equity

beyond the box

Cyber security for your World Cup 2026 fans.

A short guide to keep your team safe online while they back their side through the biggest World Cup ever.

No fear, no jargon, just a few smart habits that should keep the criminals on the bench.

The biggest tournament - the biggest target

FIFA World Cup 2026 is the largest sporting event in history: 48 teams, 104 matches, 16 host cities and billions watching.

It's also the largest cyberattack surface sport has ever seen.

It might be in North America, but cybercrime doesn't respect borders, and broadcast rights don't firewall British fans.

Any UK business with staff glued to the football is part of the attack surface.

Big events focus on the three things criminals love:

urgency, money & distraction

and they time their attacks for kick-off, half-time and the shootout, **when nobody's checking** a web address.

The four risks….

- **The “free stream” trap. Fake streaming sites serve malware and harvest logins; late kick-offs send tired fans searching for “free streams”.**
- ***Watch on the official channels – they’re free, legal and safe.***

- **Deepfakes & disinformation. Hijacked broadcaster and social accounts push fake “breaking” clips.**
- ***Be sceptical of anything urging you to click, pay or share.***

- **Data & ransomware. 270,000+ FIFA-linked credentials are already on the dark web via “infostealer” malware — which doesn’t check passports.**
- ***Fix: never install dodgy “score tracker” apps on a work device.***

- **Ticket & travel scams. Cloned ticketing and hospitality sites arrive via paid Facebook/Instagram ads and fake resale accounts.**
- ***Fix: official FIFA channels only, and pay on a card with fraud protection.***

UNITED2026

equity
beyond the box

& some simple fixes

Your quick game plan

1. Only watch on official channels and avoid “free stream” searches entirely.
2. Switch on Multi factor Authentication (MFA) + a password manager for email, banking and key accounts.
3. Don’t trust the hype. Sponsored ads and sensational clips are often bait.
4. Keep devices clean. No side-loaded apps; keep updates current; avoid public Wi-Fi for anything sensitive.
5. Buy safe. Official channels and a protected card - never bank transfers or crypto.
6. Report it. Scam emails to report@phishing.gov.uk, texts to 7726, fraud to Action Fraud.

Share this with your colleagues and associates now, enforce phishing-resistant MFA, watch for leaked credentials, lock down unmanaged devices.

Enjoy the tournament.
Just don’t let your guard down.