Travel can expose you to a number of high-risk situations, such as unsecured networks, activity monitoring, and malware targeting. Information is always attractive to anyone seeking a competitive advantage, to increase market share, or to build economic prosperity. In addition to personal information, all types of business strategy information are also targeted.

# How is information obtained?

A number of methods are leveraged to obtain information from business travelers.

## Hacking electronic media and devices

## Luggage or hotel room searches

## Activity surveillance

## Business negotiations

## Conversations at conferences and trade shows

# What are the ways to protect your mobile phone?

## Password protect your phone

## Turn off your phone when not in use

## Remove the battery until it is needed

## Avoid misplacing your device

# How do I safeguard my laptop?

## Ensure antivirus software and security programs are up-to-date

## Avoid connecting to any storage device such as CDs or USB drives that is not yours

## Use secure passwords

## Remove non-essential files

## Encrypt your hard drive

## Keep your laptop with you at all times

# How do I minimize Wi-Fi risks?

You can minimize the risks of hacking and the introduction of malware when using Wi-Fi by using secured connections (VPN) to transfer data, accessing secure websites (https:), and disabling auto-connect on tablets and smartphones.

# What is juice jacking and how do I avoid it?

“Juice jacking” is the term applied to interrupting the data flow from your mobile phone when you connect to an unsecure power supply such as those in an airport kiosk.

Fully charge your device before traveling, use a personal charger, and carry a backup battery. When using a public charging station, power down your device when charging and use the manufacturer’s cable.

# What is “shoulder surfing”?

“Shoulder surfing” is the use of direct observation, such as looking over someone's shoulder or video surveillance, to obtain information.

To prevent shoulder surfing, shield yourself as much as possible when entering sensitive information. If using your laptop in a public place, use a privacy screen.

# Follow best practices.

To mitigate your exposure when traveling, before leaving on any international business trip, contact your firm’s Technology Department to learn the best practices for international travel.

## Limit the number of devices and files that you carry

## Implement good security methods on every device

## Prevent wireless threats by exercising caution and using secure connections

## Circumvent “shoulder surfing” and “juice jacking”

## Scan devices for viruses and malware, and change passwords and ATM PIN numbers upon returning home