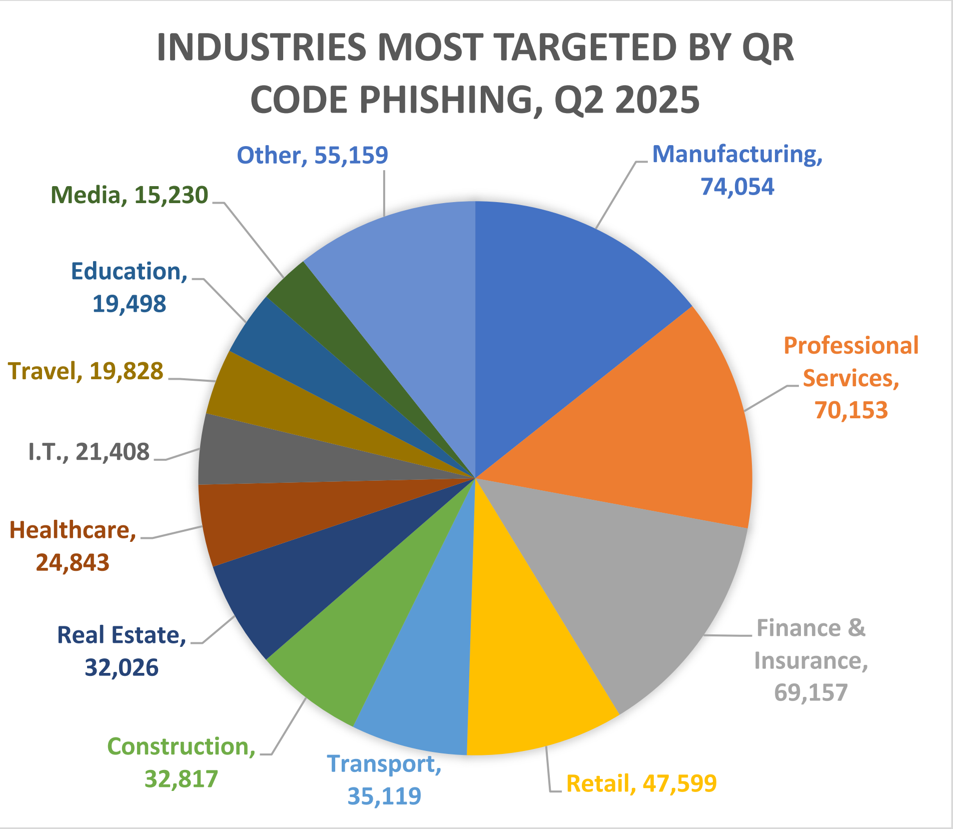
- While some QR code generators require a subscription, others are free. Free services naturally tend to devote fewer resources to preventing and shutting down malicious use.
- Many QR generators offer tracking—they allow their customers to see how many times a QR code has been scanned and when, and 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 in Q2 2025:

1. **O2O[.]TO** was the most-used QR code generator, used to create 214,353 unique malicious QR codes. While this service is used by famous brands, threat actors heavily exploited its infrastructure for phishing and fraud campaigns.
2. **QR[.]PRO** is owned by QR-Code.io. It was used to generate 126,929 unique malicious QR codes.
3. **ZIGPOLL[.]COM** offers polling and feedback tools to companies, including to large brands. Zigpoll's survey tool was abused by phishers to create 120,000 codes that pointed to phishing and fraud sites.

Most-Targeted Industries

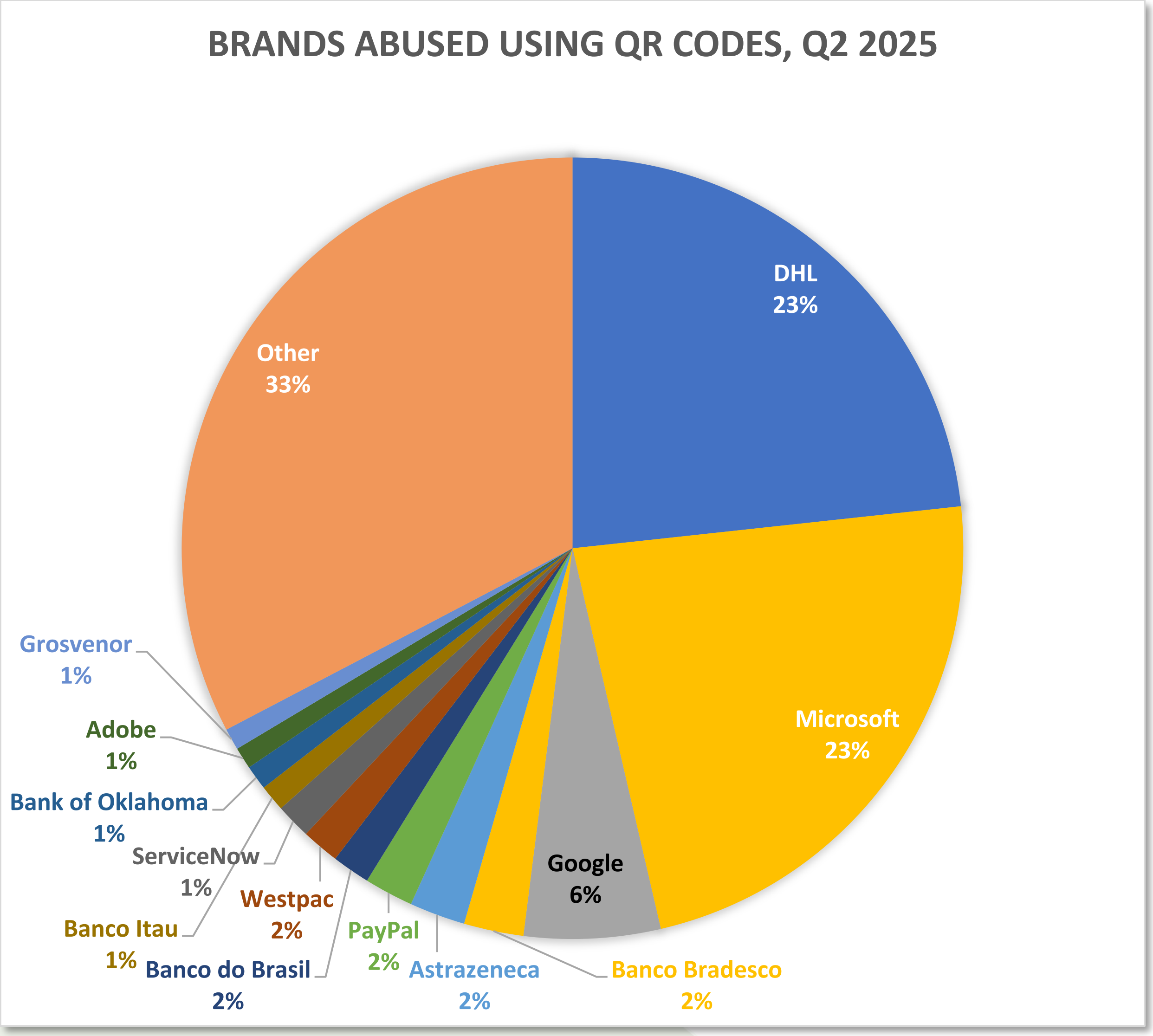
No single industry stood out as particularly vulnerable during this time period—criminals attacked multiple sectors. Manufacturing was the most-often-attacked sector, with 74,054 detections, after being #2 in Q1 2025. Attacks against the Construction sector fell significantly, from #2 to #6. The attack distribution reflects strategic focus on industries with high digital transaction volumes and customer interaction touchpoints, rather than opportunistic targeting.



Brands Most Targeted by Malicious QR Code Phishing

Mimecast counted 1,642 brands that were targeted by criminals using QR codes. Delivery company DHL was attacked most often, with 3,543 different QR codes, followed closely by Microsoft.

There was a great deal of volatility in the rankings. DHL did not appear in the ten-most-attacked brands in Q1 2025. Mastercard was the most-attacked brand in Q1, but was only attacked with three QR codes in Q2, coming in a #290. Microsoft was in the #2 position in Q1 and in Q2.

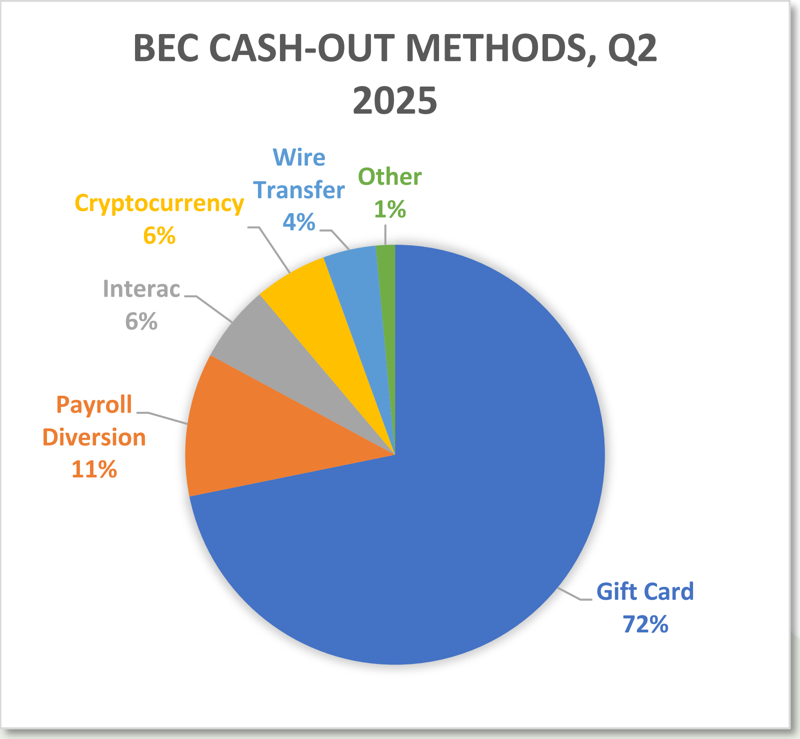


Banks and payment processing companies such as PayPal were attacked regularly. The attackers were likely collecting credentials they could turn into cash, such as by buying physical goods with stolen credit card data.

Business e-Mail Compromise (BEC), 2nd 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 Q2 2025. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

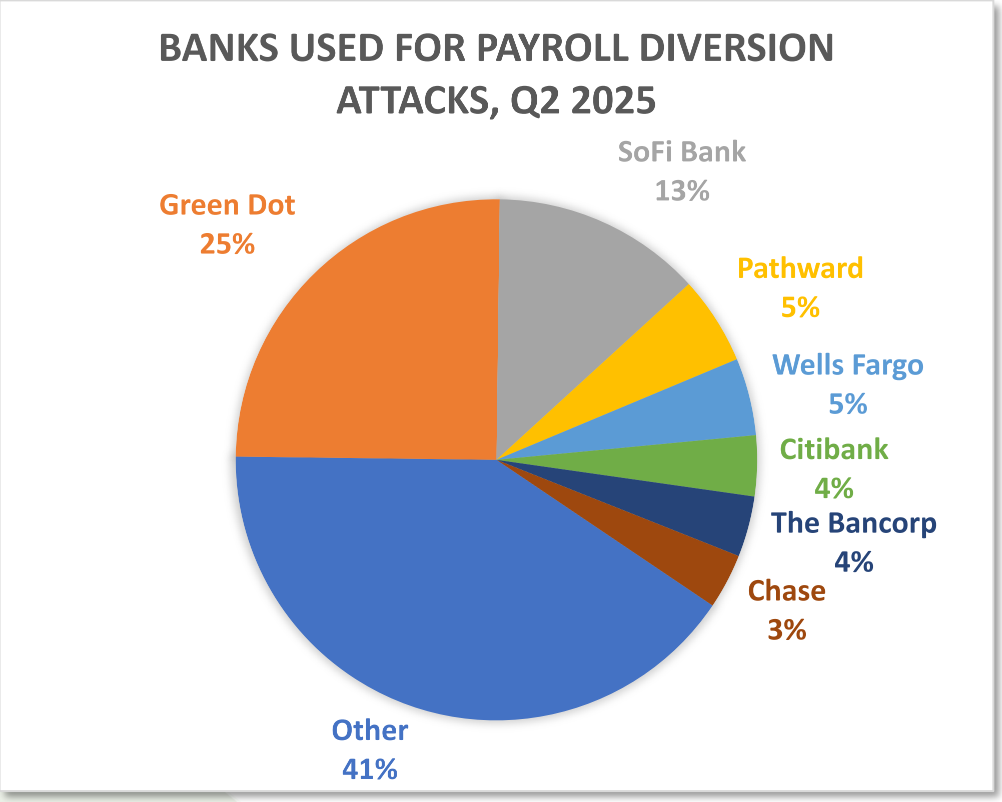
Fortra found that the average amount requested in wire transfer BEC attacks in Q2 2025 was $83,099, a 97 percent increase from the prior quarter's average of $42,236. The total number of wire transfer BEC attacks observed by Fortra in Q2 2025 increased by 27 percent compared to the previous quarter.

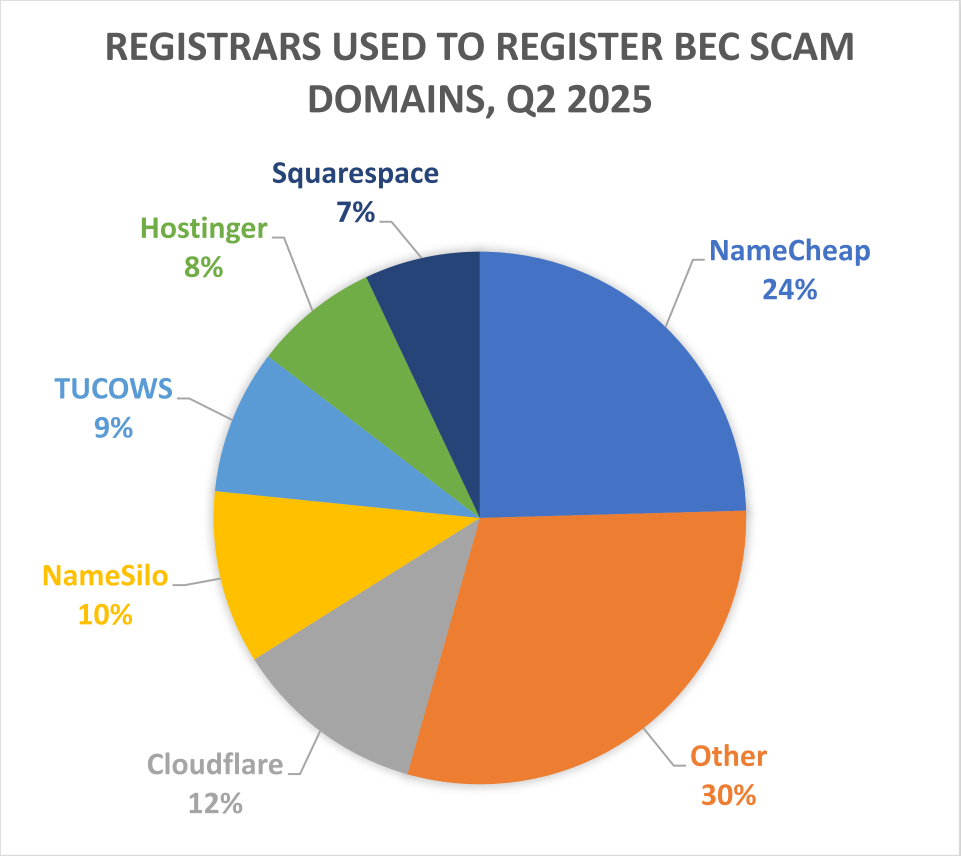


The increase was driven by a rash of executive coaching scam messages. The messages purport to come from various executive coaching firms and contain two PDF attachments. The first attachment is an invoice while the second is a completed IRS form W-9. The messages include a spoofed reply chain between the executive and the coaching firm. The threat actors conducting this scam are in South Africa, Turkey, and Nigeria.

During the second quarter of 2025, gift card scams were once again the most popular scam type. About 11 percent of attacks attempted to conduct payroll diversion scams. Extortion scams and QR code phishing were also popular scams, each comprising around 7 percent of the incidents tracked between April and June 2025.

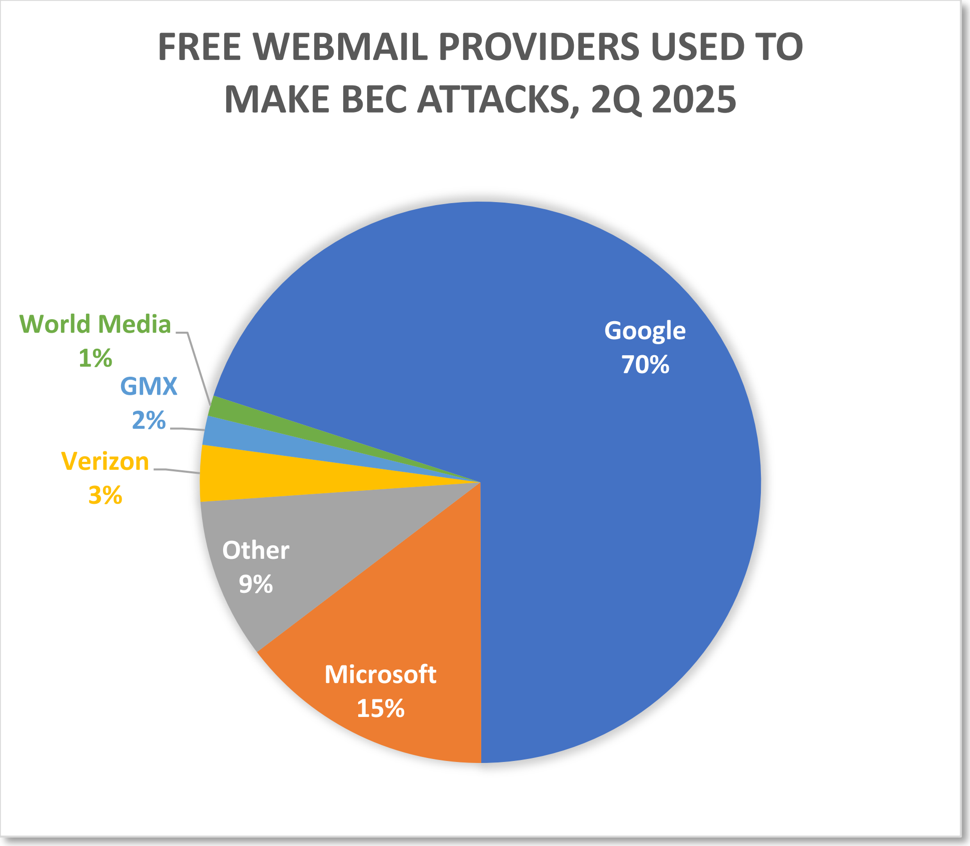
Green Dot was once again the preferred bank of payroll diversion scammers, with one in four payroll diversion attempts directed towards accounts at one of Green Dot's brands. SoFi was the second most popular bank for payroll diversion scammers, followed by Pathward and Wells Fargo. While scammers may prefer certain banks, no bank is immune. In all, Fortra collected mule accounts at 84 different banks this quarter.





Domain registrar NameCheap was used most often by BEC scammers. Registrar Cloudflare dropped to the #2 position, after being the most-popular registrar with BEC scammers in Q1 2025.

Fortra observed that 68 percent of BEC attacks in Q2 2025 were launched using a free webmail account. The remaining 32 percent of BEC attacks in Q2 2025 utilized non-webmail domains. Google's Gmail was by far the most popular free webmail provider used by BEC scammers — Gmail was used for 70 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 15 percent.


FREE WEBMAIL PROVIDERS USED TO MAKE BEC ATTACKS, 2Q 2025
Google 70%
Microsoft 15%
Other 9%
Verizon 3%
GMX 2%
World Media 1%

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
Crane Authentication Crane Authentication/OpSec Security *is* the leading provider of integrated online protection and on-product authentication solutions for brands and governments. http://www.craneauthentication.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 of Crane Authentication/OpSec Security (stefanie.wood@craneauthentication.com); Jessica Ryan of Fortra (Agari and PhishLabs) (jessica.ryan@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 an 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.

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

Symposium on Electronic Crime Research

APWG 2006 - 2025 IEEE COMPUTER SOCIETY TCSP Technical Community on Security and Privacy

Register Now for eCrime 2025 San Diego: apwg.org/events/ecrime2025

Sponsorships: eCrime2025@apwg.org

eCrime correspondence: eCrime2025@apwg.org