COMPASS
CYBER SECURITY

A TRAVELERS GUIDE TO MOBILE DEVICE SECURITY

According to the Department of Transportation, U.S. and foreign airlines flew over 895 million passengers through U.S. based airports in 2015. This number is expected to increase in 2016 and beyond. Regardless of whether their travel is for business or pleasure, most individuals who travel take 2-3 mobile devices (smartphone, tablet, laptop) with them. Today's society is increasingly mobile and traveling whether by plane, train, or automobile. Threat actors know this and target travelers whose mobile devices are often insecure (or used in insecure manners) yet contain vast amounts of sensitive data. **This guide is intended to provide travelers and mobile employees with key tips and security best practices for keeping their devices and data safe and secure.**

GENERAL TIPS

- Take the minimal number of devices necessary.
- Use a loaner mobile device (if an option) that does not have any sensitive data saved locally.
- Never leave any of your devices unattended.
- Avoid traveling with USB drives since they are easily lost; if you do, make sure it is encrypted.
- Research current cyber threats so you can spot early warning signs.

MOBILE DEVICE TIPS

- Configure your mobile devices' security settings (settings vary for iPhone and Android devices).
- Enable WiFi and Bluetooth only when you are using them.
- Configure Bluetooth to require a password before connecting.
- Encrypt all mobile devices.
- Make sure you install app patches as they are released.
  - A lot of the apps contain security related patches
  - Check for updates before traveling
- Enable the ability to remotely wipe device if lost or stolen.
- Ensure that you have an up to date anti-virus/anti-malware application.
- Backup all of your data prior to traveling.
- Enable the ability to locate your device (ex. Find my iPhone).
- Perform an anti-virus and/or vulnerability scan before connecting to the corporate network after travel.
- Never let an unknown person borrow one of your devices.

ACCESSING PUBLIC WIFI

- Don't use public WiFi for accessing any sensitive information or email unless absolutely necessary.
  - Always verify the authenticity of the WiFi access point before connecting.
  - Use a virtual private network (VPN) if you have to use public WiFi.
  - Even if you use a VPN minimize your access to sensitive data.
- Use your cellular data plan if available as an alternative option.
- If you use your mobile device in a public place:
  - Avoid sitting with your screen facing a public area.
  - Cover up your keyboard when entering passwords/ passcodes.
  - Use a screen protector if available for your device.

250 South President Street, Suite 2300, Baltimore, MD 21202 | 667-401-5108 | mflora@compasscyber.com

COMPASSCYBER.COM