



2023 Women's World Cup Australia and New Zealand

| Event Assessment |

Introduction

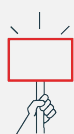
The 2023 Women's World Cup runs from July 20 to August 20, 2023. Hosting will be split between Australia and New Zealand, making this the first time two countries have shared duties for the women's tournament and the second time in history (Japan and South Korea dual-hosted the men's tournament in 2002). The distance between the two countries may cause issues with travel for teams and spectators, but there are no concerns around enmity between local fans, as Australians and Kiwis have a great affinity for each other and are unified by commonalities of language, history, and culture. There are also few concerns about visiting spectators; the only potential concern is between Australian and Chinese citizens due to local issues involving racism against Chinese-Australians and geopolitical tensions between the two countries. However, a lack of major tension points at present suggests a relatively low likelihood of significant problems related to this.

Australia and New Zealand are both highly-developed and relatively very safe countries with crime rates that are low even by Western standards. While a major event will invite opportunistic thieves and scammers, travelers who maintain good personal security practices should not encounter much trouble.



Source: <https://www.fifa.com/fifaplus/en/tournaments/womens>

Key Threats



The most likely sources of major protest are the athletes themselves, due to controversies over actions by national soccer federations.



The official World Cup app could be impersonated in order to steal information such as banking details.



Ticketing scams are common at major sporting events.



Tourists are attractive targets for street crime such as theft.



Dual-country hosting means events that disrupt travel could be more problematic than normal.



Tensions between local and Chinese fans could escalate due to regional political issues.

Key Findings

- Hosting the World Cup across two countries may cause scheduling and transportation issues.
- Geopolitical tensions—particularly between China and Australia—do exist, but on the whole this World Cup is far less controversial than the Qatar 2022 Men's World Cup event.
- Scams targeting tourists are likely to occur in downtown areas near stadiums.
- Fraudulent ticketing apps are a near certainty.
- Issues over gender-parity pay with the Men's World Cup participants could emerge during the games.
- Alcohol-induced crime and disorder is likely.



Challenges of Dual-Country Hosting

The 2023 Women's World Cup will be split roughly 50/50 between Australia and New Zealand. For the Group Stage, each group will be held entirely within one country, with New Zealand hosting A, C, E, and G and Australia hosting B, D, F, and H. Half of the knockout stages up to the semifinals will be held primarily in New Zealand and the other half entirely in Australia, with the finals and third-place game both occurring in Australia.[1]

This splitting creates the potential for problems to arise in travel between the two countries. Australia and New Zealand are "close" neighbors in concept but are, in fact, more than 4,000 kilometers apart. Though the schedule has been designed to minimize the number of teams that will have to fly that distance, it was not possible to entirely eliminate it. Whichever teams advance in Groups E and G will play group stages in New Zealand and then fly to Australia for a knockout match. The advancing teams from those knockouts will then fly back to New Zealand for the quarterfinals and potentially back to Australia for the finals or third-place game. Notably, this may happen to the U.S. team, as it is seeded into Group E. Not only will the team have to travel, but so will fans who have come to support their favorite players.

Uneven weather patterns are another concern. Due to the distance, one of the hosts could experience perfect weather while the other has torrential rain that forces the delay of multiple games. This might force rescheduling of games, throwing the travel plans of thousands of fans into chaos.

Game Locations for the 2023 Women's World Cup



Source: <https://www.roadtrips.com/soccer-packages/2023-womens-world-cup/venue-and-map/>

World Cup App

Tickets for World Cup games will be purchased and stored on the Official FIFA Women's World Cup 2023™ mobile ticketing app.[2] Centralizing the ticketing process through this single official app should reduce potential sources of confusion but does carry risks should it be compromised, and fraudulent imitator apps are nearly certain to appear.

Tickets for the games will be purchased on [Fifa.com/tickets](https://fifa.com/tickets) and can be accessed close to the game start dates via the mobile ticketing app. The link between the two is the email address used. This means that, should a scammer compromise a user's email address, they would be able to access that user's tickets. Tickets purchased for guests can be forwarded, again via email, creating opportunities for scams that prompt inadvertent ticket forwarding.[3]

Fraudulent imitator apps are also a near-certainty. Scammers will create these fake apps and entice unwary users to download them, at which point a variety of scams are possible. The fake app may track user activity, attempt to steal stored emails/passwords/bank credentials, or offer fraudulent ticket sales in order to farm payment information directly.[4]

Assessment:

- It is much easier for scammers to create fake apps than it is to directly attack the official app.
- A compromise of the official app would be high-impact, while imitation apps are low-impact.

Recommendations:

- Users should ensure they only download the official app, preferably via a link from FIFA's official website.
- Tickets cannot be purchased on the app, so if users are prompted to enter payment details they should delete and uninstall.
- Users should exercise caution when transferring tickets to guests.

FOOTNOTES

- [1] <https://olympics.com/en/news/fifa-women-world-cup-2023-full-schedule>
[2] <https://www.theworldcupguide.com/using-the-mobile-tickets-app-for-2023-world-cup/>
[3] <https://www.youtube.com/watch?v=tNq4qo7RQ2I>
[4] <https://www.spiceworks.com/it-security/security-general/news/fifa-world-cup-scams/>



| Pickpocketing and Theft

The influx of tourists gathering for the World Cup increases the threat of street crime such as pickpocketing, snatch-and-grabs, and the like. Street crime is the most prevalent form of crime in the major cities of Australia and New Zealand [5, 6], as these cities have vibrant downtown areas that attract potential victims. Many of the World Cup attendees will spend time in these areas when not attending games. Australian heatmaps of crime statistics tend to show an elevated number of crimes in the population-dense Central Business Districts, which then immediately drop off when going to the direct neighboring suburbs before picking up again when reaching the poorer outer suburbs [7]. New Zealand follows the same pattern, though with even lower overall crime rates [8].

Most fans able to travel for the games are unlikely to find themselves in the most dangerous suburbs, which in Australian cities tend to be located tens of kilometers from the city center and stadiums. However many will make use of public transit infrastructure such as Sydney's Metro and Light Rail or the Melbourne Tram system. Trains are the fifth most common location for crime, as thieves can quickly approach and escape from targets [9].

► Assessment:

- Pickpocketing and other types of street theft are major forms of crime in central business districts and in/around stadiums.
- Public transit such as trains are also attractive zones for thieves.

► Recommendations:

- Travelers should keep wallets and other valuables in a secure place on their person.
- Practice situational awareness of those around you, especially when moving through a crowd.
- Hold on tightly to the main body of bags, purses, backpacks, and the like, not just the strap (which can be easily cut).

| Geopolitical Tensions

Watching a national soccer team tends to fill fans with pride in their country. While this is generally a positive, it can turn dark when national rivalries swell as a result of events happening on or off the pitch. During the 2022 World Cup, Argentine and Mexican fans came to blows in advance of a critical game, resulting in many injuries [10].

Adding alcohol to the mix further raises the possibilities for fan violence. New Zealand and especially Australia have major drinking cultures and large amounts of bars and nightlife [11]. When groups of fans encounter each other, especially while inebriated, many different circumstances can cause an eruption of violence. Controversial plays, upcoming elimination matches, or insults against star players are all common flashpoints. It is impossible to predict which teams might be most affected by this, though a good principle is nations that neighbor each other and have a fraught shared history are more at risk. For example, Japan, South Korea, and China have longstanding tensions related to the legacy of World War II, so if any pairing of those occurs the likelihood of fan violence increases.

One possible flashpoint involves Chinese and Australian fans and is due to geopolitical tensions rooted in local issues. Australia has welcomed many Chinese immigrants, such that there is a strong local community of Chinese-Australians who recognize a national heritage but consider themselves fully Australian in life outlook. Australia has also welcomed many Chinese students, who come to the country for school but plan to return to China thereafter. There are major tensions between more Western-aligned Chinese-Australians and the Chinese students over issues of political freedom of expression. These tensions were recently inflamed by Beijing's insistence that Australia cease "harboring" dissidents who were involved in the Hong Kong protests during 2019 [12]. The Australian government has refused, insisting that these individuals have done nothing illegal by expressing their political opinions, a position broadly popular among Australian citizens.

FOOTNOTES

[5] <https://my.police.qld.gov.au/>
[6] <https://www.crimestatistics.vic.gov.au/>
[7] <https://www.crimestatistics.vic.gov.au/crime-statistics/latest-crime-data-by-area>
[8] <https://www.police.govt.nz/crime-snapshot>
[9] <https://www.crimestatistics.vic.gov.au/>

[10] <https://www.express.co.uk/sport/football/700891/world-cup-violence-qatar-mexico-argentina-fans-clash>
[11] https://www.vicheadth.vic.gov.au/sites/default/files/drinking-related-lifestyles_Summary.pdf
[12] <https://www.npr.org/2023/07/03/1185795838/hong-kong-arrest-warrants-activists-nathan-law>



| Social Engineering

Social engineering poses one of the greatest threats to organizations and spectators participating in the 2023 Women's World Cup. There is likely to be a spike in tournament-related lures both in the lead-up to and during the event, as threat actors will aim to capitalize on heightened global interest to harvest credentials, deploy follow-on payloads, and conduct financial fraud.

Social engineering campaigns during the World Cup are almost certain to vary in complexity from low-level, rudimentary email and SMS-based scams targeting mass audiences to sophisticated spear phishing attacks directed at specific organizations and individuals associated with the tournament, such as diplomats, journalists, and high-profile executives [13]. Most lures are very likely to use trademarks from FIFA and tournament sponsors to appear legitimate, as well as attempt to impersonate businesses operating in support of the event, such as hospitality, retail, and travel companies. The most prevalent scams and fraudulent activity observed in previous tournaments [14] include:

- Fake lottery win notifications
- Illegitimate accommodation and local experience offers
- Malicious streaming and gambling sites
- Counterfeit ticket and merchandise sites

> Assessment:

- The Women's World Cup is an attractive hunting ground for scammers, as many social engineers can find success using the games as initial lures.
- Scams can be simple (such as mass-sent SMSes) or highly complex (involving sophisticated duplication of legitimate materials).

> Recommendations:

- Visitors should stay vigilant about messaging from people they do not know or suspicious communications from people they do know.
- Remember that "if it sounds too good to be true, it probably is."

| Cyberattacks

As one of the most-watched and lucrative global events, the World Cup has become a prime target for both financially and politically-motivated actors. As such, threat actors will almost certainly leverage the tournament to target fans, organizations, and host-nation entities; cyber risks will significantly increase for brands and sponsors associated with the World Cup, as well as football clubs and governing bodies.

Cyberattacks against high-profile sporting events are an omnipresent risk. For instance, Russia claimed to have experienced roughly 25 million attacks while hosting the men's tournament in 2018 [15], and South Korea's Winter Olympics in 2018 were targeted by North Korean attackers [16]. However, France's 2019 Women's World Cup was largely spared, as was Qatar's 2022 Men's World Cup.

While criminal actors targeting the games could originate anywhere, if nation-state attacks do occur against Australia and New Zealand they will most likely derive from China. A spate of cyberattacks against Australian businesses and government agencies throughout 2022 was attributed to state-sponsored hacking groups in the People's Republic of China [17]. While tensions between Australia and China have been gradually easing, this does not fully preclude the possibility of an attack. Russia could also be an originator, with the Kremlin seeking to punish Australia for its continued support of Ukraine during Russia's ongoing invasion.

> Assessment:

- Cyberattacks are always attempted against high-profile events, though not all events see serious nation-state efforts.
- Australia and New Zealand are relatively unlikely targets, but both China and Russia have potential rationales for carrying out attacks.

> Recommendations:

- Organizations involved with event sponsorship or located in countries which Russia or China deem as hostile should be extremely vigilant against potential cyberattack activity.
- Organizations should remain aware of geopolitical developments throughout the event which could elicit a hostile cyber reaction.

FOOTNOTES

[13] <https://www.group-ib.com/media-center/press-releases/scammers-on-the-pitch/>

[14] *Ibid*

[15] <https://www.securityweek.com/russia-targeted-almost-25-million-cyber-attacks-during-world-cup-putin/>

[16] <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>

[17] <https://www.skynews.com.au/australia-news/chinese-cyber-attack-on-australia-targets-defence-and-energy-information-in-months-long-hack/news-story/23f5f01c93e7b5827120bf48c4def67>



Potential for Protests

Major sporting events often bring protests, as they create a platform for political speech. Notably, during this World Cup there is greater potential for protests by the players themselves than by outside groups.

Women's soccer has historically been the "lesser cousin" [18] to the men's game in the eyes of the national federations that govern a country's overall programs. The U.S. Women's team, despite achieving much greater on-field success than their male counterparts, were engaged in a long-running dispute with the U.S. Soccer Federation over the issue of pay equality. Though the American team resolved this dispute in 2022 [19], many other teams participating in the tournament are still engaged in fights over both pay issues and allegations of sexual harassment that their federations ignored or swept under the rug. Canada's team played matches earlier this year under protest due to their federation's reticence on pay equality. [20] Similarly, Nigeria's national team saw its pre-tournament camp cancelled, prompting their coach to speak out about the lack of support provided by the federation. Rumors are swirling that the team may forfeit its first match of the group stage in protest. [21]

Protests off the field do also remain possible. Australia has recently seen a spate of disruptive climate change activism—petroleum company Qatar Energy in particular may be a target. A protest targeting sponsor Optus over its data breach last year could also arise.

Assessment:

- Major protests are more likely to occur on the field from players and/or teams than off due to controversies involving national soccer federations.
- The likelihood of protests becoming violent is low.

Recommendations:

- Spectators should not be surprised to see athletes taking a stand for the cause of equality.
- Visitors to games are encouraged to anticipate security arrangements to prevent in-stadium protests by spectators and budget time accordingly.

APPENDIX:

Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that
TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use TLP: CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400

FOOTNOTES

- [18] <https://www.yahoo.com/entertainment/watch-only-men-apos-soccer-191909717.html>
[19] <https://www.nytimes.com/2022/02/22/sports/soccer/us-womens-soccer-equal-pay.html>
[20] <https://www.cnn.com/2023/02/16/football/canada-soccer-pay-dispute-intl-spt/index.html>
[21] <https://www.dailymail.co.uk/sport/football/article-12277433/Nigeria-BOYCOTT-opening-match-Womens-World-Cup-ugly-pay-dispute.html>

