+44 345 094 0945
www.waterstons.com
Article

Say ‘Hayya’ to spyware

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

Nov 2022

Say ‘Hayya’ to spyware

The 2022 FIFA World Cup has started and with Qatar expecting around 1.5 million visitors over the course of the tournament, a huge surface area for a potential cyber-attack or data breach has been created.

Categories Cyber Security Strategy, Cyber Resilience

Nov 2022

Rhianne Short

Information Security Consultant

Email

rhianne.short@waterstons.com

Organisers have asked supporters to download two apps to be able to enter the stadium:

- Ehteraz – a Covid 19 tracking app
- Hayya – Qatar’s official World Cup app, which is to be used for entering games as well as to gain free access to Qatar’s public transportation for ticket holders

This makes sense to maintain crowd control and gather data, but security concerns have been raised across both apps; Ehetraz asks users to allow remote access to pictures and videos, make unprompted calls, and read or modify device data. Hayya permissions included full network access, unrestricted access to personal data, even preventing devices from going into sleep mode. Both apps also track users' locations.

Several European governments have issued advice to mitigate privacy and security concerns, with the Norwegian Data Protection Authority stating that they are 'alarmed by the extensive access the apps require [meaning] there is a real possibility that visitors to Qatar, and especially vulnerable groups, will be monitored by the Qatari authorities' and have suggested that fans travelling to the Middle Eastern nation for the World Cup consider bringing two mobile phones.

The German data protection agency, BfDI and France's data protection authority CNIL shared similar advice, and the UK Information Commissioner's Office said it is 'aware of media reports on this matter and will consider the potential impact on the privacy rights of UK citizens'.

After users have accepted the terms and conditions of the apps, moderators could have complete control of the device, including the ability to remotely unlock it. This includes access to all personal content, the ability to edit, share and extract the data as well as access to data from other applications on your device.

As it is unclear how Qatar is securing data provided through the applications and their permissions, this could lead to further risks for fans. Without effective security controls in place, the data can be used in future cyber-attacks due to being sold on forums and marketplaces on the deep and dark webs, ultimately being used for illegal activities such as fraud, identity theft and targeted phishing campaigns.

For fans attending the World Cup games in Qatar there are a number of additional steps that you can take to protect yourself:

- If you can, use another phone solely for the use of the apps
- Before leaving, back up your phone in case it becomes necessary to restore it later
- Avoid connecting to open or unsecured WiFi networks
- Avoid using USB charging ports in hotel rooms, public transport, airports, etc. use a charger with a wall plug
- Avoid installing anything while you are away, and turn off automatic app updates, software updates, and automatic backups should also be turned off
- Remove as much personal and work data from your device as possible, including photos and videos

Unfortunately, the threat isn't just for those attending the matches in Qatar as cyber threat actors are using the attention on the World Cup to their advantage. Hundreds of phishing campaigns, malicious mobile apps and spoofed websites have started appearing, pertaining to be linked to the football tournament.

Through these attack vectors, threat actors will be attempting to steal data & credentials and download malicious software.

If you have received an email or are visiting a website related to the FIFA World Cup, remember:

- Do not click on any links from unknown senders
- Hover over any links & hyperlinks before clicking to see the full website address and do not click on any that look suspicious
- Avoid downloading apps from third parties
- Enable two-factor authentication as an extra layer of protection on your device
- Phishing emails can be reported by forwarding the email to report@phishing.gov.uk and phishing text messages can be reported by forwarding the original message to OFCOM via 7726, (which spells SPAM on your keypad). Finally, suspicious websites can be reported via the National Cyber Security Centre's scam website reporting service

If you or your team encounter any suspicious activity related to the World Cup (or anything else), or you are concerned about potentially being a target, get in touch with our team of cyber security experts who can help build your business resilience.