World Cup Fever: Don’t Let Scammers Score

A Chance of a Lifetime – Stolen

Diego had waited years for this moment. The 2026 World Cup was finally here, and for the first time ever he had both the time and money to attend in person. When he saw a post on social media offering “last-minute official tickets” to a sold-out match, he felt lucky. The seller claimed to work with an authorized distributor and even shared what looked like a confirmation email from the tournament organizers.

The price was high, but not outrageous. The seller warned him that tickets were “almost gone,” and that several buyers were already interested. Not wanting to miss his chance, Diego transferred the money through an instant payment app.

The tickets never arrived. The seller’s account disappeared. The website linked in the message was taken down within days. Diego didn’t just lose money, he missed out on the chance to attend a once-in-a-lifetime event.

Why Major Sporting Events Attract Scammers

Global events like the World Cup create a perfect storm for scams. There is massive demand for tickets, travel, merchandise, and streaming access. People are excited, emotionally invested, and often acting quickly. The combination of urgency and emotion makes it easier for attackers to manipulate victims.

Criminals understand human behavior. They know that when something is scarce, people feel pressure to act fast. They know when millions of people are searching online for the same thing, fake websites and phishing messages can easily blend in. Attackers consistently exploit urgency, fear, and excitement to push people into making quick decisions that lead to financial and personal losses.

What These Attacks Look Like

Fake Ticket Sales: Criminals create professional-looking websites or social media posts that appear legitimate. Some copy official branding and logos, while others purchase online advertisements so their fake sites appear at the top of search results. Victims pay for tickets that are never delivered, or they receive digital tickets that fail at the stadium entrance. Often, payment is requested through wire transfers, cryptocurrency, or peer-to-peer apps, which are difficult to reverse.

`© SANS Institute 2026

Urgent Messages: You receive emails or text messages claiming to be from tournament organizers, airlines, hotels, or streaming services. These messages often warn that your ticket purchase failed or that your booking will be canceled unless you confirm payment immediately. These messages are crafted to look urgent and legitimate to entice the buyer to act quickly without thinking logically. The link ultimately leads to a fake login page designed to steal your credentials. Just as with other scam campaigns, attackers rely heavily on urgency and the fear of losing access.

Streaming Scams: Criminals create fake platforms offering "free live coverage" of matches. To watch, you are asked to create an account and enter payment details. Instead of viewing the match, you may unknowingly install malware or have your financial information stolen.

Bad Merchandise: Even merchandise and giveaways become tools for exploitation. For example, fake contests can promise official jerseys or exclusive prizes in exchange for personal information. Counterfeit online stores can sell discounted gear but either ship low-quality fakes or nothing at all.

How to Protect Yourself

The good news is that these scams are preventable if you slow down and verify before acting. Only purchase tickets, travel, and merchandise from official partners or well-known vendors. Instead of clicking links in emails, social media posts, or other unverified media, type the official website address directly into your browser or use a trusted mobile app. Bookmark legitimate sites once verified so you return to the correct location each time.

Be especially cautious with any message that pressures you to act immediately. Scammers depend on speed. If you receive a warning about a canceled booking or failed payment, do not click the link. Instead, independently contact the company using verified contact information.

Finally, be wary of unusual payment methods. Requests for cryptocurrency, wire transfers, or gift cards should immediately raise concern. Legitimate vendors rarely require these forms of payment. In addition, major credit cards or well-known electronic payment systems like PayPal provide you with additional forms of purchase protection.

Be cautious in your purchases and actions; cyber criminals thrive on rushing people into making mistakes.

Guest Editor

Karyn DiMassa is a cybersecurity, internal audit, risk, and control specialist with expertise in incident response, disaster recovery, and business continuity management; cybersecurity assessments, gap analysis and remediation; internal risk and controls identification, assessment, and remediation; enterprise risk management; and internal audit.

Resources

How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Top Three Ways Cyber Attackers Target You: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you
How Cybercriminals Steal Your Password: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

OUCH! Is published by SANS Security Awareness and distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch