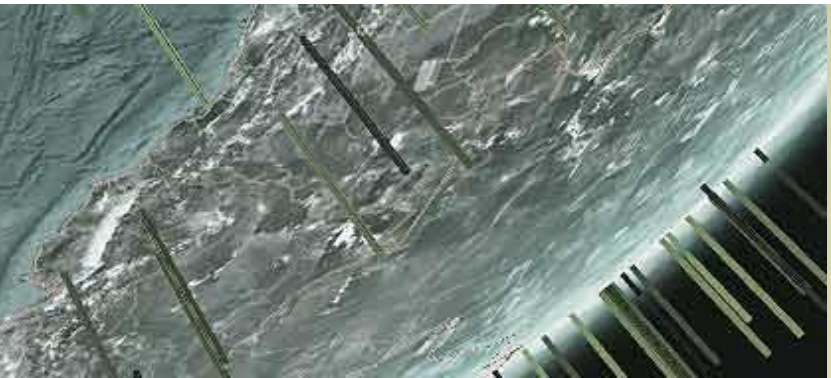
PHISHING ACTIVITY TRENDS REPORT

1st Quarter 2026

APWG

Unifying the
Global Response
To Cybercrime



Activity January-March 2026

Published 21 May 2026

Phishing Report Scope

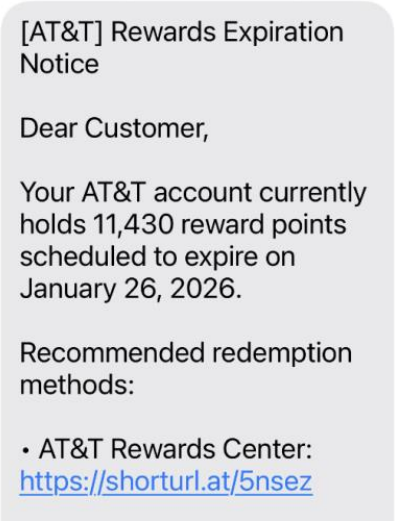
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG 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, Scams Expand on All Social Media as Telecoms Targeting Rises


[AT&T] Rewards Expiration Notice

Dear Customer,

Your AT&T account currently holds 11,430 reward points scheduled to expire on January 26, 2026.

Recommended redemption methods:

• AT&T Rewards Center: https://shorturl.at/5nsez

Phishing Activity Trends Summary

- Phishing attacks rose 13.8 percent in early 2026, from 853,244 in Q4 2025 to 971,181 in Q1 2026. [pp. 3-4]
- Threat volume increased in Q1 2026 on every social media platform, predominantly in two formats: Scams (27.1 percent of all threats) and Impersonation (43.8 percent of all threats). [pp. 6-8]
- Phishers targeted the Telecom and SaaS/Webmail sectors most frequently. [pp. 4-5]
- The total number of wire transfer BEC attacks observed decreased in Q1 2026. [pp. 9-10]
- Domain registrars NameSilo and NameCheap continued to be the domain registrars used most often by BEC scammers. [p. 12]

Statistical Highlights for the 4th Quarter 2025

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:

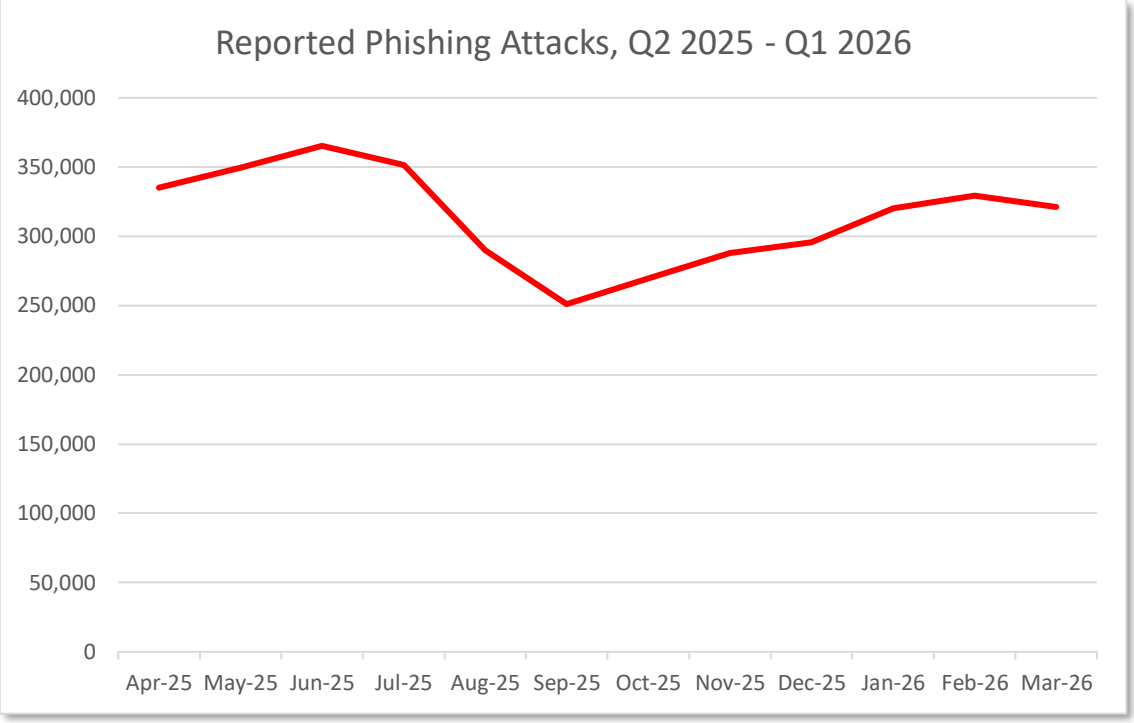
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically 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.
- 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) reported	320,264	329,625	321,292
Unique phishing email campaigns	16,165	14,790	19.790
Number of brands targeted by phishing campaigns	470	475	457

Phishing attacks rose 13.8 percent in early 2026, from 853,244 phishing attacks in the last quarter of 2025 to 971,181 in Q1 2026.

The number of spam campaigns that were reported to APWG dropped dramatically, from 81,710 in Q3 2025 to 45,355 in Q4 2025 to 35,583 in Q1 2026. Email systems are preventing users from forwarding phishing lure emails and sending phishing URLs to APWG and similar organizations, because the mail systems perceive those as harmful. This cuts into the number of successful reports to *reportphishing@apwg.org*, one of APWG's main collection methods.

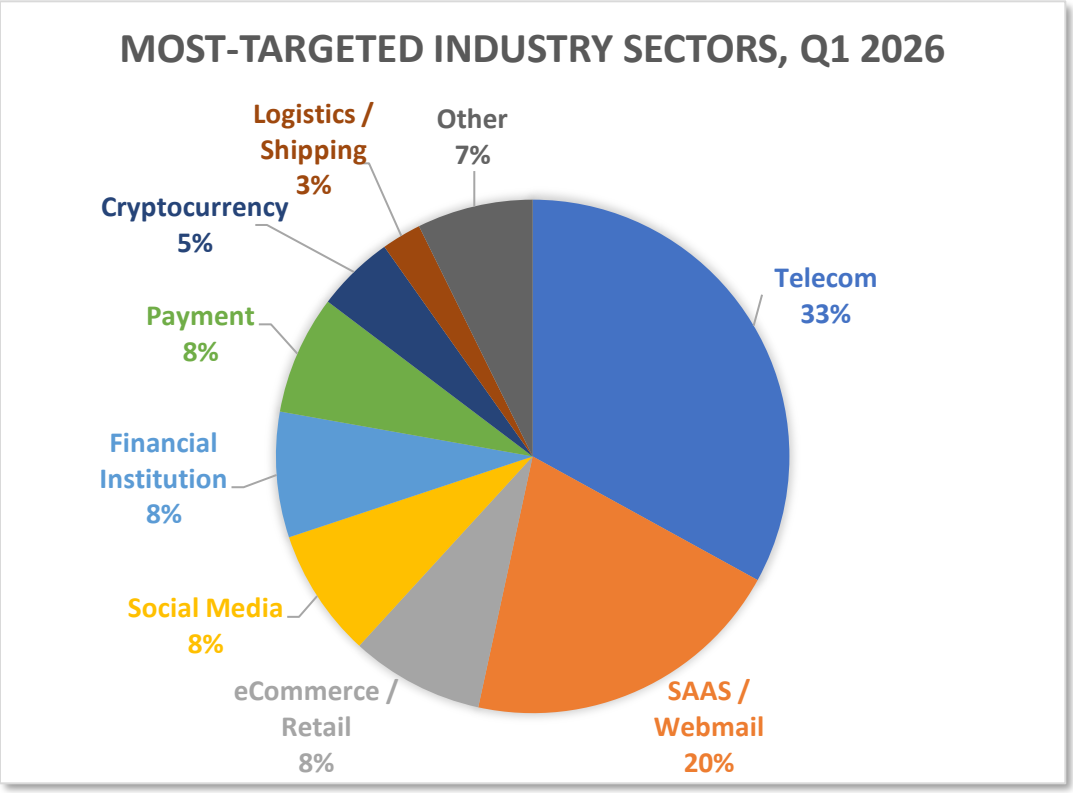
A total of 766 unique brands were identified in the reports across the quarter.



Most-Targeted Industry Sectors

In the first quarter of 2026, APWG founding member Crane Authentication found that the Telecom category was the most-attacked, rising from 5.9 percent of all attacks in Q3 2025 to 33 percent of all attacks in Q1 2026. "We continue to observe the trend where many never-before-phished organizations are now being targeted, particularly within the telecom sector, where URL phishing frequency has increased 75 percent since Q4 2025," said Matthew Harris, Senior Product Manager, Fraud at Crane Authentication. The Social Media and SAAS/Webmail sectors remained notable targets.

Crane Authentication detected a slight decrease in overall URL phishing volumes in Q1 2026 as compared to Q4 2025. However, Crane Authentication found that telephone-based fraud ("vishing" or voice call phishing plus "smishing" or phishing via SMS and text messages) continued to rise, increasing 15 percent from Q4 2025 to Q1 2026.



Crane Authentication noted two recent trends:

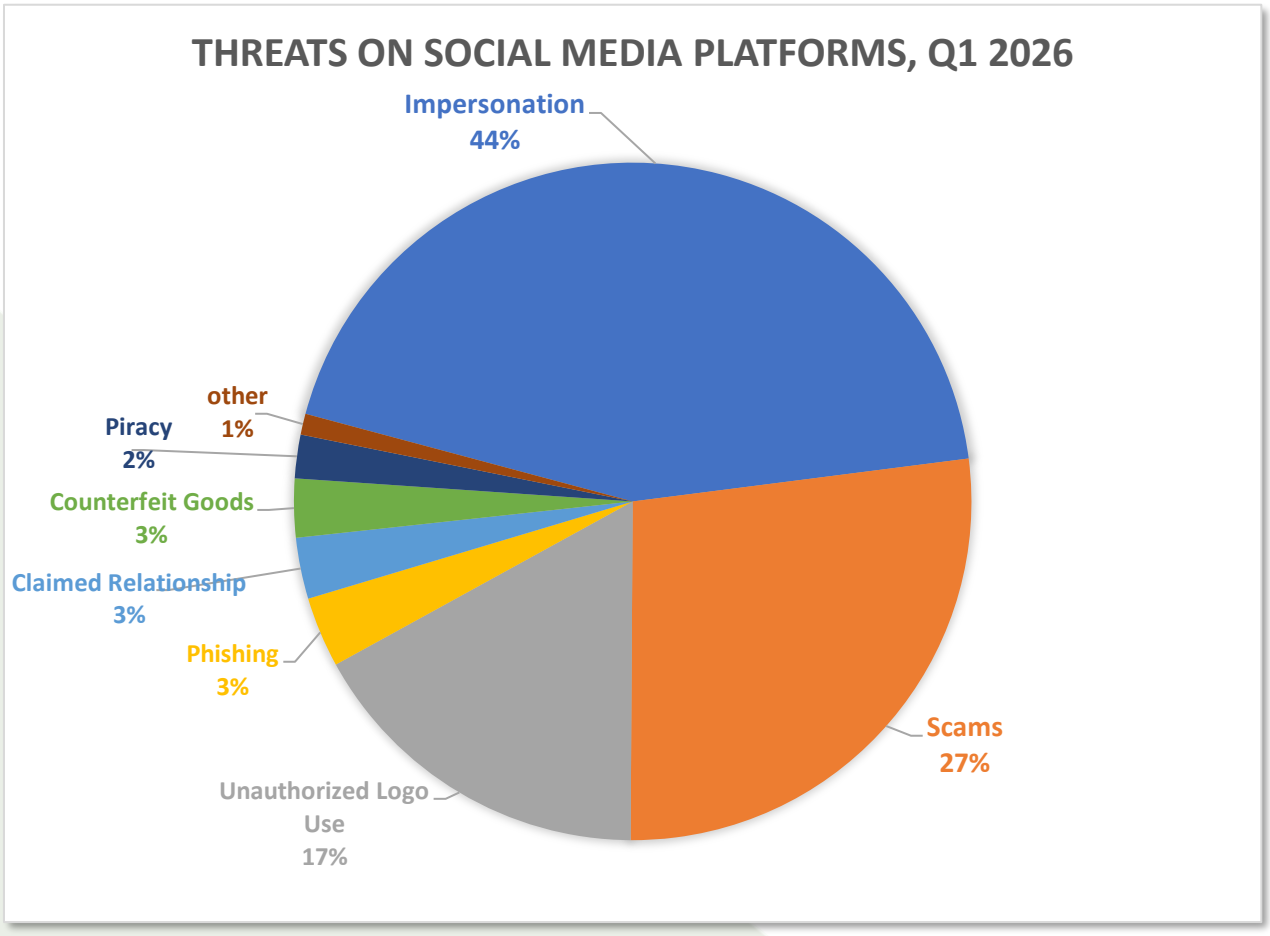
- Fraudsters are continuing to leverage domain registrations to capitalize on current events, such as setting up scam websites that offer U.S. tariff refunds or donations to war-torn areas. Crane Authentication found more than 500 newly registered domains associated with "tariff refund" scam sites in Q1 2026.
- Fraudsters appear to be using more intricate and elaborate methods to hide their scam and phishing sites. Phishers are still employing well-known techniques such as geo/IP blocking and user-agent blocking. But an increasing number of sites only show fraudulent content when the referrer is a certain site or kind of site. For example, the fraud site is only displayed if the user came from the Bing search engine and had searched for "[bank name]bank login", or visited from a certain social media site (i.e. a user clicked on a comment in a Tiktok video). Otherwise, the visitors will see innocuous-looking content, or may be redirected to another site.

Crane Authentication offers expertise and cutting-edge innovations that protect and enhance products, secure identities, and safeguard revenues.

Social Media Threats

APWG member ZeroFox detects and remediates targeted phishing attacks, credential compromises, brand hijacking, and other threats. ZeroFox monitors the entire Internet, the domains space, and major social media platforms for its customers, finding threats that affect organizations, individuals, or assets.

ZeroFox found that threats on social media in early 2026 were predominantly of two types: Scams (27.1 percent of all threats) and Impersonation (43.8 percent of all threats). Impersonation became more prevalent than in the previous quarter. Impersonation is frequently the opening move in a scam campaign, with threat actors establishing a fake identity before advancing to financial fraud. Seen through that lens, the two categories remain deeply intertwined, and their combined 70.9 percent share still represents the core of the threat landscape.

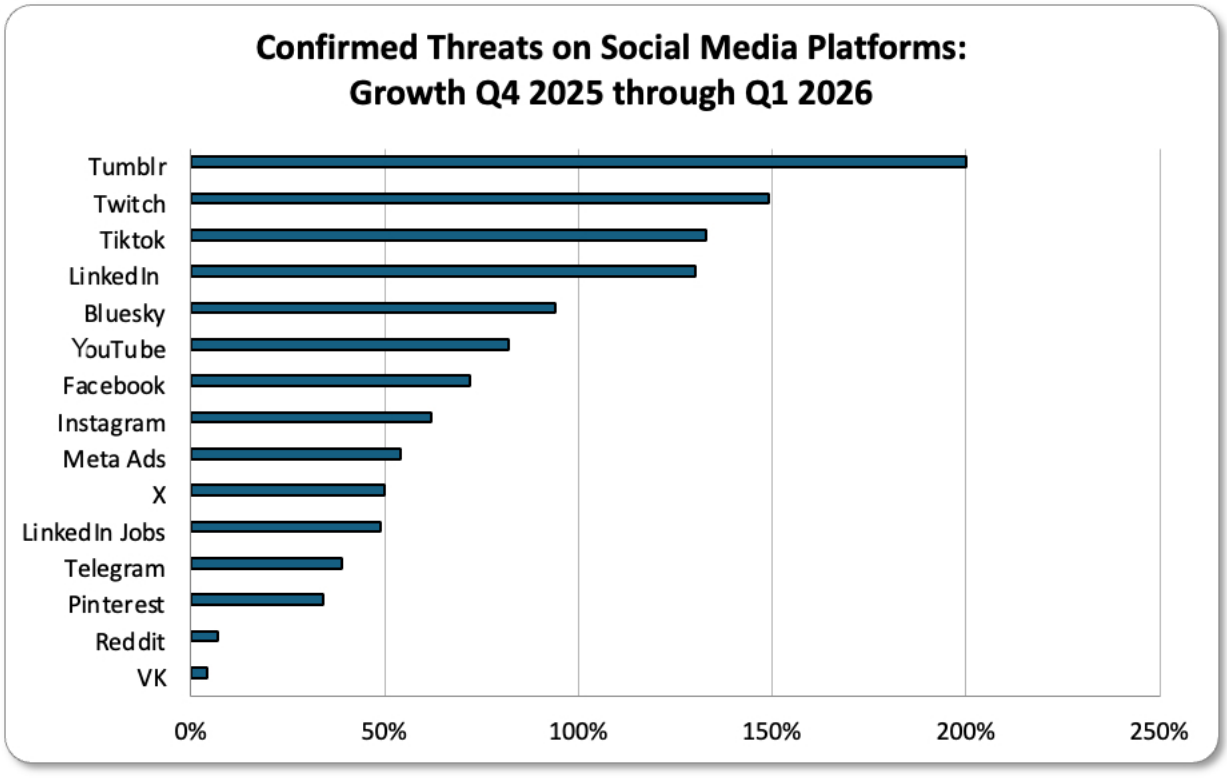


Unauthorized Logo Use nearly doubled its 2025 share from 9.5 percent to 16.9 percent, reinforcing that brand abuse is a growing tool in the same playbook, Other threat categories, including piracy, counterfeit goods, phishing, and physical threats, collectively made up the other 12.2 percent.

Definitions:

- Scams: content uses deceptive tactics to defraud users of money or personal information.
- Impersonation: content falsely claims to be from a real person, brand, or organization.
- Unauthorized logo use: use of an organization's logo by a threat actor posing as that organization, with a malicious purpose.
- Claimed relationship: content falsely claims affiliation or endorsement in order to mislead users.
- Piracy: the practice of downloading and distributing copyright protected content digitally without permission, such as music, movies, or software.
- Other categories: Malvertising, Phishing, Doxxing, Physical threats to employees. unauthorized data disclosures.

During the first quarter of 2026, ZeroFox found that threat volume increased on every social media platform. Threats on Tumblr grew 200 percent, Twitch followed at 149 percent, and Bluesky had 94 percent growth. These platforms had no reported volume in prior quarters. TikTok (133 percent growth) and LinkedIn (130 percent) continued their upward trajectories from 2025.

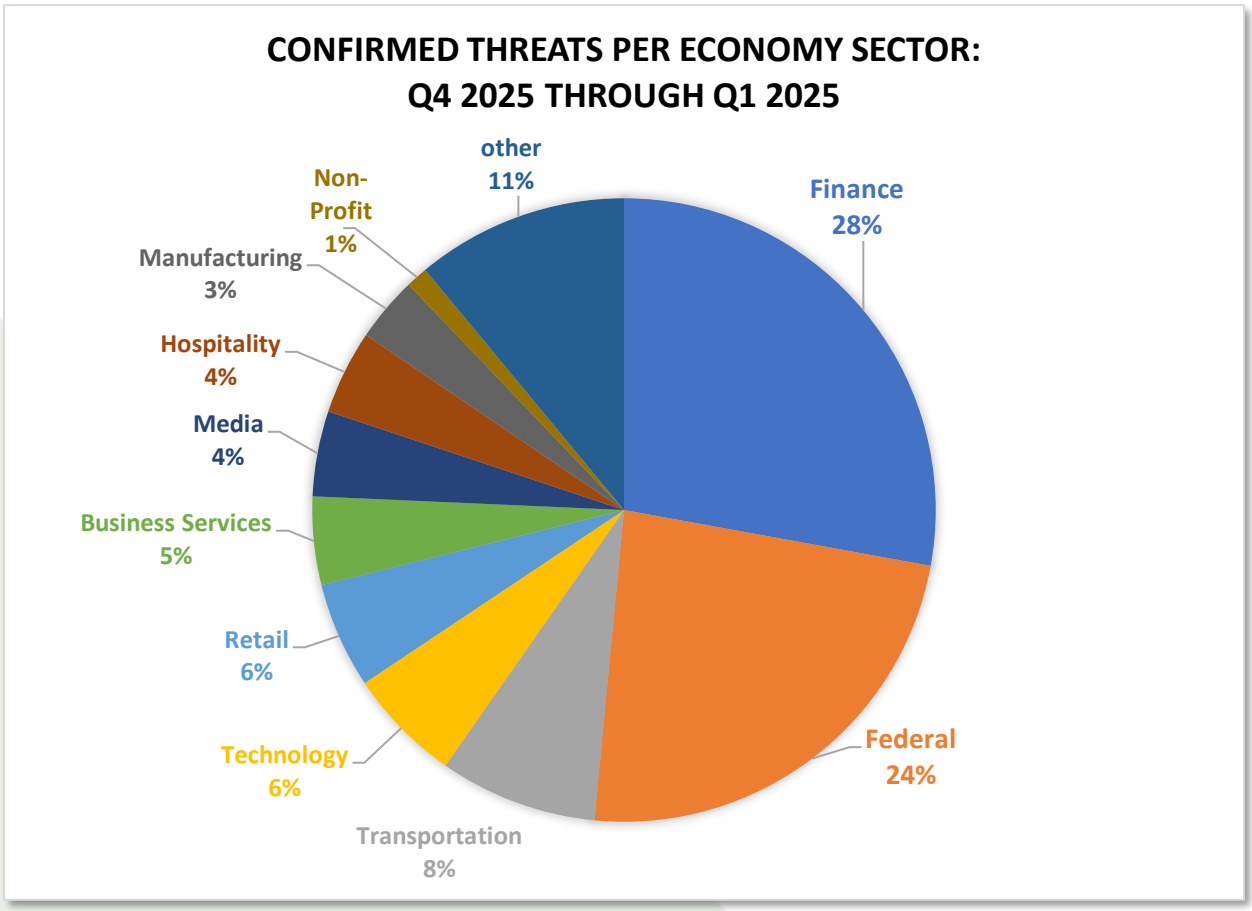


At the other end, Reddit (7 percent) and VK (4 percent) posted the lowest growth rates, though stabilization at any positive number still means the threat volume is growing, just more slowly than before. Note that these are growth rates, not the *number* of incidents that occurred on any of the platforms.

Definitions:

- LinkedIn Jobs: malicious postings in the Job section of LinkedIn, made for purposes such identity theft, fraud, fake job postings, etc. These are separate from user-created posts made elsewhere on LinkedIn.
- Meta Ads: advertisements across all Meta platforms (such as on Facebook and Instagram) that are identified as being malicious. These are separate from posts made on Facebook and Instagram.

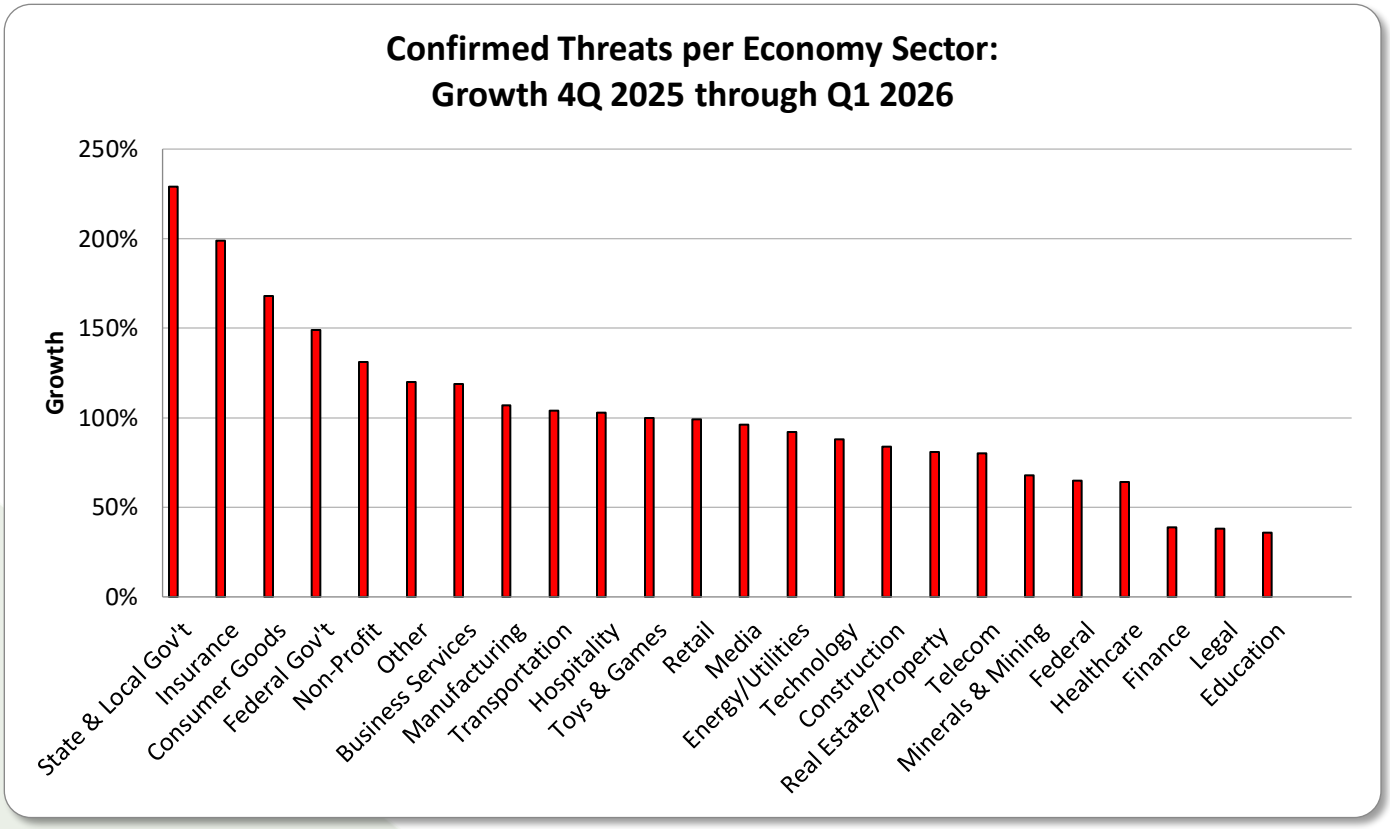
Finance remained the top target, suffering 27.9 percent of all attacks, but that is meaningfully down from 35.5 percent last year. Attacks against the U.S. Federal Government moved up sharply to 23.6percent from 15.7 percent. The biggest drop belonged to Retail, which fell from second place in 2025 at 17.7 percent all the way down to 5.5 percent, likely reflecting a post-holiday shift.



Attack volume rose against all sectors. Some of the industry sectors targeted by threats in Q1 2026 were among the quietest during 2025. Hospitality and Retail, which posted the two lowest average quarterly

growth rates in all of last year at 56 percent and 55 percent respectively, faced 103 percent and 99 percent growth in Q1 2026. Threats to the Non-Profit sector jumped 131 percent.

Threats against State and Local Government grew 229 percent. "This is notable because the Government sector already saw a 950 percent spike from Q2 to Q3 in 2025. This suggests a sustained focus on government institutions rather than a one-time surge," said Carlos Alvarez, Disruption Partnerships Lead at ZeroFox. The Finance sector recorded the second-lowest growth rate in Q1 2026 (39 percent), though it remains by far the largest sector by volume, accounting for 27.9 percent of all confirmed threats.



Analysis of the confirmed threats across 2025 reveals that three sectors—Finance, Retail, and Federal—collectively accounted for nearly 70 percent of all confirmed threats on social media. The Finance sector was the primary target, 35.5 percent of the time, followed by the Retail sector at 17.7 percent, and the Federal sector at 15.7 percent, indicating where threat actors are directing the majority of their attention and resources. Conversely, sectors like Healthcare were rarely targeted.

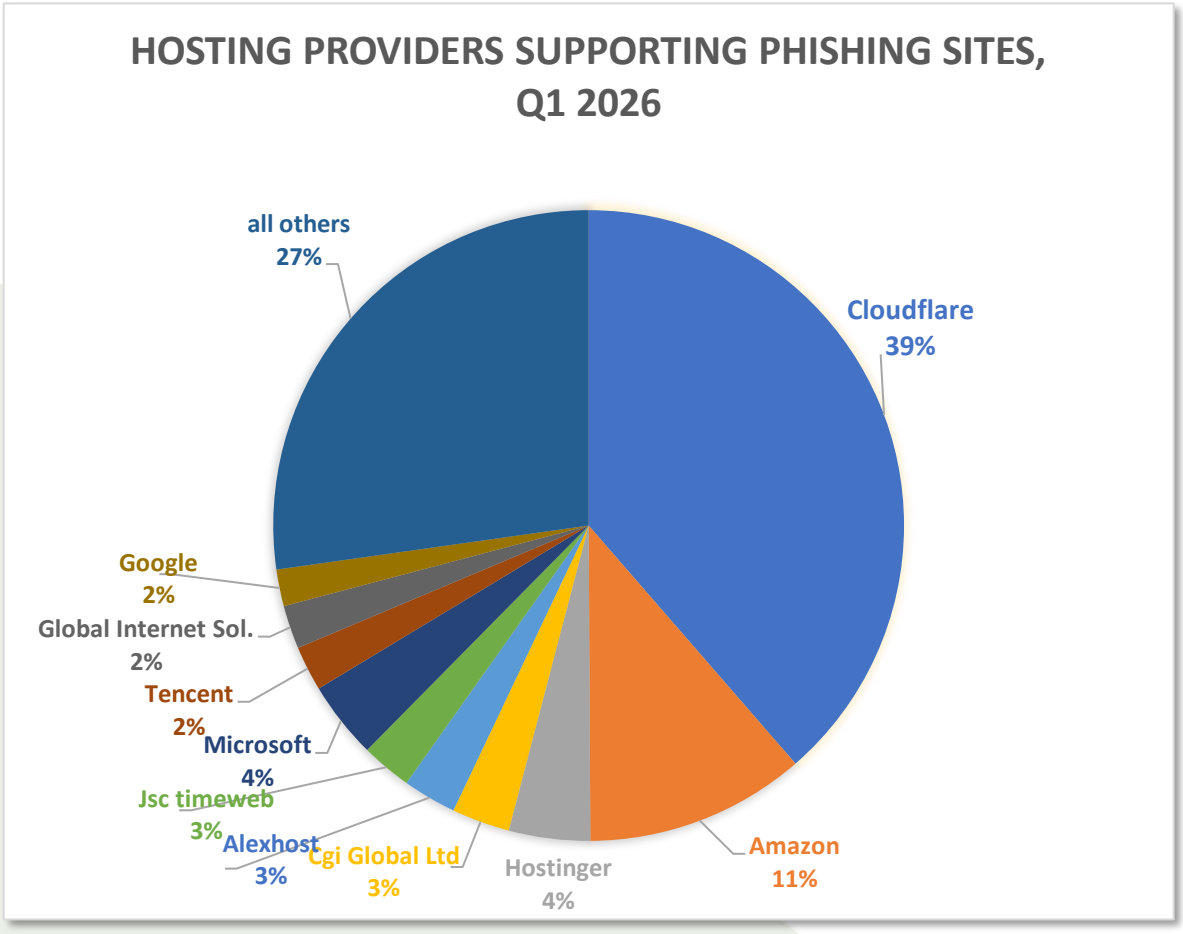
Business e-Mail Compromise (BEC)

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.8 billion dollars in *reported* losses in the U.S. in 2024 according to the

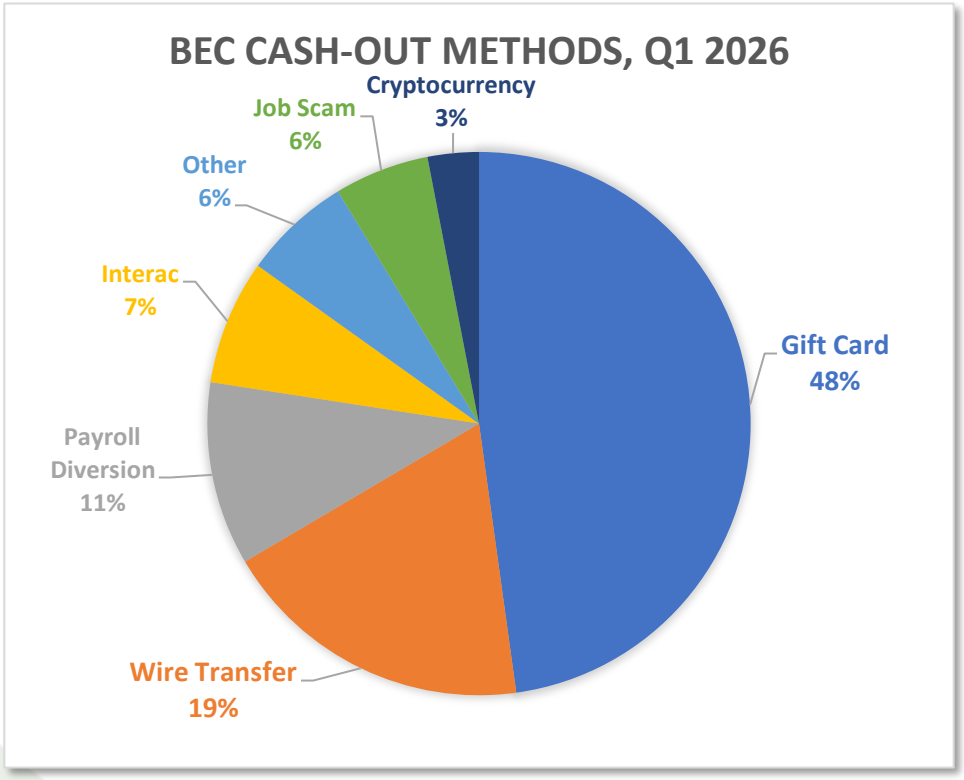
FBI's Internet Crime Complaint Center (IC3). (Many more losses go unreported.) In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q1 2026. 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 Q1 2026 was $42,663, a 15 percent decrease from the prior quarter's average of $50,297. The total number of wire transfer BEC attacks observed by Fortra in Q1 2026 decreased by 25 percent compared to the previous quarter.

Fortra performed many thousands of phishing takedowns for its clients during Q1 2026. Fortra contacted the hosting providers that were hosting the phishing sites, asking that they be disabled. Cloudflare was the most frequently contacted provider: some 39 percent of those phishing sites were using Cloudflare's DNS proxy service, which hides the true hosting location of the sites.

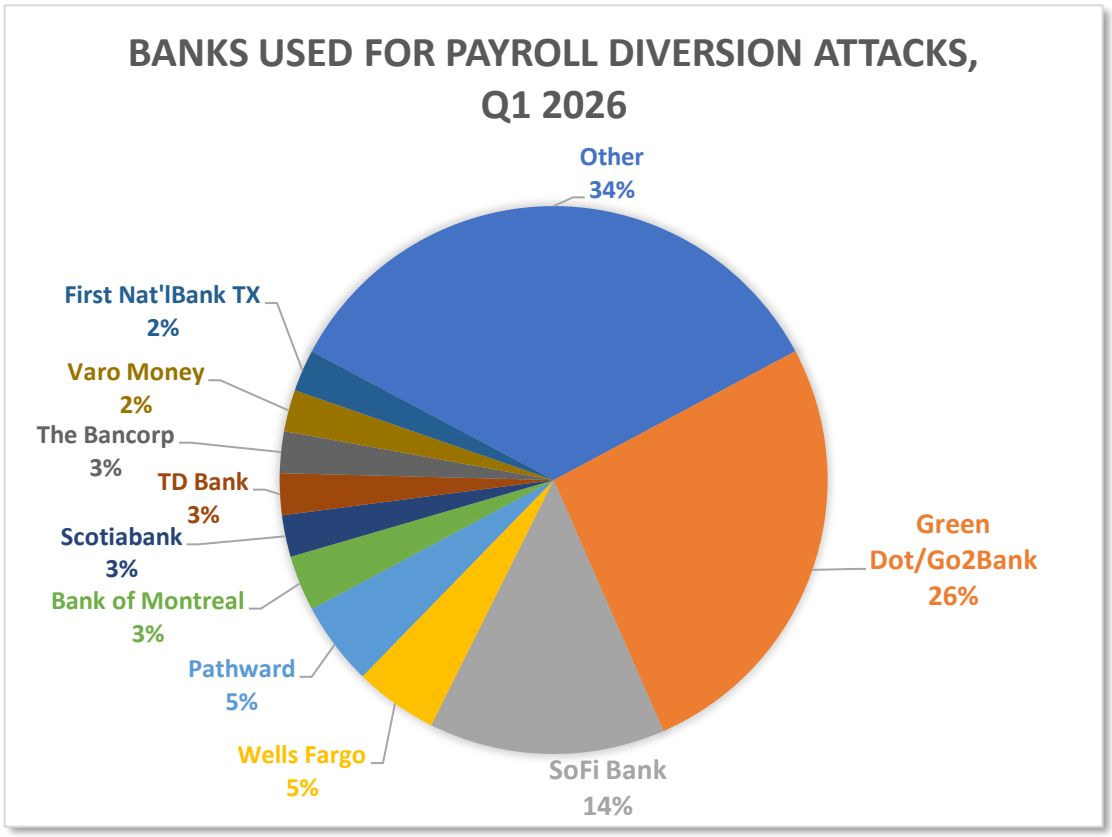


During the first quarter of 2026, gift card scams were once again the most popular scam type, making up 48 percent of the total compared to 19 percent of attackers requesting a wire transfer payment. Interac (7 percent) and payroll diversion (11 percent) were also popular cashout methods in the first quarter of 2026. Compared to the prior quarter, there was a marked shift from gift card scams to wire transfer requests and job scams.

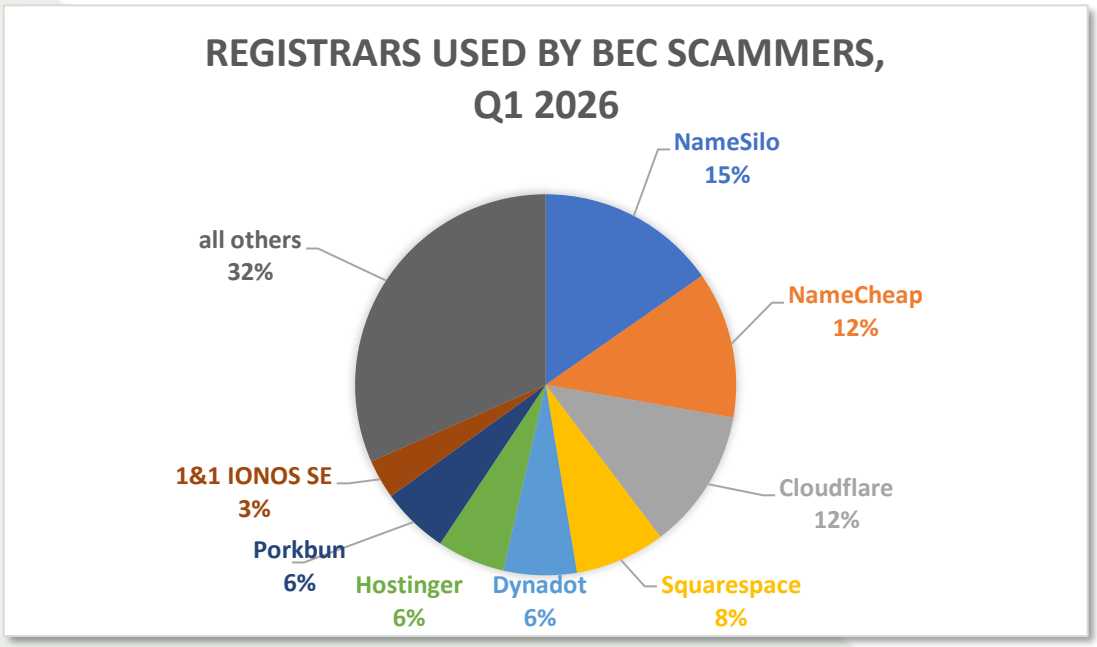


Fortra observed that 72 percent of BEC attacks in Q1 2026 were launched using a free webmail domain. The remaining 28 percent of BEC attacks in Q1 2026 utilized non-webmail domains. Of the free webmail providers, Google's Gmail was used most often, in 53 percent of cases.

Just as in the previous quarter, Green Dot/Go2Bank was the bank of choice for Scripted Sparrow, world's most prolific BEC gang, accounting for 45 percent of the group's mule accounts in Q1 2026. After not even breaking the top 10 in the previous quarter, Column N.A./Mercury rose to become Scripted Sparrow's second-most-popular financial institution in Q1 2026. While Scripted Sparrow may prefer certain banks, no bank is immune. In all, Fortra collected Scripted Sparrow mule accounts at 24 different financial institutions in the first quarter of 2026.



Domain registrars NameSilo and NameCheap continued to be the domain registrars used most often by BEC scammers. Cloudflare's registrar moved into the #3 position.



APWG Phishing Activity Trends Report Contributors

Crane Authentication Crane Authentication is the leading provider of integrated online protection and on-product authentication solutions for brands and governments. www.craneauthentication.com/	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	ZEROFOX ZeroFox provides cyber + physical threat intelligence to discover, validate, and disrupt threats, neutralizing adversaries before they harm brands, domains, people, and assets. www.zerofox.com

 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 of Crane Authentication (stefanie.wood@craneauthentication.com); Jessica Ryan of Fortra (Agari and PhishLabs) (jessica.ryan@fortra.com); and Carlos Alvarez of ZeroFox (caalvarez@zerofox.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 and curator of the eCrime eXchange, the apex clearinghouse for cybercrime event data; the STOP. THINK. CONNECT. Messaging Convention, Inc., a US-based non-profit 501(c)3 corporation; and APWG Applied Research 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's clearinghouse for cybercrime-related data sends 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.

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, published (IEEE Digital Xplore since 2008) conference dedicated exclusively to cybercrime studies. Join as eCrime 2026 ushers in our third decade in publication. Contact ecrime2026@apwg.org for more details on participation and sponsorship.