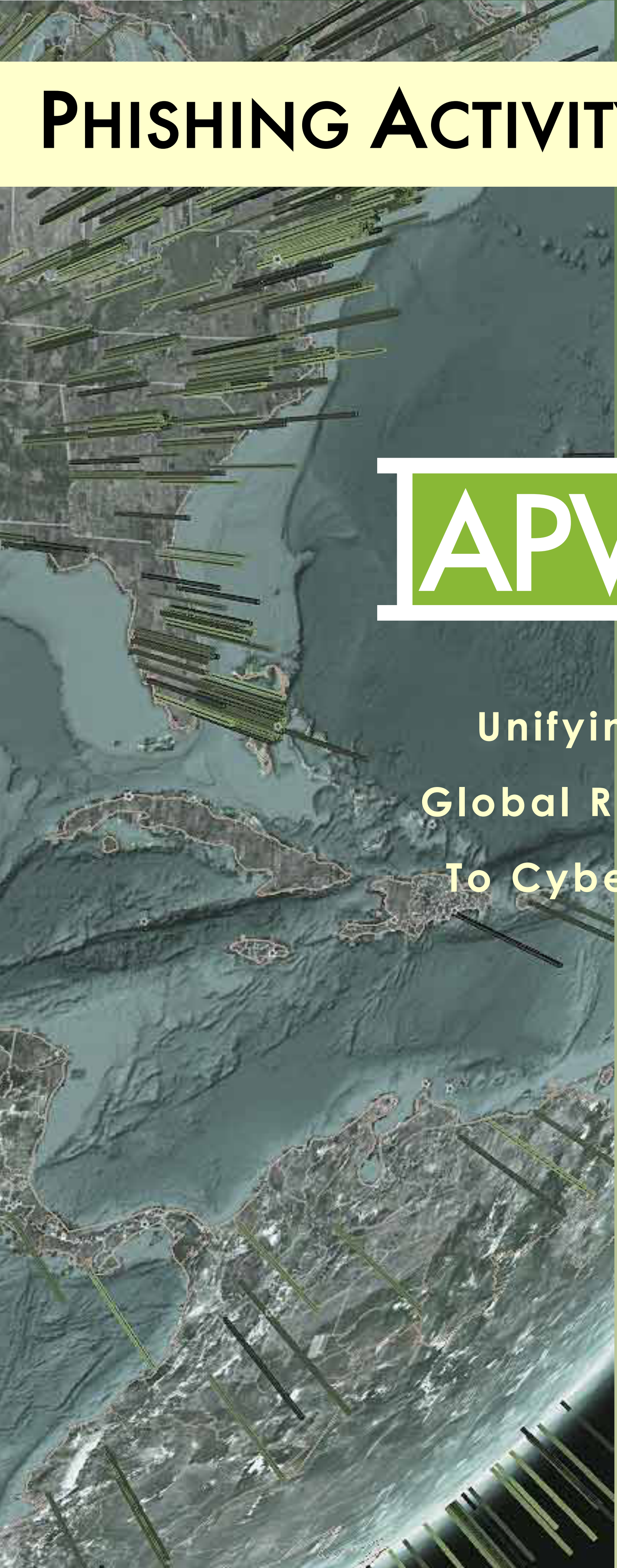
Phishing Activity Trends Report



2nd Quarter 2024

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2024

Published 21 August 2024

Phishing Report Scope

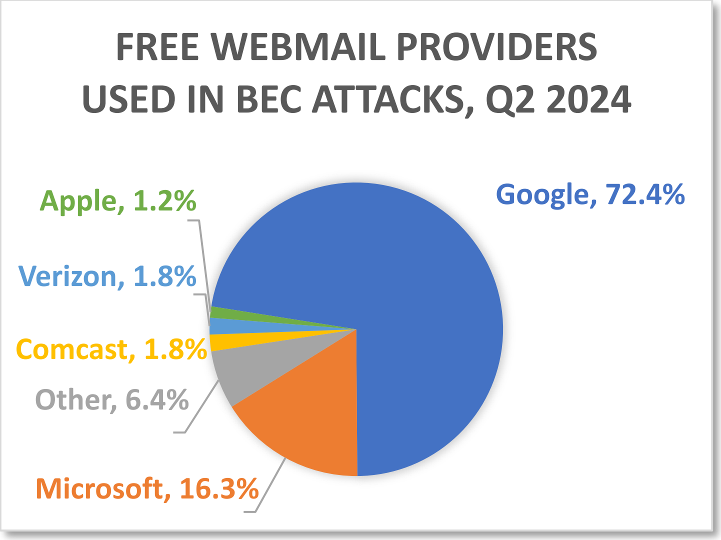
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG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



Google Gmail accounts were used in 72.4 percent of all Business Email Compromise (BEC) scams. [pp. 7-8]

Phishing Activity Trends Summary

- In Q2 2024, APWG observed 877,536 phishing attacks while the number of reported phishing attacks has remained generally steady. [pp. 3-4]
- Phishing via phone calls and text messages is being used with increasing frequency to attack bank customers and payment service users. [p. 5]
- Social media platforms were once again the most frequently attacked sector, representing 32.9 percent all phishing attacks. [p. 4]
- The average wire transfer amount requested in BEC attacks in Q1 2024 was $89,520, up from the prior quarter. [p. 6]
- Google Gmail accounts were used in 72.4 percent of all Business Email Compromise (BEC) scams. [pp. 7-8]

Statistical Highlights for the 1st Quarter 2024

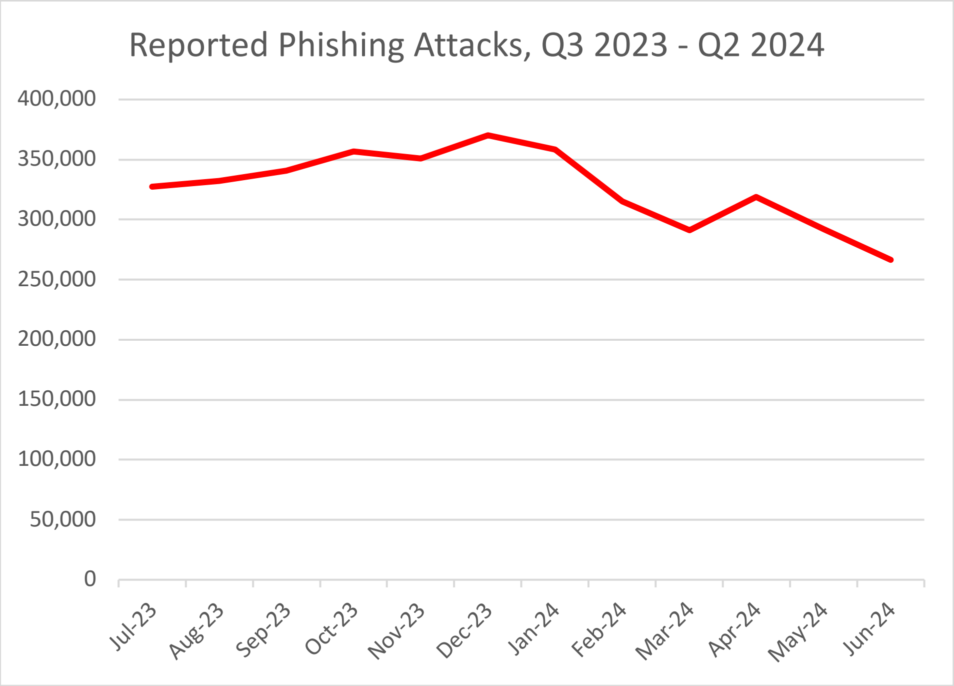
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange (eCX).

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	318,651	292,428	266,457
Unique phishing email campaigns	31,005	33,874	31,173
Number of brands targeted by phishing campaigns	324	320	301

In the first quarter of 2024, APWG observed 963,994 phishing attacks. In the second quarter, the number fell to 877,536. We suspect that the decrease is due in part to a recent reporting issue: email providers have been making it more difficult for users to report phishing to APWG and to other anti-abuse actors and law enforcement authorities. For years, APWG has asked users to forward suspected phishing emails to *reportphishing@apwg.org* for analysis. It has become apparent from complaints and testing that some major email providers are now blocking these outbound messages forwarded by the original recipients. (Ironically, these providers deliver the phishing emails to their users, but then prevent their users from reporting out the phishing.) The situation suggests the providers are not finding the phishing URLs in the emails they are delivering to their users, but are later finding the phishing URLs when the user tried to forward a message. To help get around this issue, APWG is setting up new web forms for users.



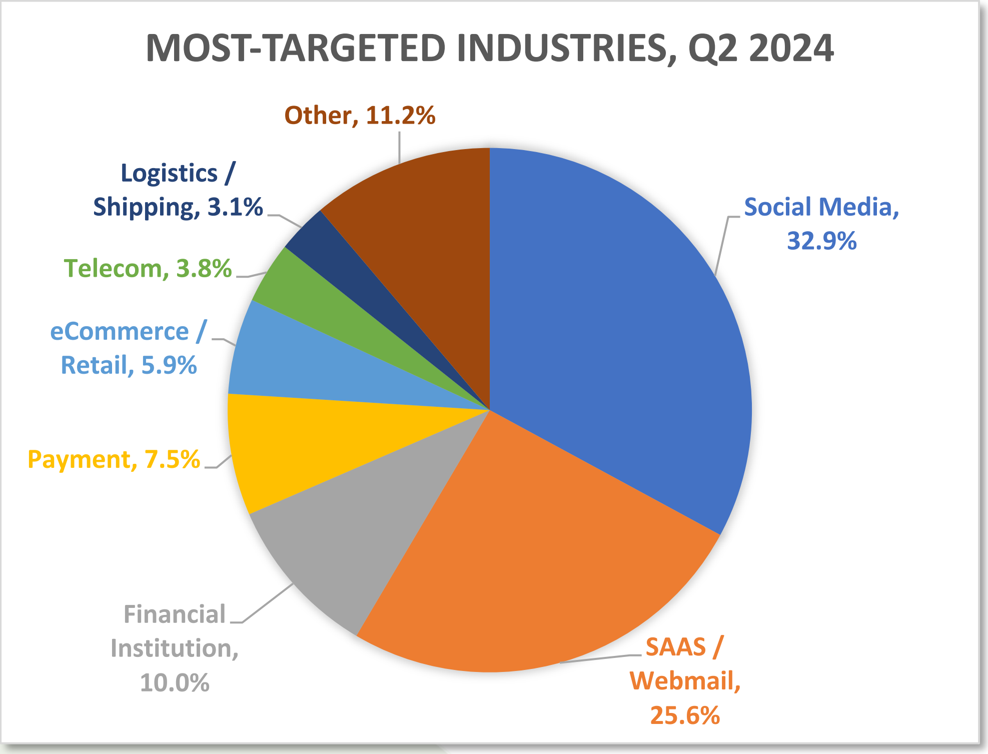
In general, the number of reported phishing attacks appears to have been steady over the last year. Interisle Consulting recently published a global study of phishing that took place from May 2023 to April 2024. Interisle used the phishing reports made to APWG's eCrime Exchange, plus reports from OpenPhish, Spamhaus, and PhishTank. Interisle found that year-over-year, the number of phishing attacks grew by 50,000, to just under 1.9 million attacks, a slight rise. APWG member OpSec Security recorded a 10 percent increase in URL-based fraud in Q2 2024 versus Q1 2024.

Most-Targeted Industry Sectors – 2nd Quarter 2024

In the second quarter of 2024, APWG founding member OpSec Security found that social media platforms were once again the most frequently attacked sector, representing 32.9 percent all phishing attacks. Phishing against the Financial Institution (banking) segment were mostly steady at 10 percent, down from 24.9 percent of all attacks in Q3 2023 and 14 percent in Q4 2023. Attacks against online payment services (such as PayPal, Venmo, Stripe, and similar companies) were also steady, with another 7.5 percent of all attacks.

Matthew Harris, Senior Product Manager, Fraud at OpSec, explained why banking and payment sites are being attacked less frequently. "We have observed an increased share of fraud being targeted towards sites that do not require high security, such as social media sites like Facebook and LinkedIn, and SAAS and Webmail accounts such as Microsoft Outlook and Netflix." Phishing that uses email lures is being hampered by advanced filtering technologies and sending requirements, making it more difficult for scammers to get their emails into victim in-boxes.

Harris added: "It's assumed that banks and similar institutions are becoming more difficult targets to phish using traditional email lures." Banks require two-factor authentication for online banking, such as codes sent the users' mobile phones. Without those authentication codes, phishers can't get into victims' online financial accounts. So instead, fraudsters are using phone-based methods to phish bank and payment service users. These are more immediate contact methods, and allow the fraudster to talk victims out of their sensitive information. Phone-based fraud is initiated by different methods. One is voice phishing or *vishing* -- where fraudsters call potential victims. Another is SMS-based phishing or *smishing* – in which fraudsters advertise the URLs of phishing sites within SMS (Short Message Service) and Internet-generated, phone-to-phone text messages.

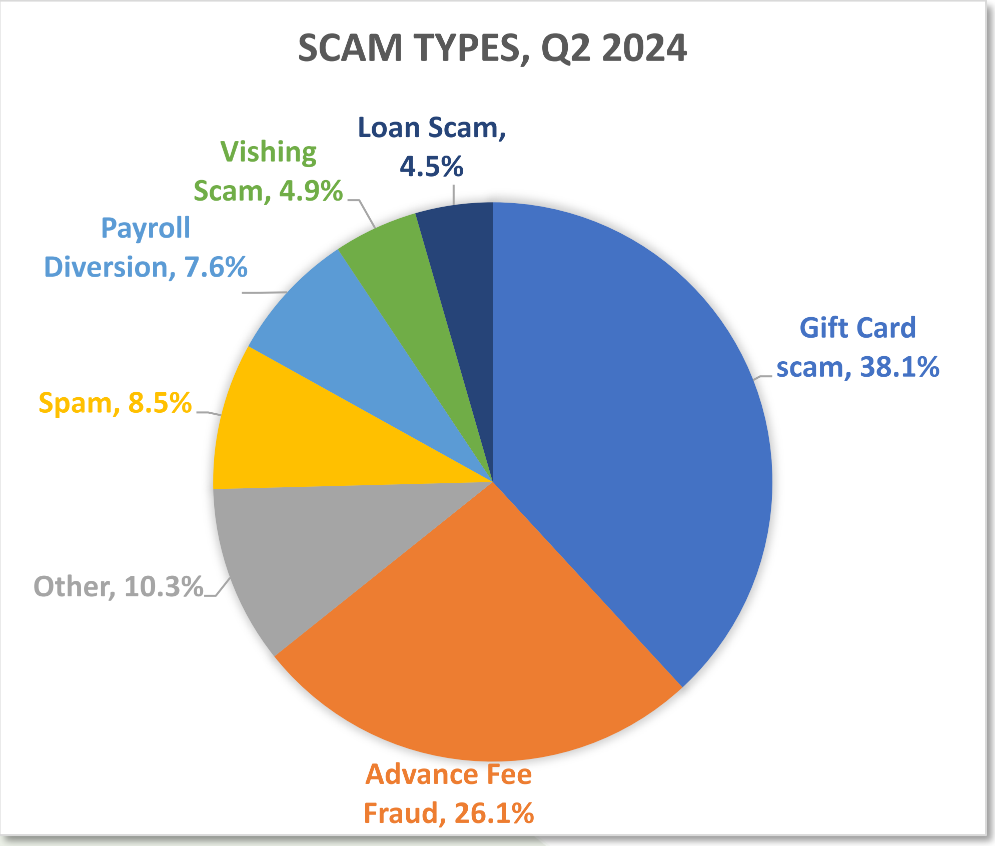


OpSec Security offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 2nd Quarter 2024

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI's Internet Crime Complaint Center (IC3). 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 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

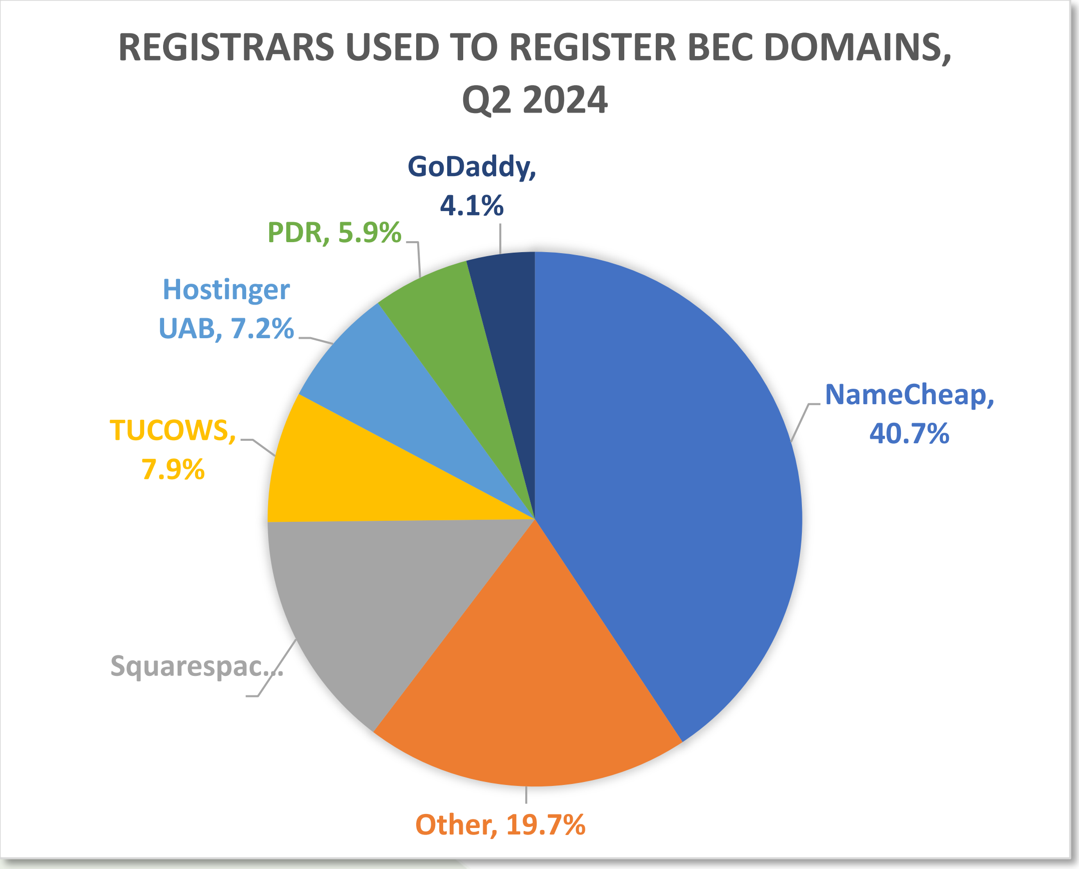
Fortra found that the average amount requested in wire transfer BEC attacks in Q2 2024 was $89,520, up 6.5% from Q1's average of $84,059. The volume of wire transfer BEC attacks in Q2 2024 decreased by 8.4 percent compared to Q1. This suggests the bad actors behind BEC wire transfer attacks did not significantly change their tactics compared to the prior quarter.



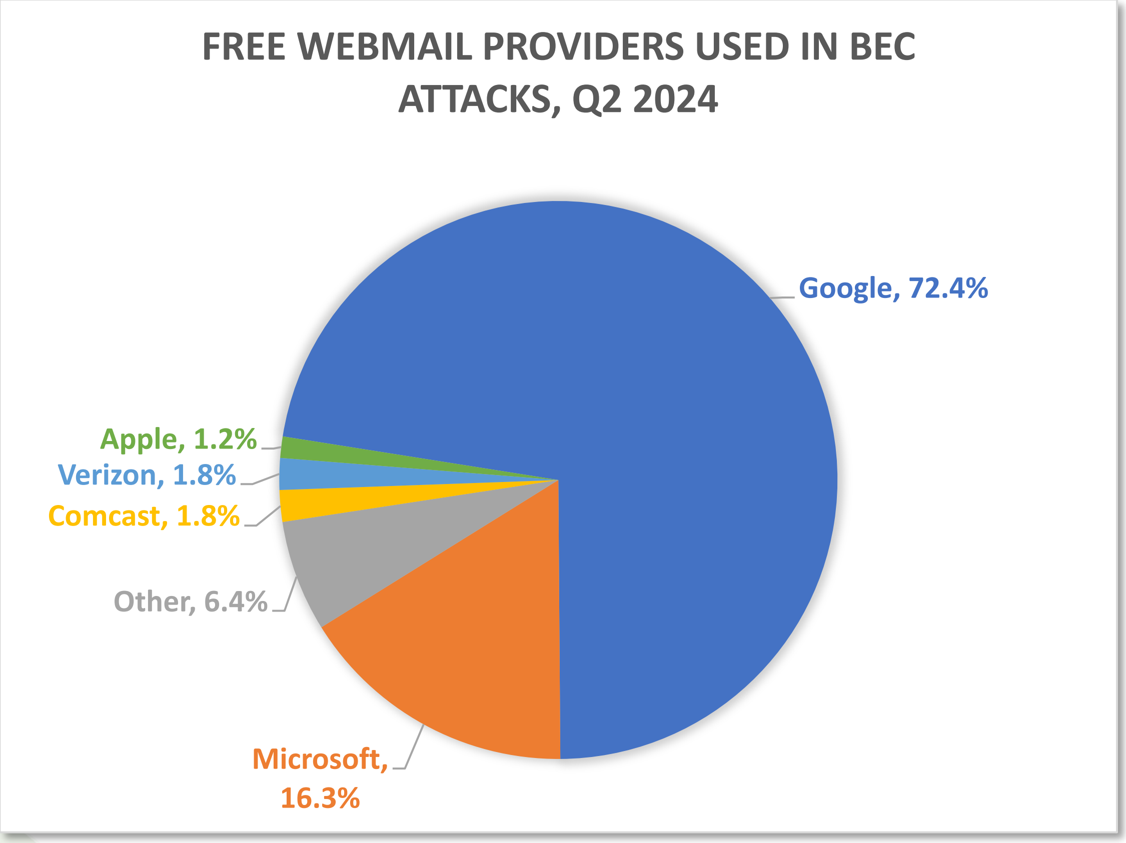
During the second quarter of 2024, gift card scams were once again the most popular type of scam, comprising 38.1 percent of all attacks that Fortra tracked. Some 26.1 percent of attacks were advance fee fraud scams. Payroll diversion remained a popular attack type, making up 7.6 percent in Forta's tracking. Hybrid vishing, which was rarely seen before 2023, made up 4.9 percent of the cases Fortra tracked.

"The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service," said John Wilson, Senior Fellow, Threat Research at Fortra. "The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. In the second quarter of 2024, Norton/LifeLock was the most popular brand used as a lure in these attacks, mentioned in 39 percent of the hybrid vishing messages we encountered in Q2 2024. Geek Squad was the second-most-used, at 25 percent of attack messages. That was followed by PayPal at 22 percent, and McAfee at 6 percent."

Fraudsters acquired domain name that they used to run their BEC attacks at the following domain name registrars:



Fortra found that 72 percent of BEC attacks in Q2 2024 were launched using a free webmail domain. This was virtually unchanged from the 73 percent share observed in the prior quarter. The remaining 28 percent of BEC attacks utilized a combination of maliciously registered domains and compromised email accounts. Google's Gmail was by far the most popular free webmail provider for BEC scammers, used for 72.4 percent of the free webmail accounts that scammers set up for BEC scams in Q2 2024. Microsoft's webmail properties powered 16.3 percent of webmail-based BEC attacks in Q2, dwarfing the remaining webmail providers:



Fortra notes that 35% of payroll diversion attempts requested the victim's salary be routed to an account at Green Dot. The 3rd most popular bank for payroll diversions was GoBank, which is also owned by Green Dot. This suggests that Green Dot is doing a poor job of vetting its account holders, in dereliction of its Know Your Customer duties as outlined in FINRA 2090.

APWG Phishing Activity Trends Report Contributors

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

OpSec Security is the leading provider of integrated online protection and on-product authentication solutions for brands and governments.

www.opsecsecurity.com

The *APWG Phishing Activity Trends Report* is published by and © the APWG. For info about the APWG, please contact APWG Deputy Secretary General Foy Shiver (foy@apwg.org, +1.404.434.728). 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). **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; the APWG.EU, the institution's European chapter established in Barcelona in 2013 as a non-profit research foundation incorporated in Spain and managed by an independent board; 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.

APWG eCrimeX

APWG's clearinghouses for cybercrime-related data send 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.

STOP | THINK | CONNECT
MESSAGING CONVENTION

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 conference dedicated exclusively to cybercrime studies.