Cyber Security Guidance: International Travel

Traveling abroad presents unique challenges for cyber security. Here are some essential tips to help you stay safe online while exploring new destinations:

1. Secure Your Devices Before You Go

- **Update Everything:** Ensure your operating system, apps, and antivirus software are up to date.
- **Backup Data:** Back up important files and photos to a secure cloud service or external drive.
- **Export Control:** assess whether your devices contain any work, data, or technology that may be subject to export control legislation. **Important:** Exporting controlled items without the appropriate licence is a criminal offence. – see Appendix A for further guidance on export control considerations.

2. Use Strong Passwords

- **Create Unique Passwords:** Use complex passwords for each account. Consider a password manager to keep track of them.
- **Enable Multi Factor Authentication (MFA):** Ensure your university accounts have MFA enabled, and that you have set-up the MS Authenticator App.

3. Be Cautious with Public Wi-Fi

- **Avoid Sensitive Activities:** Refrain from accessing banking sites or entering sensitive University information on public networks.

4. Limit Device Exposure

- **Use Airplane Mode:** Turn on airplane mode when not using your device to prevent unauthorised access.
- **Keep Devices Locked:** Use strong passwords or biometric locks (fingerprint or face recognition) for your devices.

5. Be Wary of Phishing Scams

- **Check Email Addresses:** Verify the sender's email before clicking links or downloading attachments.
- **Look for Signs of Phishing:** Be cautious of urgent messages or offers that seem too good to be true.

6. Limit Data Sharing

- **Control App Permissions:** Review and limit permissions for apps, especially those that request access to personal information.
- **Turn Off Location Services:** Disable GPS tracking when not needed to protect your privacy.

7. Use Secure Payment Methods

- **Opt for Credit Cards:** Use credit cards instead of debit cards for better fraud protection.
- **Monitor Transactions:** Regularly check your bank statements for unauthorised charges.

8. Educate Yourself on Local Cyber Threats

- **Research Common Scams:** Understand prevalent cyber threats in your destination to stay vigilant.
- **Engage with Local Communities:** Join online forums or groups to get tips from expats or locals about safe online practices.

9. Avoid Connecting to Unknown Networks

- **Be Selective:** Only connect to networks you trust, like those provided by hotels or established businesses.
- **Forget Networks After Use:** Remove any connections you no longer need from your device's settings.

10. Report Any Issues

- **Contact Local Authorities:** If you encounter cybercrime or suspicious activity, report it to local law enforcement or your embassy.

11. Disconnect Regularly

- **Limit Screen Time:** Take breaks from technology to enjoy your surroundings and reduce the risk of cyber threats.

By following these guidelines, you can significantly enhance your cyber security while traveling abroad, allowing you to focus on enjoying your adventure. Safe travels!

APPENDIX A

Export Control Considerations

Before travelling abroad, assess whether your devices contain any work, data, or technology that may be subject to export control legislation. This includes laptops, phones and other electronic devices.

UK Export Control Overview
UK strategic export controls focus on high-risk activities such as applied research. These controls may apply if you:

- Collaborate with overseas colleagues on research projects
- Take research materials or technology abroad
- Export technology or data

Important: Exporting controlled items without the appropriate licence is a criminal offence. Penalties may include:

- Revocation of licences
- Seizure of items
- Financial penalties
- Imprisonment (up to 10 years)

Travelling Abroad with Controlled Items

1. If You Have an Export Licence

- Notify RSDO by emailing trustedresearch@brunel.ac.uk before travelling on university business with controlled items.
- You may use your electronic devices as normal, including accessing Outlook and downloading attachments.
- You are permitted to carry out all controlled work as specified in your export control licence.

2. If You Do Not Have an Export Licence

- Do **not** take any electronic devices containing controlled data, research, or technology abroad.
- If you need a laptop for travel:
    - Request a blank device from IT Service Desk for non-controlled data
    - Or remove all controlled information from your current device before travel
- Use **Webmail** (not Outlook) to access emails while abroad.
    - Do **not** open attachments suspected to contain controlled data.
- Do **not** access controlled information via university shared drives or servers while overseas.

If you are unsure whether your work falls under the UK Strategic Export Control List, please contact the Trusted Research team at trusted.research@brunel.ac.uk to request an Export Control assessment.