PHISHING ACTIVITY TRENDS REPORT

4th Quarter 2024

APWG

Unifying the
Global Response
To Cybercrime

Activity October-December-
September 2024

Published 19 March 2025

Phishing Report Scope

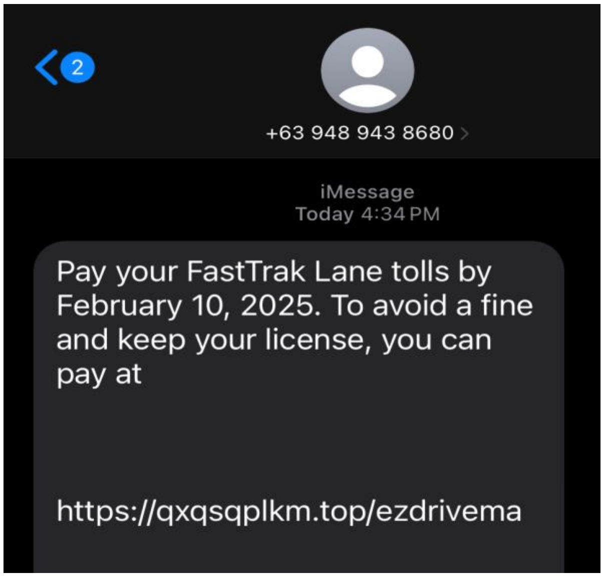
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG 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 messages, bogus web sites, and deceptive domain names. 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 Trends Upward: Toll Road Scams Flood Phones



iMessage
Today 4:34 PM

Pay your FastTrak Lane tolls by February 10, 2025. To avoid a fine and keep your license, you can pay at

https://qxqsqplkm.top/ezdrivema

Leveraging new phishing kits and the .TOP gTLD, Chinese phishers are flooding smartphones with SMS-based phishing messages

Phishing Activity Trends Summary

- In the fourth quarter of 2024, APWG observed 989,123 phishing attacks, up from 877,536 in Q2 and 932,923 in Q3. [pp. 3-4]
- Chinese phishers are sending floods of SMS phishing messages, enabled by a new phishing kit and .TOP domain names. [pp. 4-6]
- The SAAS/Webmail category was the most-attacked sector, with social media sites close behind. [p. 7]
- The average amount requested in wire transfer BEC attacks in Q4 2024 was $128,980—nearly double the third quarter's average. [p. 8]

Statistical Highlights for the 4th Quarter 2024

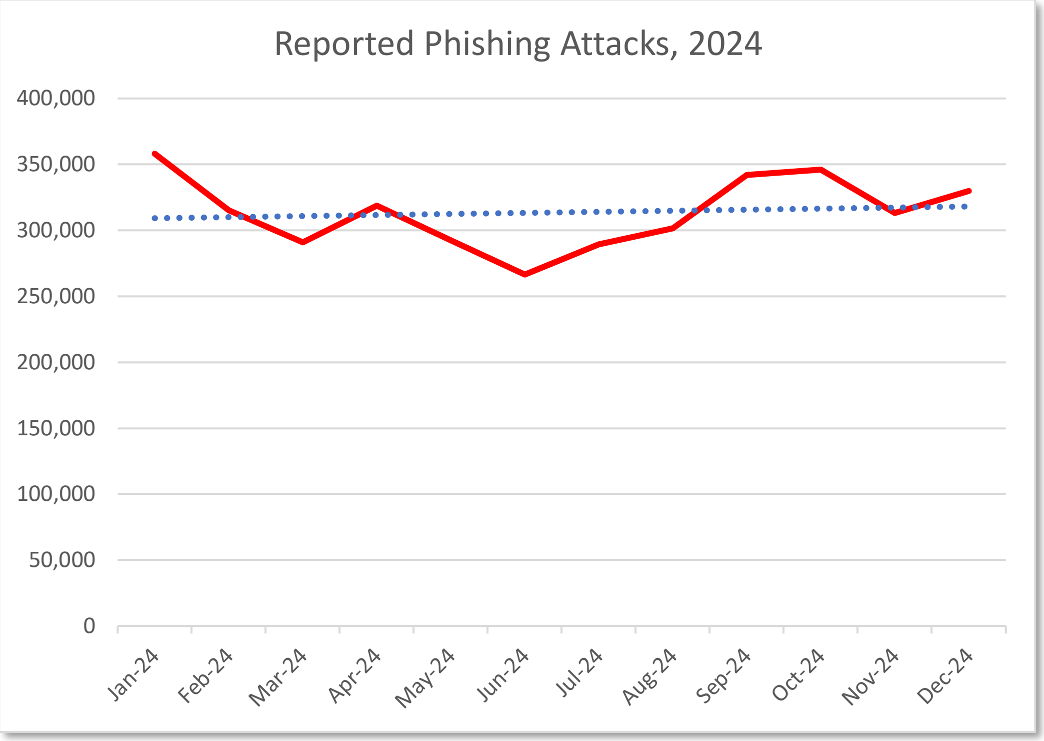
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

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	345,881	313,288	329,954
Unique phishing email campaigns	28,327	27,668	33,899
Number of brands targeted by phishing campaigns	315	333	309

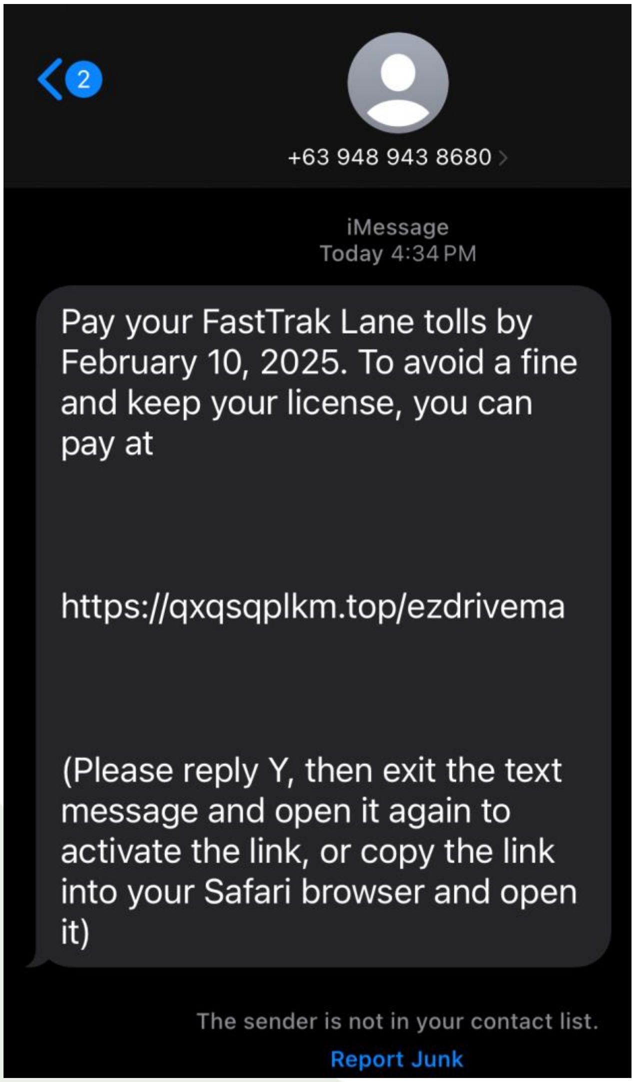
In the fourth quarter of 2024, APWG observed 989,123 phishing attacks, up from 877,536 in Q2 and 932,923 in Q3. Phishing generally declined across the first half of 2024, and then trended upward in the second half of the year. The number of phish in the quarter ranged between 290,000 and 358,000 attacks per month:



Current Phishing Trend: SMS Phishing Attacks Toll Operators

Residents of the United States are being bombarded with text messages from Chinese phishers, purporting to come from U.S. toll road operators, including the multi-state EZPass system. The messages warn recipients that they face fines or loss of their driving license if they don't pay their tolls online. Researchers have found that this "smishing" (SMS phishing) is enabled by an upgraded phishing kit sold in China, which makes it simple to send text messages and launch phishing sites that spoof toll road operators in multiple U.S. states. The phone numbers that the phishers send the messages to are usually random—they are sometimes sent to people who do not use toll roads at all, or target users in the wrong state. Note: Some of the text messages are sent from phone numbers in countries other than China.

A typical example is:



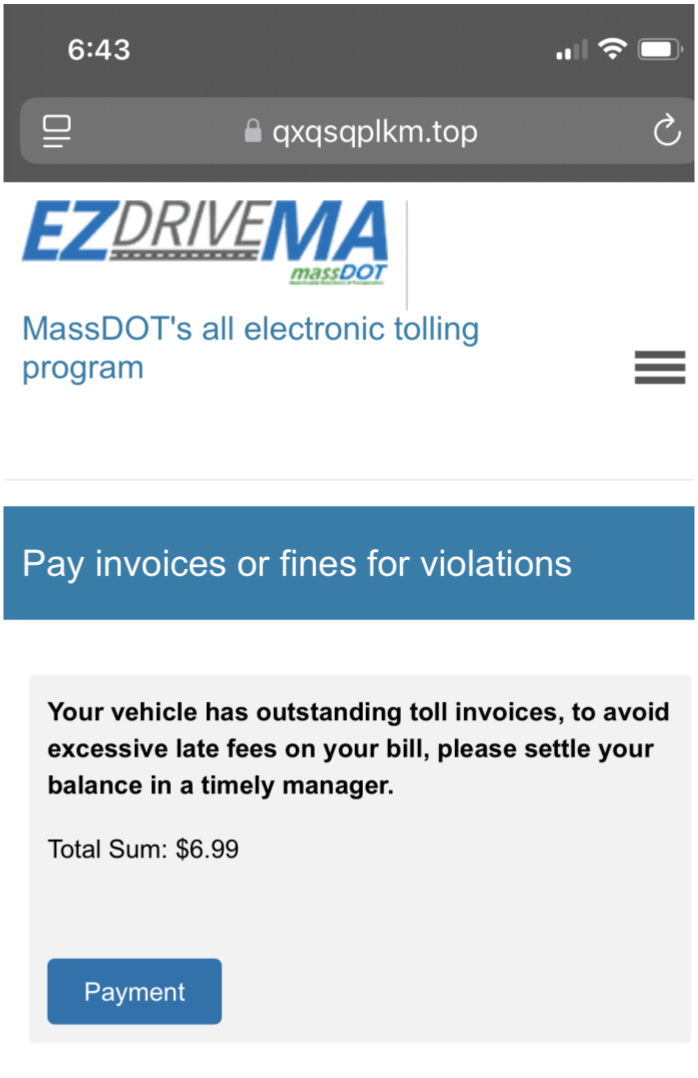
iMessage
Today 4:34 PM

Pay your FastTrak Lane tolls by February 10, 2025. To avoid a fine and keep your license, you can pay at

https://qxqsqplkm.top/ezdrivema

(Please reply Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)

The sender is not in your contact list.



MassDOT's all electronic tolling program

Pay invoices or fines for violations

Your vehicle has outstanding toll invoices, to avoid excessive late fees on your bill, please settle your balance in a timely manager.

Total Sum: $6.99

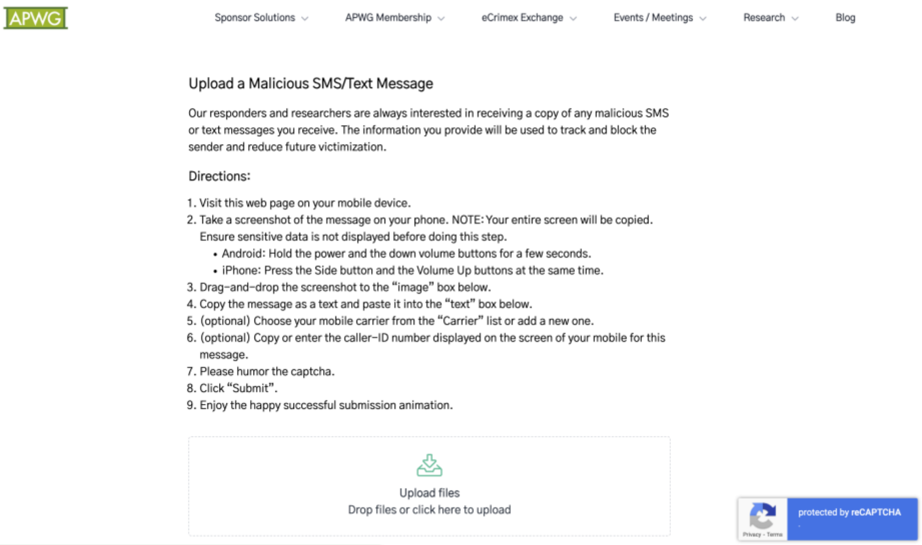
*Above: a phishing text message (**left**), and the mobile web site to which it was linked (**right**), February 10, 2025. The phishing site was on a .TOP domain name, and the lure message was sent from a phone number apparently originating a call from a telephone exchange in the Philippines.*

APWG Senior Research Fellow Greg Aaron notes: "The phishers set up these phishing sites using cheap domain names they register in lesser-known top-level domains such as .TOP, .CYOU, and .XIN. This is one way to spot these scam messages. The .TOP domain registry is operated in China, and has a notable history of being used by phishers."

The .TOP Registry also has long-running compliance problems. ICANN issued a breach letter to .TOP Registry in July 2024, citing .TOP's failures to comply with abuse reporting and mitigation requirements, and as of March 2025 the case is still listed as unresolved on ICANN's Web site. [ICANN can issue breach letters to contracted parties, Registrars and Registries, as notification of their failure to correct a violation of rules or contract terms with ICANN, an escalation that notifies the contracted party of the possibility of de-accreditation.] Many of the domain names are being registered at the Chinese registrar Dominet (HK) Limited. Dominet was formerly known as Alibaba.com Singapore E-Commerce Private Limited, and was re-named in August 2024, after receiving a breach letter from ICANN for not taking steps to investigate and respond to abuse complaints.

The real toll operators never ask customers to click a link to pay for tolls. To avoid text scams like this:

- Don't click on any links in, or respond to, unexpected texts. Scammers want you to react quickly — but instead, take time to check it out.
- Check to see if the text is legitimate. Reach out to the company using a phone number or website you know is real — don't use info from the text.
- Report (and then delete) suspicious text messages directly to the APWG's global **eCrime eXchange** (eCX) to help update alerting/blocking mechanims that protect billions of devices and software clients worldwide. Directions here: https://apwg.org/sms



Upload a Malicious SMS/Text Message

Our responders and researchers are always interested in receiving a copy of any malicious SMS or text messages you receive. The information you provide will be used to track and block the sender and reduce future victimization.

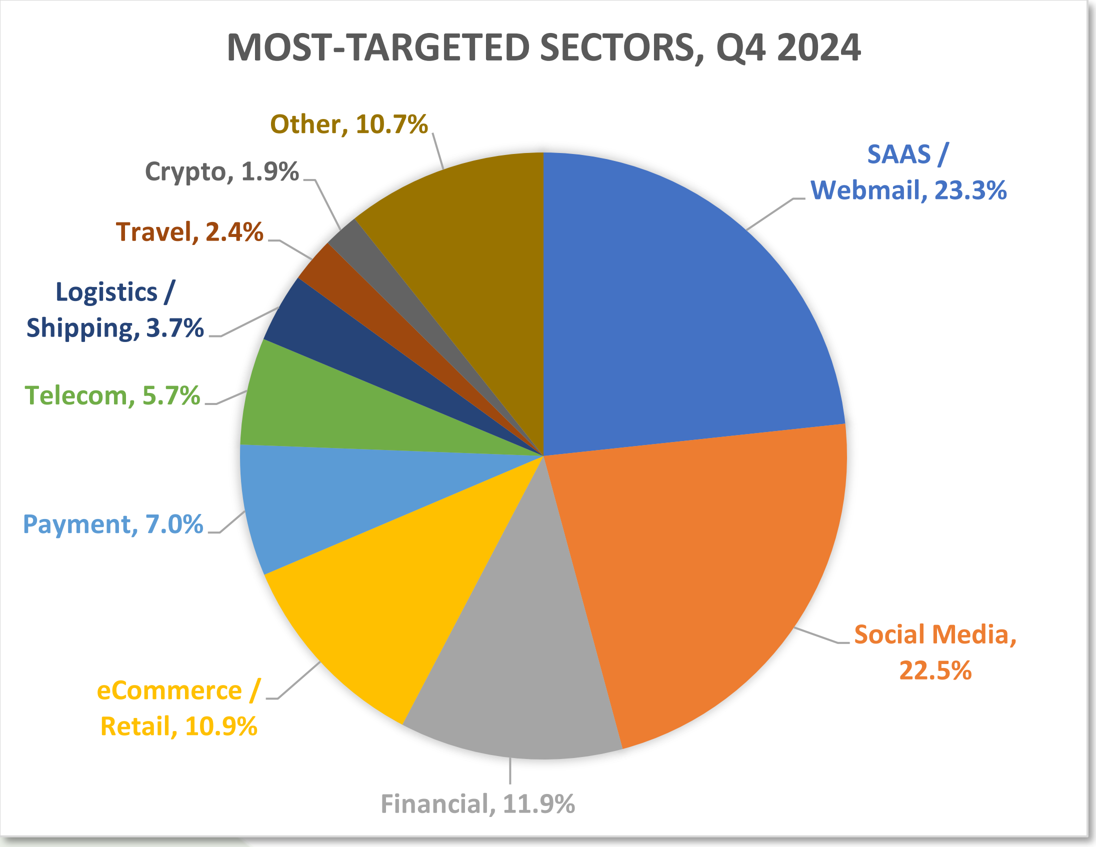
Directions:

1. Visit this web page on your mobile device.
2. Take a screenshot of the message on your phone. NOTE: Your entire screen will be copied. Ensure sensitive data is not displayed before doing this step.
   - Android: Hold the power and the down volume buttons for a few seconds.
   - iPhone: Press the Side button and the Volume Up buttons at the same time.
3. Drag-and-drop the screenshot to the "image" box below.
4. Copy the message as a text and paste it into the "text" box below.
5. (optional) Choose your mobile carrier from the "Carrier" list or add a new one.
6. (optional) Copy or enter the caller-ID number displayed on the screen of your mobile for this message.
7. Please humor the captcha.
8. Click "Submit".
9. Enjoy the happy successful submission animation.

- APWG member organizations' responders and researchers are assisted by receiving a copy of any malicious SMS or text messages you receive – for tracking and blocking the sender to reduce future victimizations.
- You can also use your phones' "report junk" option to report unwanted texts in the messaging app, or forward them to 7726 (SPAM). Or, report to IC3.

Most-Targeted Industry Sectors – 4th Quarter 2024

In the fourth quarter of 2024, APWG founding member OpSec Security found that the SAAS/Webmail category was the most-attacked sector, with 23.3 percent of all phishing attacks. Attacks against social media platforms fell to #2, with 22.5 percent of all attacks, down from 30.5 percent in Q3. Phishing against the Financial Institution (banking) segment continued to fall, to 11.9 percent of all attacks, down from 13 percent in Q3 2024, and down from 24.9 percent of all attacks in Q3 2023.



APWG contributing member OpSec Security detected a decrease in overall phishing attacks in Q4 as compared to Q3. However, the amount of phishing by phone call (voice phishing, or "vishing") was generally higher in Q4 than in Q3, except during a lull around the December holidays. OpsSec believe this is a seasonal drop, and that vishing will remain popular.

OpSec Security also observed a 30 percent increase in the number of unique brands targeted from Q3 to Q4. The number of targeted brands had been steady until the rise in Q4; this might be an indication that scammers are expanding their target scope to increase their return on investment.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, remains concerned about vishing. Harris said: "OpSec has recently deployed new detection mechanisms, and we expect these to bring in additional detections in the future, especially fraud being communicated via SMS messages. We are continuing to see scammers branching out to attack new companies and industries, such as public utilities, car parking meter systems, and bridge toll collection systems."

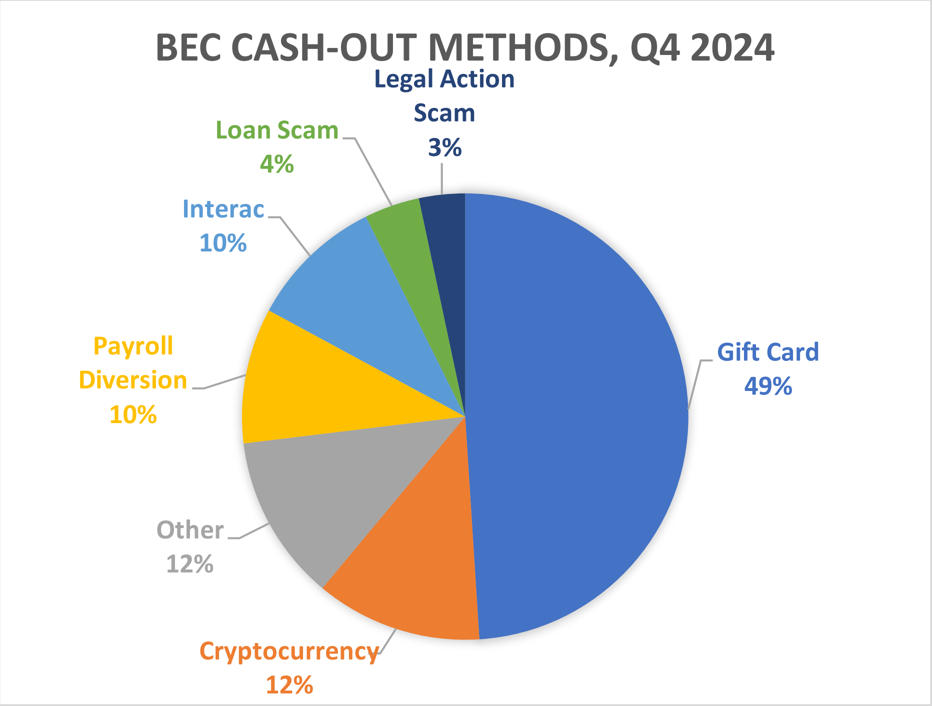
OpSec Security offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 4th Quarter 2024

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 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 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

Fortra found that the average amount requested in wire transfer BEC attacks in Q4 2024 was $128,980, nearly double the third quarter's average of $67,145. The total number of wire transfer BEC attacks in Q4 decreased by 21 percent compared to the third quarter.

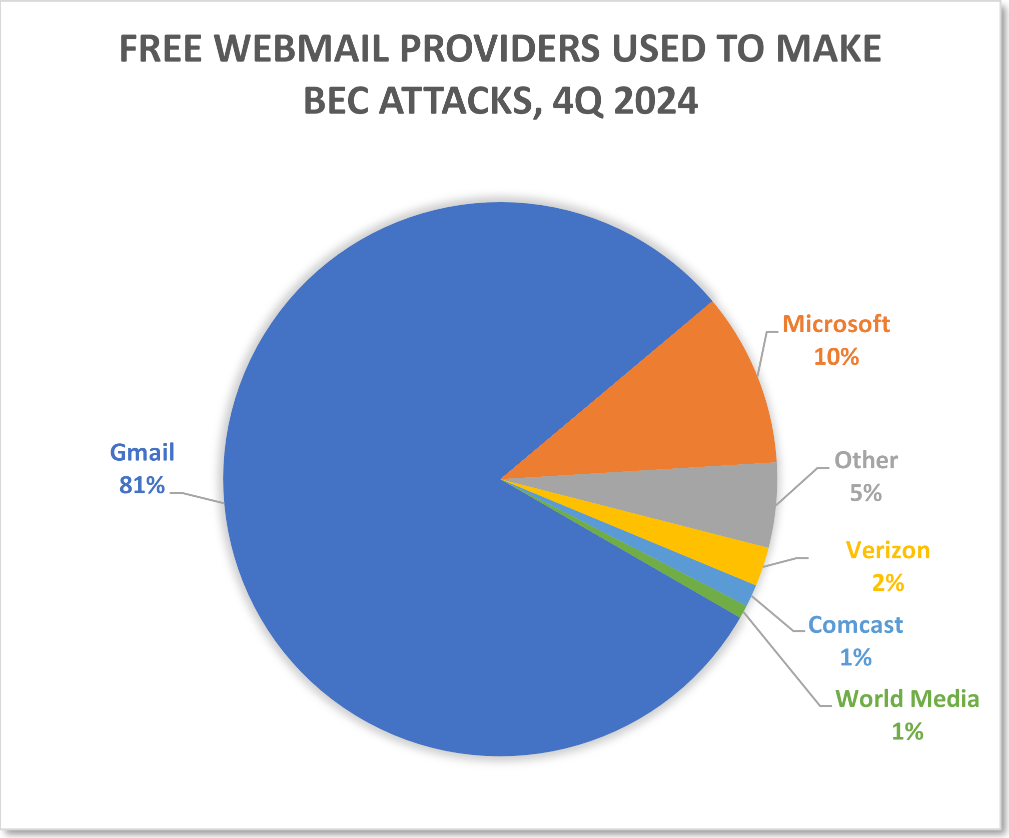
During the fourth quarter of 2024, gift card scams were once again the most popular type of scam, making up 49 percent of the total scam attempts. Scams demanding cryptocurrency as payment made up 12 percent of the attacks—a significant uptick from the previous quarter, when just 2.7 percent of attacks demanded cryptocurrency. John Wilson, Senior Fellow, Threat Research at Forta, said: "The big increase in extortion scams that demand cryptocurrency is likely due in part to record-high Bitcoin prices."



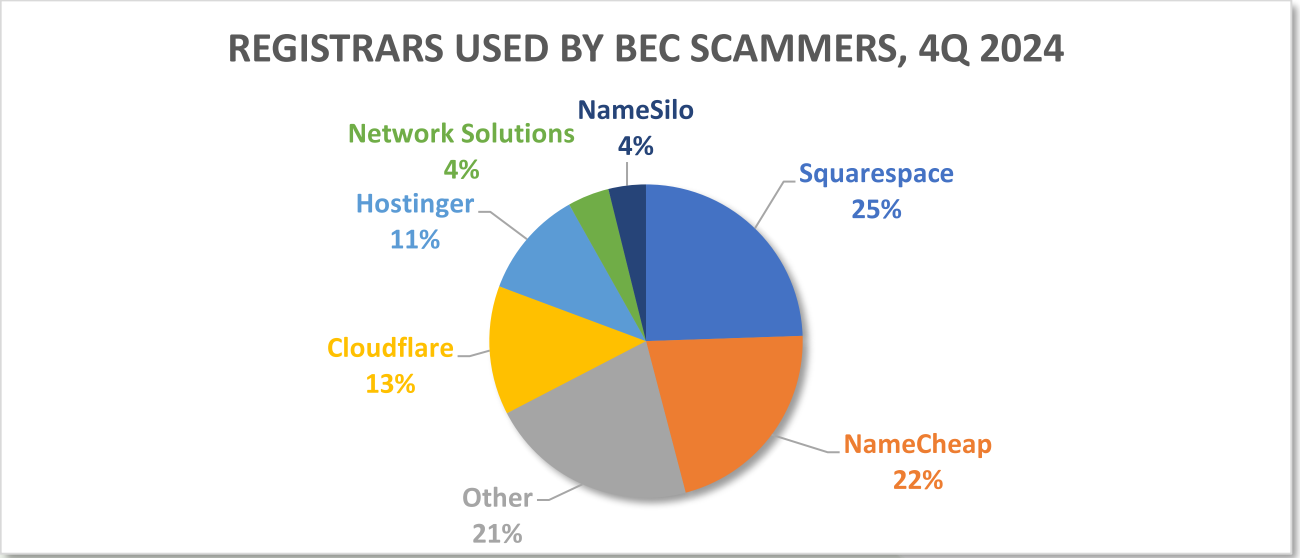
Loan scams made up 4 percent of attacks. A loan scam is a type of advance fee fraud where a bad actor poses as a lender offering low-interest financing. The scammer typically offers large loans for no collateral at below-market interest rates; however, the victim must pay various loan origination fees. The scammer will ghost the victim once the upfront fees are paid, and the loan is never funded.

Legal action extortion scams made up 3.3 percent of the quarter's total. These scams present attackers as agents of a national law enforcement agency. The email messages claim the victim is wanted for viewing CSAM (Child Sexual Abuse Material) online and must immediately pay a fine or face arrest.

Google's Gmail was by far the most popular free webmail provider used by BEC scammers —used for 81 percent of the free webmail accounts set up for BEC scams. Far below that at #2 were Microsoft's webmail properties, which were used for just 10 percent of webmail-based BEC attacks in Q4 2024:



John Wilson, Senior Fellow, Threat Research at Forta, observed: “Fortra notes that Cloudflare was the third-most-popular domain name registrar used by BEC scammers in Q4 2024. This is the first time Cloudflare made Fortra's list of top BEC domain registrars.”



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.fortra.com	ILLUMINTEL Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce. www.illumintel.com	OP SEC 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 is © 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 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 data send more than two billion data elements per month to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of users, software clients, and devices worldwide.

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.

STOP | THINK | CONNECT MESSAGING CONVENTION

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.