Twelve Security Tips that Turn away Technical Troubles when Travelling

The first thing to consider is if you need to travel with your device. If you won't need your iPad, mobile or laptop, it will be safer at home. If you will need to travel with your device, please consider the following recommendations:

1. **Avoid leaving your device/s unattended:** Do not leave your device unattended or lend it to someone you just met.
2. **Keep your devices in nondescript baggage:** when travelling with your devices, use a backpack instead of a laptop bag. It is better to carry devices in carry-on luggage, rather than in 'checked' luggage.
3. **Ensure your device is locked when not in use:** set a password (or pin, for devices that don't support passwords) for all your devices, and lock devices when not in use.
4. **Avoid using untrusted external storage media:** Cyber criminals have been known to infect USB sticks with malware and 'drop' them in public places. Untrusted external storage media (e.g. flash drive, SD cards etc.), can be infected with malware intended to steal your data. Try to plan ahead and take all the necessary accessories with you, but if you must purchase any of them abroad, make sure it is from a reputable and reliable source.
5. **Avoid adding personal information into public computers:** Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for its users. If you need to use public computers, avoid entering any Personal or business sensitive data if possible.
6. **Ensure you have backed up your information:** plan ahead and back up your information. If it happens that your data is compromised whilst travelling abroad and you need to reset to factory default, then you can restore your information from the backup.
7. **Turn off your WiFi when not in use:** Attackers can easily spoof WiFi network names to connect to devices within range for eavesdropping. To help you avoid accidentally connecting your device/s to rogue WiFi networks, once you are finished using a network, disconnect from that network and turn off WiFi on your device.
8. **Use secure remote access connection (i.e. Citrix for Western Sydney University's systems):** If you need to connect to the University's network remotely while on holiday, connect through Citrix – this solution is a secured connection, and is supported by ITDS. For organisations other than the University, contact that organisation's service desk to inquire whether a secured remote connection tool is available.
9. **Use a non-privileged account:** If you have a privileged access account (i.e. administrator accounts), use it only when necessary, and use your regular (non-privileged) account at all other times. This will provide additional protection against malware infections.
10. **Practice safe web browsing whilst using public WiFi networks:** It's tempting to stay in touch with friends and colleagues as you travel by connecting to publicly available WiFi networks (e.g. at public cafes, hotel lobbies, airports). However, public Wi-Fi in hotels, airports and even cafes can be a prime spot for phishing. It's also best not to do banking or access sensitive accounts on a public network. To protect yourself while browsing websites abroad:
    A. **Connect to HTTPS websites** (HTTP only is not encrypted and less secure)
    B. **Do not click on suspicious links and attachments**
    C. **Clear browsing session information when using devices that do not belong to you**
11. **Ensure your devices are up-to-date and compromise free before and after travelling.** Before you leave, ensure there are no updates waiting installation. Run an antivirus scan of your device before and after the holiday. These steps will make your device more resilient to compromise.
12. **Consider changing your passwords upon your return.** If you have any reason to think any passwords used on your trip may have been compromised, consider changing them on a trusted and secure device once you return.

If you lose any device/s issued by the University or containing University data, please inform the IT Service Desk as soon as practical (email itservicedesk@westernsydney.edu.au, or call 02 9852 5111).