

PHISHING ACTIVITY TRENDS REPORT

4th Quarter

2022

APWG

Unifying the
Global Response
To Cybercrime

Activity October - December 2022

Published 9 May 2022

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

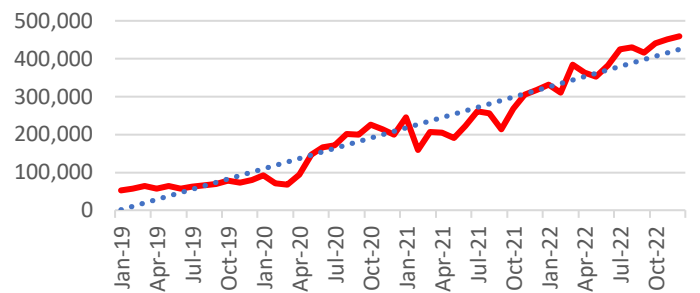
Phishing is a crime employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as 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

Statistical Highlights	3
Most-Targeted Industry Sectors	5
Business E-mail Compromise (BEC)	8
Email-Based Threats	7
APWG Phishing Trends Report Contributors	8
About the APWG	9

Phishing Reaches New Quarterly High in Late 2022

Phishing Attacks, Jan 2019 to Dec 2022



The year 2022 was another record-shattering year for phishing, with the APWG logging more than 4.7 million attacks

Phishing Activity Trends Summary

- 2022 was a record year for phishing, with the APWG logging more than 4.7 million attacks. Since the beginning of 2019, the number of phishing attacks has grown by more than 150% per year. [pp. 3-4]
- The 101,104 unique email subjects received in October 2022 was the single largest month sample APWG had ever seen. [p. 3]
- The APWG observed 1,350,037 total phishing attacks in Q4 2022. This was up slightly from the record third quarter, when APWG recorded 1,270,883 total phishing attacks. [pp. 3-4]
- Attacks against the financial sector represented 27.7% of all phishing attacks. [p. 5]
- Business Email Compromise (BEC) attacks continued to menace enterprises. The average BEC attack attempted to steal \$132,559. [p. 6]

Statistical Highlights for the 4th Quarter 2022

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:

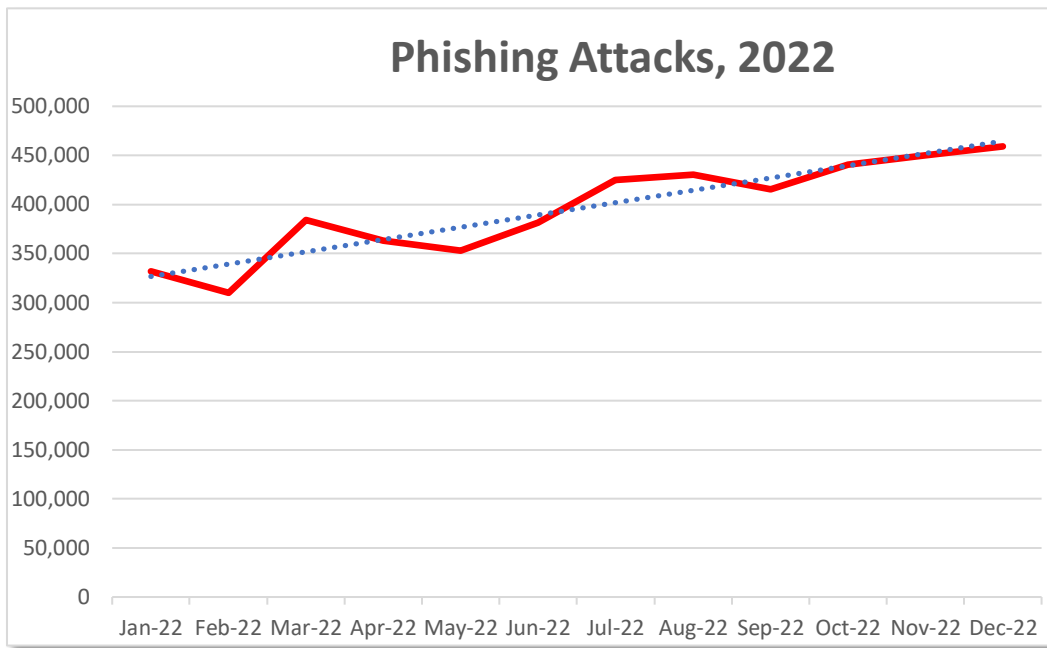
- **Unique phishing sites.** This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically 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	440,508	450,390	459,139
Unique phishing email subjects	101,104	77,469	74,250
Number of brands targeted by phishing campaigns	599	610	577

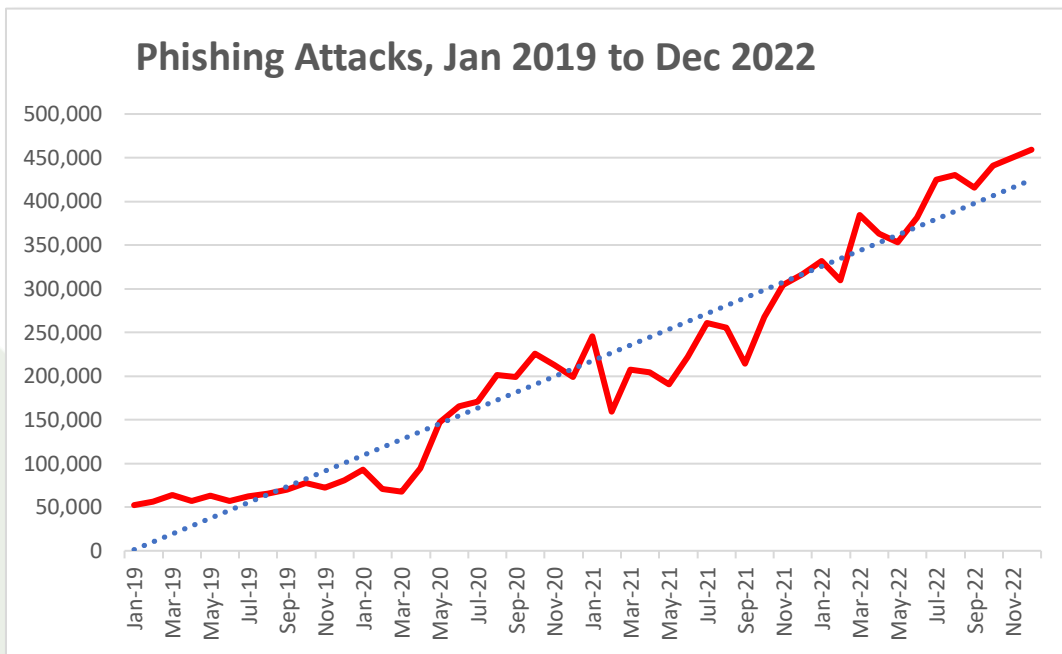
In the fourth quarter of 2022, APWG observed 1,350,037 total phishing attacks. This was up slightly from the third quarter, when APWG recorded 1,270,883 total phishing attacks, which was a new record at the time and the worst quarter for phishing that APWG has ever observed. In 4Q 2022, APWG also received increased phishing email submissions from its members and the public. The 101,104 unique email subjects received in October 2022 was the largest APWG had seen.

Phishing Activity Trends Report, 4th Quarter 2022

In general, the number of phishing sites seen each month climbed across 2022:



Looking across four years, APWG has seen *steep increases, accelerating to more than 150% per year:*



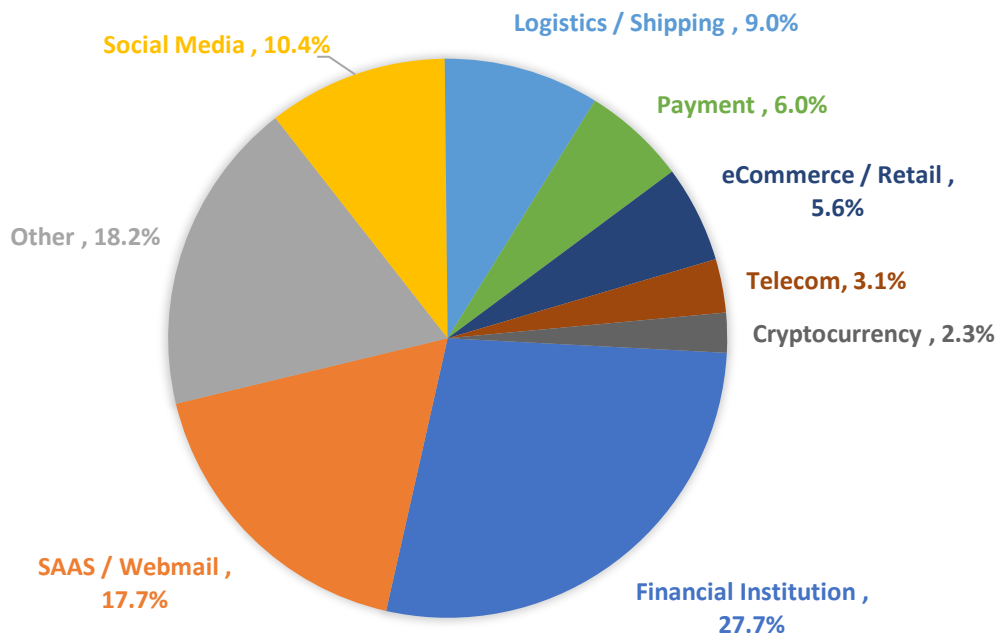
Most-Targeted Industry Sectors – 4th Quarter 2022

In the fourth quarter of 2022, APWG founding member OpSec Security found that phishing attacks against the financial sector, which includes banks, remained the largest set of attacks, accounting for 27.7 percent of all phishing, up from 23.2 percent in Q32022. Attacks against webmail and software-as-a-service (SAAS) providers were next in prominence, at 17.7 percent, declining slightly from Q3. Attacks against payment processors such as PayPal, Venmo, and VISA accounted for another 6 percent.

Phishing against social media companies trended downward, after fluctuating from 8.5 percent of all attacks in 4Q2021 to 15.5 percent in 2Q2022. Phishing against cryptocurrency targets — such as cryptocurrency exchanges and wallet providers — fell from 4.5 percent in Q2 to 2.0 percent in Q3 and 2.3 percent in Q4, as the crypto market continued to be roiled by falling values.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, noted: “The logistics and shipping industry saw a large fraud volume increase, specifically because of more attacks against the U.S. Postal Service. We also tracked a huge increase in mobile phone-based fraud, with vishing detection volumes swelling in Q4, more than 40 percent as in Q3.”

MOST-TARGETED INDUSTRIES, 4Q2022



OpSec Security offers world-class brand protection solutions.

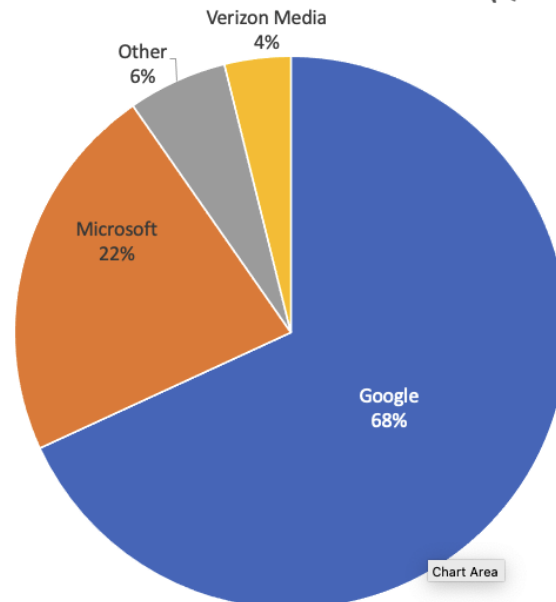
Business e-Mail Compromise (BEC), 4th Quarter 2022

APWG member Agari by Fortra tracks the identity theft technique known as “business e-mail compromise” or BEC, which has caused aggregate losses in the billions of dollars, at large and small companies. In a BEC attack, a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts (a “spear phishing” attack). Agari examined thousands of BEC attacks during Q4 2022. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive data. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

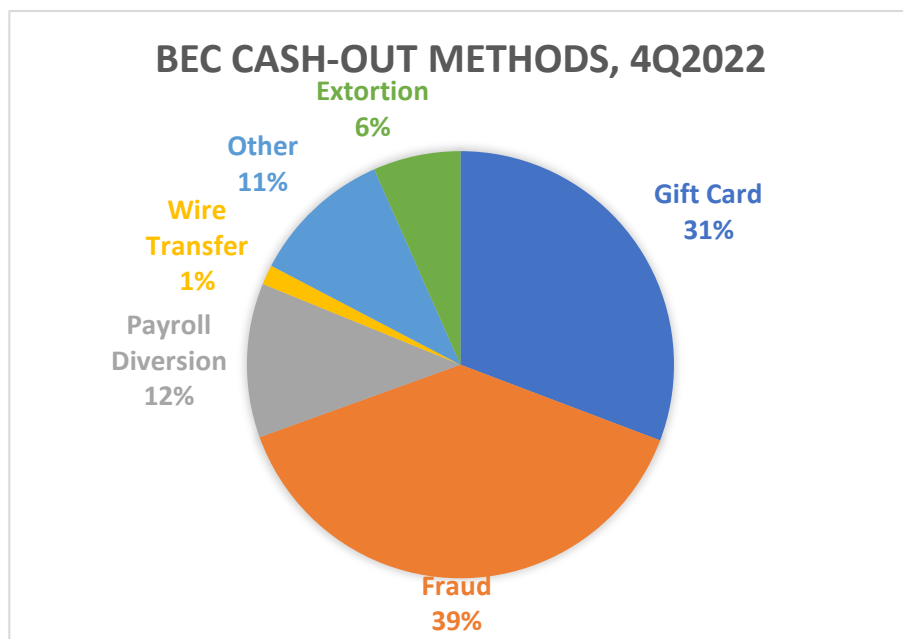
Fortra found that the average amount requested in wire transfer BEC attacks in 4Q 2022 was \$132,559, up 41 percent from the Q3 average of \$93,881. The volume of wire transfer BEC attacks in Q4 decreased by 64 percent compared to the prior quarter. This suggests the bad actors behind BEC wire transfer incidents focused their attention on fewer but more impactful attacks.

During the fourth quarter of 2022, advance fee fraud scams surpassed gift card requests as the most popular cash out method, comprising 39 percent of the total compared to just 31 percent of attackers requesting gift cards as payment. Payroll diversion remained a popular attack type, making up 12 percent of our engagements. Extortion attacks, which included threats of imprisonment and public embarrassment, made up 7 percent of the attacks we monitored. Wire transfer attacks made up less than 1 percent of the total. A variety of miscellaneous cash out methods accounted for the balance.

Free Webmail Providers Used in BEC Attacks (Q4 2022)



Amazon was the overwhelming favorite card type for scammers, with 60 percent requesting Amazon gift cards as payment. Apple's gift card offerings were the second most popular, with 9 percent requesting iTunes and 9 percent requesting Apple Store cards. Requests for liquid cards, such as American Express, Visa, and Vanilla made up 11.4 percent of gift card requests.



Fortra found that 89 percent of BEC attacks in Q4 2022 were launched using a free webmail domain, up from 84% in Q3. The remaining 11 percent of BEC attacks in Q4 utilized maliciously registered domains and compromised email accounts. John Wilson, Senior Fellow, Threat Research at Fortra notes that "Google was the technology provider of choice for BEC scammers in Q4 2022, with 68 percent of free webmail accounts hosted at Gmail and 27 percent of maliciously registered BEC domains using Google as their registrar."

Microsoft's webmail properties powered 22% of webmail based BEC attacks in Q4. Verizon Media, which includes Yahoo and AOL, accounted for just 4% of the free webmail accounts used for BEC in Q4 2022.





Email-based Threats, 4th Quarter 2022

APWG member PhishLabs by HelpSystems analyzes malicious emails reported by corporate users. John Wilson, Senior Fellow, Threat Research at Fortra observed: "For the fourth consecutive quarter, the share of response-based email threats targeting enterprise users increased, with a corresponding decrease in credential theft attacks."

Phishing Activity Trends Report, 4th Quarter 2022

"Physical threats, which comprised just 0.3 percent of the social media threats we saw one year ago, made up 1.02 percent of Q4 2022 social media threats," noted John Wilson.

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, 4th Quarter 2022

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](#) send 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 27 nations, 14 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.

