

APWG Report: Cybercrime Gangs' Command of Internet-Enabled Media Increases in Q2 2026

In Q2,, APWG found phishing attacks and frauds continued to increase, with criminals menacing victims using email, phone, message services, and social media.

CAMBRIDGE, MA, UNITED STATES, September 2, 2026 /EINPresswire.com/ -- The APWG's new [Phishing](#) Activity Trends Report rounds up phishing and fraud activity that took place in the second quarter of 2026. Phishing attacks rose, and the volume of scams and frauds continued to increase, with criminals menacing increasing numbers of users worldwide via users email, phone, message services, and social media.



Reported Phishing Attacks, Q3 2025 - Q2 2026

“

According to APWG, phishing attacks rose 10%, from 971,181 in Q1 2026 to 1,069,681 in Q2 2026. APWG tallied 425,808 attacks in June 2026, which was the highest monthly total since April 2023.”

APWG

According to data reported to the APWG, phishing attacks rose 10%, from 971,181 in Q1 2026 to 1,069,681 in Q2 2026. APWG tallied 425,808 attacks in June 2026, which was the highest monthly total since April 2023.

During the second quarter of 2026, APWG contributing member ZeroFox found that most threats spread on social media platforms were various forms of fraud. Almost 33 percent of all threats were classified as Impersonation—a fraud attempt that falsely claims to be a communication or offer from a real person, brand, or organization.

Scams accounted for almost 23 percent of threats—these are other kinds of content that uses deceptive tactics to defraud users of money or personal information. Phishing specifically (a web site spoofing a known brand in order to steal a victim's credentials) was another 3.5 percent of

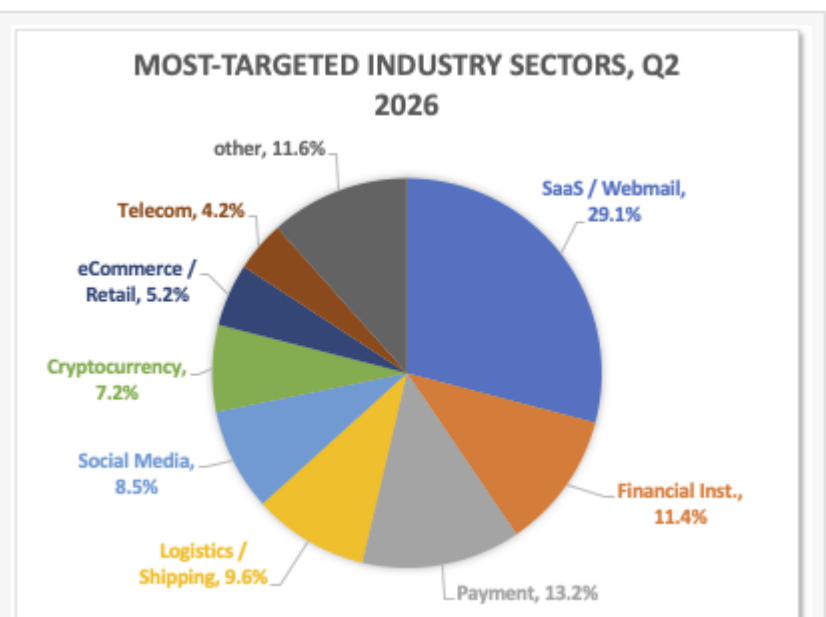
threats. APWG member ZeroFox found that the growth rates of these types of threats on social media platforms continues to grow, doubling on a number of platforms from Q1 2026 to Q2 2026.

“Business e-mail compromise” or BEC attacks were more frequent and more costly in early 2026. APWG contributing member 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 Q1 2026.

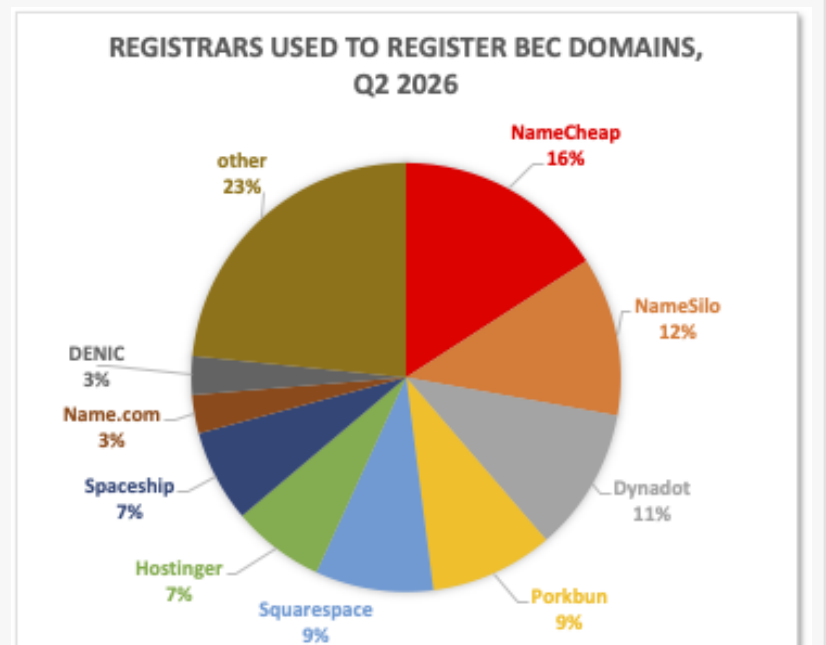
John Wilson, Senior Fellow, Threat Research at Fortra, noted an increased use of a sophisticated phishing technique. “We saw an uptick two-step phishing, where the phisher first sends an email with what appears to be a legitimate business inquiry. If the victim replies, the phisher follows up with a message containing a phishing link.” The initial phishing emails slip past some email filters more easily than typical phishing emails, and help lull potential victims into a false sense of security.

In the first quarter of 2026, APWG founding member Crane Authentication found that the SaaS / Webmail category was the most-attacked, totaling 29.1 percent all attacks in Q1 2026. Crane Authentication found that telephone-based fraud continued to rise. Crane Authentication found that “vishing” (voice call phishing) hit highs and increased by 20%, and “smishing” (phishing via SMS and text messages) increased by 40% from Q1 to Q2 2026. The full text of the report is available here:

https://docs.apwg.org/reports/apwg_trends_report_q2_2026.pdf



MOST-TARGETED INDUSTRY SECTORS, Q2 2026



REGISTRARS USED TO REGISTER BEC DOMAINS, Q2 2026

APWG members and research collaborators from around the world will be meeting in November in Lisbon to consider civilization-wide responses to [cybercrime](#) during their annual APWG [eCrime](#) conference. This year's theme is "Cybercrime's Demise Imagined":

<https://apwg.org/events/ecrime2026>

The 2026 Symposium on Electronic Crime Research (eCrime 2026) in Lisbon examines essential factors for managing the impacts of the global cybercrime plexus to secure IT users, commercial enterprises, governments, national infrastructures, and operational technologies. eCrime 2026 on November 2-6 will be the 21st annual peer-reviewed, publishing symposium hosted by APWG:

<https://apwg.org/events/ecrime2026>

APWG eCrime 2026 Lisboa is a uniquely constructed symposium designed to to examine responses to cybercrime as well as to showcase the very latest research into counter-cybercrime techniques and technologies. As the only peer-reviewed, publishing research conference focused exclusively on cybercrime, APWG eCrime is also the most important venue for discovering those path-finding, thought-leading managers and investigators whom your organization has yet to hire - and needs to meet: <https://apwg.org/events/ecrime2026>

The APWG Phishing Activity Trends Report is published by and is copyright © the APWG. For info about the APWG, please contact info@apwg.org. 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

Peter Cassidy
Anti-Phishing Working Group
+1 617 669 1123
[email us here](#)

Visit us on social media:

[LinkedIn](#)
[Facebook](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/938908615>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.