

## EUROPE

# TraCR REPORT

TRAVEL CYBERSECURITY RISK

**Risk Level: High**

Updated: October 2022

Due to high-income economies, the transitioning of traditional infrastructures to online and cloud-based solutions, advanced technologies, and the growing threat of cyberattacks due to the EU's support of Ukraine in its present conflict with Russia, countries in Europe present a high risk of cybercrime for travelers. This risk is exacerbated by a high density of public Wi-Fi networks and smartphone usage but mitigated by cyber legislation and increasing cooperation between security forces.

### REGION RISKS

- Cyber attacks can plant malware on travelers' devices.
- Targeted ransomware attacks can be launched against corporations.
- False Wi-Fi spots in locations such as hotels, commuter locations, or restaurants pose an increased risk to travelers.
- Travelers' devices are also susceptible to Cryptojacking of a victim's device to mine cryptocurrencies without the knowledge of the user. Countries in Eastern Europe, such as Poland and Romania are at a higher risk of attacks due to their proximity to and support of Ukraine.

### 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\\*](#)
- Install remote wipe capability on devices

#### DO NOT...

- Leave Bluetooth and Wi-Fi enabled
- Advertise your travel on social media
- Avoid connecting to unsecured Wi-Fi at hotels, airports and cafes by using Mi-Fi devices or using cell phones as hotspots.

### HOW CAN YOU PREVENT BECOMING 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](http://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.