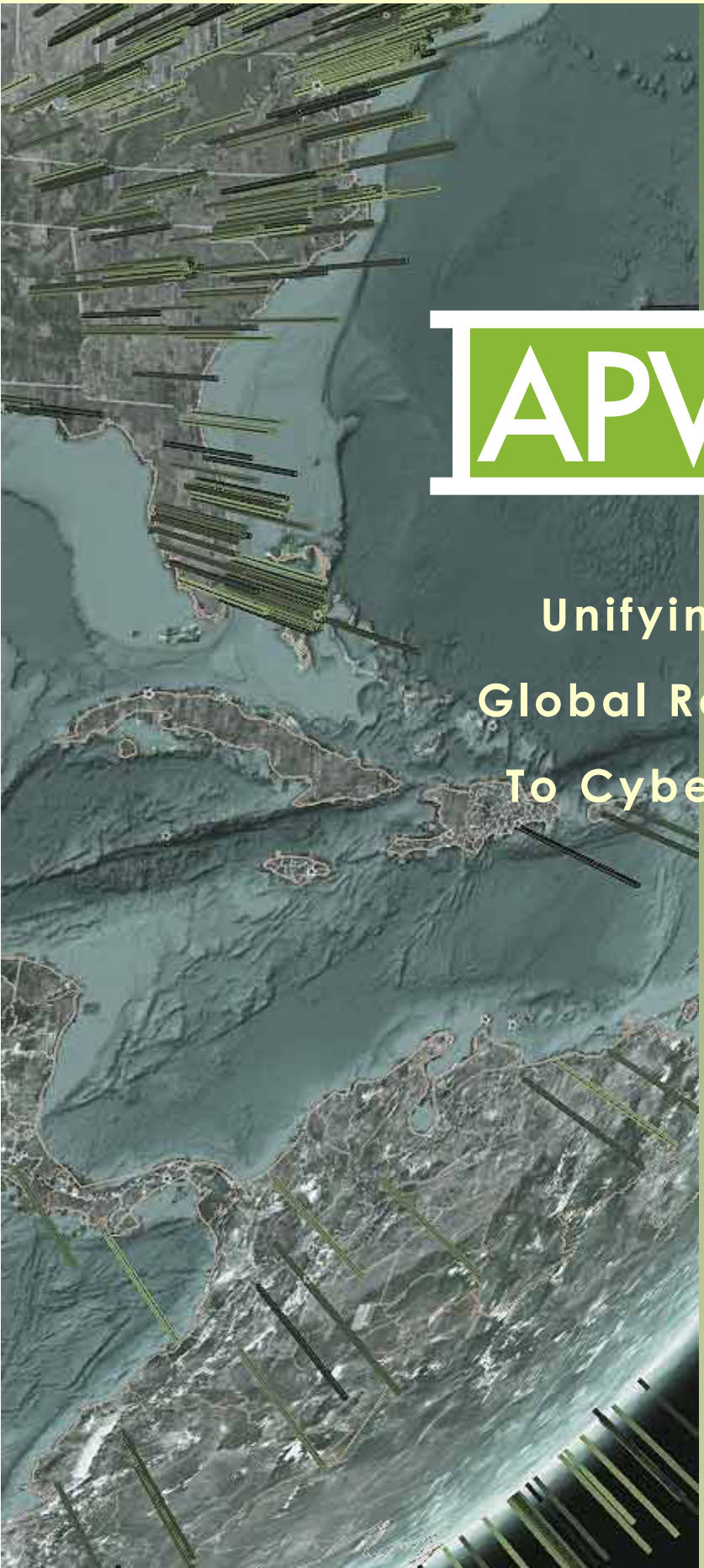
Phishing Activity Trends Report



3rd Quarter 2023

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2023

Published 13 November 2023

Phishing Report Scope

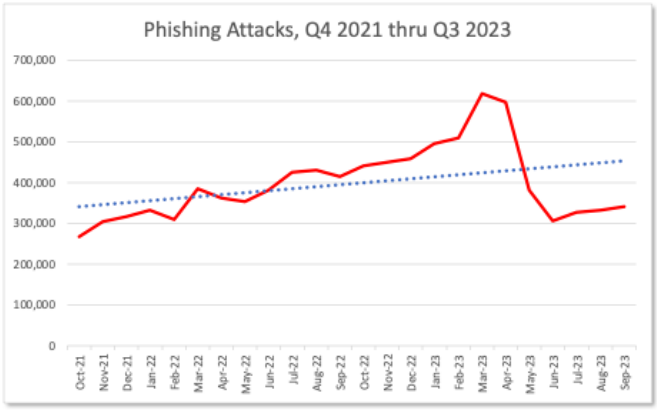
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org.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

Phishing Drops from Record High; Returns to 2022 Levels



In Q3 2023, unique email subject lines (campaigns) received by the APWG stabilized around 32,000 month, after averaging 40,000+ per month in Q1 2023. Total email reports APWG received also dipped between Q2 and Q3

Phishing Activity Trends Summary

- In the third quarter of 2023, the APWG observed 999,956 phishing attacks. This represented a 37.5 percent drop from the first quarter of 2023. Phishing fell back to the levels seen in late 2021. [pp. 3-4]
- The number of voice-mail phishing, or vishing, as a sub-category of phishing swelled 40 percent from Q1 2023 through Q3 2023. [pp. 5-6]
- The average amount requested in wire transfer BEC attacks in Q3 2023 was $164,645, down 44 percent from the Q2 average of $293,359. However, the volume of wire transfer BEC attacks in Q3 increased by 55 percent. [pp. 5-6]
- The financial sector continued to be the most-attacked sector, with 24.9 percent of all phishing attacks. Attacks against social media companies were second, at 18.9 percent. [pp. 4- 5]

Statistical Highlights for the 3rd Quarter 2023

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	Sept
Number of unique phishing Web sites (attacks) detected	327,294	331,962	340,700
Unique phishing email campaigns	29,110	32,162	32,740
Number of brands targeted by phishing campaigns	477	499	508

In the third quarter of 2023, APWG observed 999,956 phishing attacks. This was down from the 1,286,208 seen in Q2, and the 1,624,144 attacks seen in 1Q 2023, which was the record high quarter in our historical observations. **The 306,847 attacks reported to APWG in June 2023 was the smallest monthly total since November 2021**.

Put another way, the APWG observed a 37.5 percent drop in phishing between the first quarter and the third quarter of 2023. Looking at the last two years, the new data confirmed a trend: phishing fell back to the levels seen in late 2021:

In Q3 2023, the number of unique email subject lines (campaigns) received by the APWG also stabilized around 32,000 month, after averaging more than than 40,000 per month in Q1 2023. The number of total email reports that APWG received also dipped between Q2 and Q3.

The overall phishing trend that the APWG data shows was also seen by other observers. The Cybercrime Information Center (https://www.cybercrimeinfocenter.org/), which collects phishing data from several sources. The Cybercrime Information Center saw phishing peak in late 2022 into January 2023, and then drop back to levels seen in mid-2022. APWG contributor OpSec Security independently noted a fraud volume decrease from Q1 to Q2 2023, and then stabilizing across Q3 2023 (see below).

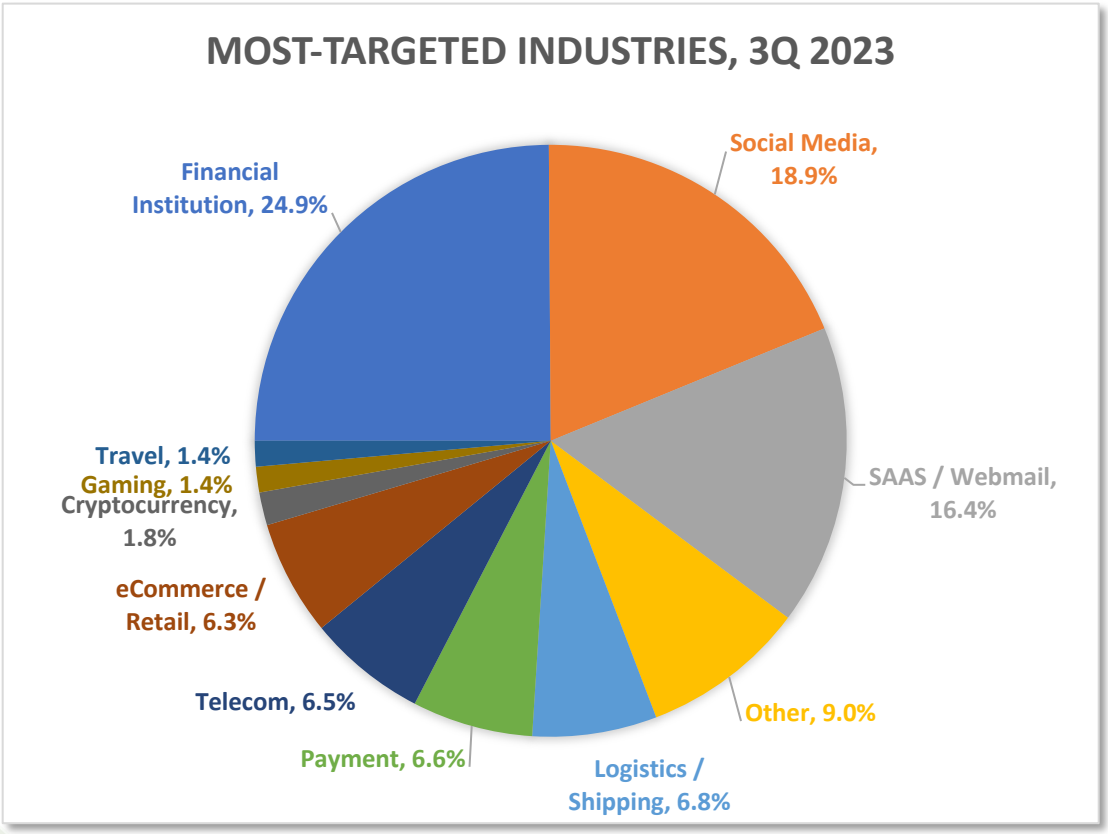
Most-Targeted Industry Sectors – 3rd Quarter 2023

In the third quarter of 2023, APWG founding member OpSec Security found that phishing attacks against the financial sector (which includes banks) remained the largest set of attacks, accounting for 24.9 percent of all phishing – up from 23.5 percent in Q2 2023. Attacks against online payment services were another 6.6 percent of all attacks.

Attacks against social media companies remian the second-largest category. Social media attacks were 18.9 percent of all attacks in 3Q 2023, after being 22.3 percent in Q2 2023.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, noted: "Our measurements show that there was a fraud volume decrease from Q1 to Q2 2023, and that the volumes in Q2 and Q3 were nearly identical."

Harris added: "We continue to track a strong increase in mobile phone-based fraud, or voice phishing. Vishing detection volumes swelled 40 percent from Q1 2023 through Q3 2023."



OpSec Security offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 2nd Quarter 2023

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $50.8 billion dollars in losses between October 2013 and December 2022, according to the FBI's Internet Crime Complaint Center (IC3). In a BEC attack, a threat actor impersonates

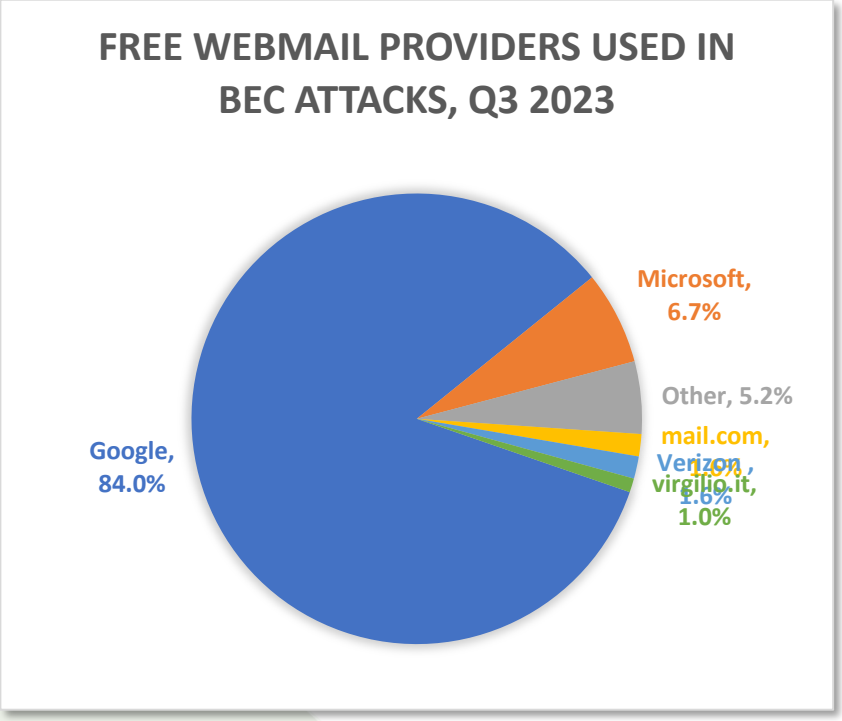
an employee, vendor, or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q2 2023.

Fortra found that the average amount requested in wire transfer BEC attacks in Q3 2023 was $164,645, down 44 percent from the Q2 average of $293,359. However, the volume of wire transfer BEC attacks in Q3 increased by 55 percent compared to the prior quarter.

"For the first time ever, hybrid vishing attacks were the most common type of email scam that we observed," said John Wilson, Senior Fellow, Threat Research at Fortra. "These made up 44 percent of the response-based email scams we observed in Q3 2023. Advanced fee fraud, which is traditionally the most common email scam we see, came in second with a 22 percent share. These were followed by gift card scams at 19 percent, and payroll diversion attempts at 4 precent."

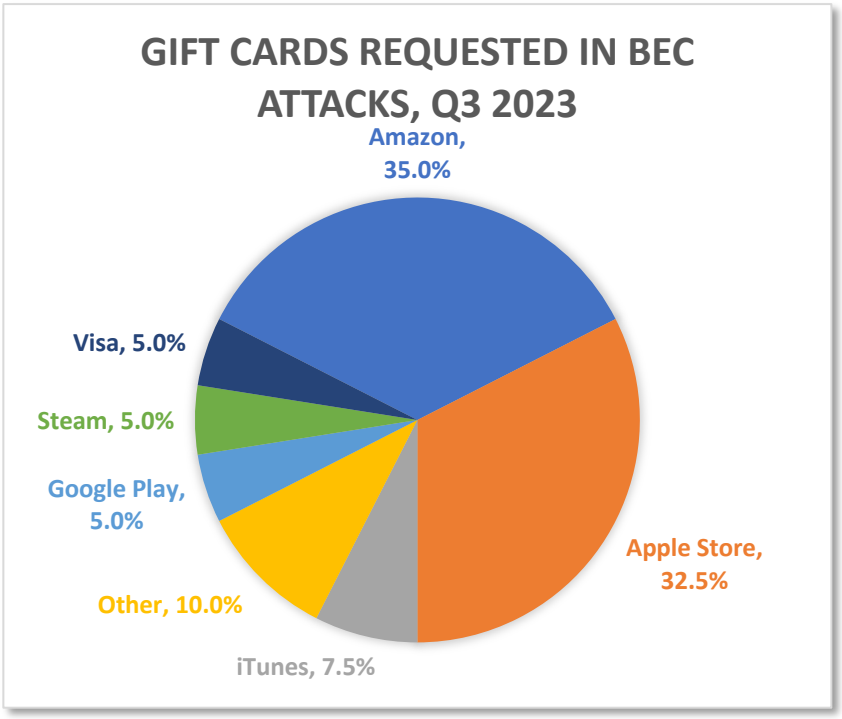
Wilson noted: "The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service. The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. Fortra identified 250 unique phone numbers impersonating 15 different brands in Q3 hybrid vishing attacks."

Fortra found that 79 percent of BEC attacks launched in Q3 2023 utilized a free webmail domain, a decrease from the 87 percent share observed in the previous quarter.



The remaining 21 percent of BEC attacks in Q3 2023 utilized maliciously registered domains and compromised email accounts. Google was once again the overwhelmingly most popular webmail provider among BEC scammers, with Gmail addresses making up 84 percent of the scammer webmail accounts that Forta observed in Q3.

When BEC scammers requested to be paid in gift cards, they usually requested Amazon and Apple Store cards, with iTunes cards a distant third:



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

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.forta.com	ILLUMINTEL Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce. www.illumintel.com	OpSec SECURITY 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 multilateral 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 machine event data sends more than two billion data elements per month outbound to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of software clients and devices worldwide. APWG Engineering continues to work with data correspondents worldwide to develop new data resources.

STOP|THINK|CONNECT MESSAGING CONVENTION

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.

eCrime2024