PHISHING ACTIVITY TRENDS REPORT

2nd Quarter 2023

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2023

Published 7 November 2023

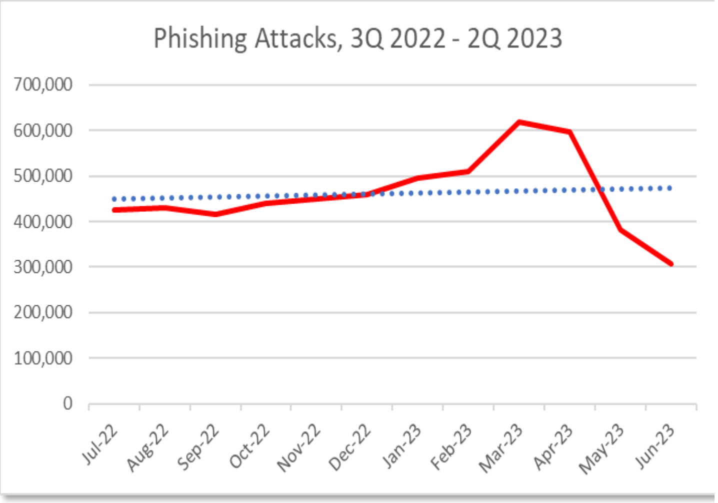
Phishing Report Scope

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.

Phishing Remained High in Q2 2023, but Trending Downward



Phishing Activity Trends Summary

- In the second quarter of 2023, the APWG observed 1,286,208 phishing attacks. This was the third-highest querterly total that the APWG has ever recorded. However, phishing trended downward. [pp. 3-4]
- The average wire transfer amount requested in BEC attacks in Q2 2023 was $293,359. This was up 57 percent from Q1's average of $187,053. [pp. 5-6]
- The financial sector continued to be the most-attacked sector, with 23.5 percent of all phishing attacks. Attacks against online payment services were another 5.8 percent of all attacks. [pp. 4- 5]
- Voice-mail phishing, or vishing, volume continues to rise. [pp. 4-5]

Table of Contents

Statistical Highlights for the 2nd 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.

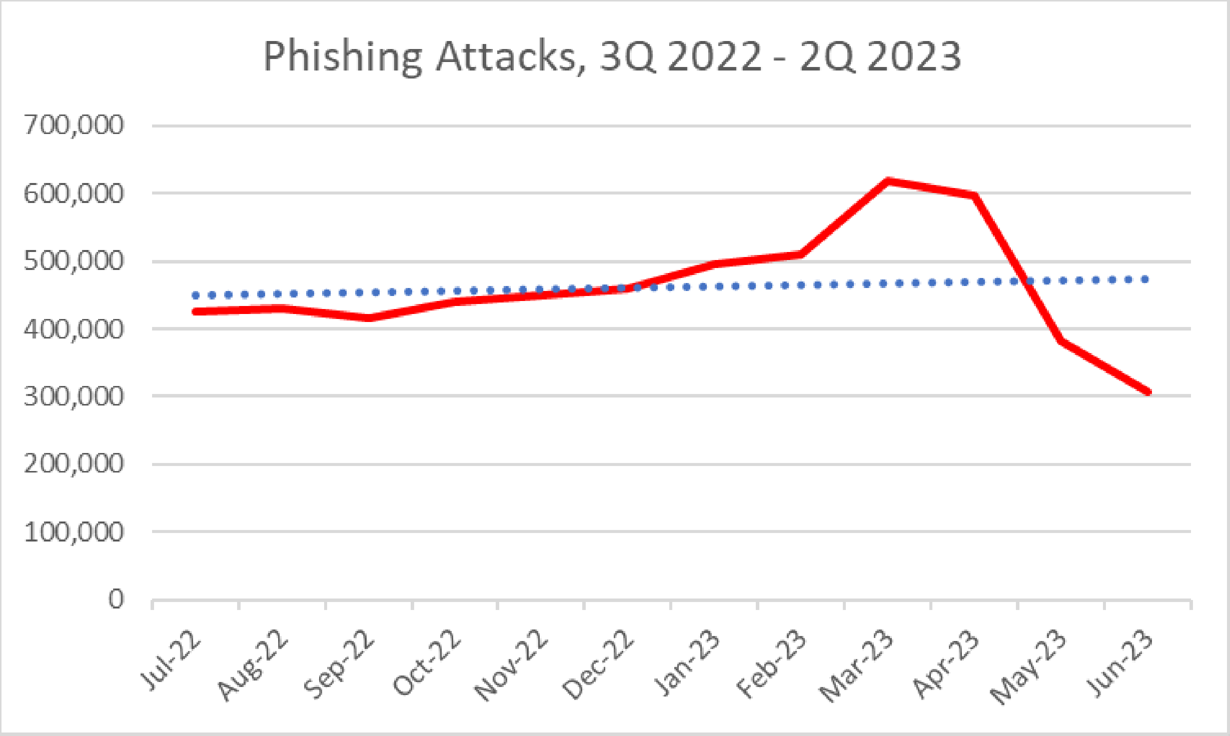
The APWG tracks:

- **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.

	April	May	June
Number of unique phishing Web sites (attacks) detected	597,789	381,572	306,847
Unique phishing email campaigns	41,083	30,717	22,610
Number of brands targeted by phishing campaigns	544	521	498

In the second quarter of 2023, APWG observed 1,286,208 phishing attacks. This was down from the 1,624,144 attacks seen in 1Q 2023, which was the record high quarter in our historical observations. The 2Q 2023 total was the third-highest quarterly tally that the APWG has ever observed. It was much higher than the 888,585 in 4Q 2022, and about equal to the 1,270,883 phishing attacks in 3Q 2022. However, phishing fell notably by the end of the second quarter. The 306,847 attacks seen in June 2023 was the smallest monthly total since November 2021.

The number of phishing sites seen over the last year was:



In 2Q 2023, the number of unique email subjects (campaigns) received also dipped, after averaging more than 40,000 per month in 1Q 2023. The number of total email reports that APWG received also dipped; the number received in June was a little more than half the number received in April.

Most-Targeted Industry Sectors – 2nd Quarter 2023

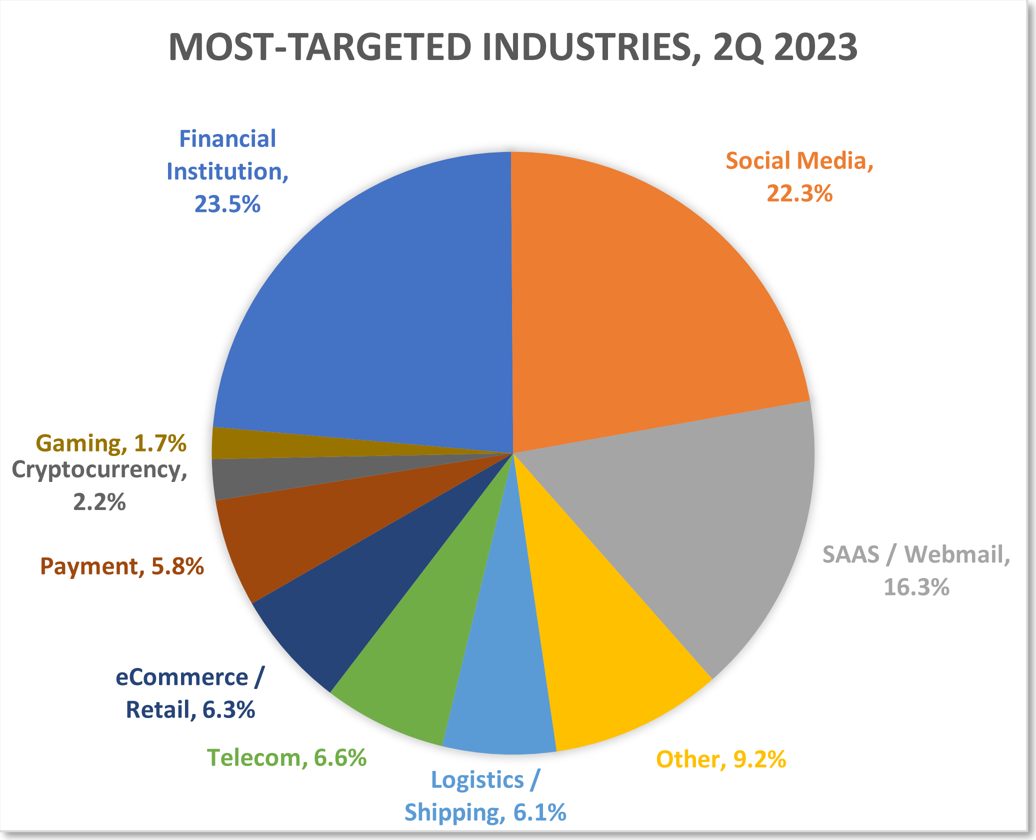
In the second quarter of 2023, APWG founding member OpSec Security found that phishing attacks against the financial sector (which includes banks) remained the largest set of attacks, accounting for 23.5 percent of all phishing -- the same as in 1Q 2023 2022. Attacks against online payment services were another 5.8 percent of all attacks.

Attacks against social media companies have grown to become a larger share of all attacks. In Q2 2023, they were 22.3 percent of all attacks worldwide. That was up from 18.2 percent in 1Q 2023, 15.5 percent in 2Q 2022, and just 8.5 percent of all attacks in 4Q 2021.

OpSec Security also detected a fraud volume decrease from Q1 to Q2 2023.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, noted: "The SAAS/Webmail category fell to third in our ranking, primarily driven by a reduction in the number of phish targeting Microsoft Outlook."

Harris added: "Continuing trends we observed in 2022, we're again tracking a strong increase in mobile phone-based fraud, or voice phishing. The volume of 'vishing' continues to rise. Quarter-over-quarter, we are seeing a steady 10 percent increase in the number of companies being targeted by vishing."



OpSec Security offers world-class brand protection solutions.

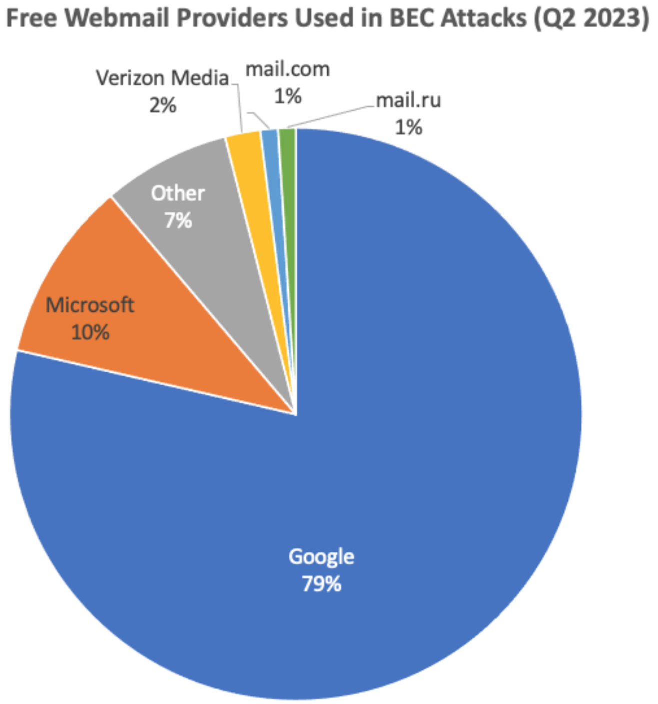
Business e-Mail Compromise (BEC), 2nd Quarter 2023

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 Q2 2023 was $293,359, up 57 percent from Q1's average of $187,053. The volume of wire transfer BEC attacks in Q2 decreased by 29 percent compared to the prior quarter. This suggests the bad actors behind BEC wire transfer incidents focused their attention on fewer but higher-amount attacks.

During the second quarter of 2023, advance fee fraud scams were the most popular cash-out method, comprising 44 percent of the total. Attackers requested gift cards as payment 34 percent of the time. Amazon and Apple Store cards were most popular. Payroll diversion remained a popular attack type, making up 8 percent of attempts.

The second quarter saw the emergence of hybrid vishing (voice phishing) as an attack type. Five percent of the response-based attacks Forta observed fell into this category. John Wilson, Senior Fellow, Threat Research at Forta, said: "The hybrid vishing attacks we track typically begin as an email stating that the recipient has been charged for a product or service. The message instructs the recipient to call a phone number if they wish to cancel the order and obtain a refund. PayPal was the most common brand used as a lure in these attacks, making up 38 percent of the total. This was followed by Geek Squad, McAfee, and Norton/LifeLock each with 19 percent of cases we observed."



Fortra found that 87 percent of BEC attacks in Q2 2023 were launched using a free webmail address, an increase from 73 percent in Q2 2022. The remaining 13 percent of BEC attacks in Q2 2023 utilized maliciously registered domains and compromised email accounts.

Google’s Gmail remained the favorite email provider amongst BEC scammers, accounting for 79 percent of the free webmail accounts used in Q2 2023 BEC scams. This was up 7 percentage points compared to the same period last year. Microsoft’s webmail properties powered 10 percent of webmail-based BEC attacks in Q2 2023. Verizon Media, which includes Yahoo and AOL, accounted for just 2 percent of the free webmail accounts used for BEC in the second quarter of 2023.

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'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.

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.

APWG
BARCELONA
eCrime 2023
November
15 - 17
THE EVOLUTION OF CYBERCRIME IN AN EPOCH OF AI CRIME & ACCELERATING COMPLEXITY

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.