Prepare Your Laptop for Traveling

Stephanie Obodda - 2016-01-04 - 0 Comments - in 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 severely 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).
Files共享服务倾向于在您的网络上宣传您的存在。在像机场、咖啡馆，甚至酒店这样的公共场所，您不希望吸引对您的计算机上网络的注意。

- **Configure your firewall to block inbound connections.**
  在Windows防火墙中，这可以通过单击“无例外”选项来实现。任何您不知道的开放端口将无法接受连接。

2. Prepare the Wireless Card

- **Keep the wireless card off when not being used.**
  Wi-Fi卡会扫描空气以查找已知和/或可用的网络。黑客可以监听此流量，检测您的存在，并看到您通常连接的SSID。不使用时关闭无线卡是一个好主意，无论是旅行还是不旅行。关闭闲置的无线卡可以节省电池并阻止您的系统通过广告它所使用的网络来宣传。
- **Disable auto-connect features.**
  您的计算机可能会被设置为自动将您连接到黑客，他们可以将他们的系统设计成一个可用的接入点（AP）。注意Windows客户端被设计成在您的首选网络列表（PNL）中首先自动将其连接到网络。如果它找不到一个，它将然后尝试自动将您连接到任何可用的开放网络。
- **Configure the card to use infrastructure networks only.**
  基础设施网络是客户端到网络类型的网络，而不是ad-hoc（“随身”类型）的网络，它们是客户端到客户端的。让ad hoc假装是合法的AP是一个容易且可能偶尔是无意的黑客。

3. Be Vigilant

- **Don’t use public wireless, unless you take precautions.**
  公共无线网络固然是不安全的。大多数酒店、机场和“热点”几乎没有或没有安全措施，这意味着您的连接很容易被嗅探——特别是当使用未加密协议时，如许多即时消息应用程序和许多电子邮件应用程序和网站。总是假设热点网络至少有一个黑客。
- **Never connect to an ad hoc network, especially in a hot spot.**
  检查您的文档并了解ad hoc网络在您的客户端软件中看起来如何。在Windows中，它看起来像是两个PC “beaming”给对方。
- **Establish a VPN connection into Brown if working with sensitive info, or if on a public or guest network.**
  为什么？电子邮件和IM通常都是以明文形式发送的。这将确保您网络流量在您的PC被加密，至少在它到达Brown的VPN集线器时。一旦连接，所有您的应用流量，如电子邮件、IM、RDP等，都会通过隧道发送，是加密的。
- **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.