

# A Traveler's Cybersecurity Guide"

As you embark on your journeys, this guide will be your trusted companion in navigating the digital landscape while ensuring your online safety. This guide gives you practical tips to help you protect your personal and sensitive information while enjoying your travels to the fullest.

## Before & During Your Trip

Protect Your Identity	Protect Your Devices	Protect Your Data & Device Traffic
<p>Consider placing a credit freeze on all your credit score accounts.</p> <ul style="list-style-type: none"><li>• Transunion</li><li>• Innovis</li><li>• Equifax</li><li>• NCTUE</li><li>• Experian</li><li>• ChexSystems</li></ul>	<p>When carrying electronic devices:</p> <ul style="list-style-type: none"><li>• <i>Back up your data.</i></li><li>• <i>Update OS, apps, and enable auto-updates.</i></li><li>• <i>Use an updated antivirus.</i></li><li>• Don't plug in unknown USB sticks to avoid potential viruses.</li></ul>	<p>Turn off WiFi, Bluetooth, and GPS when possible to prevent your devices from being attacked and you from being tracked. (Yes, this actually happens.)</p>
<p>Secure your online identity to prevent impersonation and unauthorized access to important accounts like Social Security, Post Office, IRS, and banking.</p>	<p>For privacy:</p> <ul style="list-style-type: none"><li>• Get a laptop privacy screen filter.</li><li>• Carry your own wall outlet phone charger instead of using public USB ports to avoid potential infections. one</li></ul>	<p>Use a VPN for encryption, especially on public networks abroad.</p> <p>Pro tip: test public Wi-Fi security by entering an incorrect password; if you connect, it's likely insecure.</p>
<p>Enable MFA for online</p>	<p>Avoid transporting</p>	<ul style="list-style-type: none"><li>• Be cautious with public</li></ul>

accounts and set up PIN and encryption on your phone to prevent unauthorized access in case of loss or theft.

Use credit cards, not debit cards, for safer transactions abroad. Credit cards have a \$50 liability limit, unlike debit cards. Remember your Credit Card PIN; it's often required internationally.

electronic devices in checked baggage.

If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, assume that the device's hard drive has been copied.

computers, especially abroad; assume your data may be captured.

- When sharing research, consider diverse legal and professional standards for intellectual property among your audience.

## When You Return

### Reset

Change all the passwords you used on your trip.

### Scan

Run a full Anti-Virus scan of your computer.

### Monitor

Consider monitoring all the credit cards you used and accounts you accessed while traveling.



## Traveling to China or Russia?



### Access

Be aware that access to many sites such as Gmail, Google apps, Wikipedia, and Yahoo Web Mail may be blocked or filtered.

### Surveillance

Connections are never secure and may be monitored by the government.

### Insecurity

VPN users in these countries face prolonged connection issues, resorting to unsafe networks. Hotel staff and officials have

accessed rooms and safes;  
**keep your devices with you  
always.**

# Conclusion

A Traveler's Guide to Cybersecurity equips you with the knowledge and tools to navigate the digital realm securely while on your adventures. By following the tips and precautions outlined in this guide, you can safeguard your online identity, protect your personal information, and enjoy your travels with peace of mind. Remember, cybersecurity is an essential part of modern travel, and being proactive is the key to a worry-free journey. Safe travels!



## **BW Information Technology**

Website: [help.bw.edu](http://help.bw.edu)  
Email: [helpdesk@bw.edu](mailto:helpdesk@bw.edu)  
Phone: 440-826-7000

