FEDERAL BUREAU OF INVESTIGATION
Public Service Announcement

Alert Number: I-052726-PSA | 27 May 2026
Threat Actors Spoofing FIFA Websites in Advance of the 2026 World Cup

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement (PSA) to warn the public that cyber threat actors are conducting spoofing attacks against the Fédération Internationale de Football Association (FIFA) website in advance of the 2026 FIFA World Cup. A spoofed website is designed to pose as a legitimate website, with branding, product listings, etc., and malicious actors use them to further illegal activity like personal information theft and facilitating monetary scams.

Threat actors often create spoofed websites by slightly altering characteristics of legitimate website domains, with the purpose of gathering personally identifiable information (PII) entered by a user into the site, including name, home address, phone number, email address, and banking information. For example, spoofed website domains may feature alternate spellings of words or use an alternative top-level domain to impersonate a legitimate website. Members of the public could unknowingly visit spoofed websites while attempting to access FIFA's website.

How the Scam Works

Threat actors create a deceptive version of a legitimate website (www.fifa.com) with the goal of tricking users into believing they're interacting with an official brand. The FBI has identified actors engaging in this activity to collect personal information, sell fake World Cup tickets and hospitality products, and to possibly facilitate other malicious activity. If a threat actor gains access to a victim's PII, they can create new accounts in a victim's name and ultimately defraud the victim.

Spoofed websites may mimic the legitimate URL by using a minor misspelling, such as fiffa[.]com, or alternative top-level domains, such as .org rather than .com. This form of cyberattack — called typo squatting — relies on Internet users making mistakes, such as common typos, when visiting a URL. Threat actors may also register illegitimate websites such as jobs-fifa[.]com to impersonate legitimate subdomains.

The FBI is aware of the following domains spoofing the legitimate FIFA website and anticipates additional fake domains to be created leading up to, and throughout, the 2026 World Cup. Below are examples of domains already identified; however, the public should be aware that new websites will continue to appear.

- www.fifa[.]cab
- www.fifa[.]blue
- FIFA[.]city
- fifa[.]beer
- www.fifa[.]pink
- www.fifa[.]pub
- Fifa[.]bio
- fifa[.]click

- fifa[.]cam
- fifa[.]help
- fifa-online[.]com
- jobs-fifa[.]com
- fifa-careerhub[.]com
- fifa-hiring[.]com
- fifa-ticket[.]live
- fifaworldcup26[.]sale
- worldcup2026-tickets.com[.]mx
- 2026fifaworldcuptickets[.]online
- fwc2026.web[.]app
- fifa2026fworldcup[.]com
- ww-fifa[.]com
- www.fifa-com[.]services
- fifa[.]ceo
- filfa[.]org
- https://fifa-2026[.]xyz
- fifa-hr[.]com
- fifaworldcup-careers[.]com
- fifahiring[.]com
- fifastore.us[.]com
- fifaworldcup26.xcover-staging[.]com
- worldcup26ticket[.]com
- fwc2026[.]net
- www.fifa2026p[.]com
- wvvw-fifa[.]com
- fifa-com[.]com
- quiniela-fifa-2026.pages[.]dev

Tips to Protect Yourself

The FBI recommends individuals take the following precautions:

- When navigating to FIFA's official website, type fifa.com directly into the address bar located at the top of your Internet browser, rather than using a search engine.
- If using a search engine, avoid any "sponsored" results as these can be paid imitators looking to deter traffic from the legitimate FIFA website.
- Verify that the URL of the FIFA website ends in [.]com and is correctly entered as www.fifa.com. Avoid clicking on any link whose URL differs from the legitimate FIFA website to mitigate risk of fraud.
- Use Bookmarks or Favorites for navigating to login websites rather than clicking on Internet search results or advertisements.
- Navigate to subdomains such as plus.fifa.com directly from the official FIFA homepage. Exercise caution when typing subdomains directly into the address bar.
- Never click on links that may include suspicious artifacts or graphics, such as unprofessional or low-quality graphics used to imitate a legitimate website.
- Never share sensitive information if you are unsure of the website's legitimacy
- Exercise caution when clicking on advertisements. Before clicking on an advertisement, check the URL to make sure the site is authentic. Malicious advertisements may redirect users to a different website than indicated.

Report It

If you or someone you know has fallen victim to this scam, file a complaint with the IC3 at www.ic3.gov. Be sure to include any available information including:

- Domain of the fake website, such as fifa[.]city.
- Description of your interaction with the website, including what information you provided and any other details pertinent to your complaint.

- Financial transaction information such as date, type of payment, amount, account numbers involved, the name and address of the receiving financial institution, and receiving cryptocurrency addresses.

For additional information on similar scams, please see previous Public Service Announcements:

- IC3 | "Threat Actors Spoofing the FBI IC3 Website for Possible Malicious Activity"
- IC3 | "Cyber Criminals Impersonating Employee Self-Service Websites to Steal Victim Information and Funds"