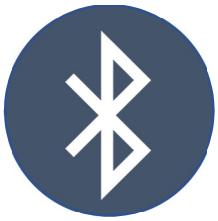
TRAVEL SAFELY WITH YOUR TECHNOLOGY

Have device. Will travel.

This is Information Age – we all know it. We have smart pads, smart phones, smart watches, and smart homes. And, while technology has benefitted and enriched our lives, it's also changed us so quickly that many of us are still struggling to understand last year's technology, let alone the latest trends.

Regardless of your level of technology savvy, there are fail-safe ways that you can safeguard all of your mobile devices. Whether you're just headed up to the coffee shop for a meeting, or flying across the country for a conference, you're on the go…



1. Disable Bluetooth & Wi-Fi.

Disable or turn off auto-connect on your Bluetooth and Wi-Fi. If your Bluetooth or Wi-Fi auto-connects to a network, it could be a crime of opportunity. You might unknowingly connect to a criminal who could access your data wirelessly

2. Password Protect Your Device.

There are multiple ways to secure your phone: passcode, fingerprint, or face scan, etc. Please be sure that all of your mobile devices have password protection. And, although it's a slightly inconvenient to have to unlock your device every few minutes, it's a lot less inconvenient than having your unlocked device lost or stolen. You definitely don't want an unlocked device in the wrong hands.

3. Think Before You Connect.

Free, public Wi-Fi is very convenient and can be a real time-saver—but think whether you trust that network before you connect. If you decide to use the free, public Wi-Fi, avoid accessing your work emails, bank/financial institution, or online shopping. Anyone with the right skills and tools will be able to steal your data on an unsecure wireless connection.

Need Help?

Check with your local help desk or information system security officers for help securing your mobile devices. Your organization has policies in place to safely travel with your government furnished equipment. For additional resources, see the DHS Cybersecurity Tip Card.