

PHISHING ACTIVITY TRENDS REPORT

1st Quarter

2023

APWG

Unifying the
Global Response
To Cybercrime

Activity January- March 2023

Published 2 November 2023

Phishing Report Scope

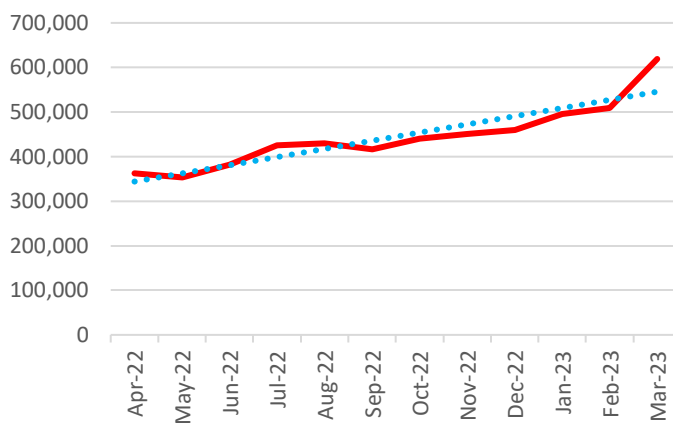
The APWG *Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at <http://www.apwg.org>, and by e-mail submissions to reportphishing@antiphishing.org. 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 Reaches Yet Another New High in Early 2023

Phishing Attacks, 2Q2022-1Q2023



Phishing Activity Trends Summary

- In the first quarter of 2023, APWG observed 1,624,144 phishing attacks. This is a record high -- the worst quarter for phishing that APWG has ever observed. [pp. 3-4]
- The financial sector continued to be the most-attacked sector, with 23.5 percent of all phishing attacks. [pp. 4- 5]
- Voice-mail phishing, or vishing, volume swelled more than 40 percent as compared to 4Q 2022. [p. 5]
- Phishing against cryptocurrency targets has been falling, as the crypto industry has been roiled by controversy. [p. 5]

Table of Contents

Statistical Highlights	3
Most-Targeted Industry Sectors	4
APWG Phishing Trends Report Contributors	6
About the APWG	6

Phishing Activity Trends Report, 1st Quarter 2023

Statistical Highlights for the 1st 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 (eCX).

The APWG tracks:

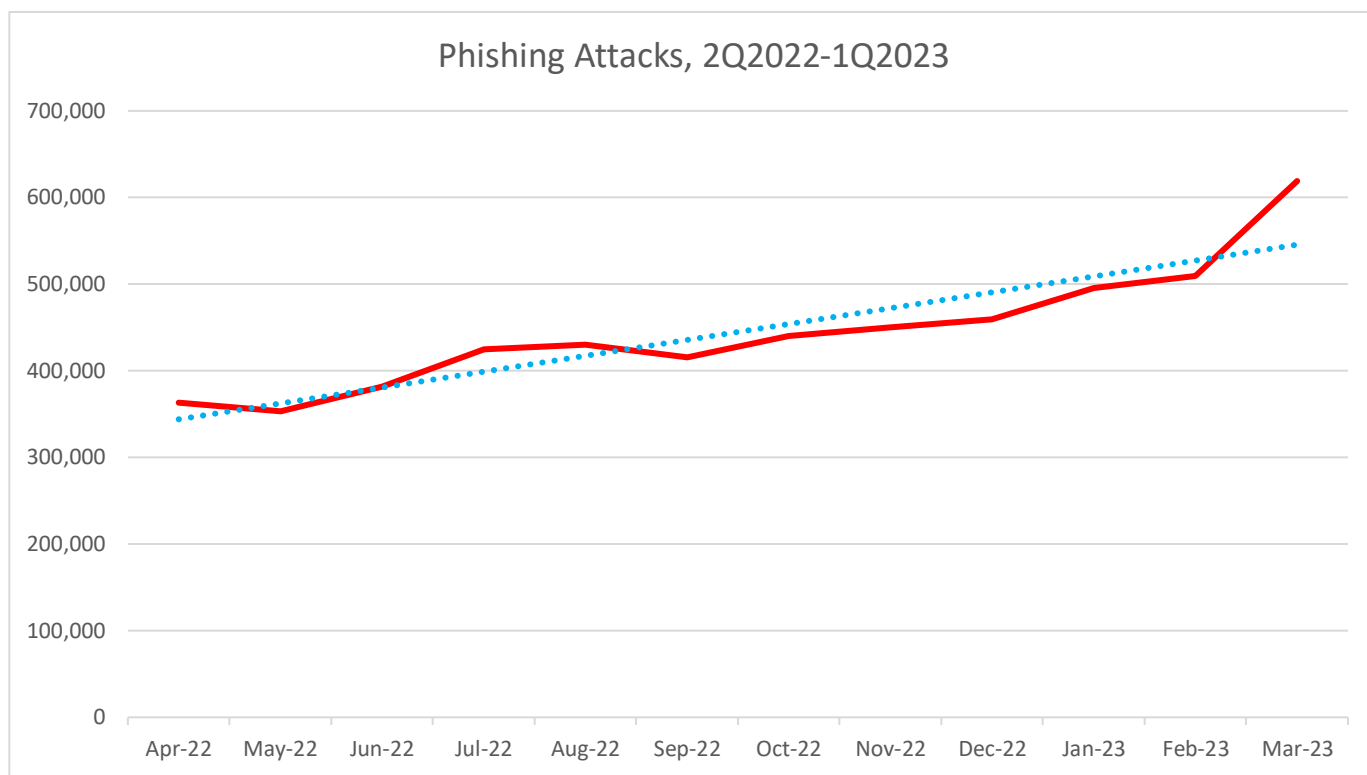
- **Unique phishing sites.** This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically 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.

	January	February	March
Number of unique phishing Web sites (attacks) detected	495,690	509,394	619,060
Unique phishing email campaigns	40,863	45,259	40,742
Number of brands targeted by phishing campaigns	561	549	576

In the first quarter of 2023, APWG observed 1,624,144 phishing attacks. This is a record high in our observations -- the worst quarter for phishing that APWG has ever observed. The total was up from 888,585 in 4Q 2022, and above the 1,270,883 phishing attacks in 3Q 2022, which was the record at the time.

In 1Q 2022, the number of number of email reports that APWG received, and the number of unique email subjects received, returned to previous levels seen in mid-2022.

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

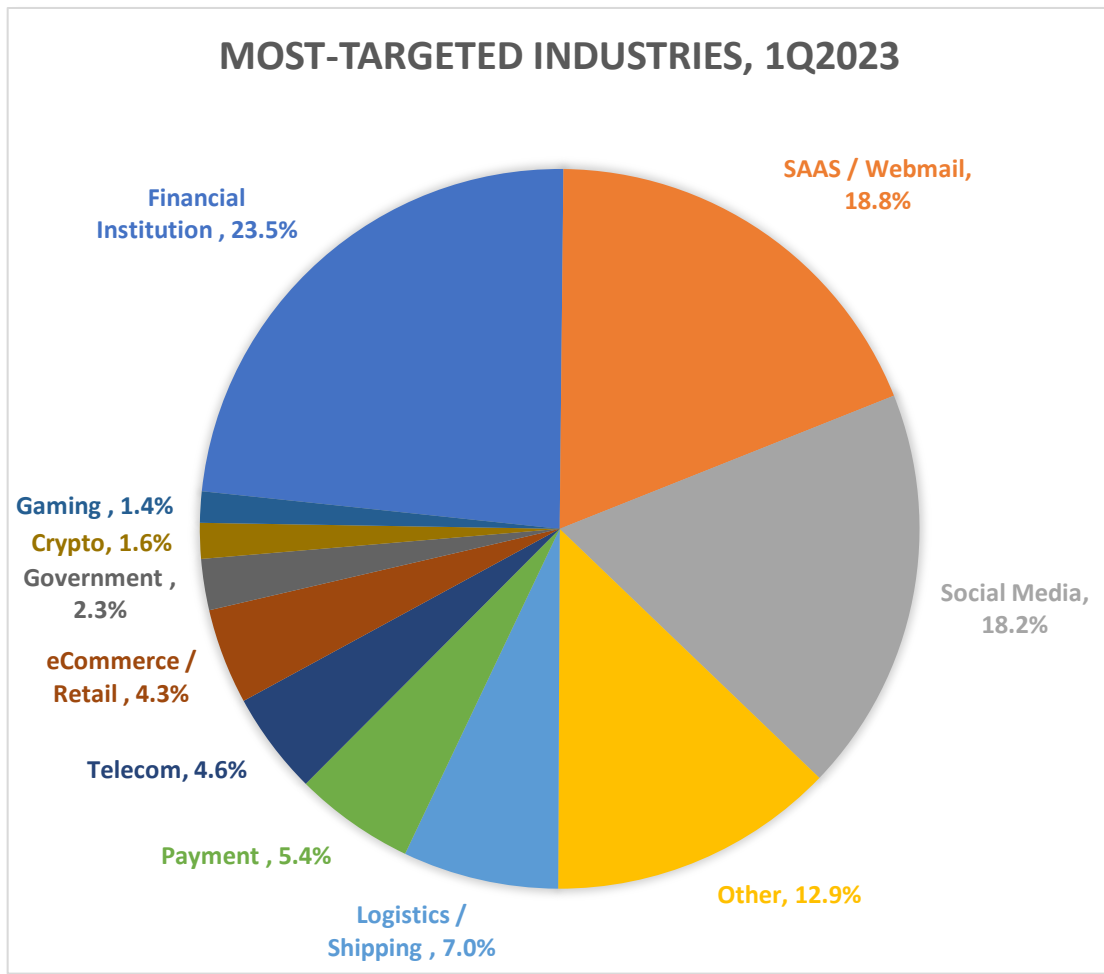


Most-Targeted Industry Sectors – 1st Quarter 2023

In the first 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, down from 27.7 percent in 4Q 2022. Attacks against webmail and software-as-a-service (SAAS) providers were next in prominence at 18.8 percent, up slightly from 17.7 percent in 4Q2022. Attacks against payment processors such as PayPal, Venmo, and VISA were another 5.4 percent.





Phishing against social media companies trended upward to 18.2 percent of all phishing attacks, after varying from just 8.5 percent of all attacks in 4Q 2021 to as high as 15.5 percent in 2Q2022. Phishing against cryptocurrency targets – such as cryptocurrency exchanges and wallet providers – fell to 2%. This was down from 4.5 percent in 2Q 2022 and 2.3 percent in 4Q2022, as the crypto market was roiled by the collapse of FTX in November 2022.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, noted: “We’re tracking a continued strong increase in mobile phone-based fraud. This voice-phishing, or vishing, volume swelled more than 40% as compared to 4Q 2022 totals, and representing nearly a ten-times increase as compared to 1Q 2022.”



OpSec Security offers world-class brand protection solutions.

APWG Phishing Activity Trends Report Contributors

 <p>Agari by Fortra protects organizations against phishing, business email compromise (BEC) scams, and other advanced email threats.</p>	 <p>Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.</p>	 <p>OpSec Security offers world-class brand protection solutions.</p>
 <p>PhishLabs by Fortra provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.</p>		

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver (foy@apwg.org, +1.404.434.728). For media inquiries related to the company-content of 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.,** www.illumintel.com

Phishing Activity Trends Report, 1st Quarter 2023

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 protect 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.

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.

