Port53

Top Tips for

AVOIDING CYBER ATTACKS WHILE TRAVELING

1

AVOID PUBLIC WIFI NETWORKS

Using a public Wifi network can make you an easy target for hackers trying to steal your personal or company data. Public Wifi Networks are often unencrypted and unsecured, leaving you vulnerable.If you do use public WiFi, never access sites or accounts that contain sensitive data.

2

CONSIDER THE PHYSICAL SECURITY OF YOUR DEVICE

Do not leave your device unattended or unlocked. Turn it off and lock it before going through the security screenings in ports of transportation. Consider purchasing and using a privacy screen to block out potential onlookers.

3

DISABLE BLUETOOTH

Even without actively seeking internet access, laptops, smartphones and tablets are susceptible to remote Bluetooth connections. While all Bluetooth devices have some inherent vulnerabilities, the older versions are far more susceptible to hacking and eavesdropping.

4

ALWAYS USE A PASSWORD

It goes without saying that your connected device should be password protected. Make sure to follow best practices and avoid reusing passwords. Also consider enabling the vendor provided device location service, so if your device happens to fall in the wrong hands you can remotely wipe it.

5

DISABLE FACE AND FINGERPRINT PASSWORDS

In recent years immigration officials at home and abroad have increased security screenings of connected devices, While they cannot force you to share your password it is a good idea to disable facial recognition or fingerprint log-in of your device while traveling.