Phishing Activity Trends Report

3rd Quarter 2025

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2025

Published 9 December 2025

Phishing Report Scope

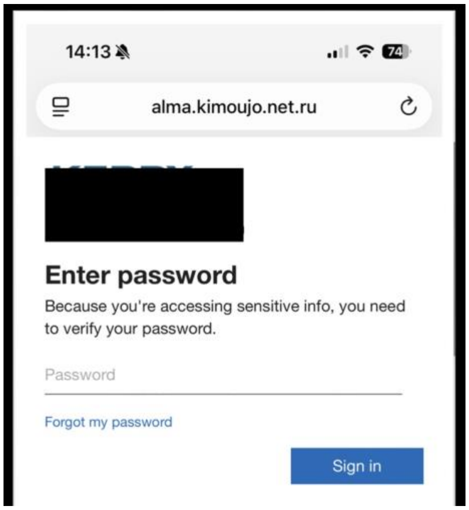
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG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

Phishers Attacking By All Media, Using Texts, QR Codes, and More



alma.kimoujo.net.ru

[redacted]

Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

Forgot my password

Sign in

Phishing Activity Trends Summary

- In the third quarter of 2025, APWG observed 892,494 phishing attacks, down from 1,130,393 in Q2 2025. [pp. 3-4]
- SMS-based fraud increased by nearly 35% in Q3. [p. 4]
- Phishers targeted the SaaS/Webmail and the Social Media sectors most frequently. [pp. 4-5]
- Total wire-transfer BEC attacks in Q3 2025 increased by 57% compared to Q2. The average amount requested was $48,115, a 42% decrease from the prior quarter's average of $83,099. [pp. 7-8]
- During Q3 2025, Mimecast detected 716,306 unique malicious QR codes used for phishing, up 13% from 635,672 in Q2. The manufacturing was the sector most often attacked with malicious QR codes. [pp. 5-7]

Statistical Highlights for the 3rd Quarter 2025

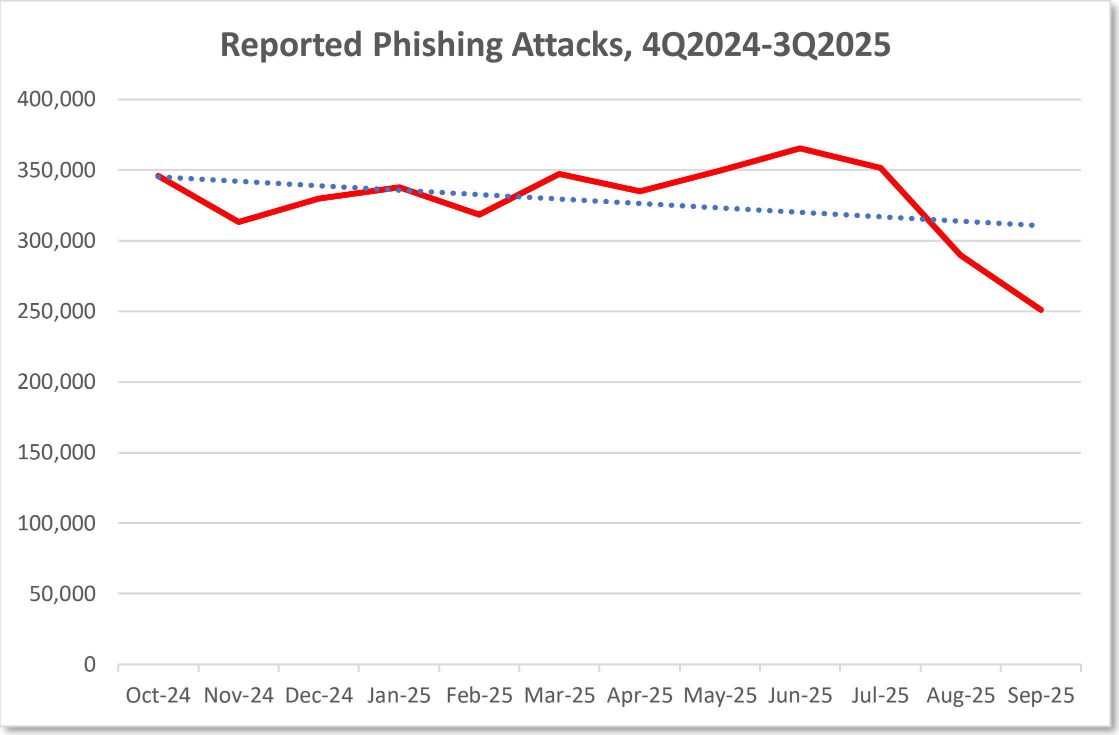
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

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.

	July	August	September
Number of unique phishing Web sites (attacks) reported	351,590	289,848	251,056
Unique phishing email campaigns	32,897	30,497	18,316
Number of brands targeted by phishing campaigns	330	351	311

In the third quarter of 2025, APWG observed 892,494 phishing attacks, with a notable dip in September. That was down from 1,130,393 attacks in Q2 2025, which was largest quarterly total seen since Q2 2023. A total of 427 unique brands were identified in the reports across the quarter.

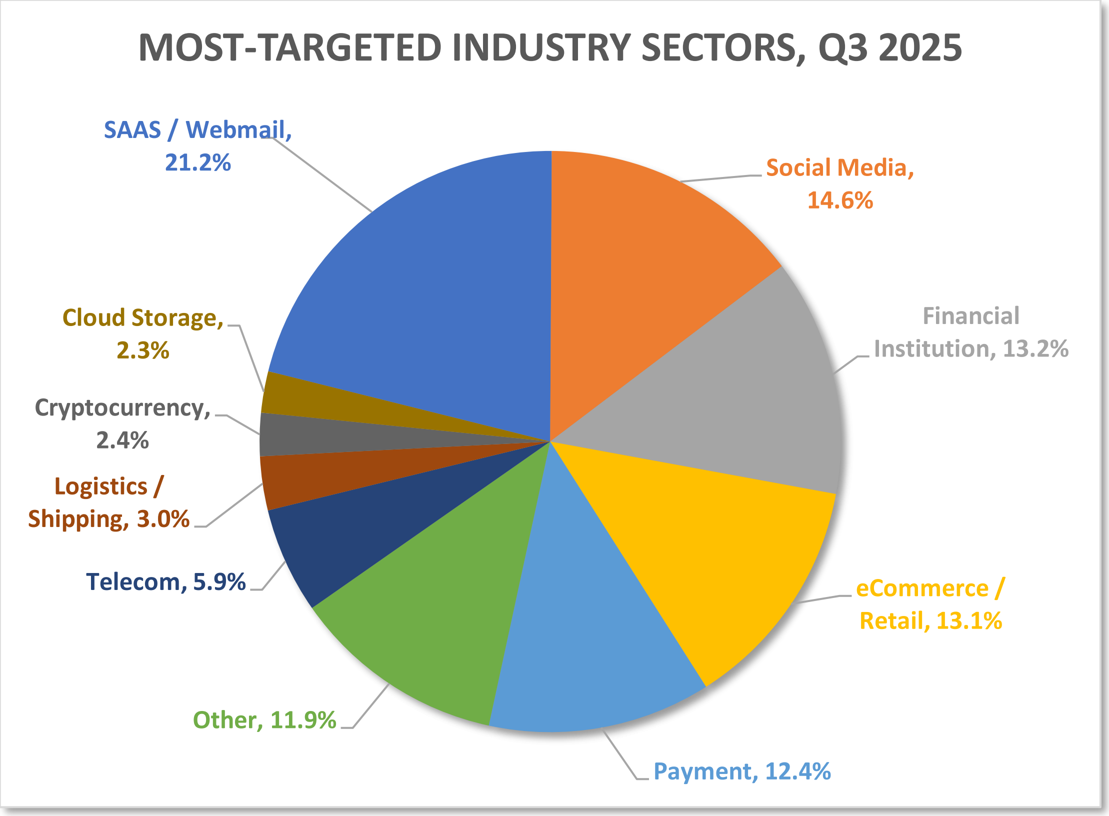


Most-Targeted Industry Sectors – 3rd Quarter 2025

In the third quarter of 2025, APWG founding member Crane Authentication (formerly OpSec Security) recorded that the SAAS/Webmail category was the sector most attacked by phishing, with 21.2 percent of all phishing attacks. Social Media came in at #2, with 14.6 percent of phishing attacks. Financial Institutions were the most-targeted sector in Q2, but fell to #3 in Q3.

In Q3 2025 Crane Authentication detected a decrease in phishing that used URLs as compared to Q2 2025. Instead, vishing/smishing volumes continued to rise. “Our SMS-based fraud detections have increased by nearly 35 percent in the last quarter” said Matthew Harris, Senior Product Manager, Fraud at Crane Authentication. He attributed the increase in part to improvements in the company’s honeypot system.

Crane Authentication offers expertise, decades in development, 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 Q3 2025, Mimecast detected 716,306 unique malicious QR codes, up 13 percent from 635,672 in Q2. Over the 12 months from Q2 2024 through Q3 2025, Mimecast detected more than 3 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:

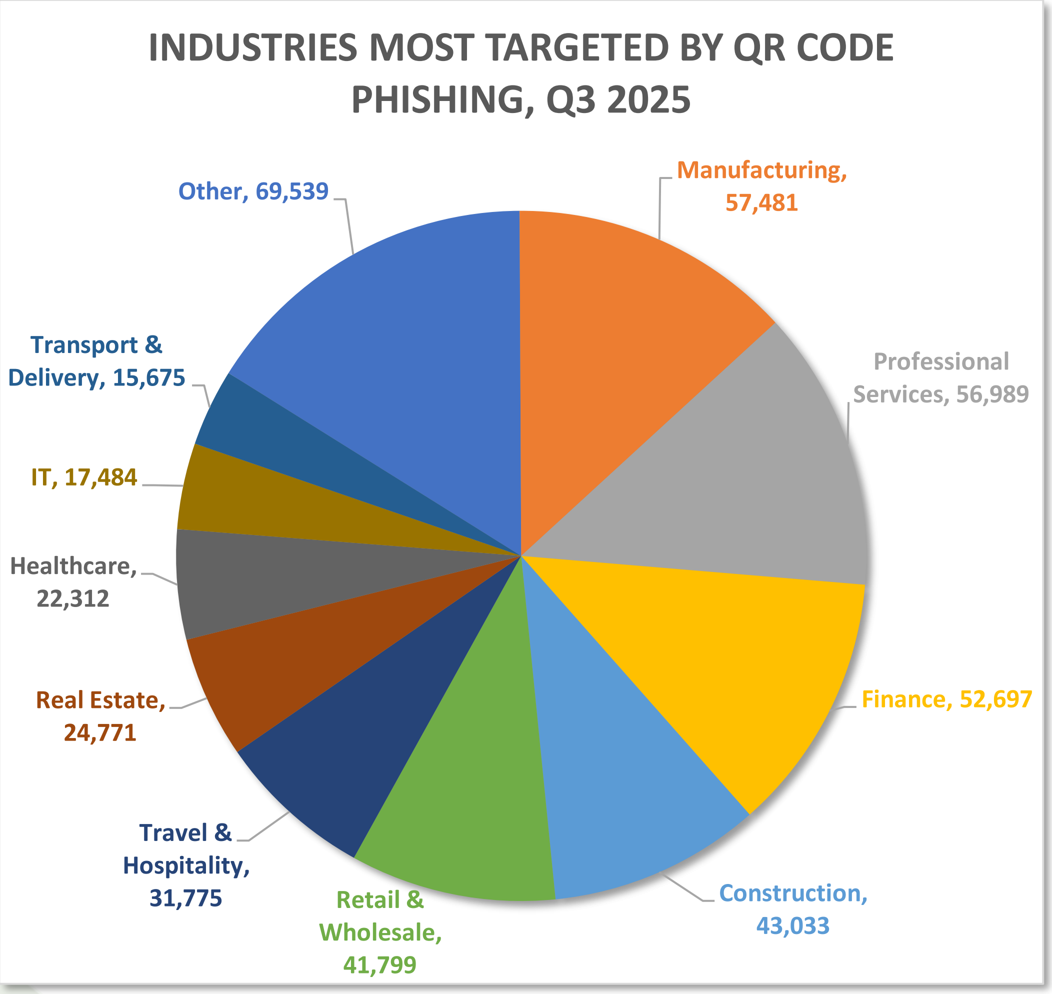
- While some QR code generators require a subscription, others are free. Free services naturally tend to devote fewer resources to preventing and shutting down malicious use.
- Many QR generators offer tracking—they allow their customers to see how many times a QR code has been scanned and when, and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

The domain JSJ[.]TOP generated 1,149,088 detections (detected attacks), establishing itself as the most prolific attack source. QR code generation platforms dominated the threat landscape: QRTO[.]ORG accounted for 205,037 detections, QR[.]PRO contributed 143,078 detections, and ME-TEAM.ORG recorded 77,351 detections. These platforms have generated persistent abuse across quarters.

The most repeated URL was a phishing page on BIO.LINK (hxxps://bio.link/nestohyperksa), which appeared 23,925 times. Bio Link is a social media link aggregation platform that allows users to create single landing pages containing multiple links—commonly used by online influencers and businesses to list their links on various online platforms. Threat actors exploit bio.link's trusted reputation in order to fool users. The platform's ease of use, free service tier, and lack of a user verification process make it attractive for rapidly deploying phishing campaigns.

Most-Targeted Industries

No single industry stood out as particularly vulnerable during this report period—criminals attacked multiple sectors. Manufacturing was the most-often-attacked sector, with 74,054 detections, as it was in Q2 2025. The attack distribution reflects strategic focus on industries with high digital transaction volumes and customer interaction touchpoints, rather than opportunistic targeting.



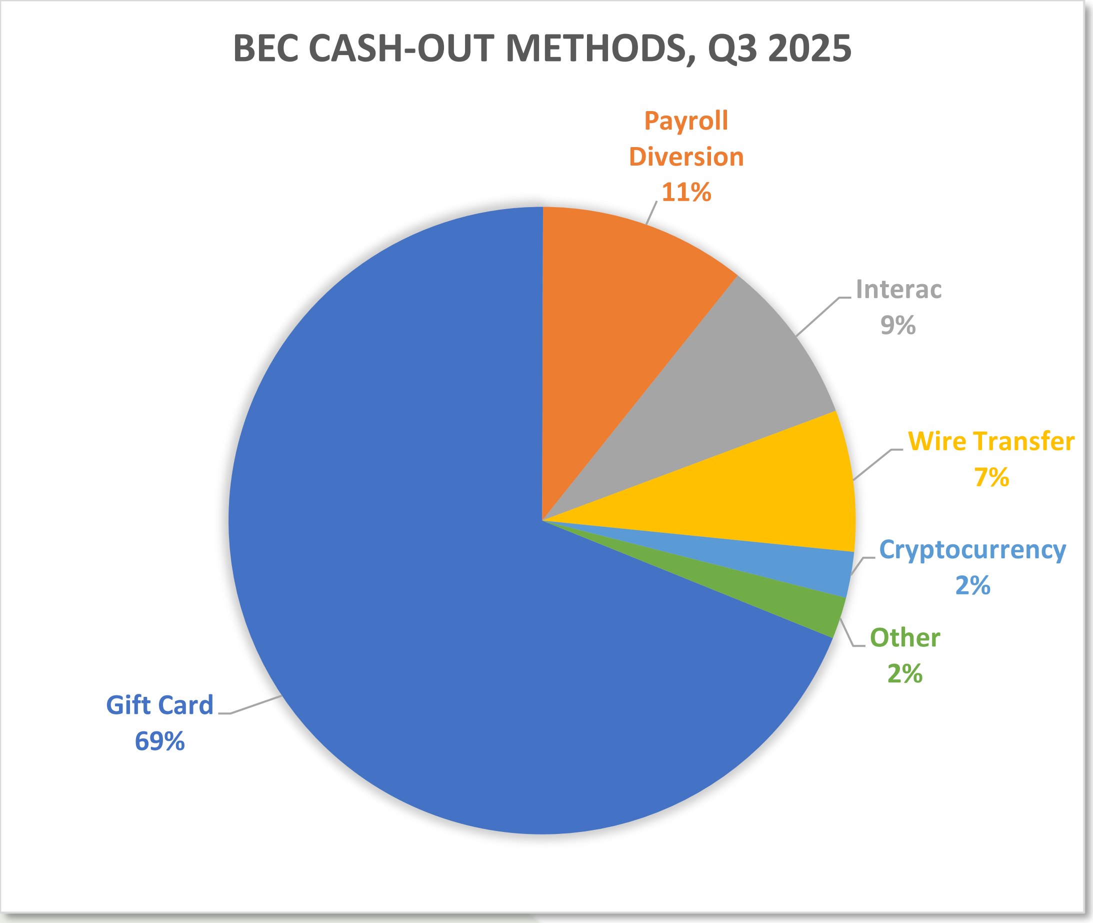
Walmart was most impersonated brand in Q3, supplanting delivery company DHL.

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 Q3 2025. Fortra protects organizations against phishing, BEC scams, and other advanced email threats

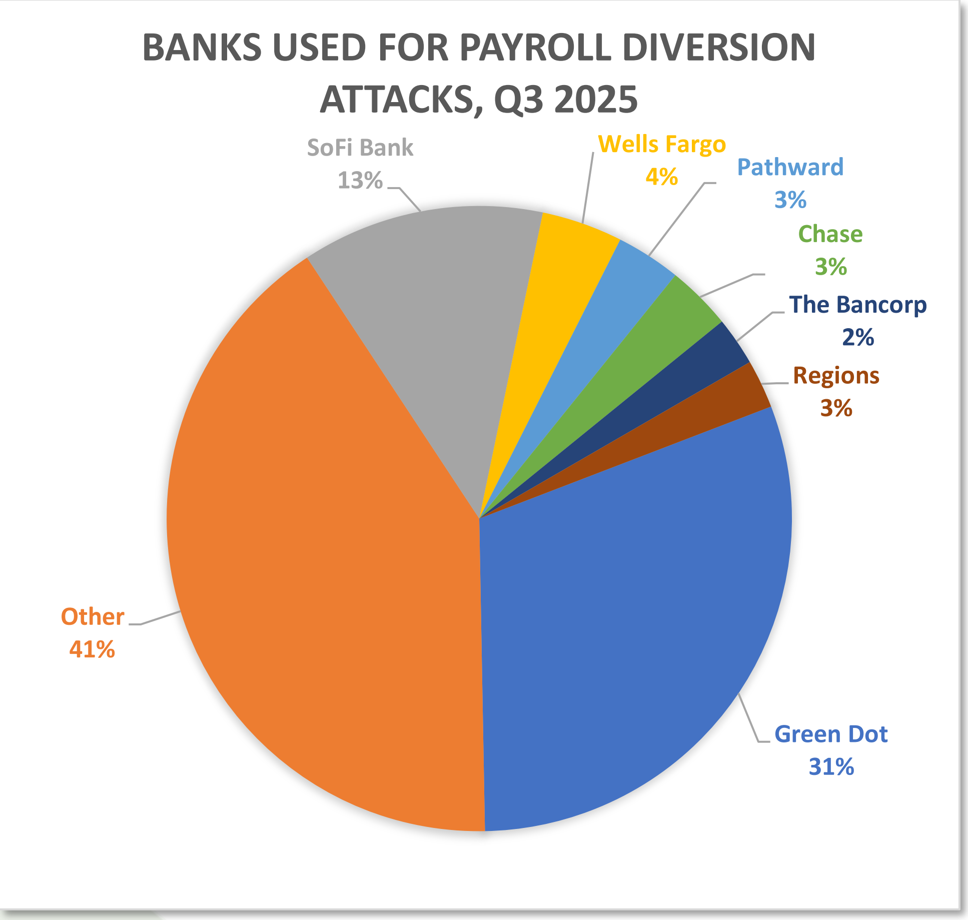
Fortra found that the average amount requested in wire transfer BEC attacks in Q3 2025 was $48,115, a 42 percent decrease from the prior quarter's average of $83,099. The total number of wire transfer BEC attacks observed by Fortra in Q3 2025 increased by 57 percent compared to the previous quarter.

Fortra attributes the increase in attack volume to a threat group it has dubbed Scripted Sparrow. Scripted Sparrow sends out large quantities of messages containing invoices for executive coaching services. The amount requested is usually just below $50,000. The group, whose members hail from South Africa, Nigeria, and Turkey uses a spoofed reply chain designed to trick the recipient into believing the expense was approved by a company executive. The volume of these attacks suggests the use of automation to generate the unique PDF attachments and message bodies.

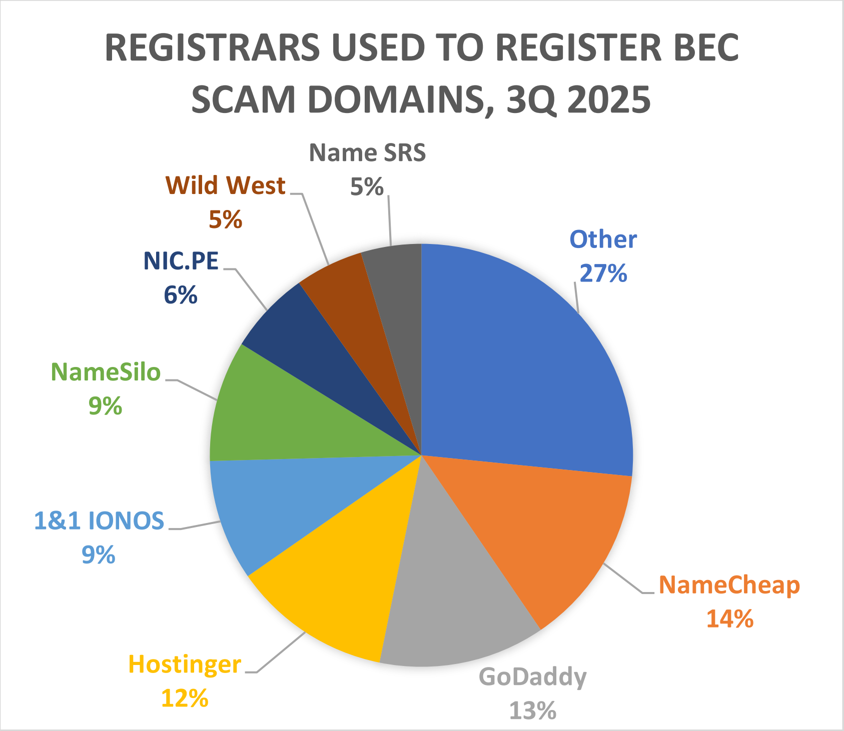


During the third quarter of 2025, gift card scams were once again the most popular scam type, making up 45 percent of the total, compared to 7 percent of attempts that conducted a payroll diversion scam. Due to the high volume of Scripted Sparrow attacks, Wire Transfer requests increased to 5 percent of the attack volume compared to just 3 percent in the previous quarter.

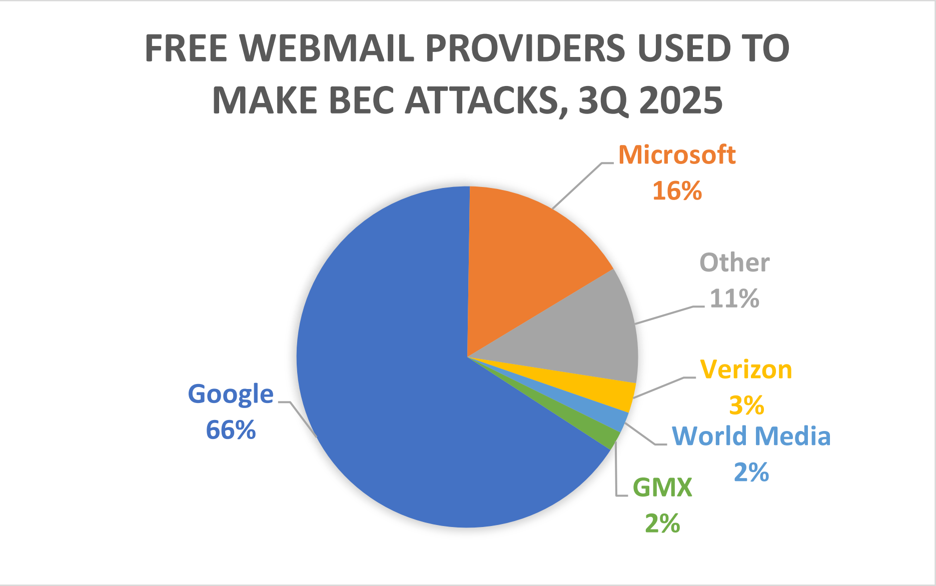
Green Dot was once again the preferred bank of payroll diversion scammers, with 31 percent of payroll diversion attempts directed towards accounts held at one of Green Dot's brands. SoFi was the second most popular bank for payroll diversion scammers, followed by Wells Fargo. While scammers may prefer certain banks, no bank is immune. In all, Fortra recorded mule accounts at 89 different banks this quarter.



Domain registrar NameCheap continued to be the domain registrar used most often by BEC scammers. Registrar Cloudflare dropped out of the top eight, after being the most-popular registrar with BEC scammers in Q2 2025.



Fortra observed that 74 percent of BEC attacks in Q3 2025 were launched using a free webmail domain. The remaining 26 percent utilized non-webmail domains. Google's Gmail was by far the most popular employed by BEC scammers—used for 66 percent of the free webmail accounts that scammers set up for BEC scams. Far below that at #2 were Microsoft's webmail properties, which were used for 16 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
Crane Authentication Crane Authentication 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 (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 3,100 enterprises worldwide that have joined the APWG since the institution's foundation.

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; and the APWG's Applied Research secretariat <http://www.ecrimeresearch.org>.

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.

The eCrime eXchange, APWG's global 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 deployed by cabinet-level ministries, government CERTs and national-scope NGOs. Contact: info@stopthinkconnect.org to join this global initiative and stop cybercrime.

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 research.