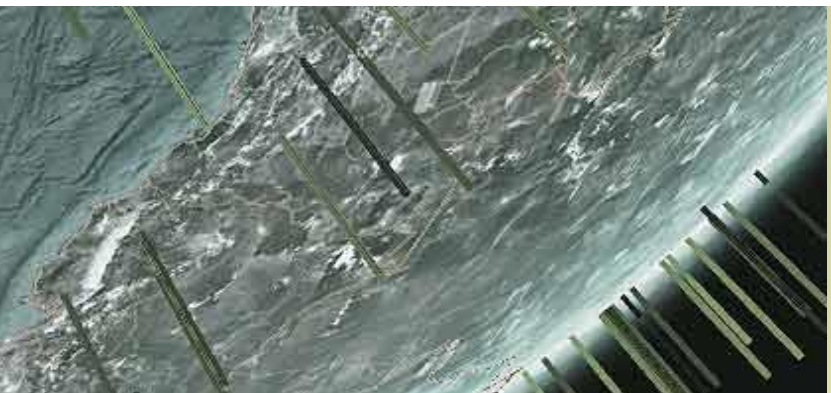
Phishing Activity Trends Report

2nd Quarter 2026

APWG

Unifying the
Global Response
To Cybercrime



Activity April-June 2026

Published 28 August 2026

Phishing Report Scope

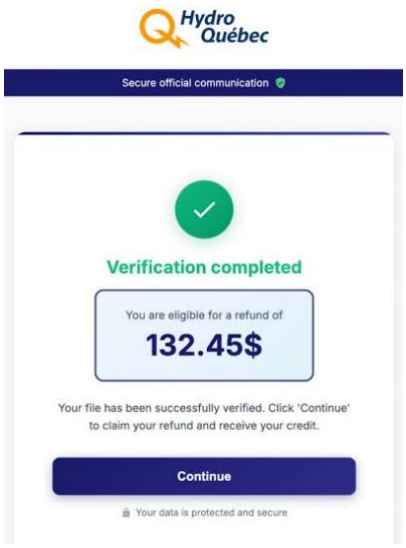
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@apwg.org. APWG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

Scams Increase Across Phone, Email, and Social Media in Q2 2026



Phishing Activity Trends Summary

- Phishing attacks rose 10.1 percent in Q2 2026. APWG tallied 425,808 attacks in June 2026, which was the highest monthly total since April 2023. [p. 3]
- Threat volume increased significantly on social media platforms, demonstrating that bad actors are weaponizing paid advertising infrastructure to reach victims at scale. [pp. 9-10]
- Telephone-based fraud continued to rise, with "smishing" (phishing via SMS and text messages) increasing by 40% from Q1 to Q2 2026. [p. 4]
- The number of wire-transfer BEC attacks increased 88%, and the amount of money fraudsters attempted to steal in those attacks was up 45% to $61,732 per attempt. [p. 6]

Statistical Highlights for the 2nd Quarter 2026

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.

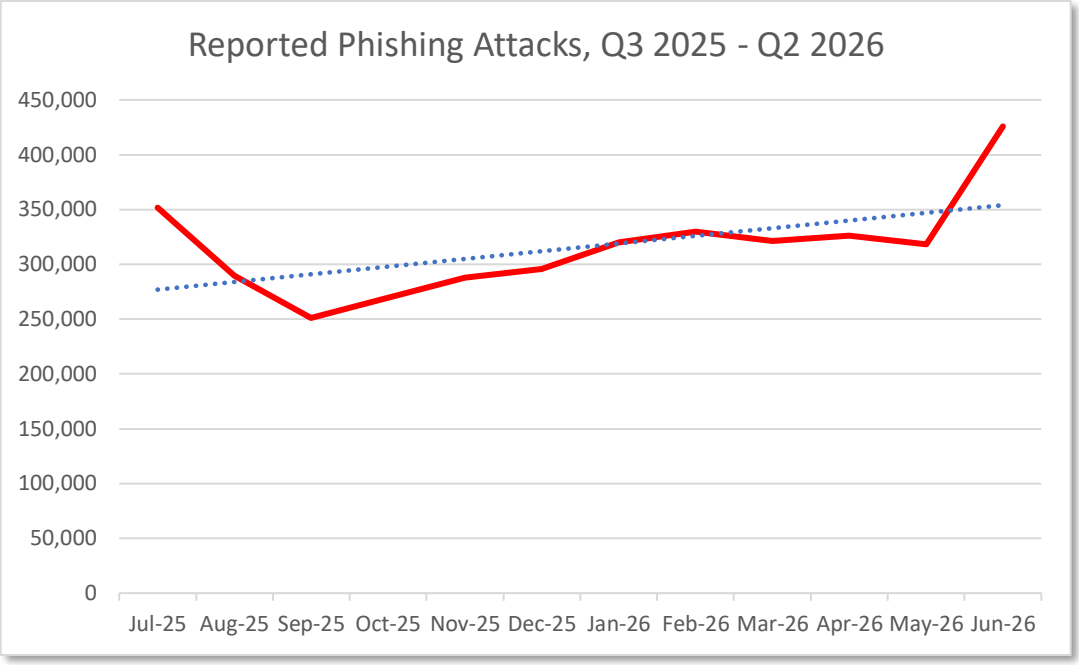
The APWG tracks:

- **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.

	April	May	June
Number of unique phishing Web sites (attacks) reported	325,934	317,940	425,808
Unique phishing email campaigns	18,666	20,129	45,156
Number of brands targeted by phishing campaigns	467	512	552

Phishing attacks rose 10.1 percent, from 971,181 in Q1 to 1,069,681 in Q2. That was the highest quarterly total APWG has observed since Q3 2025. There were 425,808 attacks recorded in June 2026, which was the highest monthly total since April 2023, when APWG tallied 597,789 attacks.

The number of phising email spam campaigns that were reported to APWG rebounded in Q2 2026. It dropped dramatically from 81,710 in Q3 2025 to 35,583 in Q1 2026, but recovered to 83,951 in Q2 2026. Email systems are sometimes preventing users from forwarding phishing lure emails and sending phishing URLs to APWG and similar organizations, because the mail systems perceive those emails as harmful. This can impact the number of successful reports to *reportphishing@apwg.org*, one of APWG's main collection methods.



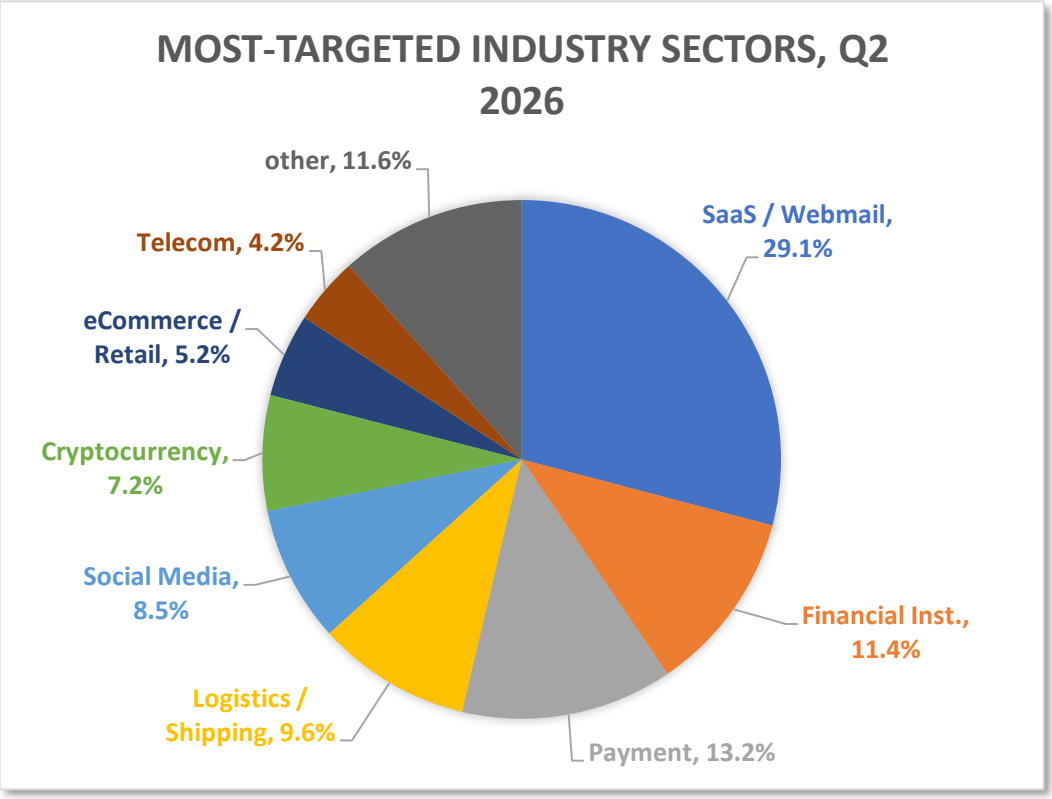
A total of 941 unique brands were identified in the reports across the quarter. Half of them were attacked five times or less. Phishers attack a diverse set of targets, and continue to create phishing page templates for attacking lesser-known and regional targets.

Most-Targeted Industry Sectors

In the second quarter of 2026, APWG founding member Crane Authentication found that the SaaS / Webmail category was the most-attacked, rising from 20 percent of all phishing attacks in Q1 2026 to 29.1 percent of all attacks in Q2.

The Telecom sector was #1 in Q1 with 33 percent of all phishing, but fell to 4.2 percent in Q2. "There scammers are most likely pivoting to other targets that offer webmail," said Matthew Harris, Secior product Manager, Fraud at Crane Authentication. "And we continue to observe a trend where many never-before-phished organizations are now being targeted, particularly within the telecom sector, where multiple communication services—voice, Internet, and email—can be purchased from a single company, which is an attractive account takeover scenario for phishers.

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 continued to rise. "Vishing" (voice call phishing) hit highs and increased by 20 percent, and "smishing" (phishing via SMS and text messages) increased by 40 percent from Q1 to Q2 2026.



Crane Authentication also noted, possibly as a reflection of the current job market or the broader health of the economy, that it is seeing an increasing volume of email- and social media-based job scams, where recruiters and their companies are being impersonated in order to gain the trust of job seekers.

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

Business e-Mail Compromise (BEC)

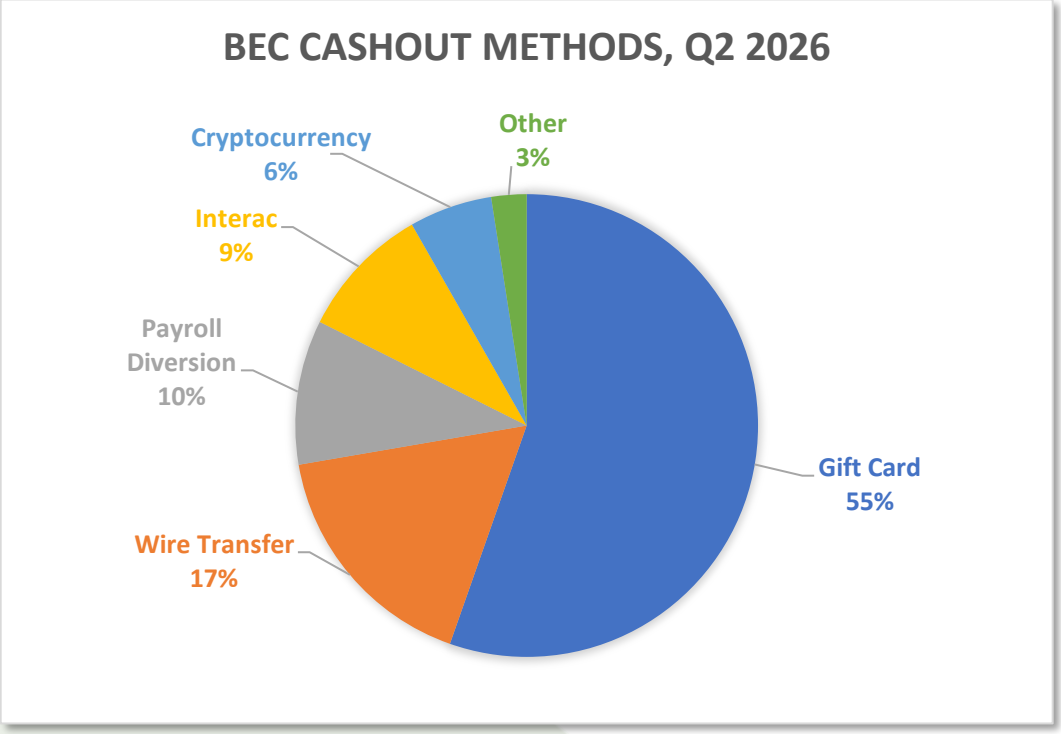
APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for more than $3 billion dollars in *reported* losses in the U.S. in 2025 according to the FBI's Internet Crime Complaint Center (IC3). (Many more losses go unreported.) In a BEC 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 Q2 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 Q2 2026 was $61,732, a 45 percent increase from the prior quarter's average of $42,663. The total number of wire transfer BEC

attacks observed by Fortra in Q2 2026 increased by 88 percent over the previous quarter. Much of this increase was driven by the BEC threat group known as Scripted Sparrow, a prolific BEC gang based in Nigeria, South Africa, and Türkiye.

"Scripted Sparrow continues to be the dominant BEC threat group on the planet," said John Wilson, Senior Fellow, Threat Research at Fortra. "Scripted Sparrow utilizies fake executive coaching invoices and a spoofed reply chain between the coaching firm and a company executive to lend credibility to their scheme." The gang controls a vast network of mule accounts, most of which are held at banks in the United States. Fortra's research suggests that the gang has numerous money mules based in the United States and Canada.

During the second quarter of 2026, gift card scams were once again the most popular BEC scam transaction type, making up 54 percent of scams, with 17 percent of attackers requesting a wire transfer payment:

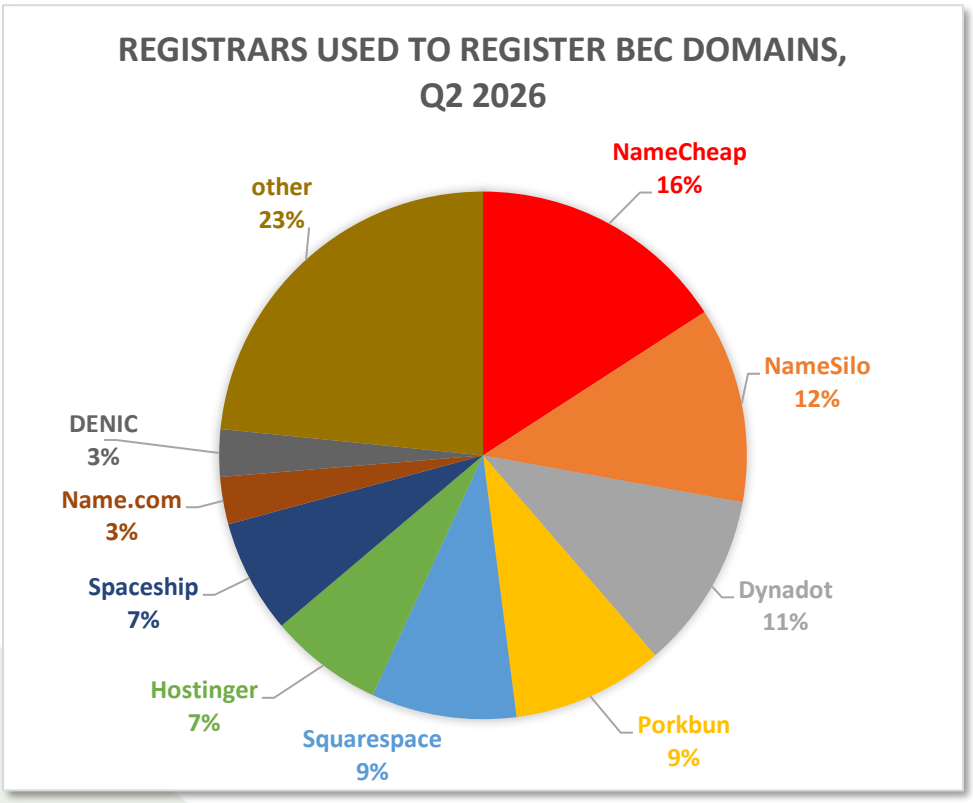


Payroll Diversion scams made up 10 percent of the email-based scams Forta saw targeting businesses, while 9 percent of the observed were French-language attempts to trick renters into paying their monthly rent using the Canadian payment service Interac.

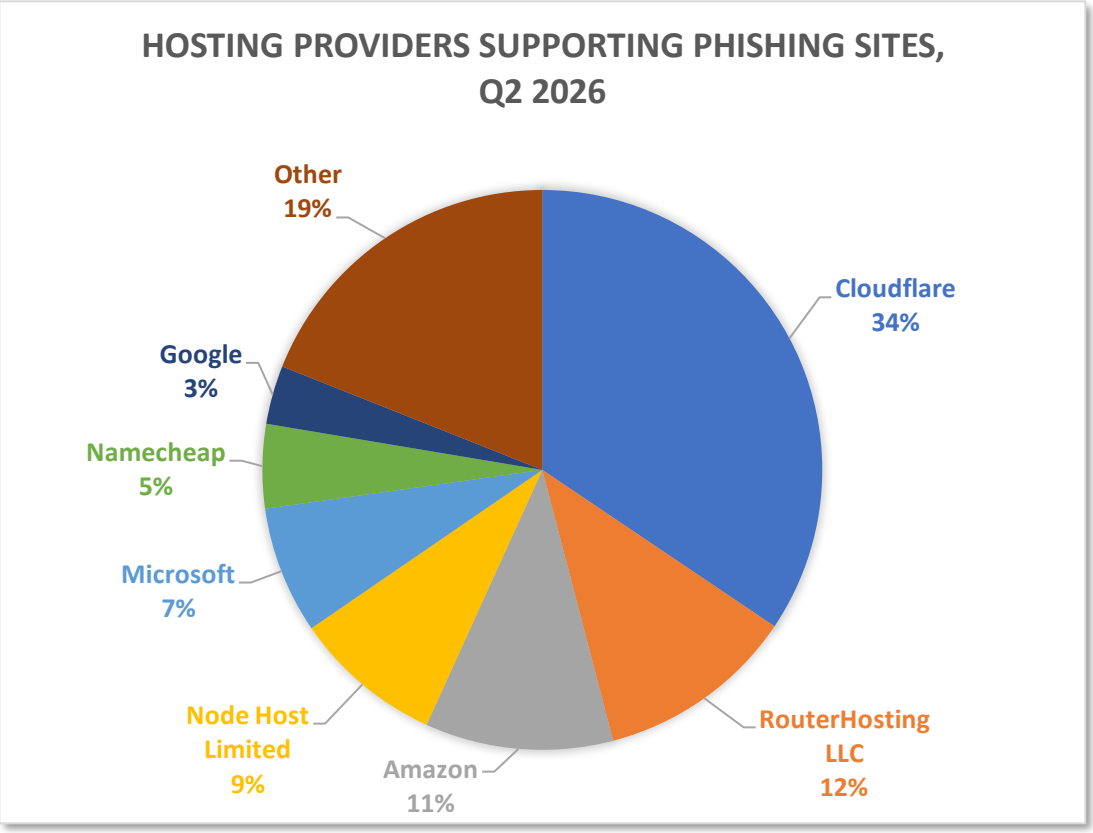
Wilson also notes that "Fortra noted an uptick two-step phishing, where the phisher first sends an email with what appears to be a legitimate business inquiry. If the victim replies, the phisher follows up with a message containing a phishing link."

Fortra also observed a significant increase in scammers swapping the sender's display name and the Subject line of emails, presumably to get around email filters that look for executives' names in the Sender display name.

Domain registrar NameCheap was used most often by BEC attackers to register domains names to carry out their schemes, followed by NameSilo and Dynadot:



Cloudflare's proxy hosting service remained popular with phishers. It was followed by RouterHosting, a virtual private server provider linked to the Dubai-based firm Cloudzy. Some of the phishing at RouterHosting attacked Canadian citizens, impersonating entities such as utility Hydro-Québec and the Government of British Columbia.

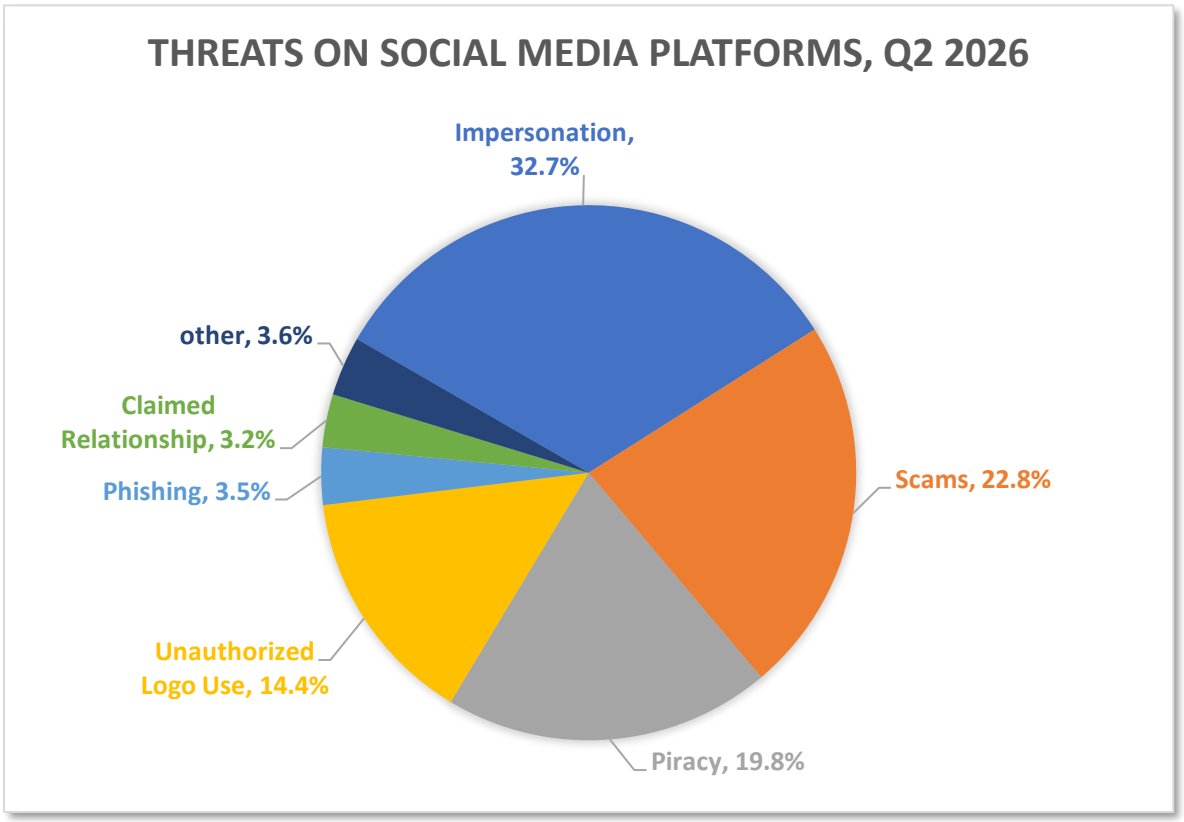


Social Media Threats

APWG member ZeroFox detects and remediates targeted phishing attacks, credential compromises, brand hijacking, and other threats. ZeroFox monitors the entire Internet, the domain 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 Q2 2026 were predominantly of two types: Scams (22.7 percent of all threats) and Impersonation (32.7 percent of all threats). Impersonation became more prevalent than in Q1. Impersonation is frequently the opening move in a scam campaign, in which a threat actor establishes a fake identity before advancing to financial fraud. Seen through that lens, the two categories remain deeply intertwined.

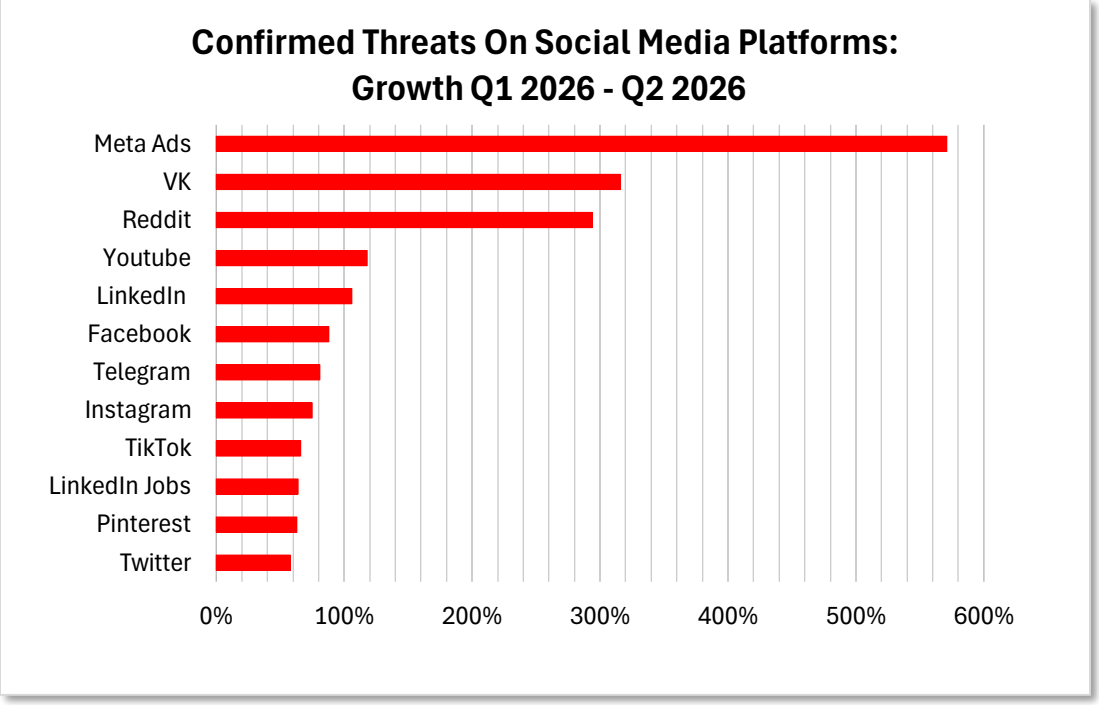
Piracy held a notable 19.8 percent share. The persistence of unauthorized logo use at 14.4 percent reflects an ongoing type of brand abuse that falls below the threshold of traditional phishing but still causes material harm to targeted organizations. Phishing itself represented 3.5 percent of total detected volume, a figure that likely reflects the continued migration of adversarial tactics toward social engineering and impersonation-based approaches rather than conventional credential harvesting.



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.

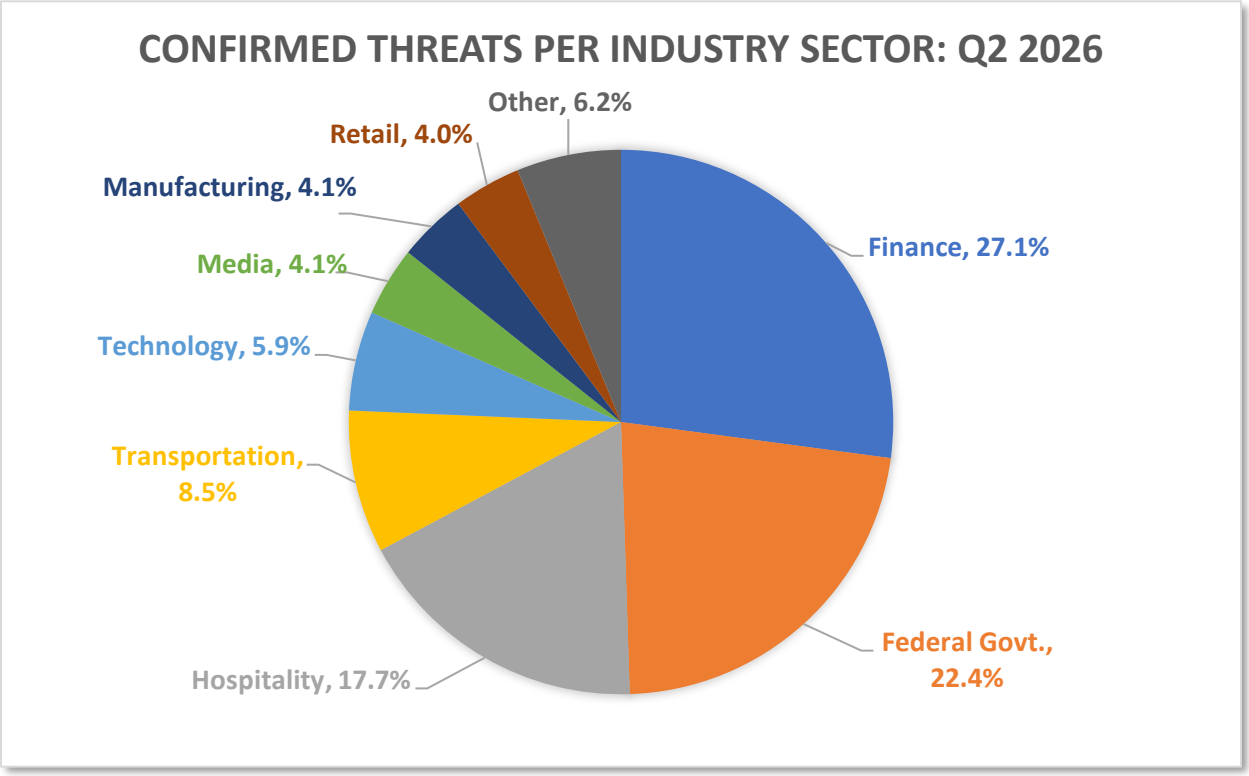
During the second quarter of 2026, ZeroFox found that threat volume increased on social media platforms. The most striking result was a 571 percent surge in threat activity across Meta Ads from Q1 to Q2, suggesting that bad actors are increasingly weaponizing paid advertising infrastructure to reach victims at scale. VK (316%) and Reddit (294%) also saw sharp increases, indicating broadening adversary interest in platforms with less mature abuse reporting ecosystems. There were also significant quarter-to-quarter increases on platforms including YouTube (118%), LinkedIn (106%), and Facebook (88%). This illustrates that threat actors continue to diversify their delivery across the full social media landscape rather than concentrating on any single channel.



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.

The Finance sector remained the most targeted sector in Q2 2026 at 27.1 percent, consistent with its historical position as the primary target for online fraud and impersonation. Federal entities accounted for 22.4 percent of attacks, and hospitality's 17.7 percent share reflects its emergence as a significant target in this reporting period. Together, these three sectors accounted for more than two-thirds of all observed threat activity. The long tail of remaining sectors, with technology at 5.91 percent and retail at 3.99 percent, illustrates that while threat concentration favors a small number of high-value verticals, no sector is exempt from sustained targeting.



State and local government entities experienced the sharpest quarter-over-quarter increase in attacks at 889 percent, a figure that warrants close attention as the 2026 U.S. federal midterm elections take place through the autumn. Hospitality followed at 462 percent, likely driven by seasonal travel patterns that make this sector an attractive target for impersonation and scam campaigns. The 224 percent increase against federal government entities, combined with the state and local surge, points to a broader pattern of adversary focus on government-adjacent infrastructure. Non-profit organizations (194%) and telecommunications providers (168%) round out the sectors showing the most attack growth.

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 (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; the annual Symposium on Electronic Crime Research; 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 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 – and to inform the research and experiments of leading industrial laboratories and university research centers 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