CONCENTRIC

RUSSIA

TraCR REPORT

TRAVEL CYBERSECURITY RISK

Risk Level: Extreme

Updated: October 2022

Due to Russian state-sponsored threat actors past and current malicious cyber activities against regional and international adversaries, Russia presents an extreme risk of cybercrime for travelers. This risk is exacerbated for travelers from the United States and other Western nations due to their support of Ukraine and placing Russia under sanctions. Travelers in the following industries and organizations are particularly vulnerable: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing.

REGION RISKS

- Targeted ransomware attacks can occur against corporations.
- Hackers monitor websites tied to banking accounts and other sensitive data.
- Hackers masquerade as a trusted acquaintance to conduct phishing attacks.
- Russia has a surveillance system, known as System of Operative Investigative Measures, that allows the government to lawfully intercept phone calls and telephone networks operating within Russia. The government has arrested locals for violations which it deems to be harmful to the country.
- Russian security forces may confiscate electronic devices without prior notice from travelers at airports and even duplicate their hard drive.
- Russia influences accessible applications and has threatened to arrest local employees of Google and Apple that do not abide by government Internet mandates.

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 occured.
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.