

eCrime Workshops Build Capacity for Adversary Analysis, Threat Modeling, Infrastructure Investigation & Data Exchange

APWG eCrime 2026 Offers Four Workshops for Cybersecurity Professionals and Researchers Focused on Counter-Cybercrime Investigations and Operations

CAMBRIDGE, MA, UNITED STATES, October 2, 2026 /EINPresswire.com/ -- APWG [eCrime 2026](#) conference week

will open with a counter-cybercrime Training Day on November 2, featuring four expert-led sessions focused on adversary analysis, threat modeling, phishing infrastructure investigation, and cybercrime-data integration. Scheduled on Monday from noon to 5:30 p.m., the program will give researchers, investigators, developers, and security professionals practical methods they can apply to their own forensic systems, investigations, intelligence operations, and security routines.

“

Workshops will focus on identifying system vulnerabilities, discovering connected malicious assets, and distributing evidence in ways that make coordination easier.”

Dr Miranda Bruce

The eCrime 2026 training sessions offer rare insights to the counter-cybercrime operations community, connecting four capabilities that are too often treated separately: anticipating adversary behavior, designing resilient systems, expanding individual threat reports into infrastructure-level investigations, and exchanging actionable intelligence through shared technical platforms.

"The workshops will help bridge the gap between collecting threat intel on individual actors, and then knowing what to do about it," says eCrime Publications Chair and Training Day director Dr Miranda Bruce.

"Specifically, the workshops will focus on identifying system vulnerabilities, discovering connected malicious assets, and distributing evidence in ways that make coordination easier. All of which are essential for APWG's bigger goal of linking researchers, financial institutions,



technology companies, infrastructure providers, governments, and law enforcement in a collective response to cybercrime,” Dr. Bruce concluded.

Combining analytical frameworks with hands-on investigation and interoperable data exchange, the program reinforces APWG’s enduring contribution: turning dispersed observations into shared knowledge and shared knowledge into faster, more coordinated operational action thereby unifying the global response to cybercrime.

Pete Herzog, co-founder of ISECOM, will lead “Modeling Adversaries Through Chaos,” a three-hour introduction to the Adversarial Analysis Model. Unlike conventional kill-chain approaches that concentrate on what an attacker has already done, this state-based framework helps analysts assess what an adversary may be positioned to do next. Participants will examine behavioral states through multiple observational perspectives and learn four analytical operations—Mirror, Twin, Opposite, and Lever—for anticipating, redirecting, or disrupting adversarial activity. A live case involving an anonymized phishing operator will be followed by hands-on participant exercises.

Laurin Weissinger of the University of California, Berkeley will present an interactive threat-modeling workshop. Beginning with an introduction to threat-modeling terminology, processes, and approaches, the session will move into small-group exercises in which participants identify threats to a sample system, evaluate their significance, and develop possible mitigations. The workshop will conclude with a review of each group’s findings and a discussion of how threat modeling relates to risk analysis, assessment, evaluation, and treatment.

Sven Krohlas of Spamhaus will lead “Amplify the Signal: Investigating Phishing Campaigns Through Domain Clustering.” This practical session will demonstrate how a single verified phishing report can reveal related malicious domains, hosting infrastructure, and rogue networks. Participants will explore passive DNS techniques and real-world phishing examples while learning how threat intelligence can move among service providers, registries, registrars, security vendors, governments, and law-enforcement agencies. The session will emphasize how shared indicators can support coordinated disruption, sometimes protecting users even before formal takedowns occur.

Carlos Ramirez of APWG Engineering will present “Practical API Integration: Connecting Applications to the eCrimex eXchange Data Clearinghouse.” Designed for developers, analysts, and technical researchers, the workshop will explain eCrimex API authentication, endpoints, methods, queries, and response formats. Participants will make test calls using tools such as Postman or cURL and review example workflows for retrieving and submitting cybercrime information. The session will also address common integration pitfalls and practices for efficient, reliable API use.

Together, these four sessions reflect APWG’s commitment to strengthening the global response to cybercrime through rigorous analysis, practical training, trusted data exchange, and

collaboration across research, industry, government, and law enforcement.

Aimee Larsen Kirkpatrick

APWG

+1 808-282-9850

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/946749222>

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.