

PHISHING ACTIVITY TRENDS REPORT

**4th Quarter
2023**

APWG

Unifying the
Global Response
To Cybercrime

Activity October-December 2023
Published 13 February 2024

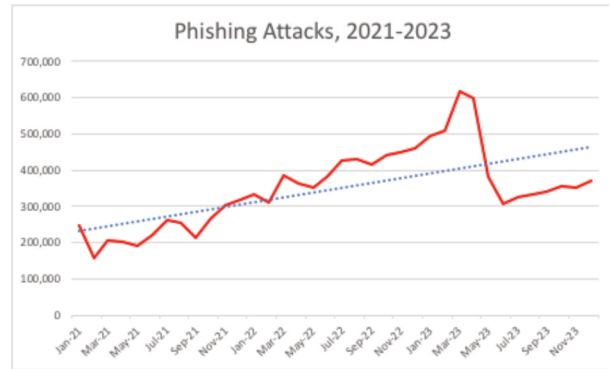
Phishing Report Scope

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@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.

2023 Was Worst Year for Phishing on Record



Even after a dramatic decrease in the second quarter, phishing rose late in the year, and the APWG observed 1,077,501 phishing attacks in the fourth quarter of 2023

Phishing Activity Trends Summary

- The APWG observed 1,077,501 phishing attacks in the fourth quarter of 2023. APWG observed almost five million phishing attacks in 2023, the worst year for phishing on record. [pp. 3-4]
- Attacks against social media platforms exploded in late 2023, and were 42.8 percent of all phishing attacks. [p. 5]
- Phishing using phone calls — also known as voice phishing or “vishing” — is increasing every quarter. [pp. 5-6]
- The number of wire transfer BEC attacks in Q4 increased by 24% compared to the prior quarter. While the number of these attacks was up, the average dollar amount per attempt went down, to \$56,195. [p. 6]

Table of Contents

Statistical Highlights	3
Most-Targeted Industry Sectors	5
Business Email Compromise	6
Free Webmail services used in BEC attacks	8
Registrars sponsoring BEC attack domains	8
APWG Phishing Trends Report Contributors	9
About the APWG	9

Phishing Activity Trends Report, 4th Quarter 2023

Statistical Highlights for the 4th 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.

	October	November	December
Number of unique phishing Web sites (attacks) detected	356,538	350,776	370,187
Unique phishing email campaigns	22,750	24,621	20,642
Number of brands targeted by phishing campaigns	477	442	420

The APWG observed almost five million phishing attacks over the course of 2023 — 4,987,809 attacks in all. This made 2023 the worst year for phishing on record, eclipsing the 4.7 million attacks seen in 2022.

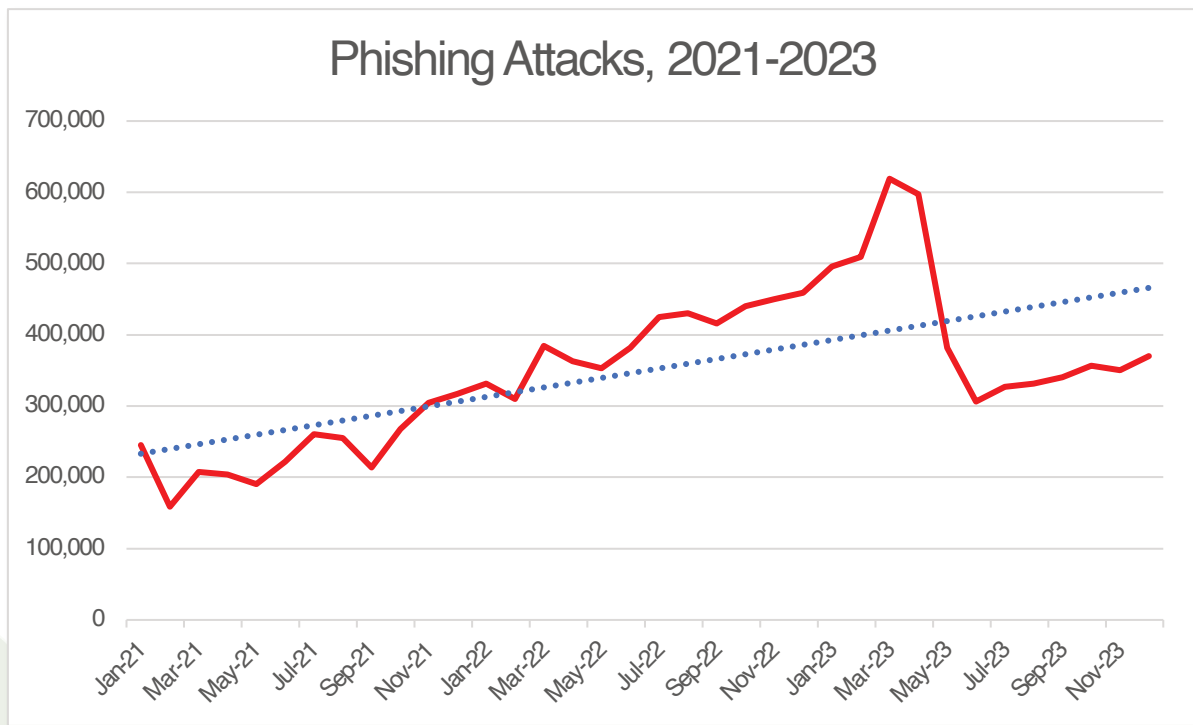
In the fourth quarter of 2023, APWG observed 1,077,501 phishing attacks. This was up slightly from the 999,956 seen in Q3, but down from the 1,286,208 seen in Q2, and far below the 1,624,144 attacks seen in Q1 2023, which was the record high quarter in APWG's historical observations.

Phishing attacks fell in the second quarter of 2023 in part due to the shut-down of the Freenom free domain name program. Freenom offered free domain name registrations in five repurposed country top-

Phishing Activity Trends Report, 4th Quarter 2023

level domains (.TK, .ML, .GA, .CF, and .GQ), and this free service was used extensively by phishers for many years. In past years Freenom domains had been used for 14 percent of all phishing attacks worldwide, and Freenom was responsible for 60 percent of the phishing domains reported in all ccTLDs in November 2022. Freenom stopped offering free registrations in January 2023, and phishing in its ccTLDs died out as phishers used up their free domain inventories in mid-2023.¹ In February 2024, Freenom announced its complete exit from the domain name business, and that it had settled a lawsuit brought by Meta, which alleged that Freenom had ignored abuse complaints about phishing websites while monetizing traffic to those abusive domains.²

After the notable decrease in Q2 2023, phishing levels began creeping up again, and reached the levels observed in early 2022:



In Q4 2023, the number of unique email subjects (campaigns) received by the APWG dropped slightly from the previous quarter. The number of total email reports that APWG received was flat between Q3 and Q4.

¹For an in-depth look at the Freenom decrease, see “Phishing Landscape 2022” by Interisle Consulting and APWG members Greg Aaron and David Piscitello: <https://www.interisle.net/PhishingLandscape2023.pdf>

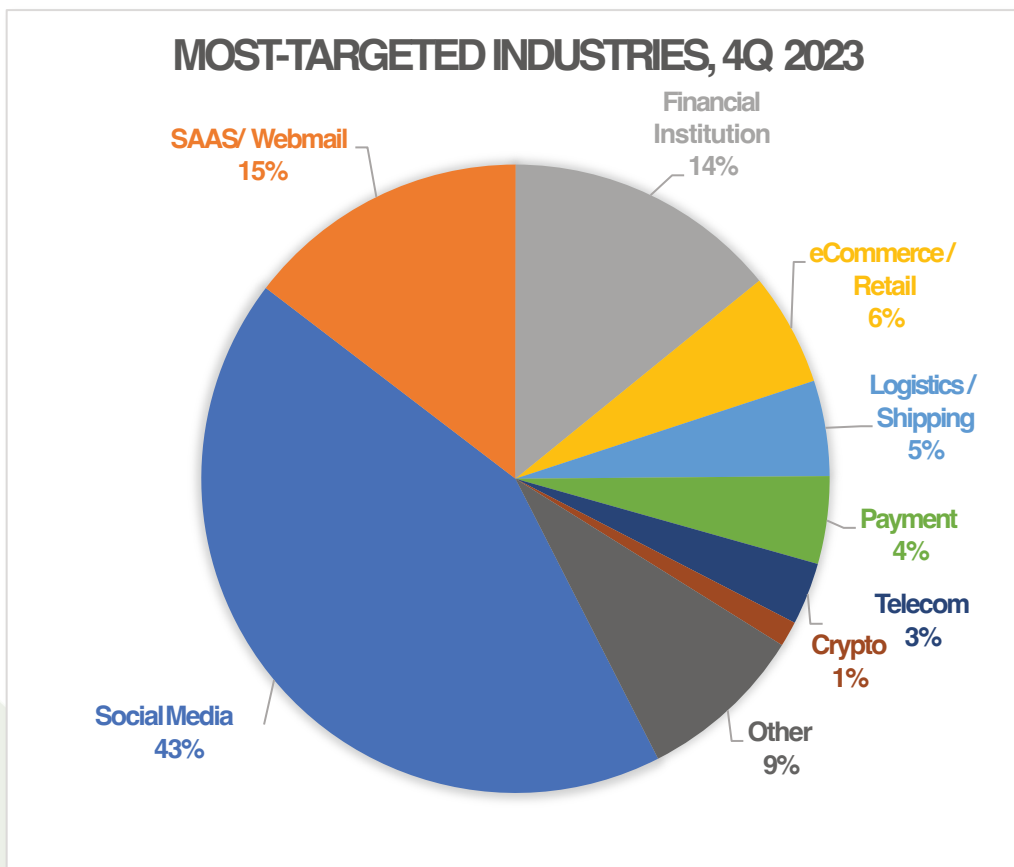
²https://www.freenom.com/en/freenom_pressstatement_02122024_v0100.pdf

Most-Targeted Industry Sectors – 4th Quarter 2023

In the fourth quarter of 2023, APWG founding member OpSec Security found that phishing attacks against social media platforms comprised 42.8 percent of all phishing attacks, exploding from 18.9 percent of all attacks in Q3. Phishing against the Financial Institution segment fell, from 24.9 percent of all attacks in Q3 to 14 percent in Q4. Attacks against online payment services were another 4 percent of all attacks.

“Continuing a trend we’ve previously observed, OpSec is tracking a strong increase in phone-based fraud, or voice phishing,” said Matt Harris, Senior Product Manager, Fraud at OpSec. “Vishing incidents increased more than 16 percent over Q3, and represented a nearly 260 percent increase over the Q4 2022 volume.”

OpSec Security offers world-class brand protection solutions.



Business e-Mail Compromise (BEC), 4th Quarter 2023

APWG member Fortra tracks the identity theft technique known as “business e-mail compromise” or BEC, which was responsible for \$51 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 Q4 2023. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

Fortra found that when criminals asked victims to send money by wire transfer, the average amount requested in Q4 2023 was \$56,195, down 64 percent from Q3’s average of \$157,422. The number of wire-transfer BEC attacks in Q4 increased by 24 percent compared to the prior quarter. This suggests bad actors behind BEC wire transfer conducted more attacks but requested smaller amounts of money in each attack.

During the fourth quarter of 2023, gift card scams were the most popular scam type, and were 37.6 percent of all scams. At number two were advance fee fraud scams, at 30.6 percent. Payroll diversion remained a popular attack type, making up 9.2 percent of Fortra’s engagements.

Hybrid vishing is phishing in which the attacker uses both email and telephone to communicate with the victim. Fortra rarely saw hybrid vishing before 2023, but these made up 6.1 percent of the attacks Fortra recorded in the fourth quarter of 2023.

“The hybrid vishing attacks we track typically begin with an email, which tells the recipient that he or she 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. Geek Squad was the most common brand used as a lure in these attacks, accounting for 32.2 percent of the Q4 2023 attacks. This was followed by Norton/LifeLock with 30.4 percent, McAfee at 20 percent, and PayPal with 11.3 percent.”

Phishing Activity Trends Report, 4th Quarter 2023

From: invoice#91202 <[REDACTED]@gmail.com>
Sent: Monday, February 12, 2024 11:18 AM
To: [REDACTED]
Subject: Don't Let Your Subscription Expire - Renew Today! ref no | ZU14: [REDACTED]



Feb 12, 2024
Billing ID: GSE3C [REDACTED]

Dear Customer,

Renewal auto-debit of \$286.42 confirmed successfully. Thank you!

It may take a few moments for this transaction to appear on your account. If you didn't authorize this transaction call our fraud protection team on +1(805) 438-2152

Type	Confirmation to buyer
Personal Home	Approved

Services Type- Online Support	Membership details
	J8976HN [REDACTED]

Product Description	Unit price	Qty	Amount
Personal Home-plan	\$286.42	1	\$286.42
		Subtotal:	\$286.42
		Total:	\$286.42
		Payment:	\$286.42

Charge show on your Credit Statement as 'PAY GEEK-SQUAD'.
Payment sent to 'Geek@Squad'.

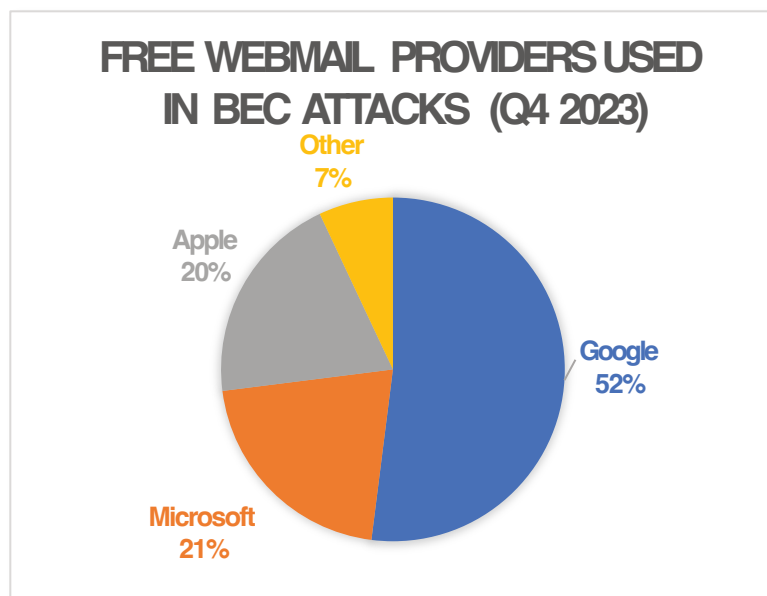
Issues with this transaction?

You have 30 days from the date of transaction to open a dispute in the Resolution Center or else call us for faster assistance on +1(805) 438-2152

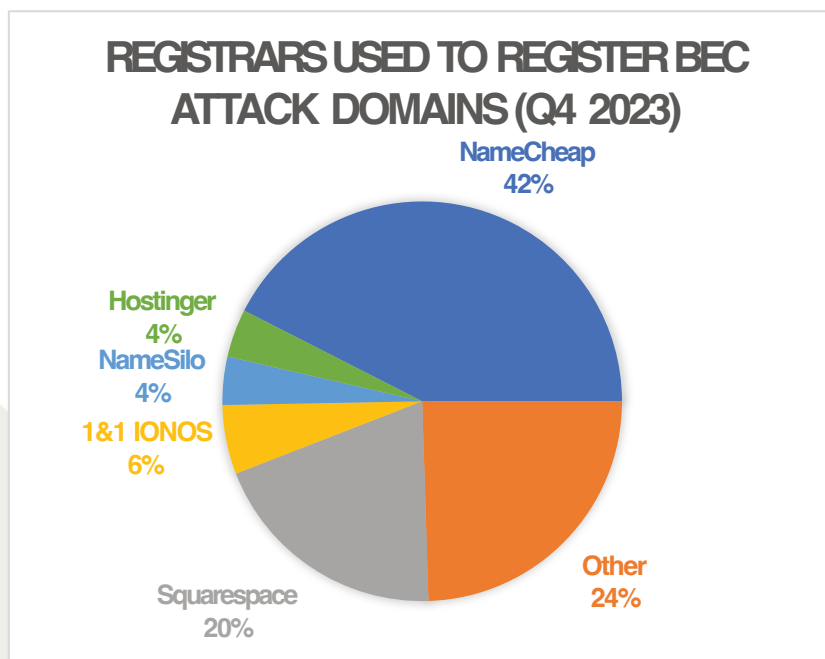
Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, login to your account and click "Contact Us" at the bottom of any page.

Above: an email lure used in a hybrid phishing attack




Fortra found that 68 percent of BEC attacks in Q4 2023 were launched using a free webmail domain, a decrease from the 72 percent observed in Q3. The remaining 32 percent of BEC attacks utilized a combination of maliciously registered domains and compromised email accounts.



Google was the most popular free webmail provider for BEC scammers, accounting for 52 percent of the free webmail accounts used in Q4 2023 BEC scams. This is a significant drop from Google’s 83 percent share Fortra observed in Q3. Microsoft’s webmail properties (e.g. Outlook and Hotmail) powered 21 percent of webmail-based BEC attacks in Q4, followed by Apple’s webmail domains (e.g. icloud.com; me.com, mac.com) at 20 percent.



APWG Phishing Activity Trends Report Contributors

 <p>Fortra's mission is to help organizations increase security maturity while decreasing operational burden. Fortra's brands include PhishLabs and Agari.</p> <p>www.fortra.com</p>	 <p>Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.</p> <p>www.illumintel.com</p>	 <p>OpSec Security is the leading provider of integrated online protection and on-product authentication solutions for brands and governments.</p> <p>www.opsecsecurity.com</p>
---	---	---

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 four 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.

STOP | THINK | CONNECT  APWG's [STOP. THINK. CONNECT.](#) cybersecurity awareness campaign **MESSAGING CONVENTION** 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.

