Staying Digitally Safe When You Travel

by Neal Jardine, BOXX Insurance

Not a day goes by that we don't hear or read about cyber attacks and the ever-evolving risks of operating in the digital age. On average, every person created 1.7 megabytes of data per second in 2020. And with increased data comes increased risk – cyber attacks increased more than 15% in 2021.

The travel industry has itself experienced cyber attacks causing disruption throughout the industry and to those that rely on it. In 2022 alone, we saw a breach of Marriott International with hackers claiming to have stolen 20 gigabytes of sensitive data, including guests' credit card information.

Theft and Crime Against Data

A cyber attack happens every 20 seconds, and hackers are highly organized. When individuals announce online over social media that they're travelling or tag themselves as away on vacation or business, it clearly marks them as a potential target to cyber criminals. The value of data is not the value to criminals, but the value to the individual that wants it back. Cyber criminals know that if they can encrypt your data, you'll pay to get it back.

Cyber attacks come in a range of forms, and most frequently through social engineering techniques: cyber criminals will target individuals by sending messages or emails pretending to be from their hotel, travel company, or tour guide with documents to sign or photos of the trip to share. Once the client downloads the photo or document, malware embedded within the file reaches out and downloads the ransomware to encrypt files. Customers are then left with one question, how much is the data, photos, and personal information stored on my device worth to me?

Social Engineering Using Your Data

Threat actors know that when travelling individuals need to make decisions quickly. Travellers are often under pressure to purchase hotel rooms, confirm plans or book tours. Not all those decisions are made with the guidance of their travel agent as they may already be on their trip. "66% of boomers are influenced by ads with informative content."

The increased use of technology to assist in travel means clients are susceptible to social engineering events. In a digital age these can come in the form of website impersonation, email spoofing, or invoicing fraud. The World Economic Forum estimates that "95% of cybersecurity issues can be traced to human error." Travellers need to be vigilant around all payments or bookings. Criminals are always looking to turn a situation into financial gain through social engineering events.

Crossing Borders with Data

Different countries around the world have different laws, restrictions, and definitions for data privacy. Carrying sensitive corporate data is a concern that needs to be taken seriously when travelling. Many counties take the position that all electronic devices going through customs may be subject to a search without the need for a warrant or probable cause. In addition, if a device is connected to an organization while travelling within a country, the data on that device can be subject to the country's privacy legislation and disclosure.

Travellers should expect that all electronic devices will be examined by immigration officials. Officers may require access to a device to review its content before it is even allowed to enter a country. On February 9, 2021, in Alasaad v. Mayorkas in the US, the First Circuit confirmed that US Border Protection may view the contents of an electronic device with "neither a warrant nor probable cause is required".

In Canada, "Failure to grant access to your digital device may result in the detention of that device under section 101 of the Customs Act, or seizure of the device under subsection 140 (1) of the Immigration and Refugee Protection Act."

Travelling with corporate data should be avoided when at all possible both to avoid situations of data inspection, but also data compromise and theft of the device itself.

Being Cyber Savvy When Travelling

1. Be vigilant – Cyber criminals know that when we're rushing we tend to make mistakes. Don't rush to pay anything. Always double check with your travel agent or hotel using a phone number listed on their website.
2. Consider a password manager – Passwords should be 12 characters or longer and contain complex character combinations. Before travelling it's good to organize your passwords and consider storing them in a secure password manager for easy access.
3. Review the data on your device – Devices should be checked to review if corporate or sensitive data can be removed and placed in the cloud for access. When travelling, if a device is confiscated or stolen, having the data in the cloud will mean that it's not tied to the device.
4. Enable a cloud-based storage application – Storing your documents and photos in Google Drive or One Drive puts them in the cloud. If your local device is encrypted, damaged, or stolen you still have a backup of your data.
5. Use a virtual private network (VPN) - VPNs create a secure password-protected connection to public open Wi-Fi networks. Most travellers naturally want to be online during trips, but using unsecured and unencrypted Wi-Fi networks carries a serious security risk – particularly in public areas such as cafes, lounges, airports and even hotels or meeting venues.
6. When in doubt be prepared – You wouldn't travel without travel insurance protecting your life, and physical possessions. Can you say the same about protecting your digital life? When travelling, you're more exposed than ever. Arranging personal and business cyber insurance will help you stay protected – not just at home but when you are on the road. ◆