LASK TRAVEL

FREE CYBERSECURITY CHECKLIST FOR TRAVELERS

Whether you're flying overseas for a long-awaited vacation or working remotely as a digital nomad, keeping your data safe while traveling can be challenging. This **Free Cybersecurity Checklist** will help you organize and secure your devices, accounts, and networks—so you can **roam confidently** without risking sensitive information.

---

1. Preparing Before You Leave

Use the table below to tick off each step before heading out. You can also add **hyperlinks** to recommended tools (VPNs, password managers, etc.) in the "Resources/Links" column as needed.

Action	Description	Resources	Check
Update Devices & Apps	Install the latest OS and app updates. Turn on auto-updates for continuous protection.	e.g., Windows Update, Mac Updates	[ ]
Install/Reinforce Security Software	Use reputable antivirus/anti-malware software on laptops and mobile devices.	e.g., Trend Micro, Malwarebytes	[ ]
Choose a Trusted VPN	Select a VPN with a no-logs policy and robust encryption for secure public Wi-Fi usage.	e.g., NordVPN	[ ]
Strengthen Passwords & MFA	Use unique passphrases and enable multi-factor authentication (2FA) wherever possible.	e.g., Keeper, Google Authenticator	[ ]
Backup Important Data	Save files to encrypted external drives or secure cloud storage. Verify backups work.	e.g., Google Drive, Dropbox, OneDrive	[ ]
Remove Unnecessary Data & Apps	Delete any apps or files you won't need, reducing potential vulnerabilities.	—	[ ]

LASK TRAVEL

FREE CYBERSECURITY CHECKLIST FOR TRAVELERS

---

2. Device Security On the Go

Print or save a copy of this table to reference **during your trip**. Check off each step as you go.

Action	Description	Resources	Check
Lock Screens & Biometric Features	Set short auto-lock times. Use PINs, fingerprints, or Face ID for swift, secure access.	—	[ ]
Disable Auto-Connect & Bluetooth	Turn off automatic Wi-Fi connections and Bluetooth in public areas.	—	[ ]
Inspect QR Codes	Watch for tampered or sticker-over codes. Verify URLs if scanning them in public places.	Latest QR Code Tips	[ ]
Beware Public Computers	Avoid logging into sensitive accounts or inserting USB drives in publicly accessible PCs.	—	[ ]
Use Secure Payment Options	Choose contactless or virtual cards. Avoid entering CC info on suspicious networks.	e.g., Apple Pay, PayPal	[ ]
Be Wary of Phishing Emails	AI-generated or urgent-sounding emails can be scams. Double-check sender details & domains.	Phishing Insights	[ ]

---

3. Safe Browsing & Communication

Action	Description	Resources	Check
Always Use a VPN on Public Wi-Fi	Encrypt data on airport, hotel, and café networks.	e.g., NordVPN, ExpressVPN, Windscribe	[ ]
Encrypt Messaging Apps	Prefer end-to-end encrypted chats (Signal, WhatsApp, Telegram) for sensitive conversations.	e.g., Signal, WhatsApp	[ ]

LASK TRAVEL

FREE CYBERSECURITY CHECKLIST FOR TRAVELERS

Action	Description	Resources	Check
Check HTTPS on Websites	Look for “https://” and a lock icon in the address bar.	SSL Checker	[ ]
Watch Out for Shoulder Surfing	Be mindful of who might be watching you type passwords or personal details in crowded places.	—	[ ]
Monitor Bank & Credit Card Alerts	Enable text/email alerts for any unusual transactions.	Bank App, Credit Card Portal	[ ]

---

4. Returning Home

Don’t forget these final steps after you land back home or settle in a new destination.

Action	Description	Resources	Check
Change Key Passwords	If you used questionable networks or suspect device tampering, update critical passwords.	—	[ ]
Run Full Antivirus/Malware Scans	Perform a deep system check to spot any hidden threats acquired while traveling.	e.g., Norton, Malwarebytes	[ ]
Review Bank Statements & Accounts	Look for suspicious charges or logins. File disputes if anything looks off.	Dispute Info	[ ]
Remove Travel Apps or Permissions	Uninstall any one-time travel apps you no longer need (e.g., local transport app).	—	[ ]
Share Experiences & Advice	Leave reviews on Wi-Fi hotspots, or let others know where to get secure connections.	—	[ ]

LASK TRAVEL

FREE CYBERSECURITY CHECKLIST FOR TRAVELERS

5. Bonus Tips & Notes

- **Use a "Clean Device"**: If you're traveling to high-risk regions, consider bringing a dedicated phone or laptop with minimal apps and data.
- **Keep Physical Security in Mind**: Use RFID-blocking wallets for cards/passports, lock your devices in a hotel safe, and watch out for petty theft.
- **Be Cautious on Social Media**: Limit real-time location sharing. Posting your exact whereabouts can signal to criminals that your home is vacant.
- **Regularly Back Up & Sync**: If the worst happens—like stolen devices—you'll have your data accessible from a safe backup.

Disclaimers & Notes

- **This checklist is for educational purposes only** and does not guarantee absolute protection. Cyber threats evolve daily, so always stay updated.
- **Follow local regulations** when using encryption, VPNs, or other security tools abroad. Certain countries have specific laws on such technology.

Final Thoughts

Travel is an adventure—don't let cyber threats spoil the fun. By following this checklist, you'll significantly reduce your risk and ensure that your **data remains safe** throughout every leg of your journey.