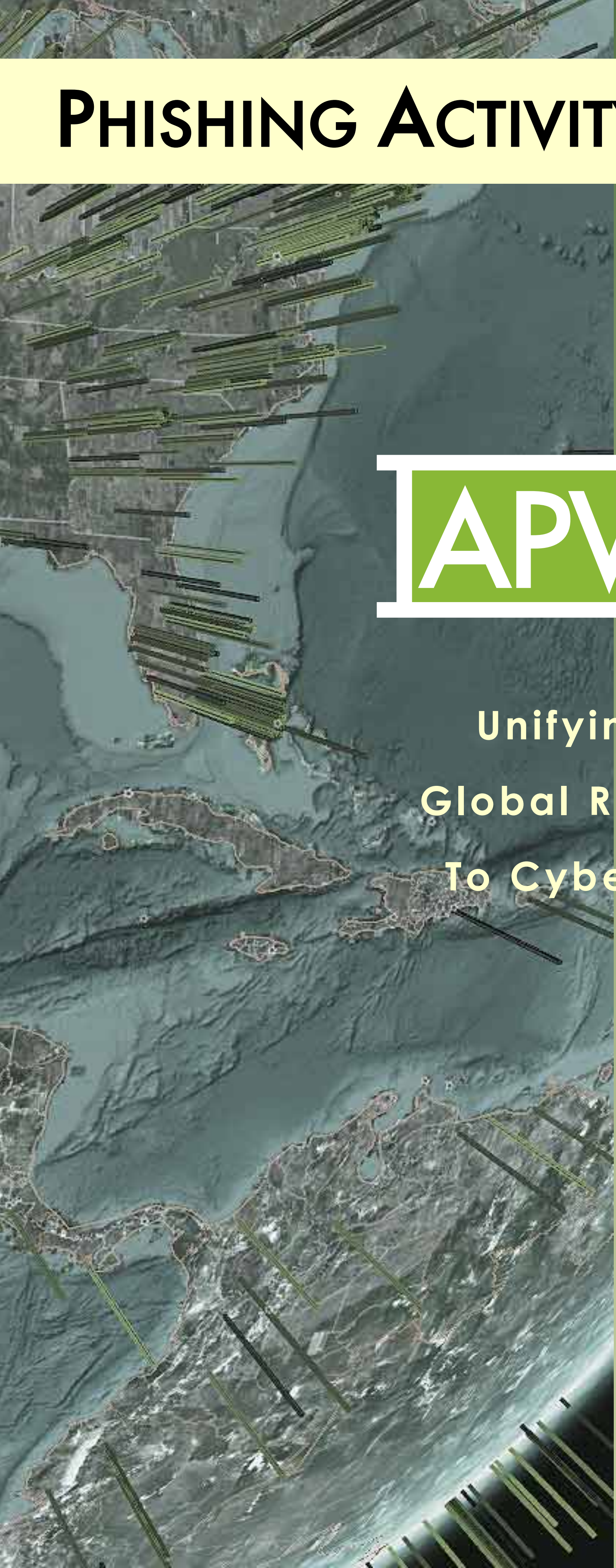
Phishing Activity Trends Report



1st Quarter 2024

APWG

Unifying the
Global Response
To Cybercrime

Activity January-March 2024

Published 14 May 2024

Phishing Report Scope

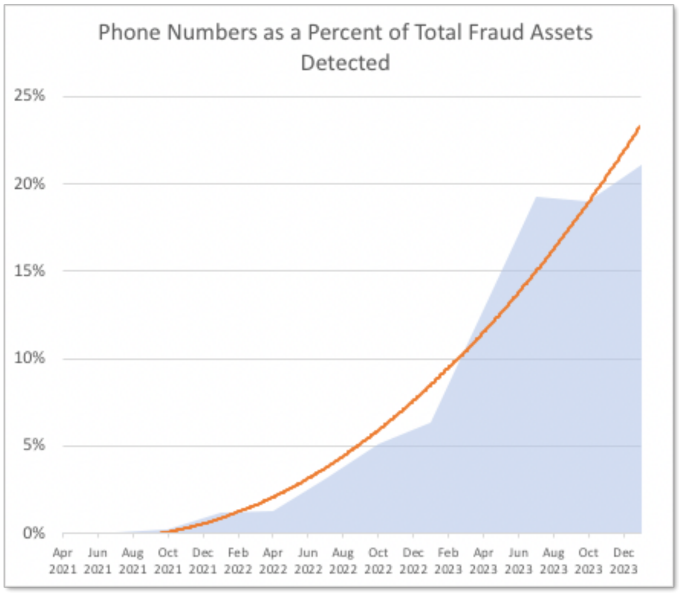
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG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

Phone-based Phishing Growing Unchecked



Little recorded just a few years ago, phone numbers used for fraud comprised more than 20% of fraud-related assets seen by OpSec in its latest report

Phishing Activity Trends Summary

- Phone-based phishing, directly engaging victims, proliferates unchecked. Phone numbers used for fraud comprised more than 20% of fraud-related assets identified by OpSec in Q1 2024. [p.6]
- Phishing using phone calls — so-called voice phishing or "vishing"— is increasing every quarter. [pp. 6-7]
- In Q1 2024, APWG observed 963,994 phishing attacks, the lowest quarterly total since Q4 2021. [p. 3]
- Social media platforms were the most frequently attacked sector, targeted by 37.4% all phishing attacks in Q1 2024. Banking-segment phishing continued to decline, down to 9.8 percent. [p. 5]
- The average wire transfer amount requested in BEC attacks in Q1 2024 was $84,059, up nearly 50% from the prior quarter's average. [p.7]

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.

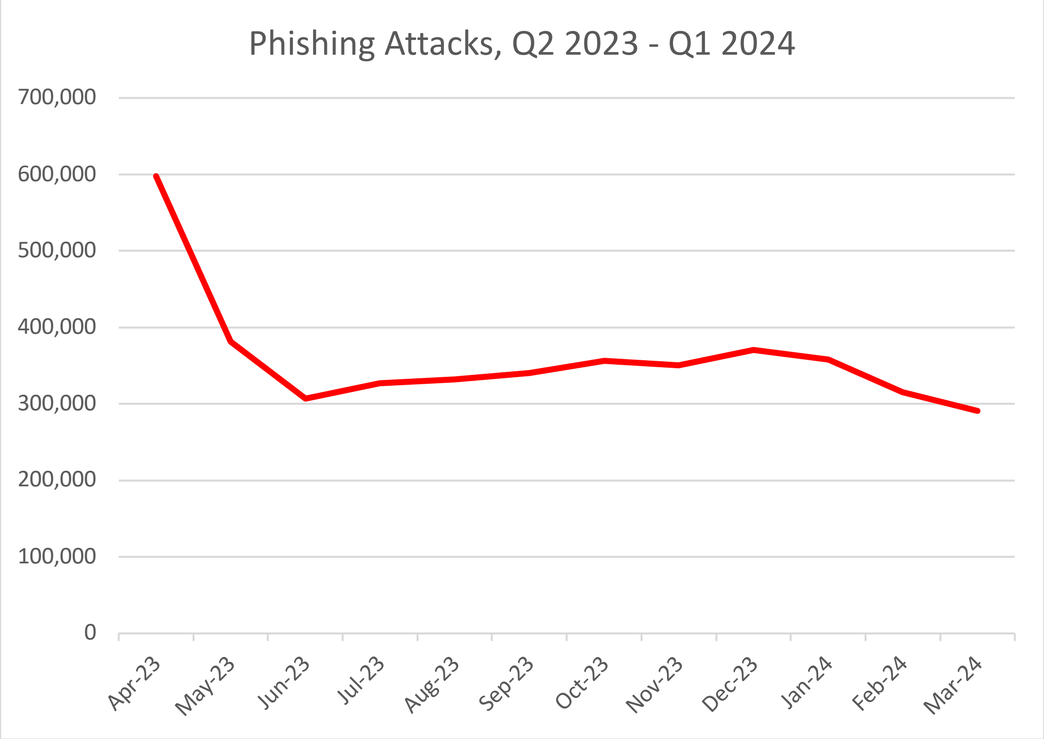
The APWG tracks:

- **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	358,107	314,974	290,913
Unique phishing email campaigns	50,837	24,086	41,550
Number of brands targeted by phishing campaigns	314	309	301

The APWG observed almost five million phishing attacks over the course of 2023, which was a record year. In the first quarter of 2024, APWG observed 963,994 phishing attacks. This was the lowest quarterly total since 4Q 2021, and far below the 1,624,144 attacks seen in Q1 2023, which was the record high quarter in APWG's historical observations. Overall, the number of attacks per month has been stable from June 2023 through March 2024.

The number of reports received was down, but the number of unique email campaigns was up 64 percent over Q4 2024, suggesting that phishers were diversifying their email subject lines in order to bypass email filtering. Recently there have also been fewer brand names reported to the APWG.

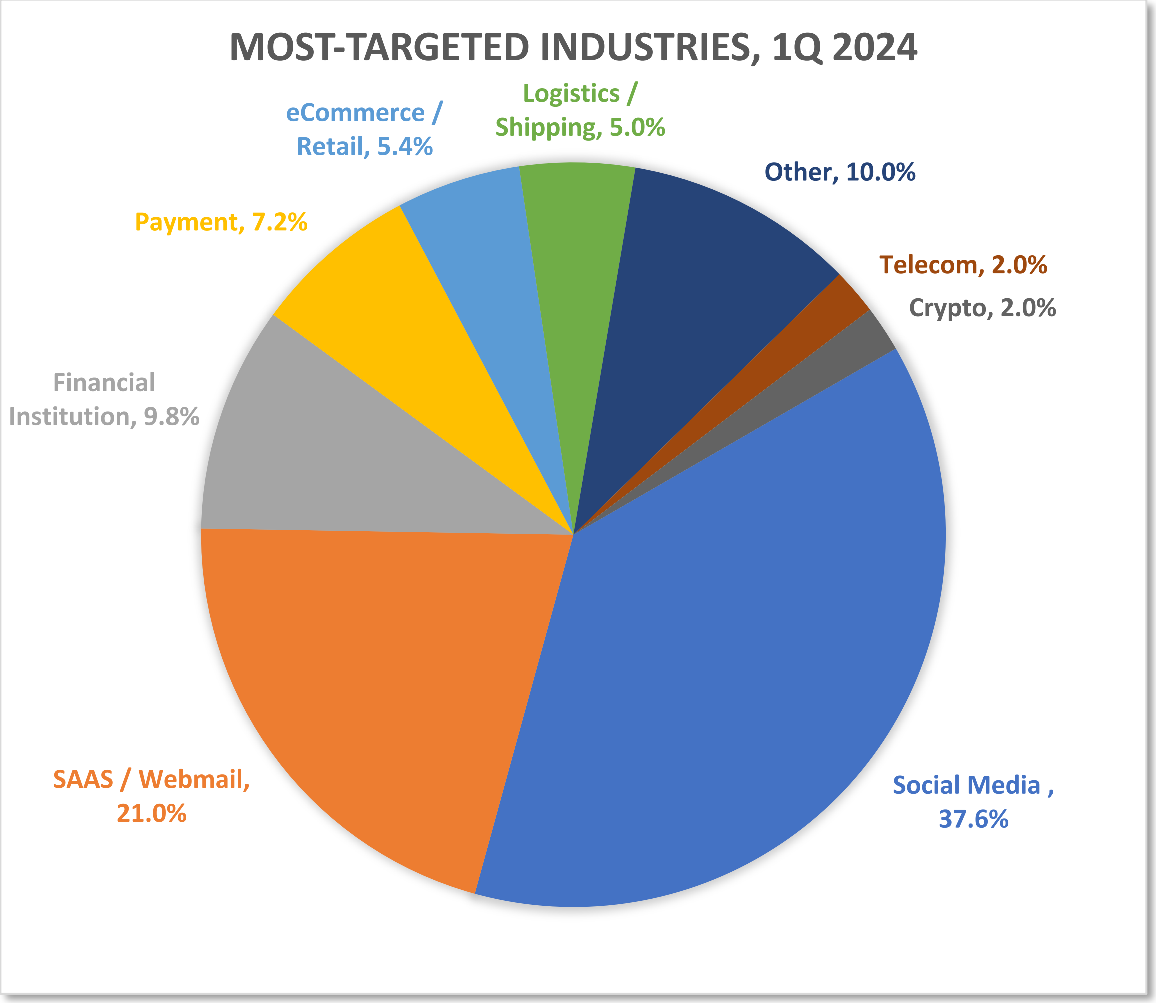


Most-Targeted Industry Sectors – 1st Quarter 2024

In the first quarter of 2024, APWG founding member OpSec Security found that social media platforms were the most frequently attacked sector, representing 37.4 percent all phishing attacks. Phishing against the Financial Institution (banking) segment continued to fall, from 24.9 percent of all attacks in Q3 2023 to 14 percent in Q4 2023, to 9.8 percent in Q1 2024. Attacks against online payment services (such as PayPal, Venmo, Stripe, and similar companies) were another 7.4 percent of all attacks.

“Social Media gave up some market share to the SaaS/Webmail industry, but those two sectors still represent nearly 60 percent of all detected phishing,” said Matthew Harris, Senior Product Manager, Fraud at OpSec. “We have observed an increased percent of phishing being targeted towards activities that do not require high security: less toward banking and more toward social media accounts, and SAAS/Webmail accounts such as Microsoft Outlook, and Netflix.”

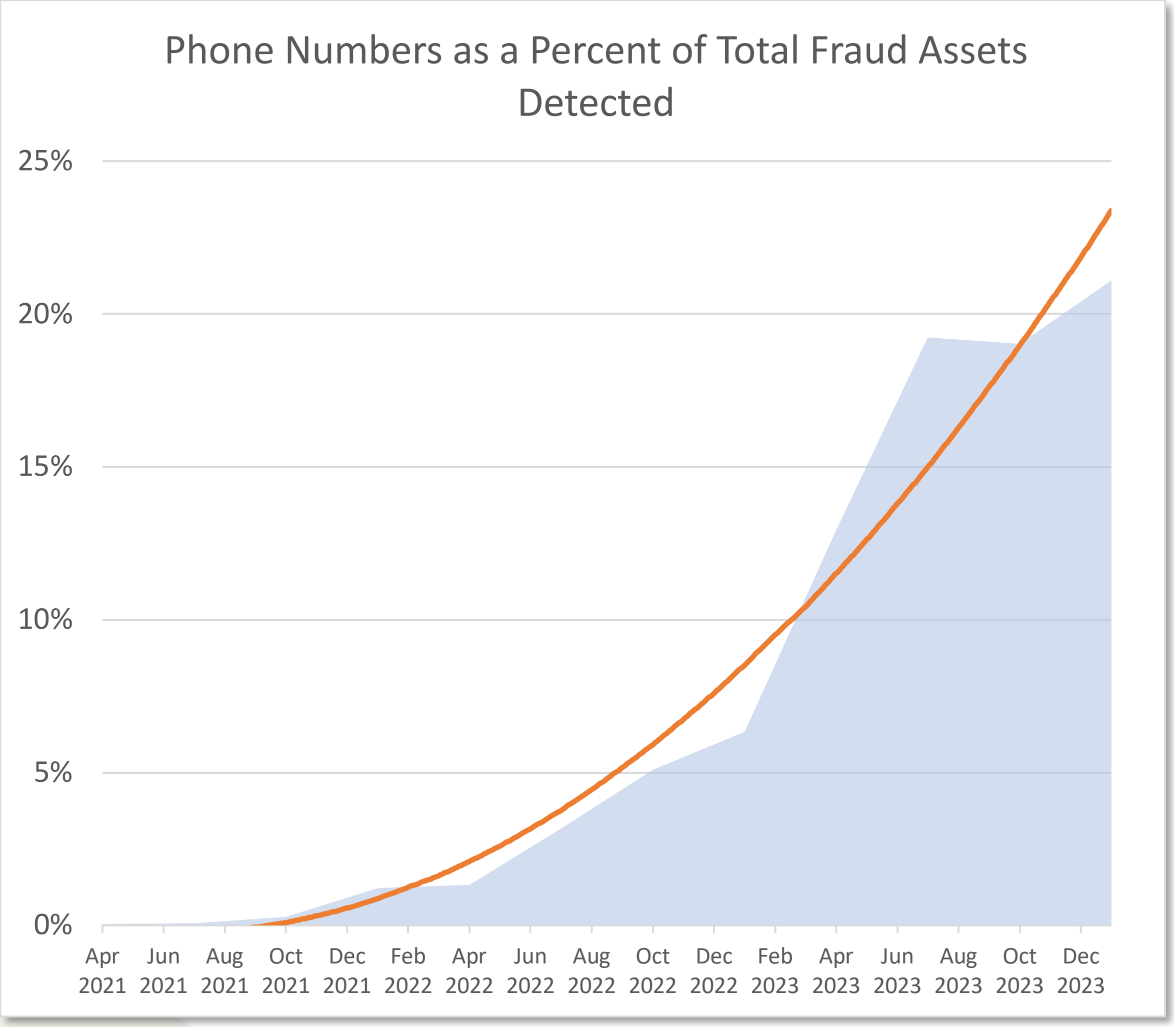
Harris also added: “Lastly, and continuing a trend we have seen for the last 15 consecutive quarters, we're again tracking a strong increase in phone-based fraud, with vishing and smishing detection volumes growing by more than 30 percent as compared to the previous quarter.”



OpSec Security offers world-class brand protection solutions.

Phone-Based Phishing, 1st Quarter 2024

APWG founding member OpSec Security found that the number of phone numbers used to perpetrate fraudulent activities has exploded over the last three years. Phone numbers used for fraud represented more than 20 percent of all fraud-related assets that OpSec identified in Q1 2024. OpsSec tallies fraud assets including fraudulent URLs (such as phishing URLs), phone numbers used in frauds, and email accounts used to perpetrate frauds (including those used for BEC attacks, job advertisement frauds, etc.).



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-mediated, phone-to-phone text messages.

The most common form of phone-based phishing OpSec has observed is known as *hybrid phishing*. The typical scam involves sending the victim a fake purchase receipt via email, commonly for a few hundred U.S. dollars, which requests that the recipient call a support phone number within a limited amount of time to dispute the charge. This "urgent call to action" is a common social engineering tactic. Once on the phone with the victim, the scammer collects the victim's personal and financial information, or persuades the victim to send money or gift cards to the scammer.

"At OpSec, we started to see vishing and smishing take off in early 2021," said Matthew Harris, Senior Product Manager, Fraud at OpSec. "That was likely a result of scammers pivoting from fraud models that have a lower return on investment to methods that have higher ones."

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. "Contrast this with phone calls, which go directly to a user with very little filtering," said Harris. "And with phone scams, the victim only sees an easily spoofable telephone number or caller name. Finally, phone calls are more engaging. A live person is calling the victim, interacting them, and has a chance to gain the victim's trust—or has a chance to alarm and confuse the victim and trick them."

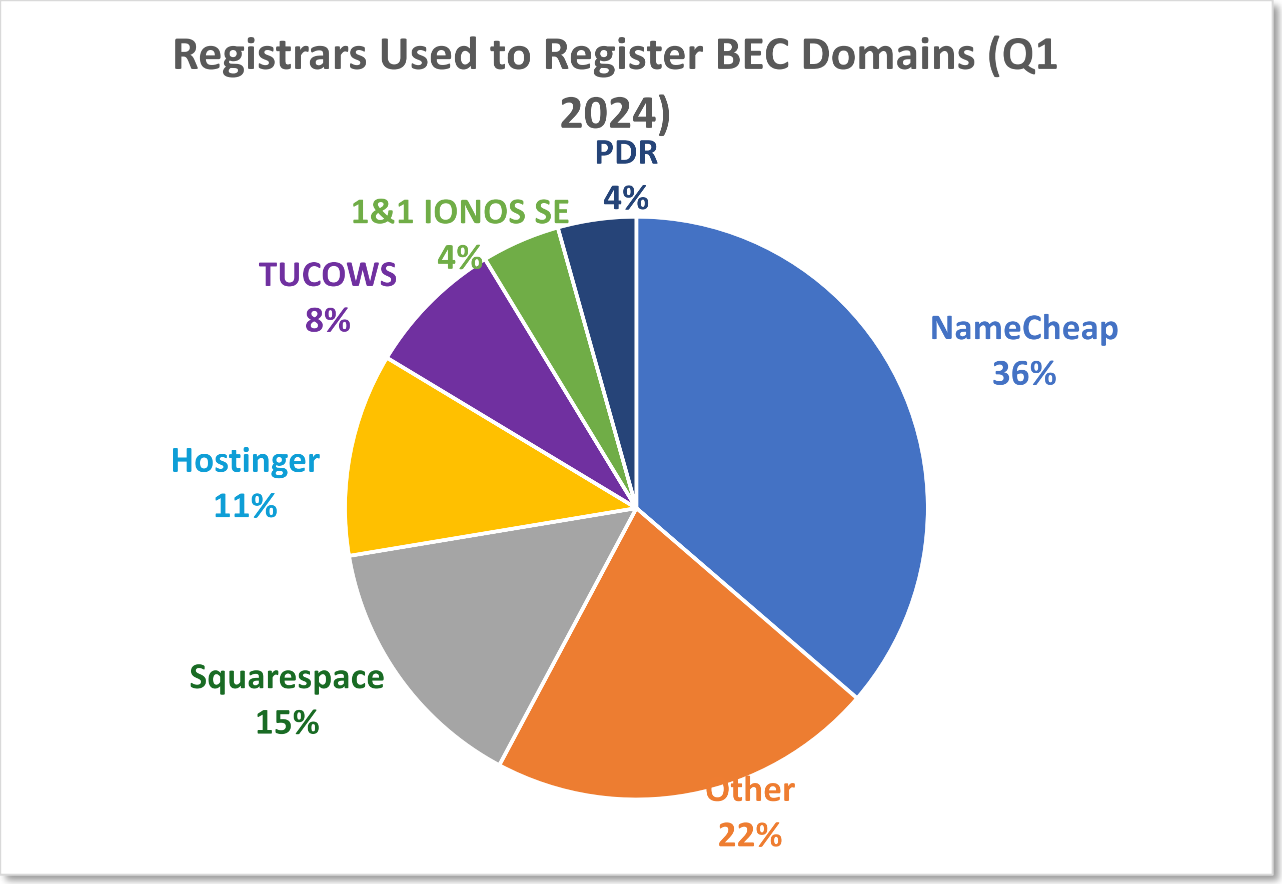
Business e-Mail Compromise (BEC), 1st Quarter 2024

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 Q1 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

During the first quarter of 2024, Fortra found gift card scams were once again the most popular scam type, comprising 37.9 percent of the total. Another 29.2 percent of attacks were *advance fee* fraud scams. Payroll diversion remained a popular attack type, making up 10.5 percent of attacks. Successful advance fee fraud and payroll diversion scams lead the victim to make a wire transfer to the scammer.

Fortra found that the average amount requested in wire transfer BEC attacks in Q1 2024 was $84,059, up nearly 50 percent from the prior quarter's average of $56,195. The volume of wire transfer BEC attacks in Q1 2024 decreased by 60 percent compared to the previous quarter. This suggests the bad actors behind BEC wire transfers conducted a smaller number of bigger-money attacks.

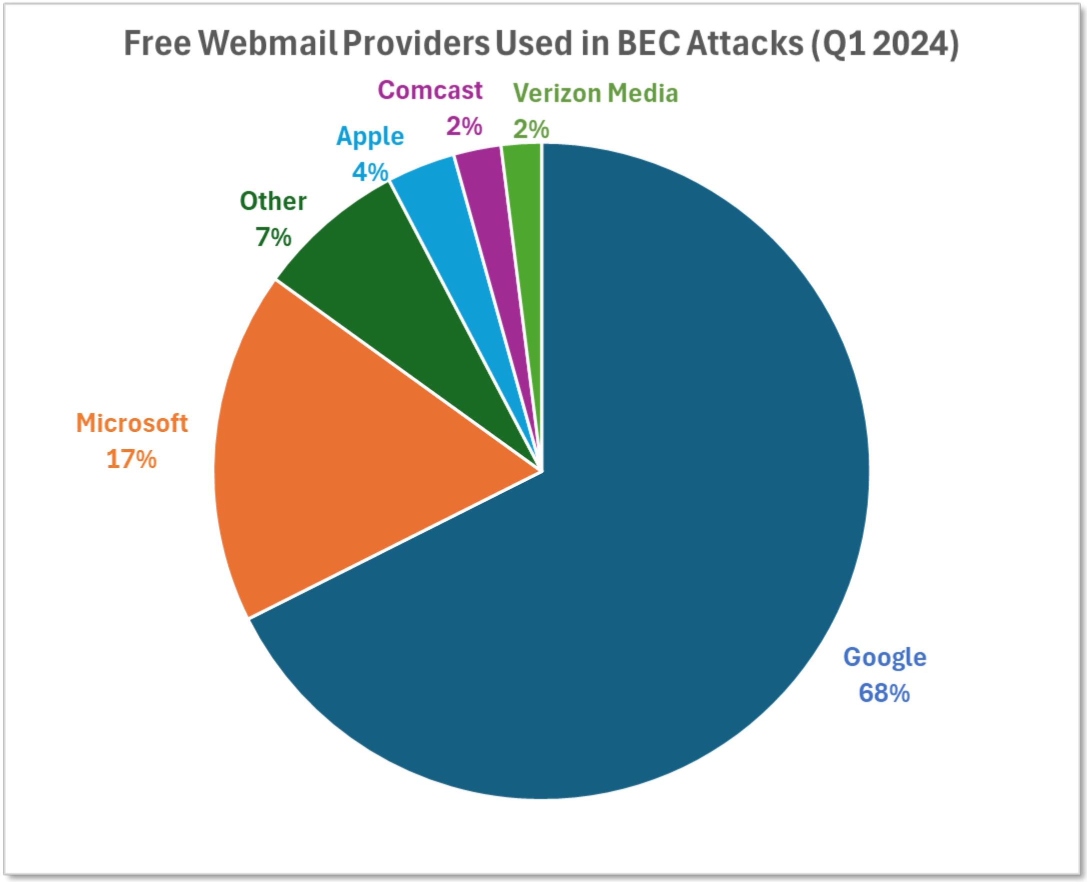
“Nearly 60 percent of malicious messages reaching corporate inboxes in Q1 2024 attempted to steal login credentials, while 40 percent were response-based,” said John Wilson, Senior Fellow, Threat Research at Fortra. “Less than half a percent of the malicious messages that landed in enterprise mailboxes attempted to deliver malware. These numbers suggest that corporate email filters still struggle to catch credential phishing and response-based attack messages.”



“Hybrid vishing, which we rarely saw before 2023, made up 5.6 percent of Fortra’s engagements in the first quarter of 2024,” said Wilson. “The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service. The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. Norton/LifeLock was the most popular brand used as a lure in these attacks, mentioned in 32 percent of the hybrid vishing messages we encountered in Q1 2024. McAfee was the second most popular lure, making up 29 percent of the Q1 attack messages. This was followed by Geek Squad (21%) and PayPal (17%).”

Fortra found that 73 percent of BEC attacks in Q1 2024 were launched using a free webmail domain, a slight increase from the 68 percent share observed in the prior quarter. The remaining 27 percent of BEC attacks in Q1 2024 utilized a combination of maliciously registered domains and compromised email accounts.

Google was by far the most popular free webmail provider for BEC scammers, accounting for 68 percent of the free webmail accounts used in Q1 2024 BEC scams. Microsoft's webmail properties powered 17 percent of webmail-based BEC attacks in Q1, followed by a long tail of other webmail providers:



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

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.

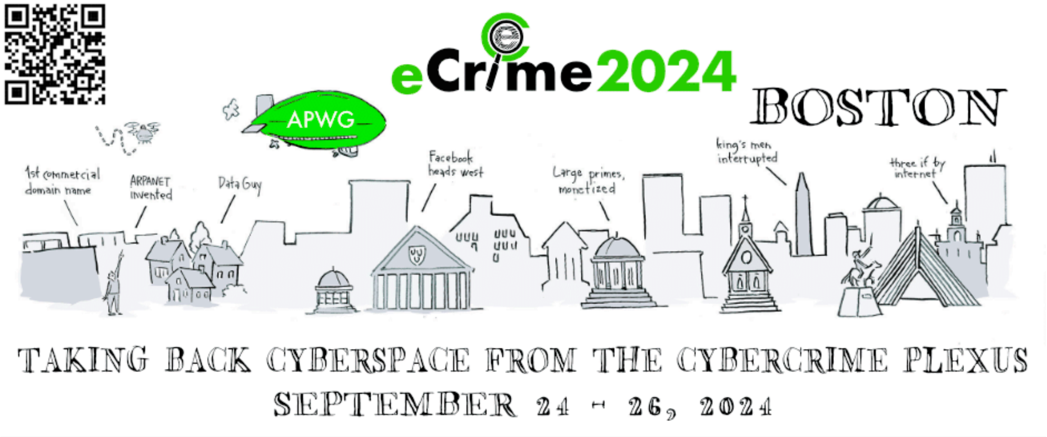
Operationally, the APWG conducts its core missions through: APWG, a US-based 501(c)6 organization; the APWG.EU, the institution's European chapter established in Barcelona in 2013 as a non-profit research foundation incorporated in Spain and managed by an independent board; the STOP. THINK. CONNECT. 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'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.

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.



TAKING BACK CYBERSPACE FROM THE CYBERCRIME PLEXUS
SEPTEMBER 24 - 26, 2024