Cybersecurity Experts On Protecting Data At The World Cup

Cybersecurity is a serious concern for fans and corporate executives in Qatar and at home. How to protect the safety and security of data at major events.

NEW YORK, NEW YORK, USA, December 2, 2022 /EINPresswire.com/ -- With the US set to play their first World Cup elimination game in eight years, high-net worth individuals and family offices are flocking Qatar to cheer on their team. But amid this excitement, it's easy to ignore a serious concern for fans and corporate executives in Qatar and at home – the safety and security of their and their company's data.

> Your data is the goal. Whether it's a corporation, a hacking group, or a government, they're all looking to walk away with more information about you."
>
> *Mike Janke, Co-founder of DataTribe*

According to Michael Janke, Co-Founder of DataTribe, a data technology and cybersecurity incubator that works with Deliotte Cyber and other contractors overseeing security at the World Cup, protecting your data deserves as much vigilance as protecting your property. DataTribe is no stranger to major impact cybersecurity moves – they have had some of the highest-profile cyber security companies in the world today come out their seed-stage foundry, such as Dragos, Strider, Enveil, BlackCloak and SixMap. The founders of these companies come out of U.S Intelligence and classified research laboratories.
"Your data is the goal." Janke says. "Whether it's being gathered by a corporation, a hacking group, or a government, they're all looking to walk away with more information about you."

More now than ever, people are unsure how to use the never-ending stream of software and tech developed to help make living in our connected world more convenient without compromising their personal safety and privacy.

Countries have different laws and customs surrounding cybersecurity and data gathering. In Qatar, cellular data is not just monitored by government entities, it is also shared freely by that government. Of course, they'll be collecting data through apps associated with the games, but they also monitor standard device usage on any device brought into the country.

Attendees of the World Cup in Qatar are not the only people who need to worry about cybersecurity. Hacking groups often use large events as targets for online scams. The World Cup

draws extra attention due to the massive media participation and attendance from a worldwide audience. This data is incredibly valuable not just for nations and governments looking to gather intelligence, but also for criminal elements looking to steal and sell data.
Major events rely on multiple companies focused on cybersecurity to work with local governments to oversee the network and ensure that attendees are as protected as possible.

Travelers to Qatar should start by thinking critically about the device itself. If possible, use a burner device with that is minimally connected any accounts. Use the device carefully, only for necessary communication, and wipe it clean upon returning home. If it's not possible to bring a clean phone or tablet , immediately turn the device to airplane mode on arrival in Qatar and use it only on trusted Wi-Fi networks with a VPN. Know that any activity on those networks is still being monitored, so keep searches and communications to necessary information, and don't sign up for any new accounts.

There are also ways to keep current phones and tablets relatively private. Use a VPN to ensure a secure network, and download secure communications apps from companies that are transparent about how they use data and conversations. Janke recommends Signal for written communication, and Secure Communications for video chat.

"Don't be afraid to call your family," Janke says, "Just make sure you're taking a second to consider the most secure way to contact them."

Finally, attendees should be wary of posting anything on social media until returning home. Cybersecurity is not just an online concern. Criminals may monitor online activity with the goal of committing crimes in an empty home.

Even for those not travelling to attend the games, fans are still vulnerable via online scams. Be wary of any offers surrounding the World Cup. Whether it's a link for a free stream or an offer for an official jersey, scammers will entice fans into clicking on links that gather data, and in some cases steal money. Before clicking on any links on social media or in emails, take a moment to consider the source, and whether the offer is too good to be legitimate.

"Always doubt any email you get," Janke says. "Pause, and don't click on anything."

Data monitoring around the World Cup is a hot topic, but secure data is not just a concern during big events. No matter where someone uses their phone, some government, corporation, or hacker will try and often succeed in gathering data. Vacation destinations like massive hotel chains or resort parks may feel like secure places to freely use the Wi-Fi, but it's important to remember that they will use the data they collect themselves and often sell it to their partners.

Using these same techniques – keeping a phone in airplane mode and on safe networks via a VPN, using apps designed for secure communication, and even keeping a separate clean device for travel – will go a long way toward protecting data online.

Harvey Briggs
FORCE Family Office
+1 608-361-8092
email us here