Report DETAILS

Attachments

OSAC Quick-Guide on Best Practices 457.59KB

Traveling with Mobile Devices; Tren 1.53MB

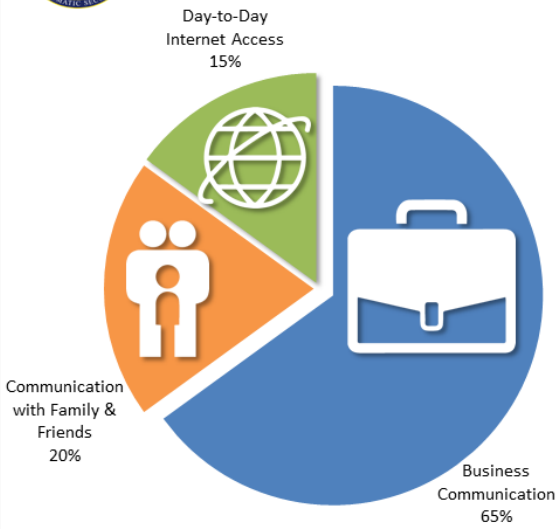
Email

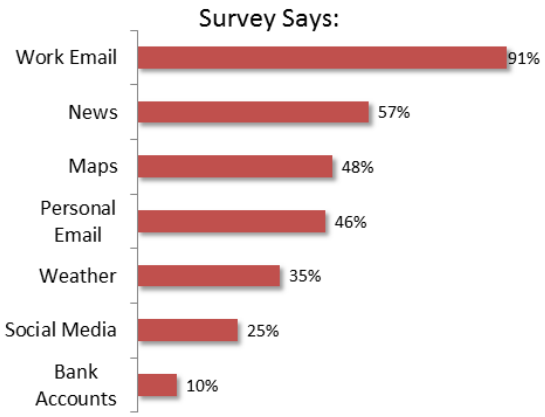
Traveling with Mobile Devices: Trends & Best Practices

Information Security; Cyber; Traveler Toolkit

7/23/2015

Why Pack your Smartphone?

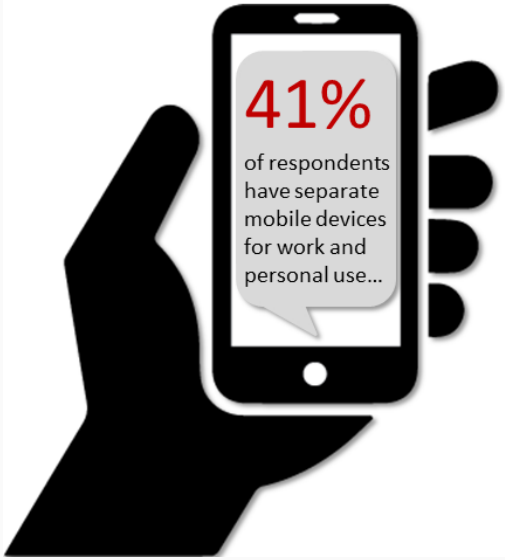




For most travelers, it comes down to business. The majority of survey respondents ranked work communications and work email as the primary use of their mobile phone while traveling overseas. Although mobile devices can facilitate connecting back to headquarters and maintaining workflow, the risk for exploitation of these devices and the information accessed can greatly increase on overseas travel. Providing employees with best practices guidelines, and/or loaned devices, to use on travel can help mitigate the potential theft of business and personal information from the growing presence of mobile malware.

Whose phone is it, anyway?

Weighing Personal vs. Business Devices



...leaving 59% – the majority of travelers – to use the same phone for personal and business functions while overseas. This can put business communications at a heightened risk, especially if users are careless with basic security practices on their personal phones. What's more, organizations do not have control over the features and applications employees use on their personal devices. It's critical to employ best-practice standards on your phone – regardless of device ownership or travel destination.

- Need to double-check your settings? Use OSAC's best-practice guide for traveling with your mobile device overseas.

Click here for **OSAC's best-practice guide** on traveling with your mobile device overseas.

Equipment Escapades

Does your organization provide a loaner phone to use on overseas travel?

...meaning employees likely don't adjust the daily business information they access, whether at home or traveling overseas. It also means that if a mobile device is compromised abroad, employees are carrying the malware home with them. This greatly increases the risk for sensitive information to be continuously exploited long after travel is completed. The benefits of loaning employees temporary phones to use on travel include:

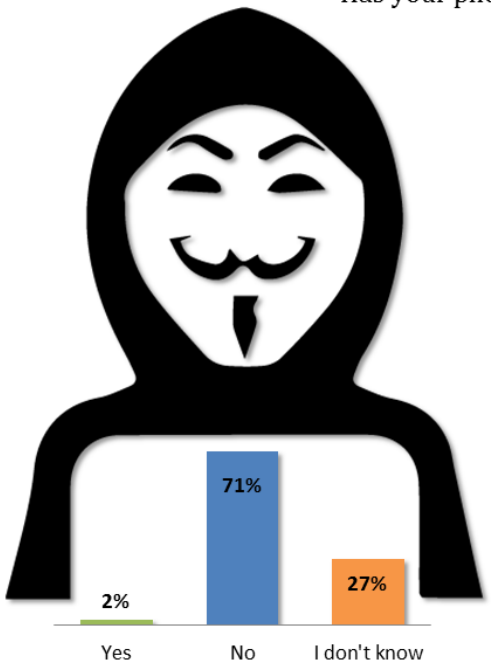
- No long-term storage of sensitive information
- Access only to information pertinent while on travel
- Ability to wipe and reset the device upon return

The average selling price of a smartphone last year was $314, whereas IP theft collectively costs the U.S. private sector up to $250 billion annually.

Click here for the Mcafee **report** on the global cost of cybercrime.

Hacking Happens

Has your phone ever been hacked while traveling overseas?



Multiple survey respondents identified **China** as their travel destination when they discovered their mobile phone had been hacked. This commonly led to disappearing apps, and disruption to the phone's primary communications functions. China has been identified as a high risk location for mobile malware, mobile device privacy attacks, and a hot spot for mobile botnets.

Kaspersky Lab annually measures the countries with the most malicious mobile software attacks on users. Here were the **Top 10 in 2014**:

1. Russia
2. India
3. Kazakhstan
4. Germany
5. Ukraine
6. Vietnam
7. Iran
8. UK
9. Malaysia
10. Brazil

Click here for the Anti-Phishing Working Group's **map** of high risk locations for mobile malware.

Hacking Happens

Case Study: Dendroid Malware

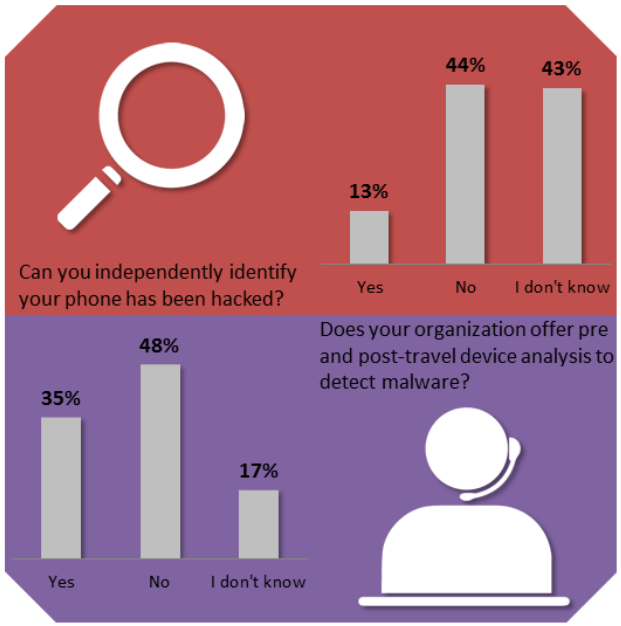
Malicious functions include:

- Make and record calls
- Delete call logs
- Intercept text messages
- Take pictures with the phone's camera
- Download existing pictures
- Record and upload audio and video
- Open applications and web pages
- Initiate denial of service

In the first few months of 2015, 5,000 new strands of Android malware were discovered *daily*. Just one of those was "Dendroid," a dynamic and difficult-to-detect remote access tool, which was at one time easily available in malware forums for a meager fee of $300. Dendroid hides inside applications and evades Google Play's malware detector, allowing it to potentially operate for extended periods of time. Its various capabilities – like turning on the microphone at will – could be used to gather trade secrets during closed-door business meetings. Intercepting voice and text communications could lead to hefty bills from premium-rate numbers, or allow malicious actors to gather intelligence on the Android owner's business and personal contacts. Users should be suspicious of apps requesting a wide variety of permissions, and can download mobile-security apps to protect against various malware threats.

Detecting an Intrusion

How do you know when you've been hacked?



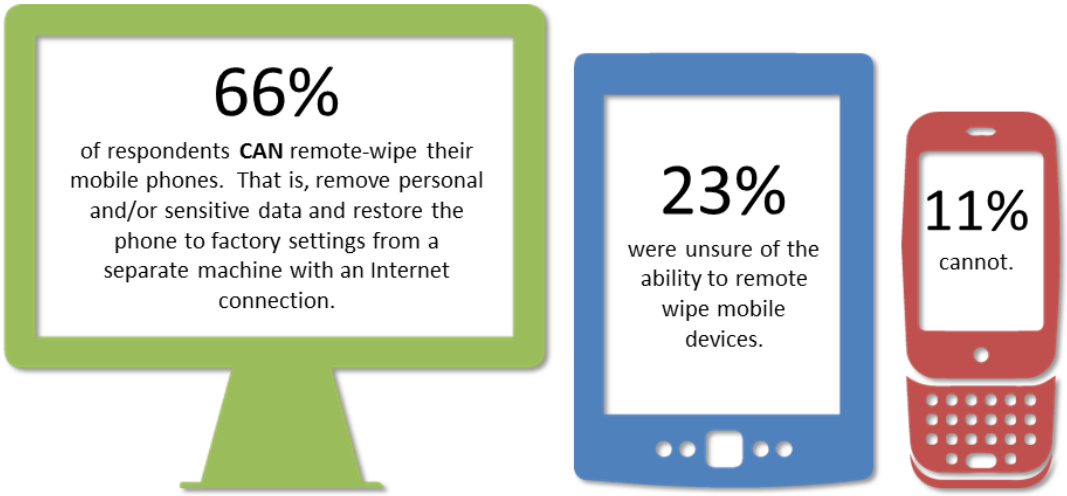
The majority of survey respondents were unsure or unable to identify a compromise on their mobile devices. This again heightens the information risk, especially if employees continue to use their phones for business purposes after a device is hacked. Often, smartphone malware is extremely difficult to detect. Some signs of compromise may include:

- Latency
- Frequently drained battery
- Increased data usage
- Appearing apps
- Disappearing apps

Unfortunately, many of the symptoms of compromise can also be confused with connecting through a foreign service provider while traveling overseas. Offering employees a loaner device or technical assistance may be the best way to mitigate undetected hacks of mobile phones.

Mitigating an Intrusion

Do you have the ability to remote wipe your mobile device?



All major smartphone providers offer the ability to remote-wipe devices – a virtual kill switch that allows sensitive data to be erased in the event a phone is lost or stolen. Although remote-wipe won't execute if the phone battery dies, a signal isn't available, or a hacker disables network connections, it is nonetheless a mitigation tactic that all employees should enable and use as soon as a phone disappears. The following links offer step-by-step guides on remote wiping Android and Apple devices.

Click here for step-by-step guides on remote wipe functions for **Android** and **Apple** devices.

Reward vs. Risk

Understanding the pros and cons of smartphone features

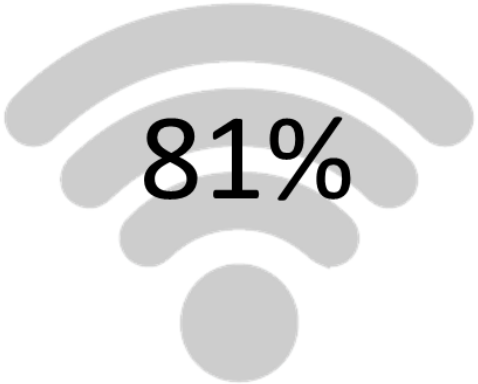
So many of the common functions that make mobile phones user-friendly are the same functions used by malicious actors to exploit them. The following survey questions assess which of these everyday features are popular among travelers while overseas, to include:

- Accessing public Wi-Fi
- Using Device Lock
- Using GPS services
- Downloading free apps

The subsequent slides highlight the functionality of these popular features, the associated risks, and potential mitigation tactics. Better understanding of the risks to these every-day mobile features can help employees use their phones more safely and effectively while abroad.

Public Wi-Fi

How many connect to public (e.g. airport, hotel) Wi-Fi hotspots on travel?



Functions

- Internet access often free of charge
- No plugs or cords necessary
- Emails and web surfing on-the-go
- Access to personal and business information from virtually anywhere a hot spot is offered

Threats

- Often no authentication
- Eavesdroppers and data interceptors
- Man-in-the-Middle attacks
- Evil twins: rogue access points disguised as legitimate ones

An overwhelming majority of survey respondents connect to public Wi-Fi while on travel, and it's easy to see why. These hot spots deliver quick and easy access to the communications, like work e-mail and news updates, that constituents prioritized while on overseas travel. However, information traversing public Wi-Fi is also at risk to eavesdropping and information theft by malicious actors sitting on the same network. Furthermore, it's not always just public networks. The Darkhotel campaign targeted business travelers after checking in and logging on to seemingly private hotel networks. No matter the network ownership, travelers should be conscious of not accessing sensitive information over Wi-Fi.

Click here for OSAC's report on the **Darkhotel** campaign.

Device Lock

How many use a fingerprint or PIN to lock phones while traveling?

Function

- Basic password protection
- Prevents information access when a phone is lost or stolen
- Locks device and associated information after periods of no use
- Can erase personal data after too many unsuccessful attempts

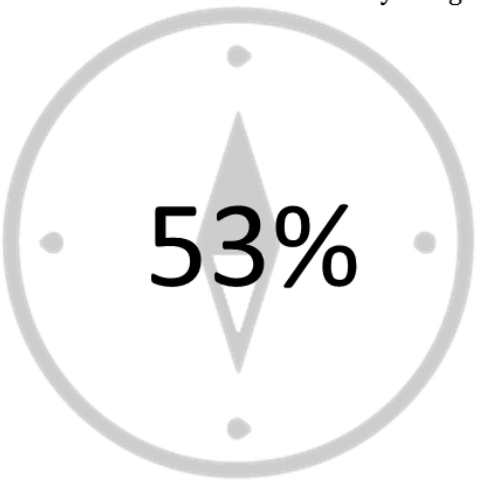
Threat

- Easy to crack 4-digit PINs
- Spoof fingerprint authentication
- Inability to change biometrics data once stolen
- Personal information and linked financial accounts easily available to attackers once hacked

With good reason, the majority of survey respondents also said to use a PIN or fingerprint device lock feature while traveling overseas. Device-lock is the first line of defense, initially securing mobile devices from the prying eyes of thieves and other malicious actors when they fall into the wrong hands. The 21% who do not enable this feature are exponentially increasing the risk to their personal and business information, especially for linked PayPal or bank accounts. However, researchers have also shown the ease of cracking a 4-digit PIN, or spoofing a fingerprint from a photo and using it to unlock a device. Users should use complex PINs consisting of at least eight characters, and change PINs following suspicion that the mobile device has been tampered with.

GPS Locators

How many use geotagging and GPS services while traveling overseas?



Function

- Determine location
- Turn-by-turn directions
- Nearby points of interest
- Gauge distance and time to meeting and office locations

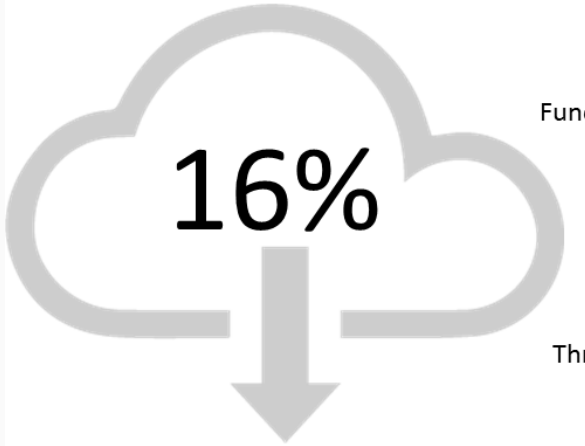
Threat

- Jammers can block or scramble signals
- Spoofed and incorrect information
- Intelligence gathering by malicious actors to determine your location at any given time

GPS can be a time- and confusion-saver while traveling overseas, whether trying to identify a current location, meeting place, or the closest restaurant. But an individual's location coordinates can also reveal too much information to a malicious actor. In a study of convicted burglars, "78% said that they strongly believed social media platforms like Facebook, Twitter and Foursquare are being used by current thieves when targeting properties." In worst case scenarios, this location information can be exploited for kidnapping and extortion purposes. Disabling GPS services when unnecessary or not in use can help mitigate these potentially physical security risks.

Free Apps

How many download free apps while traveling overseas?



Function

- New tools can be acquired to potentially assist the traveler
- Instant information access

Threat

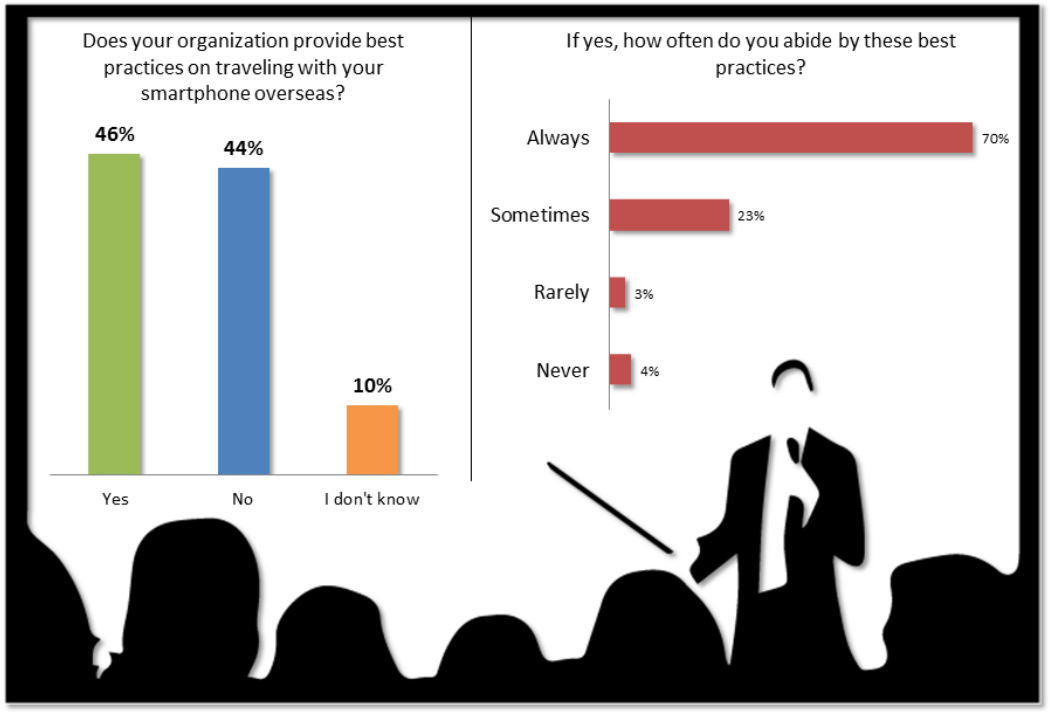
- 40% of companies don't properly secure apps
- One-third are never tested for vulnerabilities
- Can be a disguise for malware
- Often gather more user information than is necessary

Very few respondents download free apps while traveling overseas, likely due to the known risks. Free apps can disguise malware and information collection among their seemingly legitimate programs. Unfortunately for the users who downloaded the "BeNews" app, that was just the case. After installation, BeNews requested three permissions from users in order to evade Google security detection. Then, the malicious code went to work allowing actors to access the mobile devices remotely. In a separate example, a basic Flashlight app accessed a user's calendar, camera, and location services, grabbing much more personal information than was necessary to turn on the light. For potential signs of a bad app, see Trend Micro's 12 Most Abused App Permissions.

Click here for in-depth coverage on exploitation of the **BeNews** and **Flashlight** apps. Additionally, click here for Trend Micro's **12 Most Abused App Permissions**.

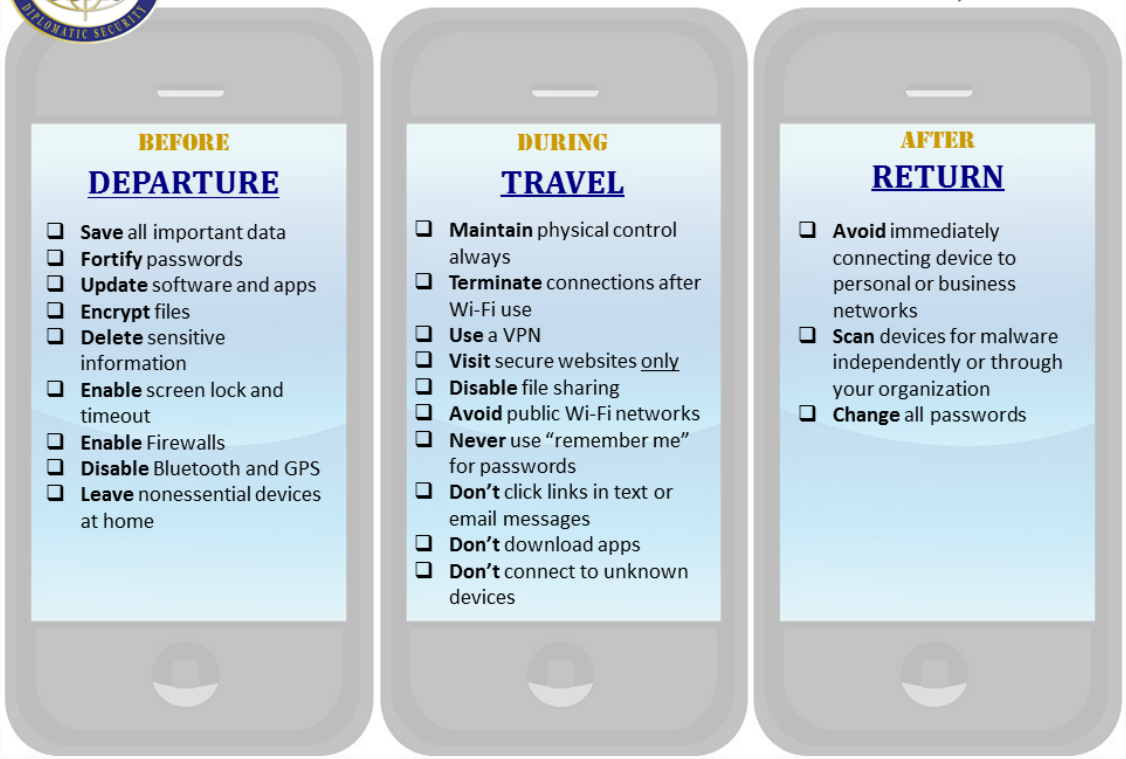
The Truth About Best Practices

We know the risks, so let's do something about it.



OSAC QUICK-GUIDE: TRAVELING WITH YOUR PHONE

When in doubt, leave it out!



Stephen P. Brunette
OSAC Executive Director

Lisa Grice
OSAC Deputy Executive Director

Daniel Schlehr
OSAC Co-Chair
Vice President, Global Security Services
Raytheon Company

Telephone: 571-345-2223

This is a U.S. Government inter-agency website managed by the Bureau of Diplomatic Security, U.S. Department of State.

Please note that all OSAC products are for internal U.S. private sector purposes only. Publishing or otherwise distributing OSAC-derived information in a manner inconsistent with this policy may result in the discontinuation of OSAC support.

The Overseas Security Advisory Council (OSAC) provides links to non-government websites as a public service only. The U.S. government, including OSAC, neither endorses nor guarantees in any way the external organizations, services, advice, or products included in these website links. For more information, please read our **full disclaimer.**

Overseas Security Advisory Council - Bureau of Diplomatic Security
U.S. Department of State - Washington, D.C. 20522-2008
Telephone: 571-345-2223 - Facsimile: 571-345-2238