Informational Threat Notification

FIFA World Cup 2026 Cyber Threat Bulletin

Date: June 11, 2026

Summary

The FIFA World Cup 2026 has started and is the largest FIFA tournament to date, hosted across the United States (U.S.), Canada, and Mexico. The event will bring together millions of spectators, international teams, sponsors, broadcasters, hospitality providers, transportation operators, government agencies, and digital service providers across multiple host cities. This scale creates a broad cyber and physical attack surface, especially because the tournament will depend heavily on online ticketing, mobile applications, digital payments, travel platforms, stadium technology, public Wi Fi, media systems, and cross border coordination [1, 2, 3].

Analysis

Key threats during the FIFA event include phishing, fraudulent ticketing, brand impersonation, malicious domains, ransomware, Distributed Denial-of-Service (DDoS) attacks, credential theft, and cyber enabled fraud targeting individuals and organizations across the U.S., Canada, and Mexico. These threats can damage organizations' reputation, disrupt tournament related operations and services, and result in significant financial losses for affected stakeholders.

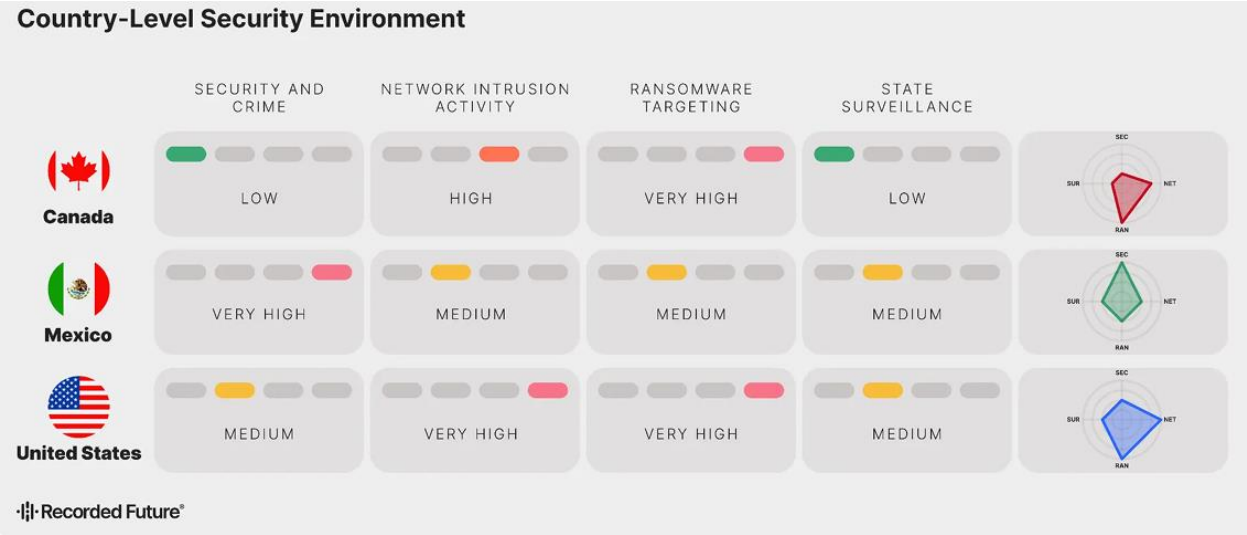

Figure 1.: Composite Country Risk Scores for Canada, Mexico, and the US [3]

Organizations and Individuals at Risk

Organizations at risk include FIFA related entities, host city authorities, stadium operators, transportation providers, hotels, airlines, broadcasters, sponsors, payment processors, telecom providers, law enforcement partners, and third-party technology vendors. These organizations may be targeted because they support high visibility services that must remain available during the tournament. Individuals at risk include fans, tourists, journalists, athletes, staff, VIP guests, and local residents in host cities. Common threats include fake ticket sales, phishing emails, fraudulent travel deals, malicious apps, fake livestreams, payment scams, and account takeover attempts.

Phishing and Social Engineering

Phishing is expected to be one of the most common threats linked to FIFA World Cup 2026. Attackers are likely to impersonate FIFA, ticketing providers, sponsors, hotels, airlines, and local transport services. These campaigns may use emails, text messages, social media ads, QR codes, and messaging apps (WhatsApp, Telegram) as Initial Access Vectors (IAVs) to steal credentials, payment details, or personal information. The demand for match tickets, travel and accommodation bookings, and fantasy gaming or betting platforms is likely to be leveraged to make phishing campaigns more convincing. Cloned websites of official FIFA website and impersonated World Cup themed websites, designed to steal payment credentials have been identified ahead of the tournament [1, 3, 5, 6, 7].

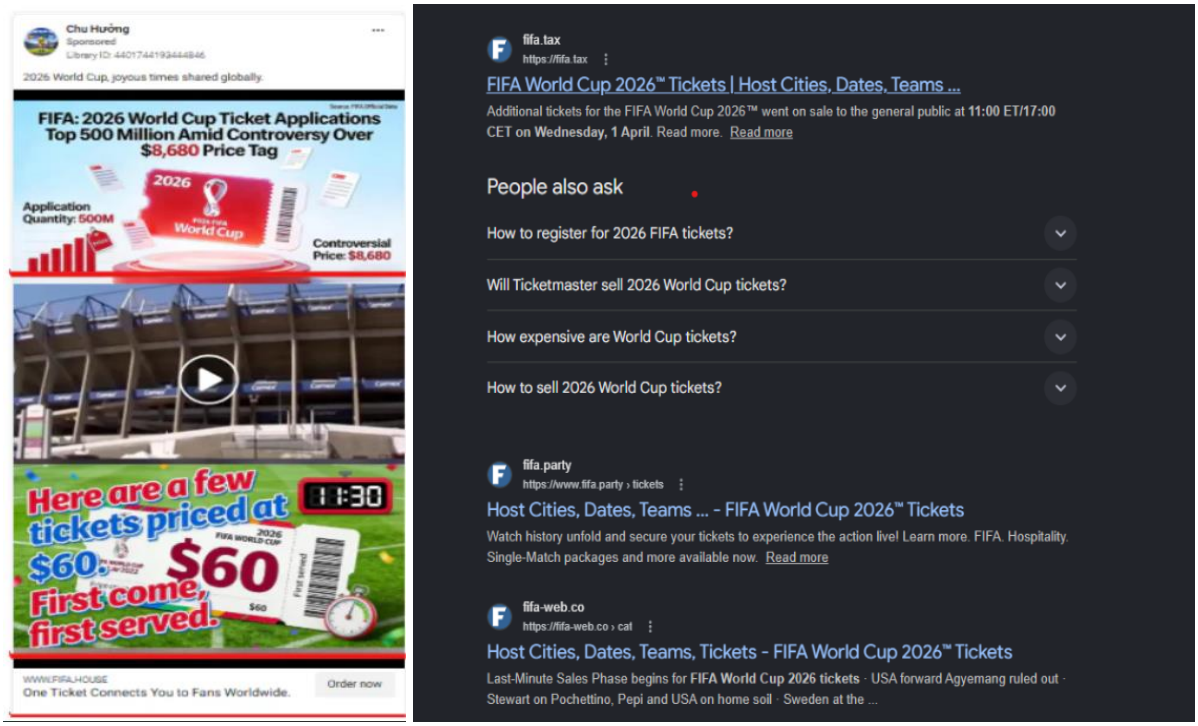

Figure 2.: Example of scam ads abusing Facebook's advertising platform and fraudulent domains impersonating FIFA's official website [7]

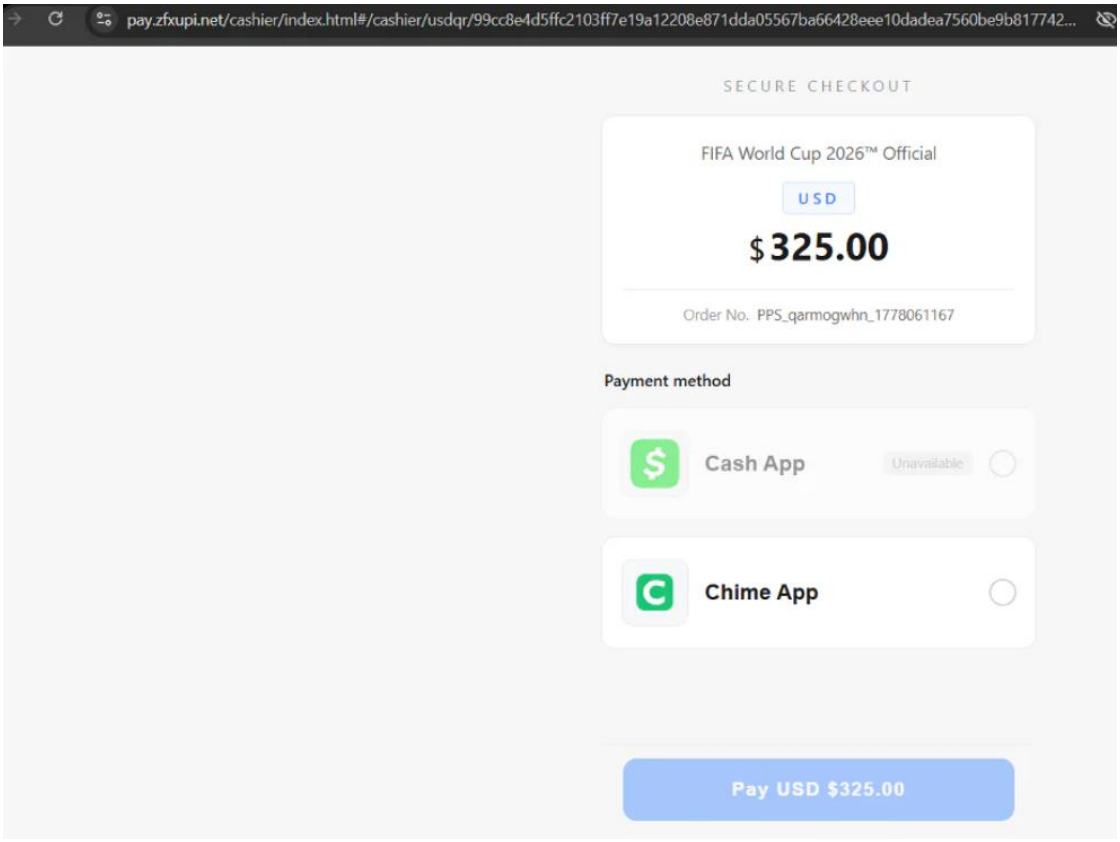

Figure 3.: Example of redirection to external payment gateways [7]

Credential Stealer Malware Campaigns

Security researchers have observed threat actors using FIFA themed lures to deliver information stealers such as Vidar, LummaC2, and RedLine. The stealer logs revealed 260 FIFA employee credentials and over 270,000 credentials being stolen ahead of the tournament. Global events like the FIFA World Cup enable threat actors to conduct opportunistic malware campaigns leveraging the IAVs discussed in Phishing and Social Engineering section [5].

DDoS Attacks Against Public Facing Services

DDoS attacks are likely to target systems and services associated with FIFA World Cup 2026, aiming to disrupt operations, impact service availability, and generate public attention during the tournament. Non state threat actors often conduct such attacks to advance ideological agendas, amplify their messaging, and damage the reputation of targeted organizations. DDoS attack during ticket sales, match day entry, transport coordination, or live broadcast windows could impact fan experience and public confidence [2, 3, 4].

Ransomware and Business Disruption

Ransomware poses a serious threat to organizations supporting tournament operations. Attackers may target hotels, transport operators, broadcasters, local governments, managed service providers, and suppliers because disruption during the tournament could create pressure to pay. During Paris 2024 Olympics, threat actors targeted multiple French entities associated with the event. While the attacks did not disrupt the event but the encrypted data including financial data was unavailable for brief period and the businesses were disrupted as impacted systems were disconnected from the network [2, 3, 4, 7].

Defacement attacks

Website and social media account defacement attacks are likely to target organizations associated with FIFA World Cup 2026, including event organizers, sponsors, and government entities. By compromising these platforms and replacing legitimate content with ideological, political, or geopolitical messaging, threat actors can leverage the tournament's global visibility to amplify their narratives and reach a wider audience. Digital signage systems such as electronic displays, advertising screens, video walls, and information boards located at venues, tourist areas, and transportation hubs may also be targeted to spread unauthorized messages or cause disruption [2, 3, 4].

Recommendations

Organizations should:

- Educate employees to stay vigilant for FIFA 2026 themed phishing emails, fraudulent domains, and brand impersonation attempts.
- Enforce MFA across email, VPN, cloud, ticketing, and administrative systems.
- Conduct phishing training focused on FIFA themed lures.
- Prepare DDoS protection for public facing systems.
- Test ransomware response and backup recovery.
- Review third party and supplier security controls.
- Review cyber response planning with physical security teams.

Individuals should:

- Buy tickets only through official FIFA channels.
- Utilize VPN when on public wifi
- Avoid unsolicited ticket, travel, livestream, or hospitality links.
- Use MFA on email, banking, travel, and ticketing accounts.
- Avoid unofficial apps and QR codes.
- Verify hotel, transport, and event information through trusted sources.

Sources

[1] BDO Internal
[2] Canadian Centre for Cyber Security “Cyber Threat Bulletin — FIFA World Cup 2026”, June 3, 2026 [Online] Available: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-fifa-world-cup-2026
[3] Recorded Future “2026 FIFA World Cup Cyber-Physical Threats Security Guide”, June 10, 2026 [Online] Available: https://www.recordedfuture.com/blog/2026-fifa-world-cup-cyber-physical-threats-security-guide
[4] Recorded Future “Threats to the FIFA World Cup”, June 4, 2026 [Online] Available: https://www.recordedfuture.com/research/threats-fifa-world-cup
[5] Fortinet “Cybercriminals Are Targeting the FIFA World Cup 2026”, June 4, 2026 [Online] Available: https://www.fortinet.com/blog/threat-research/cybercriminals-are-targeting-the-fifa-world-cup-2026
[6] FBI “IC3 Public Service Announcement”, May 27, 2026 [Online] Available: https://www.ic3.gov/PSA/2026/PSA2605277
[7] Group-IB “The GHOST STADIUM Score: Billions At Stake At The World’s Largest Football Tournament”, May 27, 2026 [Online] Available: https://www.group-ib.com/blog/ghost-stadium-football-fraud/
[7] Palo Alto “2026 World Cup: Discussing The World’s Biggest Game’s Attack Surface”, May 28, 2026 [Online] Available: 2026 World Cup: Discussing The World’s Biggest Game’s Attack Surface