



State Privacy Office December Privacy Tip



No one is exempt from the threat of cybercrime, at home or on the go, but you can follow these simple tips to stay safe online when traveling.

- **Avoid free Wi-Fi.** Although connecting to free public Wi-Fi sounds great, it is often unsecure and can expose your devices and personal information to hackers. Instead, use a VPN or your mobile phone as a hotspot when going online.
- **Confirm your network.** If you do connect to public Wi-Fi, be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
- **Disable auto-connect on your devices.** If your mobile phone or tablet automatically connects to wireless networks or Bluetooth devices, disable those features and connect manually only when you want to.
- **Secure your devices.** Keep track of your laptop, smartphone, tablet and even accessories such as USB drives – especially while on the go, and don't leave your devices unattended in public places.
- **Avoid shared computers.** If using computers at hotel business centers and other places that offer shared systems, avoid making purchases or logging into email. You don't know if the systems are up to date with the latest security software or if the machines are safe.

Copyright © 2023 [NCDIT](#). All rights reserved.
Reprinted with permission.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.