This is how to avoid cyberattacks during the Fifa World Cup in Russia

Huge international sporting events are becoming significant cyberattack targets, ordinary individual attendees included. The good news is that if you're aware of how to protect yourself against cyberattacks, you can keep yourself and your devices safe while you enjoy the games.

© tevarak11 via 123RF

Because the World Cup is in Russia this year, cybersecurity is an even greater concern.

Russian international relations are fairly controversial. Russia itself is very frequently considered to be a country that engages in international cyber attacks.

At the Rio 2016 Summer Olympics, Russians were caught attacking the computer databases of the World Anti-Doping Agency. They acquired sensitive medical data on American Olympic athletes.

The wrong technology in the wrong environment can actually increase risk

Marius Coetzee 31 May 2018

As reported by David Bisson on Tripwire's *The State of Security* blog:

> *On 13 September, the World Anti-Doping Agency (WADA) said in a statement that a Russian cyber-espionage group known as APT28 or 'Fancy Bear' gained access to its Anti-Doping Administration and Management System (ADAMS) and released some information to the public.That data ultimately appeared on Fancy Bear, a site which appears to demonstrate that gymnast Simone Biles, tennis players Serena and Venus Williams, and other U.S. athletes received permission to participate in the Rio 2016 Olympics despite testing positive for substances that are banned by the International Olympics Committee.*

This year, the English Football Association will be increasing its cybersecurity measures while in Russia because it's concerned about being attacked by a Russian spy agency.

From *Reuters*:

> *The FA (English Football Association) has written a letter to soccer's governing body Fifa expressing its concerns about sensitive information such as injuries, strategies and tactics being leaked before matches during the World Cup, British newspapers said.England players and staff have been advised not to use public Wi-Fi in Russia, including the connections provided at the team hotel.*

> *According to media reports, the FA has also strengthened firewalls, introduced encrypted passwords and have strict guidelines for players regarding social media.*

But also, Russia itself may be a target of cyberwarfare. Western military alliance, Nato, is getting into cyberwarfare and Russia may be one of its top targets.

Attention Android users! Be wary of malicious apps

7 May 2018

Retired US Air Force Colonel, Rizwan Ali, wrote in *Foreign Policy*:

> *Nato embraced the use of cyberweaponry in Nato operations. This is a marked departure from NATO's historical stance of using cyber only defensively, mainly to ward off incursions against its own networks.*

As reported by Tom O'Connor in *Newsweek*:

> *In 2008, Nato bolstered its own networks by establishing the Cyber Defense Center of Excellence in Estonia after accusing Russia of launching massive cyberattacks on the Baltic State. Estonia, along with fellowBaltic States Latvia and Lithuania, as well as nearby Poland, has become the front lines for Nato's massive military buildup along Russia's borders. Nato's decision to return to its Cold War role as a war-fighting command was taken in the wake of Moscow's 2014 annexation of the Ukraine's Crimean Peninsula and other military moves in the region.*

Earlier this year, the 2018 Pyeongchang Winter Olympics faced a cyberattack which brought down their networks, including Wi-Fi. Its official website was also attacked. Russia was banned from those games due to doping suspicions. From Motoko Rich and Nicole Perlroth via *The New York Times*:

> *Internet problems before and during the opening ceremony of the Winter Olympics on Friday night are being investigated as a possible cyberattack, officials said Saturday.Sung Baik-you, a spokesman for the Pyeongchang Organising Committee, said Saturday that some technical issues 'impacted some of our noncritical systems last night for a fewhours.'Baik-you did not elaborate and said that the committee was investigating the cause. He said the attack 'did not disrupt any event or have any effect on the safety or security of any athletes or spectators.' A spokeswoman for the*

committee said a cybersecurity team was assisting in the investigation.During the ceremony, the wireless service in the stadium stopped working as soon as the ceremony began, hampering reporters and spectators who wanted to post on social media. ”

So, with all that context in mind, here’s what you need to know.

Cybersecurity threats for World Cup organisers:

These are some of the possible kinds of cyberattacks that the World Cup may be subjected to:

1. Prior international sporting events have shown that DDoS attacks to events’ computer networks are common. The networking infrastructure for the Russia World Cup’s local network, Wi-Fi, official website, and other internet services will need to be beefed up with greater capacity, IPS devices, and properly configured firewalls in order to mitigate these attacks.
2. Sergey Korolev from Russia’s Federal Security Service is making sure that default settings and weak passwords are avoided.
   “Often Wi-Fi points at hotels have vulnerabilities due to the installation of simple passwords by their management. Examples of such passwords include ‘admin,’ or ‘admin1234.’ The current checks also focus on the assessments of permissive documentation of internet providers in the regions hosting the World Cup 2018, as well as hotels, where national football teams will be based.”

   Weak configuration of networking appliances are easy targets for cyber attackers, both within and outside of Russia.

3. Sergey Perevozchikov of Russian cybersecurity firm Cyberzachita is concerned about cyber criminals intercepting all sorts of networking communications during the World Cup.

   “That will be full-fledged surveillance. Criminals can not only watch users’ actions, but also manipulate them: for example, redirecting users to a phishing page that is visually indistinguishable from the original, or bringing a notification of the need to install an important update of legal software, causing downloading of further viruses under its guise.”

   Russian cybersecurity practitioners will be on the lookout for all sorts of session hijacking attacks.

Cybercrime is everywhere because businesses aren't educating

Simeon Tassev 11 Apr 2018

Cybersecurity tips for individual attendees:

1. **Never use open Wi-Fi anywhere**. That’s Wi-Fi which isn’t password protected, which means it isn’t encrypted. If you must use Wi-Fi, use access points which have password protected encryption.
2. **The two most common ways that Wi-Fi can be encrypted, WEP and WPA2, are no longer as secure as they used to be.** When the Krack vulnerability was discovered last October, it made WPA2 even less secure than previously believed. Gradually this year, wireless routers with the more secure WPA3 encryption standard will be deployed by enterprises, offices, restaurants and cafes, and in people’s homes. But chances are most of the encrypted Wi-Fi you’ll find in Russia will use WPA2. No matter what sort of encryption your wireless access point uses, even if it does use WPA3, you should route your communications through a VPN. A VPN will encrypt your networking transmissions from your smartphone, tablet, or laptop whether or not you’re using encrypted Wi-Fi. It’s an added level of encryption either way. If a cyber attacker intercepts your internet traffic, they will have a hard time making any sense of it. Check out various VPN providers here. Some of them even provide Android and iOS apps which will make it easy for you to use the VPN with your phone.

3. If you haven't done so already, **set up a lock screen on any phones, tablets, or laptops you bring with you to Russia.** It's possible that you will lose sight of your computing device at some point. A password, PIN, fingerprint biometrics, or swipe code protected lock screen will make it more difficult for a stranger to access your device. Another good idea is to set up a location service on each of your devices. Some Android antivirus software, such as Lookout, has that feature built in, and iPhones and iPads can be located through iCloud or the Find My iPhone app. With a properly set up location service, you can use your username and password on another computing device to remotely lock your phone, tablet, or laptop and physically locate it with GPS or cell tower triangulation.
4. **Do not access your online banking or do any online shopping on your computing devices while you're in Russia.** Even with your VPN set up, that sensitive financial data and credentials will be going through Russian telecommunications infrastructure and we don't know if it'll be intercepted somehow. Get around Russia with a limited amount of Russian cash, travelers' cheques, and perhaps a Visa or MasterCard gift card with the equivalent of a few hundred or so Euros on it. Wait until you return to your home country before you commence with your online banking and shopping. And avoid using public computers to check your email.
5. **Set up full disk encryption on any laptops, phones, or tablets you bring to Russia.** Both iOS and Android, and most major PC operating systems (including Windows, macOS, and Linux) support the feature. That way if your device gets lost, a third party cannot take your storage medium out of your device to read its data without knowing or cracking your password protection. And as far as laptops are concerned, use "hibernate" or "shut down" when it's idle. That will enable your disk encryption while you aren't using your laptop.
6. **Avoid promotional USB sticks which may be given away during World Cup events.** They may contain malware that can harm your computing device! The malware could even be spyware.

If you're headed to Russia in June to watch some exciting international football games, have fun! But remain cautious, major international sporting events are major cyberattack targets.