

Laptop Protection Away from Home

By Bart Koslow

There are many steps you can and should take to protect your laptop. There are both physical accessories, software protections and combinations of both that may be used.

Accessories should include a portable surge protector, at least one USB flash drive that is large enough to contain all your confidential programs and data, and a carry case that will carry and protect your laptop and your laptop accessories. A neoprene sleeve for additional protection inside and outside of your carry case is advisable. You may purchase one on EBay (from China) for less than \$10 delivered. I recommend the Belkin Surge Protector. model F9H220-TVL, which has a retractable power plug, 2 power outlets and modem protection. It may be purchased for about \$15 delivered. A USB flash drive that contains U3 software is extremely desirable. U3 software will enable you to password protect your flash drive and launch programs from it using any computer. If you already have a flash drive without U3 software, you may download free software that will password protect your flash drive. You may go online and download U3 software from a number of flash drive manufacturers. However, it may not work on your flash drive. The best program I have found that will password protect, encrypt and even hide your critical files on any type of drive is TrueCrypt. It will work on a USB flash drive and even on a DVD-RW. TrueCrypt is free open-source disk encryption software for Windows Vista/XP, Mac OS X and Linux. (www.truecrypt.org) There is no size limitation. You may drag and drop files into and out of the TrueCrypt container, partition or even an entire system. To create the TrueCrypt container on a USB drive you must use Traveler Mode from the TrueCrypt files extracted to your hard drive.

Away from home you will most likely use WiFi hotspots at airports, hotels, coffee shops, libraries, etc. Beware! Your computer and its information may be in great danger! Many sites are not encrypted and those that are can be hacked without difficulty. You not only have to worry about spyware, viruses, and other invasive software, but your transmissions can be detected and read by hackers with packet sniffers. Even encrypted sites are potentially dangerous as they may easily be decrypted. In addition, watch out for the Evil Twin. This is a phishing WiFi site that has a name almost the same as a legitimate one and which will attempt to obtain your personal data. When you are in a public WiFi hotspot, make sure you know the correct SSID (station identifier) for the hotspot you wish to use. Check with the provider to confirm the network name, login page appearance, and password, if any. If two SSIDs look the same, stay away altogether. It is a good idea to avoid accessing your bank accounts, brokers, or similar sites when in a public hotspot. Watch out for shoulder surfers. You cannot be too careful. When you do sign on, make sure the website is using secure SSL before you enter any passwords or other information. SSL is where you see

https:// before the URL in the address bar or you see a symbol that looks like a gold lock in the right hand corner of the page.

Like a desktop computer you must use a firewall, anti-virus and anti-spyware software on your laptop. Unlike a desktop computer you do not have a router for significant additional protection. Start by turning off file sharing. Next, turn off Ad Hoc network connections or anyone can wirelessly connect to your computer. In Win Vista the default is off, but not in Win XP. If you use Vista turn off Network Discovery to make your laptop invisible to others in the vicinity. If you use Vista and designate your network connection as Public, Network Discovery and file sharing are automatically turned off. Disable Chat for for MS Networking. Turn off Auto-Connect. Connect manually only. Configure your laptop browsers to validate servers' certificates. Go to Windows Administrative Services and disable Windows Telnet Services, Universal Plug & Play Device Host, Remote Desktop Sharing and Remote Desktop Help, Remote Registry, Routing & Remote Access and SSDP Discovery Service.

Go to your email program and turn on encryption for your outgoing email messages Consider setting up an extra Web-based email account to use when connected through hotspots. Encrypt sensitive folders by right clicking, and then selecting Properties, General, Advanced, and Encrypt Contents to Secure Data. Use the Control Panel to perform most of the protections outlined in the previous paragraphs. When you are not accessing the internet, TURN OFF YOUR WiFi.

Will all of the above make you safe? Not yet. The safe way to access the Internet at hotspots is through a VPN (virtual private network). This connects to the hotspot and then through a server that will protect you. I recommend Hotspot Shield from AnchorFree which will connect you to through their VPN to the internet. It is free up to 3GB of bandwidth every 30 days. If you need additional bandwidth you may use Always VPN free, or subscribe to hotspotVPN. Special VPN software is not required. You can use XP's or Vista's VPN capabilities. This service costs \$8.88 per month. It is also available for one, three and seven days at \$3.88, \$5.88 and \$6.88. Additionally, you may buy even more secure VPN encryption for between US\$10.88 and US\$13.88 per month. .

Have you password protected your laptop computer logon? Do it. *Make sure that all your sensitive data is on your USB flash drives (which by now you have password protected) and not on your hard drives.* Run your sensitive programs from a flash drive after opening the drive with a password and using a VPN. When not running programs from your flash drive, log out and disconnect it. When you are not accessing the internet, TURN OFF YOUR WiFi. Now you should be protected when using hotspots.

As a last resort if all else fails, phone lines are universally available. If you have any doubts or if you are not near a WiFi connection or other high speed connection, you can always use a dial up connection to connect to banks,

brokers, etc. It may be slow, but you will know you are safe from the hazards of public WiFi. Just in case, carry two phone cords, a 1 to 2 phone line adapter, and a downloaded copy of NetZero software. NetZero gives you 10 free hours a month of dial up service, and local numbers are available over the entire country.