CYBER-SAFE TRAVELS

Protecting Your Devices & Personal Information on the Go

IAN & TONYA FITZPATRICK

About The Publication

Cyber-Safe Travels: Protecting Your Devices & Personal Information on the Go is a comprehensive guide designed to help travelers safeguard their digital security while exploring the world. This publication offers up-to-date strategies, expert insights, and recommended tools to protect personal and financial data from cyber threats. Whether you're a frequent traveler, digital nomad, or casual vacationer, this guide provides essential information to ensure a secure and worry-free travel experience.

About the Authors

Hello!

We are Tonya and Ian, lawyers by profession and intrepid explorers by choice. Traveling the world is in our blood, and we both dream of inspiring others through our experiences. That's why we created ***World Footprints*** LLC and its social impact platform.

We are here to share our experiences, insights, and tips to make your travel adventures more enriching.

This ebook focuses on helping travelers, especially backpackers and those with long layovers, find the best airports for sleeping. We provide practical advice, safety tips, and essential gear recommendations to enhance your airport sleeping experience. Our goal is to make your travel as comfortable and stress-free as possible, even when you must sleep at the airport.

We hope you enjoy reading this book! Write to us and comment on our posts on Facebook and Instagram @WorldFootprints. We'd love to hear from you.

And don't forget to sign up for our newsletter at ***World Footprints*** to stay updated on our latest news, tips and stories.

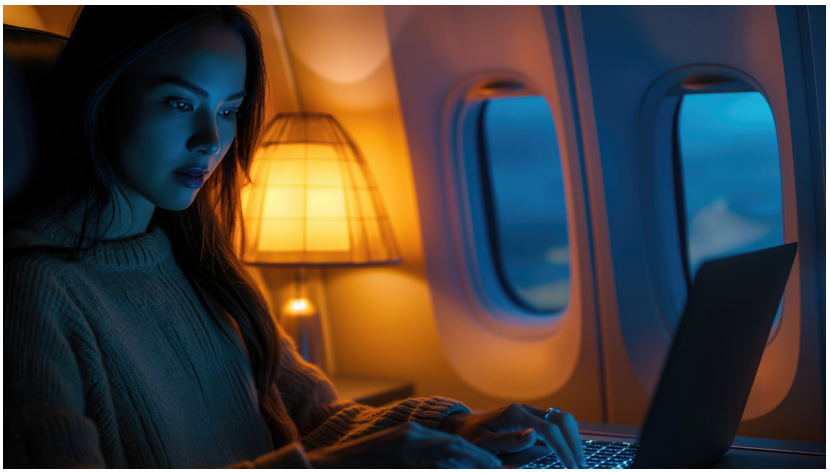
Table of Content

Introduction

Traveling offers incredible experiences, but it also comes with digital risks that can put your personal and financial information at risk. Cybercriminals exploit public Wi-Fi, unsecured devices, and social engineering tactics to steal sensitive data. Whether you're on a weekend getaway or a long-term journey, understanding cybersecurity threats and how to mitigate them is crucial. This guide will provide up-to-date security strategies, recommended tools, and expert advice to ensure your travels remain safe and stress-free.

CHAPTER ONE:

Preparing for Safe Travel



Before you even leave home, taking proactive steps can significantly reduce the risk of cyber threats. Many security breaches happen due to outdated software, weak passwords, or unsecured devices. Preparing in advance ensures your sensitive data is protected and minimizes potential disruptions during your trip.

1.1 Update Your Software & Devices

- Ensure your operating system, apps, and security software are updated before leaving.

- Enable automatic updates to stay protected against emerging threats.
- Use security-focused browsers like Brave or Mozilla Firefox for safer web experiences.

1.2 Back Up Important Data

- Use cloud storage services like Google Drive, Dropbox, or iCloud to back up essential files.
- Encrypt your backups to prevent unauthorized access.
- Consider a physical external hard drive with encryption (e.g., **Samsung T7 Shield, Western Digital My Passport**).

1.3 Secure Your Devices with Strong Passwords

- Set up strong, unique passwords or passphrases for all devices.
- Use a password manager like 1Password, LastPass, or Bitwarden to securely store credentials.
- Enable multi-factor authentication (MFA) wherever possible. Recommended MFA apps include Google Authenticator, Authy, and Microsoft Authenticator.

1.4 Invest in a Reliable VPN

- A Virtual Private Network (VPN) encrypts your internet connection and protects against data interception.

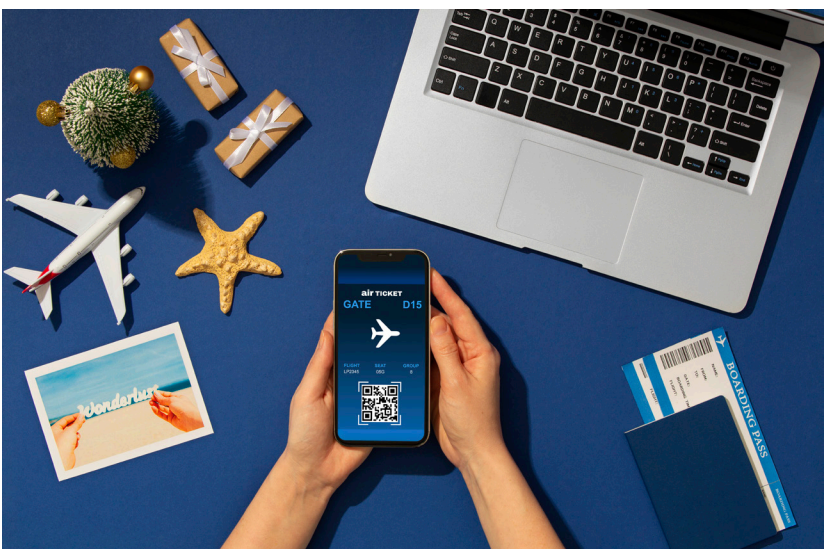
- Recommended VPNs:
    - **NordVPN –** Fast and secure with a no-log policy.
    - **ExpressVPN –** High-speed servers and excellent privacy features.
    - **ProtonVPN –** Open-source and based in Switzerland for strong privacy laws.
    - **Surfshark –** Affordable with unlimited device connections.

1.5 Activate Device Tracking & Remote Wiping

- Enable Find My iPhone (Apple), Find My Device (Android), or similar tracking features.
- Set up remote wipe functionality to erase sensitive data if your device is lost or stolen.
- Use smart tags (e.g., **Apple AirTag, Samsung SmartTag)** to track valuable belongings.

CHAPTER 2:

Protecting Your Devices in Transit



While traveling, your devices are more vulnerable to theft and unauthorized access. Whether at an airport, train station, or hotel, taking security precautions ensures your data remains private and your devices stay secure.

2.1 Use RFID-Blocking Gear

- Carry an RFID-blocking wallet or passport holder to prevent digital pickpocketing.

- Recommended products: Pacsafe **RFID-blocking wallets**, Travelon RFID-protected passport cases.
- ***Note**: Ian uses this **RFID-blocking wallet by Ekster** because it offers a pop-up card feature in a slim design and it has a place to attach an Apple AirTag.*

2.2 Avoid Public USB Charging Stations

- Use a **USB data blocker** (e.g., PortaPow Data Blocker, Juice-Jack Defender) or your own power adapter to prevent "juice jacking" (malware installation via USB charging ports).

2.3 Keep Devices in Your Carry-On

- Never check essential devices in your luggage to avoid theft or loss.
- Consider a theft-proof backpack with hidden zippers (e.g., Nomatic Backpack, Pacsafe Venturesafe).

2.4 Turn Off Bluetooth, Wi-Fi, & Location Sharing

- Disable unnecessary connectivity features when not in use to reduce exposure to cyber threats.
- Set up a travel router like the **GL.iNet Slate AX, Deeper Network** or **AirCove** for added security on public networks.

CHAPTER 3:

Staying Safe Online While Traveling

Public Wi-Fi networks are breeding grounds for cybercriminals looking to steal your information. Even hotel and airport networks may be compromised. Using secure connections and best practices will help you stay safe online.

3.1 Use a VPN When Connecting to Wi-Fi

- Avoid using public Wi-Fi without a VPN.
- If necessary, use mobile data or a personal hotspot instead.
- Consider portable Wi-Fi hotspots like **Skyroam** Solis or GlocalMe for added security.

3.2 Be Cautious with Hotel & Café Wi-Fi

- Avoid accessing sensitive accounts (banking, email) on public networks.
- Always confirm the network name with staff to prevent connecting to fake Wi-Fi hotspots.

3.3 Turn Off Auto-Connect Features

- Disable auto-connect settings for Wi-Fi and Bluetooth to prevent accidental connections to malicious networks.
- **Note**: *We learned how vulnerable our phones are when driving near out home in Maryland. A message popped up on Tonya's phone that her phone was compromised, and that the password must be reset by clicking on a "link". Tonya turned the phone off and on again and then called her service provider who stated that there was no security breach.*

3.4 Browse Securely

- Look for HTTPS in the URL when visiting websites.
- Use privacy-focused browsers like Brave or Firefox with enhanced tracking protection.
- ***Note****: The "S" means the site encrypts your data, keeping personal details like credit card info safe from hackers—especially when booking flights and hotels.*

  Why HTTPS matters:

  - **Encryption:** Protects your information from being intercepted.
  - **Trust Signal:** A padlock icon in the browser confirms a secure connection.
  - **Phishing Protection:** Reduces the risk of scams stealing your sensitive data.

3.5 Avoid Entering Sensitive Information on Shared Devices

- Never log into personal accounts on public computers (hotels, libraries, etc.).
- If necessary, use an incognito/private browsing mode and log out completely after use.

CHAPTER 4:

Protecting Personal & Financial Data

Cybercriminals often target travelers' financial information through scams, data breaches, and skimming devices. Implementing security measures will help safeguard your accounts and personal information.

4.1 Use Digital Wallets Instead of Physical Cards

- Digital payment methods (Apple Pay, Google Pay) offer more security than physical credit cards.
- Recommended travel credit cards with fraud protection: Chase Sapphire Reserve, American Express Platinum, Capital One Venture X.

4.2 Enable Transaction Alerts

- Set up SMS/email notifications for all banking transactions.
- Contact your bank immediately if you notice suspicious activity.

4.3 Limit Data Sharing on Social Media

- Avoid posting real-time location updates.
- Turn off location tagging in social media apps to prevent tracking.
- ***Note:*** *We generally do not share our photos on social networks until a day before we leave or after we return home.*

4.4 Use Encrypted Communication Apps

- Apps like Signal, WhatsApp (with end-to-end encryption), and Telegram provide secure messaging options.

4.5 Carry Only Essential Payment Cards

- Avoid bringing multiple credit/debit cards—use a travel-friendly card with fraud protection and low foreign transaction fees.

Stay Safe and Travel Smart!

By implementing these cybersecurity best practices, travelers can significantly reduce the risk of cyber threats and protect their personal and financial information. Staying informed, using recommended tools, and remaining vigilant will make for a safer, worry-free travel experience.

Resources & Further Reading

- **Official Cybersecurity Travel Guidelines** – U.S. State Department
- **Encrypted External Hard Drives** – Samsung T7 Shield, Western Digital My Passport
- **Trusted VPN Providers** – ExpressVPN, NordVPN, ProtonVPN
- **Password Managers** – LastPass, 1Password, Bitwarden
- **Mobile Security Apps** – Lookout Security, Norton Mobile Security, Kaspersky Mobile
- **Secure Travel Routers** – GL.iNet Slate AX, TP-Link AC750, AirCove, Deeper Network