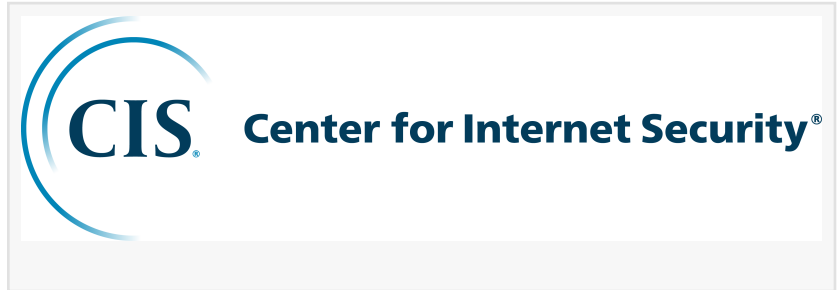


Center for Internet Security Report Warns of Illicit Betting, Fraud and Athlete Safety Risks During FIFA World Cup 2026

Report highlights increasing match integrity threats, online fraud and coercion tied to global sporting events



CLIFTON PARK, NY, UNITED STATES,
June 23, 2026 /EINPresswire.com/ --
The Center for Internet Security, Inc.®
(CIS®), in collaboration with Wein

Strategy Lab, today released a [new report](#) examining the growing risks associated with illicit sports betting, match manipulation, fraud, and athlete safety during FIFA World Cup 2026 and other upcoming large sporting events.

“

Large-scale sporting events like the World Cup attract not only fans, but also criminal actors looking to exploit the excitement surrounding the tournament.”

*John Cohen, Executive
Director, Strategic Programs
and Initiatives at CIS*

The report, *Illicit Sports Betting and Match Integrity Risks Related to Large-Scale Events*, outlines how mega sporting events create expanded opportunities for cybercriminals, organized crime networks, and fraud actors seeking to exploit heightened public interest, betting activity, and cross-border financial flows.

The paper warns that FIFA World Cup 2026, which is expected to attract millions of international visitors and billions of viewers worldwide, is a significant target for online scams, money laundering, betting manipulation, and coercion campaigns directed at athletes and officials.

The report identifies four primary fraud typologies associated with the tournament and the rapidly growing sports betting ecosystem:

- Social media scams promoting counterfeit gambling, ticketing, and investment platforms
- Unregulated prediction pools and gambling sites operating without oversight or consumer protection
- Insider tip schemes falsely claiming access to manipulated match outcomes or privileged

betting information

- Money laundering operations leveraging sports betting markets and digital payment systems to conceal illicit funds

It also raises concerns over increasing physical and digital threats targeting athletes, referees, and support staff. According to the report, criminal actors and disgruntled gamblers are increasingly using social media, encrypted messaging apps, and cyber-enabled tactics to pressure or intimidate players into influencing match outcomes.

Documented incidents cited in the report include threats of violence against athletes and their families, online harassment campaigns, and attempts to manipulate players through coercion, extortion, and recruitment efforts tied to betting schemes.

“Large-scale sporting events like the World Cup attract not only fans, but also criminal actors looking to exploit the excitement surrounding the tournament,” said John Cohen, Executive Director for the Office of Strategic Programs and Initiatives at CIS. “Law enforcement and event organizers face increasing risks from phishing campaigns, fraudulent betting networks, and AI-enabled counterfeit websites targeting unsuspecting individuals.”

Researchers recommend enhanced information-sharing among law enforcement, regulators, venue operators, and financial institutions, along with athlete awareness programs, tabletop exercises, and coordinated crisis communications planning ahead of and during the tournament.

“It is also critical that fans, spectators, and legitimate bettors understand these risks and know how to identify fraudulent platforms and suspicious activity,” Cohen added. “Public awareness is an important part of protecting both the integrity of the games and the safety of those watching, attending, and participating in them.”

For additional information or interview requests, please contact media@cisecurity.org.

###

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and

Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CIS or follow us on X: @CISecurity.

About Wein Strategy Lab

Wein Strategy Lab is a boutique consulting and advisory services company that supports a broad range of clients across national security, homeland security, sports, and cybersecurity industries. We help executives and policy makers understand and plan for emerging threats across domains. WSL specializes in strategy development, tabletop exercises, program implementation, outreach and communication plans, and policy review.

Kelly Wyland

Center for Internet Security

+1 518-256-6978

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/921370035>

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.