

CONCENTRIC

CHINA

TraCR REPORT

TRAVEL CYBERSECURITY RISK

Risk Level: Extreme

Updated: October 2022

Due to substantial cyber-attack capabilities, online censorship, prolific attacks, a ban on non-state sanctioned VPNs, and inconsistent implementation of laws, China presents an extreme risk of cybercrime for travelers. State-sponsored actors target a variety of industries and organizations, specifically from the United States and other Western nations. These organizations include healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing, communications, IT, international trade, education, video gaming, faith-based organizations, and law firms.

REGION RISKS

- Foreigners utilizing non-state sanctioned VPNs may have their devices shut down remotely.
- Hackers monitor websites tied to banking accounts and other sensitive data.
- Travelers are at risk of Chinese government surveillance of local Wi-Fi networks and internet activities.
- Chinese Government security forces may confiscate electronic devices without prior notice from travelers at airports and even duplicate their hard drive.
- The Chinese government blocks many U.S. websites, including Wikipedia, Facebook, Twitter, YouTube, Instagram, and some Google services.
- Due to government monitoring of traveler's cyber and social media presence, be aware of unique local restrictions such as posting criticisms of the Chinese government.

HOW CAN YOU PREVENT BECOMING A VICTIM OF A CYBER CRIME WHILE TRAVELING?

DO...

- Contact Concentric to help conduct risk assessment to determine vulnerabilities
- Enroll in a PII removal service, such as [Eclipse*](#)
- Consider buying burner cellular devices

DO NOT...

- Leave Bluetooth and Wi-Fi enabled
- Advertise your travel on social media
- Travel with personal devices
- Connect to public Wi-Fi at hotels, airports and cafes using personal devices

HOW CAN YOU DETECT IF YOU HAVE BECOME A VICTIM OF A CYBER CRIME WHILE TRAVELING?

- Install an antivirus application
- Perform manual scans of suspected malicious files/downloads
- Enable login notifications
- Add a fraud alert to your credit card and credit report

WHAT SHOULD YOU DO IF YOU HAVE BECOME A VICTIM OF A CYBER CRIME WHILE TRAVELING?

- 1 Containment. Delete the virus source, disconnect from Wi-Fi, and change all passwords.
- 2 Remediation. Wipe devices and inform stakeholders, by phone, an incident has occurred.
- 3 Recovery. Restore data from backups if your device was wiped or stolen.
- 4 Assessment. Determine what can be done in the future to prevent further incidents.

CONTACT CONCENTRIC 24/7 IF YOU NEED ANY URGENT ASSISTANCE OR HAVE ANY QUESTIONS.

 www.concentric.io

 +1 866 828 5855

*Eclipse is a data management solution that removes sensitive personal information (PII) from the internet. In the wrong hands, personal information can be used to stalk, doxx and profile you. The less this information can be found online, the more privacy and security you have. For more information, please inquire with your Concentric contact.