Tech Brief

ESET

11 Tips for protecting your data when you travel

- Public locations present a multitude of security risks
- Sensitive data can be lost without proper security
- Cybercriminals aim to exploit when your guard is down

By Stephen Cobb, ESET Security Evangelist

When we relayed the FBI/IC3 warning to travelers about a threat involving hotel Internet service overseas, it produced a lot of requests for advice on how to respond to the threat. In response ESET researchers developed a list of data security tips for travelers. These tips will help you keep your data safe while traveling and should defeat the threat.

1. Make sure your operating system and antivirus software are updated before you go on the road.

2. Backup your data before you head out (and store the backup in a safe place).

3. Consider leaving some data behind or move sensitive data from your laptop hard drive to an encrypted USB stick.

4. Make sure you have password protection and inactivity timeout engaged on all devices including laptops, tablets, and smartphones.

5. If possible, only use reputable hotel Internet service providers (ask the hotel who their provider is before you book).

6. If the hotel Internet asks you to update software in order to connect, immediately disconnect and tell the front desk.

7. If you use hotel Internet to connect to your company network use a VPN.

8. Do not use WiFi connections that are not encrypted with WPA and avoid WEP encrypted connections which are easily hacked.

9. Consider getting a 3G or 4G hotspot and using that instead of hotel Internet.

10. Avoid online banking and shopping while on any hotel or public Internet connection.

11. Disable pop-ups in your web browser.

Additional tips for car travel: If you are on the road and suspect that your Windows laptop has become infected you can get a free online scan from ESET.

Don't assume your laptop is safe from malware when traveling just because it is a Mac. Consider installing a reputable antivirus product, for example, you could install a free 30-day trial of ESET Cybersecurity for Mac OS X before you head out on your travels.

FBI/IC3 warns if a pop-up appears as you are signing in to the hotel Internet and asks you to perform a software update, it may actually be a malware infection.

www.eset.com

ESET BUSINESS SOLUTIONS

ESET Endpoint Solutions

ESET Endpoint Antivirus (Windows/Mac°/ Linux°)
Antivirus / Antispyware

ESET Endpoint Security (Windows)
Antivirus / Antispyware / Firewall / Antispam

ESET Mobile Security (Windows Mobile/Symbian)
Antivirus / Antispyware / Firewall / Antispam

ESET Server Solutions

ESET Mail Security (Windows/Linux)
Antivirus / Antispyware / Antispam

ESET File Security (Windows/Linux)
Antivirus / Antispyware

ESET Gateway Security (Linux)
Antivirus / Antispyware

*ESET NOD32 Antivirus Business Edition Mac OS X,
 ESET NOD32 Antivirus 4 Business Edition for Linux

> Do not use WiFi connections
> that are not encrypted with WPA
> and avoid WEP encrypted connections
> which are easily hacked.

**What not to do when on
the road with your laptop**

Do not park your car and place your laptop in the trunk. Place your laptop in the trunk before you reach the place you are parking.

The reason? Someone who sees you place a computer in the trunk and then walk away from the vehicle knows the car is worth breaking into or stealing.

**WEP/WPA? How to know which
encryption scheme an access
point offers**

If you are using a Windows 7 laptop you can see the encryption type for any available access point when you display the list of access points from the network icon in the Taskbar (typically lower right of the screen). You may have to hover over the point in the list to see the information.

If you are using a MacBook you can Option-Click the Airport icon for a list that will display the encryption type of your current connection and, on hover, other connections, as shown on the right.

*Stay up to date with the latest Internet threats—
visit **blog.eset.com**.*

*Protect your digital privacy with ESET. For more information on your security options, go to **eset.com**.*

ESET   **www.eset.com**