

Introduction

The 2022 Qatar FIFA World Cup runs from November 20 until December 18, 2022. Qatar has been a controversial host since corruption allegations emerged shortly after both Russia and Qatar were awarded hosting rights for the 2018 and 2022 World Cups, respectively, at a ceremony in 2010.[1] Controversies have continued, with the tournament needing to be moved from the traditional Northern Hemisphere off-season summer period to the mid-season winter period to accommodate Qatar's climate. However, the greatest controversies surround the infrastructure projects needed to host the event, which are vast in a small nation not accustomed to hosting international sporting events. Allegedly, 6,500 largely-migrant workers have died building the stadiums, and thousands more continue to be mistreated according to Amnesty International. This prompted calls for a boycott of the event, which have not materialized to date. However, symbolic acts of protests by teams and spectators inside stadiums are likely during the event, which could harm sponsor reputations and lead to a crackdown by security forces that have little tolerance for dissent. Protests against the politics of a participating nation could lead to geopolitical disputes that impact the tournament as well. The Human Rights record of Qatar and Iran, as well as the war in Ukraine, remain the likeliest causes of geopolitical disruptions during the event. A month prior to the tournament, hacktivists from Anonymous collective launched an operation calling for Ukraine to replace Iran at the tournament over Iran's military support to Russia. The group also called for political pressure to be applied.

While Qatar is considered overall to be a safe country—and major acts of terrorism or violence are unlikely—there are still physical security concerns. An estimated 1.5 million visitors are expected in Qatar; this amounts to a 50 percent increase in the local population and could lead to stresses on transportation infrastructure and the close grouping of eight stadiums. This will also put pressure on Qatar's limited accommodation facilities, where prices have quickly become unaffordable.

During the World Cup, there will likely be threat actors aiming to acquire personal information or monetary value through phishing and scams. Cyber threat actors may target the confluence of logistical issues with accommodation, ticketing, and betting scams. These will range in complexity from basic mass SMS scams to attacks on specific individuals and organizations. Many scams will leverage the wide array of sponsors and impersonate well-known brands operating logistics and accommodations in Doha. Qatar itself requires visitors to download two apps that could expose personally-identifiable information (PII) and other sensitive data; other fraudulent mobile and payment apps will likely be leveraged by threat actors throughout.

Key Threats



Human rights activists are encouraging boycotts and other protest activities, including hacktivism.



World Cup accommodations and transportation are inadequate.



Ticketing scams are common at major sporting events.



Threats will change as the tournament goes on, depending on which nations advance.



Financially-motivated threat actors will seek to leverage fake mobile apps.



Sponsor and brand impersonation is likely.



Qatar requires visitors to download two apps that could expose PII and other sensitive data.



Russian-backed groups are the most likely source for a nation-state cyberattack.

Key Findings

- Threats will be modified as the tournament goes on, depending on which nations advance.
- Accommodations are sparse and extremely expensive, but the limitations could ease as fewer teams advance.
- Acts of symbolic protests inside stadiums are likely.
- Qatar's housing and transportation infrastructure will be strained during the tournament, particularly at the beginning.
- The threat of terrorism during the games is currently considered low.
- Betting and ticketing scams are highly likely.
- Politically-motivated hacktivism is highly likely, in the lead up to and during the World Cup
- Social engineering leveraging tournament-related lures is anticipated as threat actors will aim to capitalize on heightened global interest to harvest credentials, deploy follow-on payloads, and conduct financial fraud.



Physical Security

Qatar's developed economy and advantageous geographic location shields it from much of the instability seen in other Middle Eastern countries. Its strong internal security apparatus maintains stability at the expense of freedoms for residents. Crime levels are generally low, but—as with any large sporting event—petty crime, including pickpocketing, could occur. Qatar has also maintained relatively good relations with its neighbors, even when those neighbors are in conflict with each other, mitigation the risk of threats from neighboring governments.

Though unlikely, threats of terrorism cannot be ruled out. A global sporting event is a tempting target for terror groups operating in the region. The United States, the United Kingdom (UK), France, Italy, Pakistan, and Turkey are contributing soldiers, intelligence services, anti-drone technology, riot police, and even warships that will assist in monitoring for and responding to various threats, including terrorism. Qatar has also expanded its Air Force with new Eurofighter Typhoon jets that will operate in an anti-terror capacity during the World Cup. Terror groups would need to overcome multiple layers of security in order to successfully conduct an operation.[2]

The possibility of large-scale hooliganism is unlikely due to the strong security posture and low tolerance from Qatari security, but cannot be ruled out. During the end of the European season in May 2022, there were several acts of hooliganism, and so localized hooliganism on a smaller scale is likely.[3]

The greatest physical threat will come from issues of overcrowding. Qatar is roughly the size of Jamaica, with a population of three million people. It is estimated that the World Cup will draw 1.5 million visitors, increasing the population by 50 percent in a short amount of time. While much of the World Cup-specific infrastructure was constructed with this in mind, other parts of the country—including the Doha metro—may quickly become overcrowded. Security staff will be posted to ensure smooth and uninterrupted movement from one place to the next.[4] The metro only reaches five of eight stadiums, which may overwhelm private transportation services and clog roadways.

> Assessment:

- Qatar's stability and good relations with neighbors makes threats from internal dissidents or neighboring governments unlikely.
- Heavy security investment from international partners will make it difficult for terror groups to conduct attacks.
- The unpredictability of large crowds will be the greatest physical threat faced by most attendees.

> Recommendations:

- Keep personal belongings, including passports, somewhere that they cannot be easily pickpocketed.
- Beware of overcrowding in tight terminals and follow directions of security staff posted to maintain crowd flow.
- Leave the area immediately if it appears the crowd could become unruly.

Broader Geopolitical Context

Qatar was a deeply controversial choice to host a World Cup. Teams are under pressure to protest the host nation's human rights record, which could see other geopolitical disputes between nations elevated. Activists allege that over 6,500 workers died while constructing World Cup infrastructure, leading many activist groups and governments to call for a boycott of the event. Qatar's status as the world's largest exporter of natural gas may incentivize some countries, especially those from Europe, to overlook these issues in the name of maintaining good relations. Athletes and civil society groups are not bound by this interest, however. This could play out through increased instances of on-field demonstrations against Qatar by athletes or activists.

Russia's war in Ukraine could also become relevant, as Russia has been banned from most international soccer activity and may view targeting the tournament as a key way to demonstrate discontent.

Recent diplomatic developments in the Middle East could also have an effect. Several Arab countries—including the United Arab Emirates (UAE), Bahrain, and Morocco—have recently normalized relations with Israel. This has received a mixed response from both citizens and other countries in the region, with protests occurring against these developments. Qatar and Israel have had ties for over two decades, though the broader context of regional engagement with Israel could heighten tensions between fans and athletes from majority-Arab countries versus those from Israel.

Finally, the ongoing protests in Iran could resurface in key matches involving Iran and the United States or the UK. Athletes may make shows of support for protesters on the field. There are calls for FIFA to ban Iran entirely from the tournament.

> Forward Look:

- Recent protests in Iran could resurface during key matches involving Iran and the United States or the UK.
- Neither Russia nor Ukraine are involved in the tournament, but shows of support for Ukraine or opposition to Russia could lead to elevated geopolitical tensions. This could take the form of Russian-backed cyber groups attempting to disrupt the games or broadcast. Something similar happened during the Eurovision song contest, which Russia was banned from and Ukraine won.[5] After disrupting an attempted Distributed Denial of Service (DDoS) attack, Italian cyber police were targeted.

> Recommendations:

- Avoid public areas where protest activity is occurring, as such activity could draw a response from security personnel or counter-protesters and lead to scuffles or greater violence.

FOOTNOTES

- [1] <https://www.nytimes.com/2020/04/06/sports/soccer/qatar-and-russia-bribery-world-cup-fifa.html>
- [2] <https://www.france24.com/en/sport/20221006-france-to-contribute-officers-to-world-cup-security-in-qatar-amid-calls-for-boycott>
- [3] <https://www.espn.com/soccer/fifa-world-cup/story/4767017/uk-bans-1300-fans-from-england-wales-at-world-cup>
- [4] <https://www.middleeasteye.net/news/qatar-world-cup-civilians-conscripted-security-duties>
- [5] <https://www.reuters.com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/>



Boycott and Protest Activity

Qatar restricts most forms of protest, but there will be significant international pressure to accommodate public dissent during the World Cup. International activists are calling for protests against Qatar's human rights record and alleged treatment of women, minorities, and migrant workers. Migrant workers themselves protested against nonpayment of wages as recently as August, when they shut down a major road in Doha. It is not clear how many migrant workers will remain in Doha during the World Cup, and security forces will likely be on the lookout for worker gatherings to head off any potential unrest.

Several French cities, including Paris, Lille, Marseille, Bordeaux, Strasbourg, and Reims, are refusing to set up public viewing areas for the World Cup in protest of Qatar's environmental and human rights record. Denmark has also released "protest kits" that include an all-black uniform to honour migrant workers who died in the lead-up to the World Cup. The monochromatic jerseys do not violate FIFA's ban on political statements on uniforms.[6] Similar on-field protests from other teams can be expected as well. The English team is having its captain wear a "one love" anti-discrimination armband to protest Qatar's law banning homosexuality. Activists have accused Qatar of arresting and abusing LGBTQ+ citizens as recently as October 2022.

Environmental activists have criticized Qatar for the large amount of outdoor air conditioning expected to be used during the World Cup. Climate activists have targeted sporting events in recent years, with one protester briefly setting his arm on fire at the 2022 Laver Cup to protest the use of private jets.[7] Smaller, individualized protest actions such as this would be easier to carry out during the World Cup than larger, coordinated actions.

Accommodation Issues

Qatar's relatively small size and low population means that much of the accommodations available for the World Cup were built for that purpose. The government has worked to provide accommodations at a range of prices, though attendees should expect to pay significantly more than a standard hotel stay. In addition to hotels, apartments, fan villages, and cruise ships, the Qatar Accommodation Agency will also release an app enabling visitors to stay with local families, similar to Airbnb or Vrbo.[8]

Attendees can get around via the Doha metro and express buses used for the World Cup; both are free of charge to attendees. The Doha metro will be accommodating roughly 500,000 passengers daily; this is five to six times its normal ridership, so overcrowding is possible. Security staff will be posted to ensure smooth crowd movement from one place to the next.[9] Another item to note is that Qatar's metro system only reaches five of the eight stadiums. Users are required to download the Hayya app that handles both match tickets as well as the metro. In addition to the numerous documented privacy issues with the app, threat actors may seek to impersonate the app to gain access to users' proprietary information. Apps impersonating well-known hotels or other accommodations services are likely.

To gain entry to Qatar, visitors must prove they are COVID-19-negative. All visitors aged six and over must show proof of a negative PCR test taken within 48 hours of their departure. Alternatively, visitors can show a negative result from a rapid antigen test taken up to 24 hours before arrival. Rapid antigen tests must be from an official medical center, not self-administered. Visitors will also be required to download a contact-tracing app before entry. Masks will be required on public transport, but vaccination is not required for the event as a whole.[10]

Qatari laws restrict expression, conduct, and sexual preference. Punishments are severe by Western standards, but it remains to be seen how strictly laws will be enforced for attendees. Qatari authorities have stated attendees could escape prosecution for minor offenses.[11] Authorities have notably not guaranteed that LGBTQ+ visitors will be shielded from local laws restricting homosexuality, though FIFA spokespeople have stated they are confident LGBTQ+ individuals will not be targeted by security services.[10] Attendees are advised to familiarize themselves with local laws ahead of time. Lastly, acts of drunkenness are unheard of in Qatar, which could lead to mass arrests or see visitors removed from their hotel or other World Cup venues.

> Assessment:

- Qatar faces international criticism for its record on human rights, treatment of migrant workers, and environmental policies.
- Large scale physical protests are rare in Qatar and unlikely at this event. However, symbolic demonstrations from players and spectators are likely especially during game broadcasts which will gain them more publicity.

> Recommendations:

- Be mindful that demonstrations of support for causes like LGBTQ+ rights, Qatar has a record of quickly clamping down on protests. The first ever LGBTQ protest ended in arrest on October 25.
- Avoid areas where protests are taking place, as this could draw a response from security forces.
- Be mindful that wearing "protest kits" in public may elicit a response from security forces.

FOOTNOTES

- [hXpss://www.theguardian.com/football/2022/sep/28/denmark-unveil-world-cup-protest-kits-over-qatar-human-rights-record](https://www.theguardian.com/football/2022/sep/28/denmark-unveil-world-cup-protest-kits-over-qatar-human-rights-record)
- [hXpss://www.bbc.com/sport/tennis/63014086](https://www.bbc.com/sport/tennis/63014086)
- [hXpss://www.cnn.com/2022/09/09/sport/qatar-olympic-housing-mime-spt-intl/index.html](https://www.cnn.com/2022/09/09/sport/qatar-olympic-housing-mime-spt-intl/index.html)
- [hXpss://thepeninsulaqatar.com/article/06/10/2022/doha-metro-ready-for-world-cups-500000-daily-passengers](https://thepeninsulaqatar.com/article/06/10/2022/doha-metro-ready-for-world-cups-500000-daily-passengers)
- [hXpss://www.middleeastmonitor.com/20220929-qatar-confirms-covid-test-requirements-for-world-cup-fans/](https://www.middleeastmonitor.com/20220929-qatar-confirms-covid-test-requirements-for-world-cup-fans/)
- [hXpss://www.france24.com/en/sport/20221006-france-to-contribute-officers-to-world-cup-security-in-qatar-amid-calls-for-boycott](https://www.france24.com/en/sport/20221006-france-to-contribute-officers-to-world-cup-security-in-qatar-amid-calls-for-boycott)
- [hXpss://www.theguardian.com/football/2022/jun/29/qatar-fails-to-offer-world-cup-safety-guarantees-to-lgbtq-fans](https://www.theguardian.com/football/2022/jun/29/qatar-fails-to-offer-world-cup-safety-guarantees-to-lgbtq-fans)



Cybersecurity Threats

As one of the most-watched and lucrative events in the world, 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. Qatar has reportedly invested over USD one billion in improving its cybersecurity framework over the last 10 years in preparation for the World Cup.[12] However, the volume of cyberattacks that Qatar will face is likely to be immense. For instance, Russia claimed to have experienced roughly 25 million attacks while hosting the tournament in 2018.[13] More so, with major sporting events becoming increasingly digitized, the attack surface for threat actors has also increased. Qatar has constructed eight state-of-the-art “smart stadiums” specifically for the World Cup, meaning sophisticated threat actors will almost certainly aim to compromise networks by exploiting vulnerabilities within interconnected stadium systems, including operational technology and Internet of Things (IoT) devices.

Social Engineering

Social engineering poses one of the greatest threats to organizations and spectators participating in the Qatar World Cup. Threat actors have been leveraging the event as a theme for some time, with phishing campaigns identified as early as 2019.[14] However, as observed in previous iterations of the 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. 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 include:

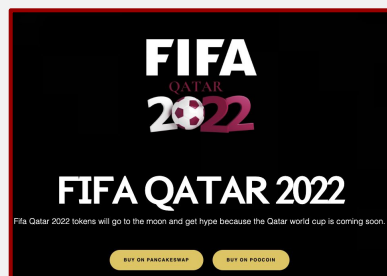
- Fake lottery win notifications
- Illegitimate accommodation and local experience offers
- Malicious streaming and gambling sites
- Counterfeit ticket and merchandise sites

Notably, ZeroFox Intelligence identified phishing sites posing as known bookie sites. The site [fifa-bet365\[.\]com](http://fifa-bet365[.]com) masquerades as a popular sports bookie site, [bet365\[.\]com](http://bet365[.]com). The translated text on this site attempts to excuse the fact that their advertised “mobile app” is not directly searchable. The domain [fifa-bet365\[.\]com](http://fifa-bet365[.]com) was created and updated on September 22, 2022, and there is no indication it is a genuine domain affiliated with [bet365\[.\]com](http://bet365[.]com), which was originally registered in 1999.



Source: [fifa-bet365\[.\]com](http://fifa-bet365[.]com)

Threat actors have also been observed exploiting the growing popularity of cryptocurrency, combining World Cup lures with crypto tokens. The site [fifaqatar-2022\[.\]com](http://fifaqatar-2022[.]com) advertises a crypto token based on FIFA QATAR 2022 and is available for trading on a decentralized token exchanged called pancakeswap. This domain is associated with that email address [flokisquidgrow@gmail\[.\]com](mailto:flokisquidgrow@gmail[.]com), which is related to another crypto scamming site, [qatar2022bsc\[.\]site](http://qatar2022bsc[.]site).



Source: [fifaqatar-2022\[.\]com](http://fifaqatar-2022[.]com)



Forward Look:

- Expect that in the lead-up and throughout the World Cup, threat actors will leverage the event as a lure due to the high international visibility of the event.
- Trademarks for FIFA and tournament sponsors are likely to be utilized in scams and illegal activity as a means of adding legitimacy to campaigns.
- Cryptocurrency scams are likely to grow in popularity as threat actors become more proficient in leveraging these scams.

Recommendations:

- Utilize caution when accessing sites associated with the World Cup, and always review for legitimacy prior to clicking on any email links.
- For event sponsors, ensure that legitimate messaging is frequent and clear to get ahead of campaigns leveraging those brands.

FOOTNOTES

[12] [https://www.sportico\[.\]com/business/tech/2022/qatar-world-cup-security-spending-cyber-threats-1234690532/](https://www.sportico[.]com/business/tech/2022/qatar-world-cup-security-spending-cyber-threats-1234690532/)

[13] [https://www.infosecurity-magazine\[.\]com/news/russia-fends-off-25-million-world/](https://www.infosecurity-magazine[.]com/news/russia-fends-off-25-million-world/)

[14] [https://www.onlinethreatalerts\[.\]com/article/2019/4/30/the-qatar-2022-fifa-world-cup-with-microsofts-online-lottery-scam/](https://www.onlinethreatalerts[.]com/article/2019/4/30/the-qatar-2022-fifa-world-cup-with-microsofts-online-lottery-scam/)



► Hacktivism

ZeroFox Intelligence assesses with high confidence that politically-motivated hacktivists will attempt to disrupt the World Cup. Hacktivists often target high-profile events, particularly those that garner a global audience, as these present the opportunity for threat actors to gain notoriety while providing maximum exposure. Hacktivism is most likely to occur through disruptive attacks such as DDoS and website defacements; these have become prevalent during major sporting events and are typically launched in an attempt to interrupt services that are essential to the occasion, including broadcasting and tournament-related websites.

During the FIFA World Cup Brazil 2014, multiple hacktivist collectives conducted large-scale DDoS attacks on Brazilian targets, impacting the websites of several government entities and tournament sponsors. This included the “#OpWorldCup” campaign by Anonymous, which targeted the event due to perceived corruption and inequality in the country.

ZeroFox Intelligence anticipates a spike in hacktivism during matches that involve Iran. On 24 October, 2022, Anonymous announced that it would be launching the #OpWorldCup campaign specifically for the tournament in Qatar.[15] In a statement directed at FIFA, the collective is demanding that Iran be removed from the tournament and replaced with Ukraine due to Russia’s reported use of Iranian drones during the ongoing conflict.

Pro-Russian hacktivist collectives, such as Killnet, also pose a significant threat to the World Cup, as such groups continue to launch persistent disruptive attacks on Western targets in retaliation for opposition towards Russia following its invasion of Ukraine. In May 2022, Killnet attempted to disrupt both the semi-final and final of the Eurovision contest hosted by Italy, from which Russia had been banned from participating.[15] In October 2022, Killnet conducted a series of DDoS attacks on U.S. organizations, temporarily causing the websites of at least 14 airports to go offline and disrupting the websites of several U.S. government entities.[16] With Russia also banned from participating in the World Cup, it is likely that groups such as Killnet will look to cause disruption to the tournament directly or by targeting sponsoring organizations, particularly those from Western nations.

The subject of human rights is likely to encourage politically-motivated hacktivism at the World Cup; the reported mistreatment of migrant workers in Qatar over the last decade almost certain will be one of the main motivations behind any attacks. Also, given that Qatar marks the first time the World Cup will be hosted in the Middle East, hacktivists are likely to view the tournament as a platform to amplify human rights causes within the region. Recent widespread unrest in Iran could contribute to an increase in hacktivism throughout the event. Notably, in October 2022, Iran’s state-run broadcast was interrupted as part of ongoing human rights protests within the country, highlighting an increase in politically-motivated hacktivists’ intent to target state entities during escalated tensions.[17]

► Nation-State Activity

ZeroFox Intelligence assesses with low confidence that nation-state or state-sponsored actors will leverage the World Cup to target the host nation and sponsoring organizations. In recent years, major sporting events have been subjected to sophisticated attacks by state-backed threat actors conducting cyber espionage, as well as to discredit and embarrass host nations.

During the opening ceremony of the 2018 Winter Olympics in South Korea, malware known as Olympic Destroyer was deployed against the event’s infrastructure, shutting down display monitors and Wi-Fi connections—as well as the official Olympic Games website. A similar attack was conducted at the 2020 Summer Olympics in Tokyo, with both campaigns later attributed to Russian state-sponsored threat actors.[18] Disruption was the objective in these attacks, likely with the aim to cause embarrassment to the Olympic committee and host nation.

State-sponsored attacks during the World Cup are most likely to involve sophisticated techniques that will allow threat actors to maintain persistent, undetected, and long-term access in compromised environments. While unlikely, disruptive attacks similar to those observed at the 2018 and 2020 Olympic Games cannot be ruled out.

Given the geopolitical situation, the main threat is likely to originate from Russian-backed groups. Russia’s expulsion from the tournament by FIFA is also very likely to contribute towards an increased intent to cause disruption to the event. Russia has a history of leveraging cyber criminal groups to advance foreign policy goals while maintaining plausible deniability—and could utilize this tactic during the World Cup. State-sponsored groups based in the Middle East, such as those from Iran and Saudi Arabia, are also likely to view the World Cup as an opportunity to conduct cyber espionage campaigns due to the global attention the World Cup will bring to the region, as will groups originating from China and North Korea.

FOOTNOTES

- [15] [https://anonymous-france\[.\]info/anonymous-operation-world-cup-is-now-operational.html](https://anonymous-france[.]info/anonymous-operation-world-cup-is-now-operational.html)
 [16] [https://www.reuters\[.\]com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/](https://www.reuters[.]com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/)
 [17] [https://www.bleepingcomputer\[.\]com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/](https://www.bleepingcomputer[.]com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/)
 [18] [https://news.sky\[.\]com/story/iranian-state-tv-hacked-as-women-protesters-tell-president-raisi-to-get-lost-12/16160](https://news.sky[.]com/story/iranian-state-tv-hacked-as-women-protesters-tell-president-raisi-to-get-lost-12/16160)
 [19] [https://www.sentinelone\[.\]com/wp-content/uploads/2022/05/POSSIBLE-THREATS-TO-FIFA2022.pdf](https://www.sentinelone[.]com/wp-content/uploads/2022/05/POSSIBLE-THREATS-TO-FIFA2022.pdf)



Mobile App Security

Everyone 18 and above entering Qatar for the World Cup will be required to download two apps called Ehteraz and Hayya. Ehteraz is a COVID-19 tracking app, while Hayya is an app used for World Cup game tickets and accessing the Qatar metro system, which reaches five of the eight stadiums. In May 2020, Amnesty's Security Lab discovered serious privacy flaws within the Ehteraz app, which has since been updated. However, these exposed vulnerabilities are likely to have gained the attention of threat actors and could be targeted for further compromise during the World Cup. Ehteraz also has an extensive list of required permissions that end users must accept when installing the app, which creates fundamental privacy problems. Ehteraz's ability to monitor locations and proximity to other app users, capture data from the device, and automatically exfiltrate data from a user's phone are some of the largest risks associated with the application. Ehteraz can disable a lock screen, make calls from the phone, and access location services.

The app could be used to find the location of someone who has downloaded it or with whom they are meeting. Critics fear downloading the app could give the Qatari government access to privileged or sensitive content on a user's phone. This is particularly notable if the user is breaking a Qatari law. It could also give Qatari authorities access to proprietary information contained on a company phone.

The Hayya app is able to access almost all personal information on a phone; it can access location services and network connections between a phone and other networks.[20] The secure flaws apply to Android and Apple users.

Assessment:

- Based on the information that the apps are requesting, these apps provide enough information to these two companies to allow them to access, read, and even alter content on mobile devices.
- Location access on mobile devices allows the companies to track where attendees are and at what time they are there.
- Privacy experts fear that the content that can be leveraged from mobile devices with the apps installed can pose significant privacy risks.

Recommendations:

- Remove sensitive content from all phones before installing the apps.
- Organizations are advised to prohibit employees from bringing their work phones (or any mobile devices that access work content) to the World Cup.

Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	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.
	Green	Clear
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	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

[20] <https://www.nrk.no/sport/everyone-going-to-the-world-cup-must-have-this-app---experts-are-now-sounding-the-alarm-116139267>

