Prepare Your Laptop for Traveling

Stephanie Obodda - 2022-05-25 - Comments (0) - Physical Security

Whether jetting to Japan, basking in Barbados or camping in the Catskills, your laptop will probably come along on the trip. If you do pack a computer, be sure to prep it for the trip. Think of the following precautions as the equivalent of bringing the sunscreen (you don't want to get "burned").

1. Prepare Your Laptop for the Trip

- ***Remove confidential information from the hard drive to prevent if from being lost or stolen.***
  If the sensitive information is not yours you could be held liable and Brown's reputation could be damaged.
- ***Use hard drive encryption if possible or use a second hard drive.***
  A login prompt is not a deterrent. Hard drive encryption will make it far more difficult for someone to retrieve the information should they gain access to the hard drive. There are several commercial packages that will perform this function that are also "user friendly." Alternately, use a second hard drive with pre-installed operating system and applications that you can swap out to your laptop's original hard drive. Use the second hard drive for trips leaving your original drive in a secure place at home. Contact your DCC for recommendations and assistance.
-
  - *If planning to travel internationally, be aware that some countries ban or severly regulate the use of encryption. You should therefore check country-specific information before traveling with a laptop. More details are available in the Learn About BitLocker and Learn About FileVault articles.*
  - *You should also become familiar and comply with all export controls (see Brown's Export Control Policy).*
- ***Turn off file and printer sharing.***
  Wireless or not, network shares expose your system to unnecessary risk while traveling. File sharing protocols often advertise your presence on the network. This applies to any other services you may running or connecting to, such as FTP and Remote Desktop software (other examples include RDP, VNC, pcAnywhere). Filesharing services tend to advertise your existence on the network. In public areas like the airport, a café, or even a hotel you don't want to draw attention to your computer on the network.
- ***Configure your firewall to block inbound connections.***

In the Windows firewall this is accomplished by clicking the “No Exceptions” check box. Any open ports that you are unaware of will not be able to accept connections.

2. Prepare the Wireless Card

- ***Keep the wireless card off when not being used.***
  Wi-Fi cards scan the air looking for known and/or available networks. Hackers can listen for this traffic, detect your presence, and see what SSIDs you typically connect on. Keeping the wireless card off when not in use is a good idea whether traveling or not. Turning off an idle wireless card conserves battery power and stops your system from advertising what networks you have been using.
- ***Disable auto-connect features.***
  Your computer may be set up to auto-connect you to a hacker, who can make their system look like a viable access point (AP). Note that Windows client is designed to auto-connect to networks in your Preferred Network List (PNL) first. If it does not find one, it will then try to auto-connect you to any available open network.
- ***Configure the card to use infrastructure networks only.***
  Infrastructure networks are client-to-network versus ad-hoc (“on-the-fly” type of) networks, which are client-to-client. Making an ad hoc pretend to be a legitimate AP is an easy and sometimes accidental hack.

3. Be Vigilant

- ***Don’t use public wireless, unless you take precautions.***
  Public wireless is inherently insecure. Most hotels, airports, and “hot spots” have little to no security, meaning your connection can easily be sniffed – especially when using unsecured protocols such as many Instant Messaging applications and many email applications and sites. Always assume the hot spot network has at least one hacker on it.
- ***Never connect to an ad hoc network, especially in a hot spot.***
  Check your documentation and know what an ad hoc network looks like in your client software. In Windows it looks like two PCs “beaming” at each other.
- ***Establish a VPN connection into Brown if working with sensitive info, or if on a public or guest network.***
  Why? Email and IM are often in clear text. This will insure that all your network traffic coming from your PC is encrypted, at least to the point when it reaches Brown’s VPN concentrators. Once connected all of your application traffic such as email, IM, RDP, etc. is sent through the tunnel and is encrypted.
- ***Do not purchase a replacement laptop when traveling to certain countries.***
  Seductively low prices may come with a hidden cost. The laptop could be a stolen or fake, made of worthless components. Even worse, malicious software could have been installed on a legitimate laptop to collect username and passwords, to steal intellectual property, and to monitor its activities once stateside again. Brown has

received reports of this happening from those who have traveled to China, for example.

Tip: See the companion document, Prepare Your Mobile Device For Traveling, for recommendations on protecting your smartphone and tablet.