INTERPOL and Kaspersky team up to defend Africa's premier international football event

The Africa Cup of Nations (AFCON)

kaspersky cybersecurity true to business

CAF

1957

Founded in 1957 to crown Africa's national football champion

24

National teams competed in the 2025 final

1.2 million

Total turnout, with over 3.4 billion views

$10 million

Prize pool

The Africa Cup of Nations (AFCON)

The Africa Cup of Nations (AFCON) is the premier international men's football competition, organized by the Confederation of African Football (CAF). Traditionally been held every 2 years, the 2025 tournament took place in Morocco from December 2025 to January 2026.

As with any high-profile international sporting event, AFCON 2025 was expected to attract heightened attention from cybercriminals.

Cybercrime activity typically peaks before and during major sporting events

Threat actors deliberately target fans

Spectator vigilance helps reduce risk

International law enforcement agencies play a key role

Yuliya Shlychkova

VP of Global Public Affairs, Kaspersky

For events of this scale, collaboration between public and private entities is crucial to aligning efforts against cybercrime and helping create a secure experience for the millions attending these global events. By contributing to INTERPOL's mission, Kaspersky supports a shared industry commitment to global cybersecurity.

Sharing intelligence

To help create a safer online community around AFCON, Kaspersky provided INTERPOL with data on a wide range of threats targeting the competition, its participants and viewers, and the host country overall.

Kaspersky
Digital Footprint
Intelligence

Monitoring external threats to protect business assets across the surface, deep and dark web

- Continuous monitoring with real-time threat alerts
- Early detection of mentions of company assets
- Auto-expanding observable perimeter
- Criticality meter to assess and prioritize threats

Active threats uncovered

Compromised credentials

To help assess credential exposure, the Kaspersky Digital Footprint Intelligence team identified more than 2 million credentials on the dark web associated with Moroccan users or resources. The corresponding accounts had been compromised by infostealer malware designed to extract credentials, financial details or other valuable information.

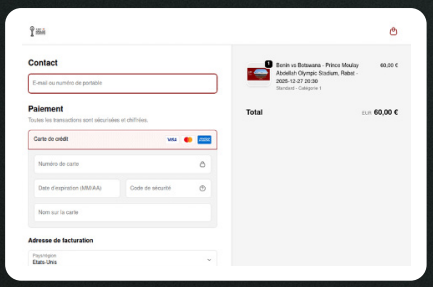
Hacktivist activity

Monitoring detected a spike in hacktivist activity in Morocco between September and December 2025. About 300 messages reporting on hacktivist attacks targeting Morocco were published in 2025, with DDoS attacks and defacement identified as the key hacktivist tools.

Scam websites

Analysts identified fraudulent websites harvesting user data and payment information under the guise of offering AFCON tickets or prizes for predicting the winning team in upcoming matches.

Example of a scam website offering fraudulent AFCON tickets



Example of a payment form on a scam website

Protecting major sporting events worldwide

INTERPOL-led efforts play a vital role in bringing together and coordinating stakeholders whose involvement is crucial for ensuring the security of major high-profile events. The partnership between INTERPOL and Kaspersky has continued through joint projects, with Kaspersky also joining INTERPOL-led cybersecurity efforts around major tournaments such as the Paris 2024 Olympic Games and the 2025 Formula 1 Singapore Grand Prix.

Kaspersky Digital Footprint Intelligence

Learn more

www.kaspersky.com

#kaspersky
#truetobusiness