May 14, 2026

Defending the Pitch: A Strategic Cybersecurity Advisory for the 2026 FIFA World Cup

Key Insights:

- The tournament's expanded footprint creates an important threat surface for politically driven attackers.
- Cybercriminals are likely to leverage generative AI and deepfakes to defraud fans. Major risks include fraudulent travel visas, cloned ticketing sites and high-pressure social engineering tactics.
- Interdependent digital systems create cascading risks. A security failure at a minor third-party vendor can paralyze core operations, including broadcasting, transportation and hospitality.
- Scalping and credential stuffing attacks are virtually guaranteed. Automated tools exploit password reuse to drain betting account balances and hoard limited ticket inventory.

The 2026 FIFA World Cup is more than a tournament; it is a national-level security priority for the United States, Canada and Mexico. For the first time, 48 teams will compete across 16 host cities in three nations, creating a digital and physical footprint at an unprecedented scale. This expanded attack surface is already being exploited by a sophisticated scam economy. The convergence of geopolitical instability, hyper-connectivity and critical infrastructure interdependence has created an environment where cybersecurity is the primary arbiter of the tournament's success.

The Convergence of Geopolitical Tensions and Symbolic Targeting

The 2026 tournament will serve as a global stage for hacktivists and state-linked actors seeking to project influence. The current landscape features adversaries using cyber operations as tools for global propaganda and disruption aiming to create social distrust. Conflicts such as the Russia-Ukraine war and tensions involving the U.S., Israel and Iran turn Western corporate assets and tournament infrastructure into symbolic targets for retaliation. Jules Boykoff, a professor at Pacific University and specialist in the politics of international sports, notes that it is unprecedented for a World Cup host to launch an attack on a participating nation just months before the tournament kicks off. Describing the situation as a historic anomaly for the sport, Boykoff remarks, "Soccer-wise, it moves us into uncharted territory."

Financial Opportunism and the Sophisticated Scam Economy

Cybercriminals are aggressively leveraging brand parasitism and generative AI to defraud a global audience. The scale of this opportunism is vast, ranging from fraudulent World Cup travel visas to cloned ticketing sites and unlicensed World Cup crypto tokens. These actors exploit the high-demand environment, where the scarcity of legitimate access creates a vacuum filled by fraudulent bargains.

Infrastructure Interdependence and Cascading Risk

The digital ecosystem of the 2026 World Cup is a complex web of shared networks and third-party vendors. Core systems, including broadcasting, ticketing, and transportation (ground and air), rely on an unevenly secured network of hundreds of suppliers. This vulnerability is magnified by the shift toward digital streaming, as evidenced by the 2024 Paris Olympics, where Namex recorded massive traffic surges synchronized with live events. While modern IXPs and CDNs are equipped for these bandwidth demands, the interconnectedness of hundreds of suppliers creates a material risk where a single weak link can paralyze the tournament's core operations.

Historical Precedents and the Evolution of the Threat

Past international events serve as the operational playbook for modern threat actors. We have observed a strategic shift where cyberattacks have moved from simple technical nuisances to sophisticated tools for reputational damage. The Olympic Destroyer malware impacted the 2018 Winter Olympics in PyeongChang. It disrupted the opening ceremonies by targeting stadium Wi-Fi and official websites, demonstrating how malware can be used for reputation damage. During the 2024 Paris Olympics, security operations centers monitored substantial malicious activity attributed primarily to Russian and Iranian-aligned hacktivist collectives. One specific Iranian campaign focused on compromising a French digital signage provider. Furthermore, telemetry from Internet Exchange Points (IXPs) revealed significant volumetric anomalies that aligned precisely with the timing of the opening ceremony. There were also pro-Russian hacktivist attempts by groups like Killnet during the 2022 and 2023 Eurovision contests, proving that high-visibility events, voting and broadcasting systems are now permanent targets for political messaging.

Recent data underscores the escalating frequency of these threats. During the lead-up to the Milano Cortina Winter Games in 2026, Italian infrastructure saw an increase in DDoS frequency compared to the previous year. The 2022 Qatar World Cup managed threats from Anonymous and Iran-linked tension. The 2026 geopolitical and digital landscape, however, has grown significantly more complex. The attack surface has expanded through the widespread deployment of 5G networks, 8K-resolution streaming, a pervasive reliance on public internet infrastructure, and the ongoing digital transformation of society and global marketplaces. Furthermore, the objective of threat actors has evolved from creating purely technical failures to boost their own

reputations and social credibility to a more strategic focus on damaging the reputations of the three host nations, portraying them as operationally insecure and incapable of protecting global participants.

FIFA, Broadcasters and the Vendor Network

Core tournament infrastructure represents the strategic center of gravity for the 2026 World Cup. Any disruption to these systems does more than cause delays; it undermines the integrity of the event on a global scale. National broadcasters and streaming channels are particularly vulnerable to Web DDoS and network DDoS attacks.

The risk environment extends deeply into the fragmented vendor network handling ticketing validation, merchandising, and hospitality. These entities often operate with lower security visibility than core FIFA systems but remain integrated into the event's shared digital ecosystem. A failure in a minor third-party vendor's system can cascade across shared networks, leading to chaos at stadium gates or the total failure of hospitality payment systems. For threat actors, these vendors represent the soft underbelly of the tournament—targets that provide the highest disruptive return for the least effort.

The Fan Experience

Scammers utilize psychological tactics, including urgency tricks and aggressive brand plagiarism, to exploit fans. By creating high-pressure environments through countdown timers and fake scarcity, they drive fans toward fraudulent decisions before they can verify sources.

Deepfakes

The use of deepfake videos and voice cloning to impersonate athletes, officials or other public figures is a concern. Deepfake technology has become accessible and helps to create convincing scams, spread misinformation or defraud victims.

The Ticket Trap

The financial stakes for fans have never been higher. With FIFA tripling the price of front-category final tickets at MetLife Stadium to $32,970 less than five weeks before the tournament, many fans are driven to unofficial resellers. Scammers capitalize on this by offering convincing fake listings. Statistics show that victims of football ticket fraud lose an average of $280 per person. In a digital-first environment, red flags include any seller offering paper tickets or screenshots, as official 2026 tickets will be delivered exclusively via the digital FIFA app.

Travel Visa Scams

The "World Cup Visa" remains one of the most dangerous fraud categories. Scammers promote fake WC2026 Visas to harvest passport data, travel plans and payment details. There is no

special tournament visa; visitors must use standard B1/B2 visas, ESTA, or the equivalent Canadian and Mexican authorizations. The official "FIFA PASS" (Priority Appointment Scheduling System) is merely a routing mechanism for earlier interview slots for ticket holders; it does not bypass the standard interview process or cost the $270 fees often cited on scam sites.

Crypto and Merchandise Scams

Fraudsters are flooding the digital landscape with World Cup crypto token scams and discount storefronts. These sites impersonate genuine partners like LEGO and Panini, using quiz challenges to harvest personal data or push victims into hidden subscription billing flows. Fans are often lured by the promise of exclusive rewards, only to have their credit cards compromised or their identities stolen through the submission of sensitive personal data.

Under the Fair Credit Billing Act (FCBA), fans who use credit cards have a critical 60-day window to dispute charges for tickets or merchandise that were never delivered. This legal protection is a vital recovery tool, but it is entirely bypassed if fans use irreversible methods like Zelle, Cash App or cryptocurrency.

Scalping

Scalping involves the rapid, automated acquisition of high-demand inventory—such as tickets, travel bookings, or retail goods—to bypass standard purchase limits. By leveraging scripts to hoard supply, actors can flip these items on secondary markets at a massive markup. Given the profile of the upcoming tournament, a surge in large-scale scalping attacks is virtually guaranteed.

The 2025 holiday season already saw a 135% year-over-year surge in malicious bot traffic specifically focused on scraping and inventory exhaustion. Threat actors increasingly utilized AI agents to mimic human browsing patterns (e.g., natural mouse movements and varied pacing) and deployed "sleeper" synthetic profiles to bypass traditional perimeter defenses.

The 2026 FIFA World Cup ticket random selection draw also saw massive demand, with over 5 million ticket requests submitted within the first 24 hours of the application window. This high-traffic phase ran from December 11, 2025, to January 13, 2026, allowing fans to apply for single-match tickets at FIFA.com/tickets. Fans aiming to get tickets have expressed severe frustration across social media platforms regarding both automated bots and the official ticketing infrastructure.

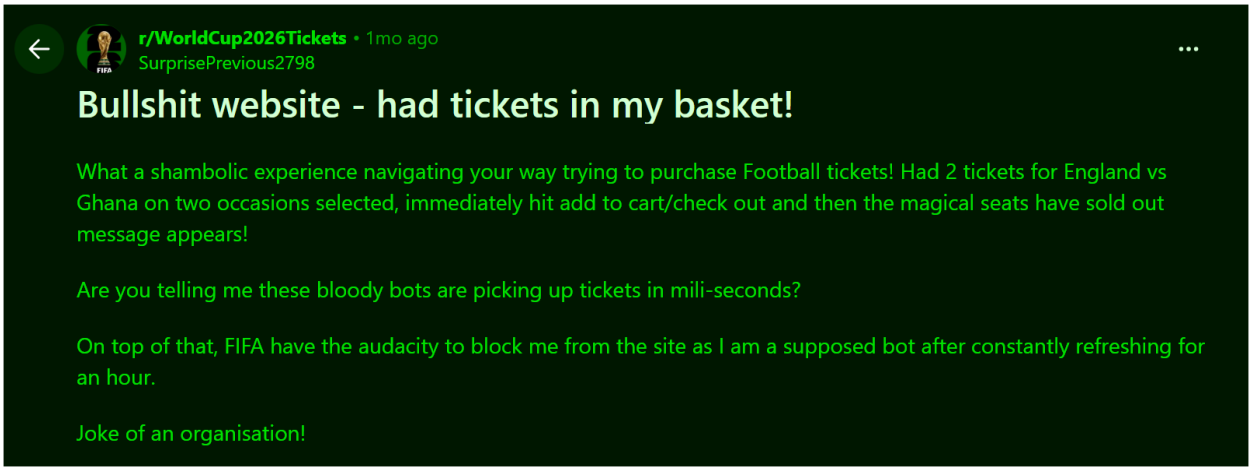

Figure 1: One of the many threads that complain about ticket availability due to bots (source: Reddit)

Users on the *r/WorldCup2026Tickets subreddit (figure 1) reported extreme frustration with cart hijacking. One user stated: "Had 2 tickets ... selected, immediately hit add to cart/check out and then the magical seats have sold out message appears! Are you telling me these bloody bots are picking up tickets in milliseconds?"

Victims also frequently cited the official FIFA platform as acting very much like a scalper, noting that the combined 30% buyer/seller fees artificially inflate the market even for legitimate fans trying to trade tickets.

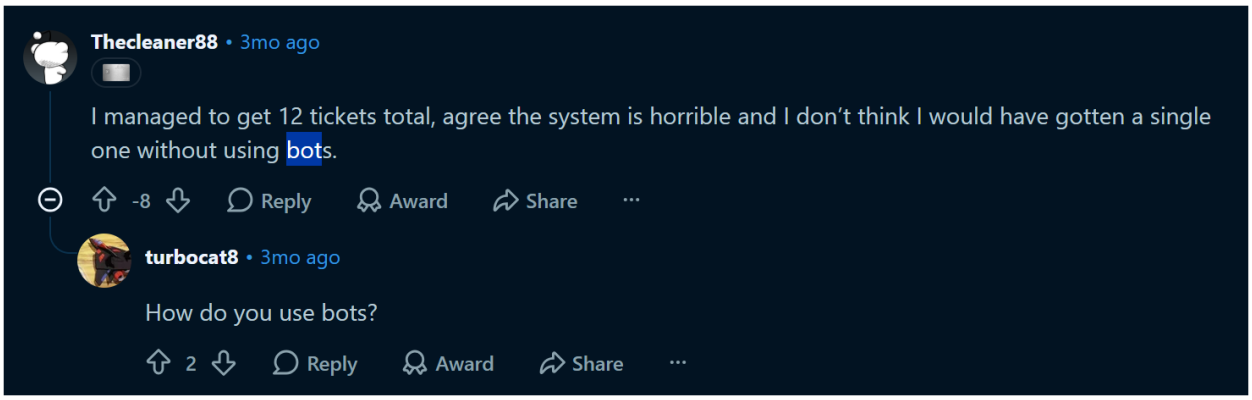

Figure 2: Ticketing bot operators confess (source: Reddit)

Users on the *r/ChaseSapphire* subreddit complained about being trapped in a "queue of death" during the draw, widely attributing instant sell-outs to aggressive bots that bypass the queue. In one of the comments, a user claimed to buy 12 tickets using a bot (figure 2).

Credential Stuffing on Sports Betting Apps

Sports betting platforms supporting the North American market are consistent targets for credential stuffing due to widespread password reuse and the financial value of such accounts.

In November 2022, a massive credential-stuffing campaign targeted DraftKings just three days after the NFL games began. Over 68,000 accounts were compromised, some with tens of thousands of dollars in their balances. The threat actors siphoned approximately $300,000 in customer funds. An 18-year-old involved in the 2022 DraftKings attack pleaded guilty and was sentenced to 18 months in federal prison.

More recently, in September 2025, DraftKings reported another massive credential stuffing attack. Attackers breached accounts by leveraging credentials exposed in earlier unrelated breaches, such as the 560 million records from the June 2024 Ticketmaster breach. While backend systems remained secure, attackers were able to access personal data, transaction histories and partial payment card details, prompting mandatory password resets and the enforcement of Multi-Factor Authentication (MFA).

Victims of sports betting account takeovers reported significant financial loss and secondary platform lockouts. In a dedicated mega thread on the "r/sportsbook" subreddit following the DraftKings breach, victims detailed severe account takeovers and the hijacking of connected financial accounts.

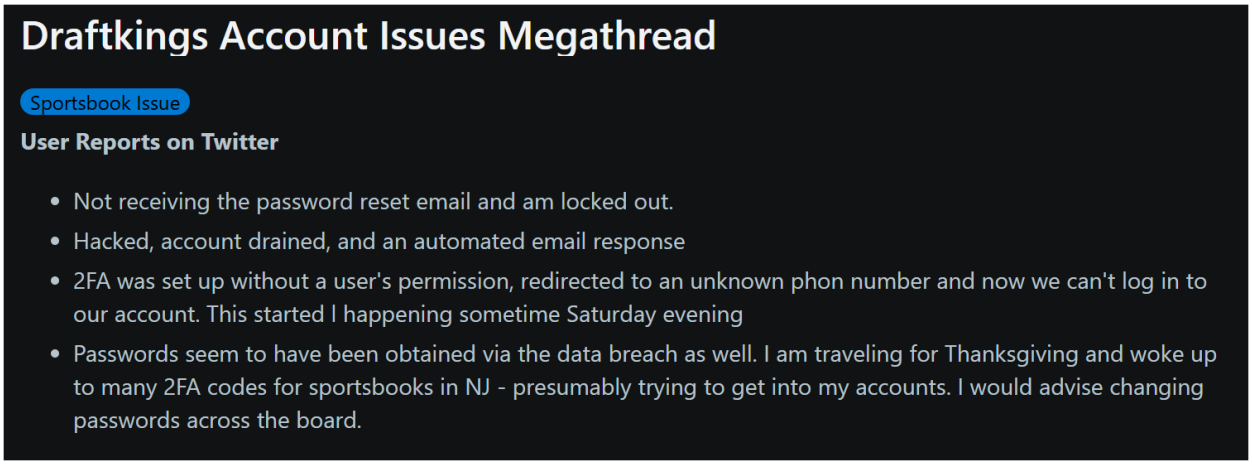

Figure 3: Ticketing bot operators confess (source: Reddit)

Victims quoted:

"2FA was set up without a user's permission, redirected to an unknown phone number, and now we can't log in to our account."*

"I've been locked out for 8 days now. $600 drafted from my Venmo account by hackers."

Users also reported that alerting customer support to the drained funds triggered internal responsible gaming flags. This automated response effectively froze their accounts, further exacerbating the lockout period rather than initiating immediate fraud recovery.

Major global tournaments like the World Cup are prime targets for credential stuffing. Attackers use automated tools to test stolen logins against gaming and betting APIs, banking on the fact that distracted fans often reuse old passwords. With account balances at an all-time high during these events, providers such as DraftKings, FanDuel and BetMGM must prepare for a massive surge in unauthorized login attempts.

Implications for Organizations and Global Business

Organizations across North America are collateral targets because of their integration into the World Cup's digital and physical supply chains. The rapid onboarding of thousands of temporary staff and volunteers creates a massive insider risk profile. Poor cyber hygiene among a temporary workforce, combined with a funding delay that has forced some agencies to compress six months of security preparation into just two, has created a significant readiness gap that sophisticated attackers are poised to exploit.

The intent profiles of nation-state actors add a layer of strategic complexity. While Russia focuses on inflicting reputational and political damage to portray the host nations as insecure, North Korean-affiliated groups focus more on financial theft and credential harvesting through long-running phishing campaigns. This geopolitical spillover means that even businesses not officially connected to FIFA will face threats as symbolic targets of Western interests.

Local businesses must also prepare for physical and operational paralysis. Road closures, hardened perimeters around stadiums, and transportation congestion will disrupt daily operations and supply chain logistics. These disruptions can paralyze everything from local deliveries to large-scale corporate logistics.

The FIFA World Cup 2026 Fan Playbook

Verify Domain Extensions: Only process visa and official documents through government-verified domains: **.gov** (U.S.), **.gc.ca** (Canada), or **.gob.mx** (Mexico). Any site offering "World Cup Visas" on a .com or .net domain is a fraudulent entity designed for identity theft.

Audit Payment Methods: Reject requests for payment via Zelle, Cash App, wire transfers, or cryptocurrency. These are irreversible and preferred by scammers. Use credit cards to ensure protection under the Fair Credit Billing Act and the 60-day dispute window.

Identify Brand Parasitism: Be skeptical of pre-release offers or discounts exceeding 80% on licensed merchandise. Official partners like LEGO and Panini do not use high-pressure countdown timers or quiz-funnels to sell premium sets. Verify all offers through the canonical brand websites before entering data.

Use Official Ticketing Channels Only: Purchase tickets exclusively through FIFA.com/tickets or the official FIFA app, as these are the primary verified platforms. Be extremely wary of sellers offering paper tickets or screenshots, as most legitimate 2026 World Cup tickets will be delivered electronically.

Avoid "Official" Crypto Tokens: Steer clear of cryptocurrency projects marketing themselves as the "official community token" of the 2026 World Cup. There is no official World Cup token, and these sites use brand parasitism to trick users into signing malicious wallet transactions or buying into speculative schemes.

Practice Digital Hygiene at the Event: When attending matches or fan zones, disable your device's Wi-Fi and Bluetooth when not in use to prevent unauthorized connections. If you must connect to the internet, only use the official event Wi-Fi, alongside a virtual private network (VPN) to protect your personal data.

Protect Physical Payment Methods: Equip yourself with RFID shields to protect your identity and credit cards from wireless data theft in crowded stadium environments. Additionally, always inspect ATMs for card skimmers before withdrawing cash.

Steer Clear of Unlicensed "Predictor" Sites: Avoid participating in unregulated "World Cup Predictor" prize pools where you pay for entries into a pooled outcome. These sites often operate as unlicensed betting platforms without clear oversight, regulatory authority, or verified payment processors.

Document and Report Fraud Immediately: If you suspect you have been scammed, do not delete any messages or emails. Save all receipts, seller profiles, and screenshots of the transaction, and report the fraud immediately to your bank and to authorities like the FTC.

The FIFA World Cup 2026 Business Playbook

Deploy Behavioral DDoS Protection: Organizations must shift from simple rate-limiting to behavior-based detection. This is the only effective way to distinguish between legitimate spikes in fan traffic and high-throughput/packet-rate intensive DDoS attacks designed to sustain pressure on streaming and voting APIs.

Utilize Hybrid DDoS Protection: In addition to behavior-based detection, organizations should implement hybrid DDoS protection that combines on-premises and cloud solutions. This ensures real-time attack prevention while simultaneously addressing extremely high-volume attacks.

Manage Insider and Vendor Risk: Treat the credentials of all temporary staff and third-party vendors with zero-trust scrutiny. Enforce strict multi-factor authentication (MFA) and segment all venue-specific operational technology (OT) to prevent a compromise in a minor vendor from cascading into core corporate or broadcast networks.

Monitor for Disinformation and Narrative Manipulation: Geopolitical tensions increase the likelihood of coordinated disinformation campaigns. Businesses and event organizers should actively monitor online narratives to quickly identify false reports of evacuations, threats or infrastructure failures that could trigger panic, strain emergency response systems or damage a host city's reputation.

Implement Comprehensive Web Application and API Security: Cybercriminals will launch application attacks such as SQL injections, password cracking, credential stuffing and session hijacking to steal spectator and operational data. Organizations must secure their APIs and track activity, while also deploying bot protection and device fingerprinting to thwart automated threats.

Establish a Dedicated Cybersecurity Emergency Response Plan: Assemble a dedicated emergency response team with expertise in handling outbreaks and mitigating zero-day threats. This team should leverage real-time intelligence on active threat actors to preemptively protect networks and swiftly restore services.

Audit Networks and Secure Access Points: Conduct regular network audits to identify vulnerabilities. Security teams must actively scan for rogue access points or "evil twins" designed to intercept fan traffic, update firmware, reset default passwords and use Access Control Lists (ACLs) to filter network traffic effectively where possible.

Summary and Conclusion: Resilience in a Fragmented Environment

The security of the 2026 FIFA World Cup depends on seamless cross-border coordination between the U.S., Canada and Mexico. Because the digital footprint is so vast and the timelines for preparation have been compressed, no single entity can secure the ecosystem in isolation.

True resilience requires stakeholders to move beyond traditional perimeter defense and treat identity systems as critical infrastructure. By strictly enforcing multi-factor authentication (MFA) and segmenting venue technology from core corporate networks, organizations can reduce the blast radius of inevitable attacks. Success will be measured not by the absence of threats, but by the speed of response and the ability to maintain operational integrity in a fragmented and high-pressure environment.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.