

Kiplinger.com

Safe trip

Source: THE GUARDIAN

My partner and I are planning a round-the-world "trip of a lifetime" and expect to be away for several months. We will still have to manage our bank and credit card accounts. We do this mostly by internet, but how can we continue to do this on the road? I have reservations about internet cafes: how do I know they are not running software to record my account and password details? Presumably an internet cafe would not want me to plug my laptop into their network, for their own security.

Tony Wyers

Jack Schofield replies: I have not been round the world, but I have usually managed to find a cybercafe that would let me use my laptop, and some offer it as a service. You can't guarantee that a cybercafe will not have a "packet sniffer" that could capture your data. However, if your banks use SSL (Secure Sockets Layer) connections - look for https in the address, and a padlock at the bottom of the browser - then the information sent between your PC and the bank is already encrypted.

Still, it would be a better idea to use your notebook from a good hotel. Many now offer broadband to the room, or at least to the business centre, and you can ask to use that even if you are not staying there. Some hotels and airports also offer Wi-Fi wireless connections, but these are not very secure unless Wi-Fi Protected Access (WPA) is used.

I would not recommend using cybercafe computers for financial transactions. If you don't have a choice, reduce the risk by always using SSL. When you have finished, close all browser windows, open one new browser window, empty the cache of temporary internet files, and reboot the PC. Change your passwords often and, obviously, don't make the operating system remember them.

Most internet service providers have a number that can be dialled from overseas, via a modem, so make sure to get this and try it before you go. Long distance calls are expensive but may be cheaper than getting your accounts hacked.

An interesting alternative is the StealthSurfer, which is basically a USB drive. The browser (a modified Netscape 7) and security software, your data, and any temporary files are all stored on the thumb-drive so you can unplug it and take it away when you have finished. See www.stealthsurfer.biz

Another idea would be to access your home PC remotely, if it has an always-on internet connection. You can do this via a secure VPN (Virtual Private Network) connection. The website at GoToMyPC.com lets you access your home PC securely via the web. Again, you would need to test this before setting off.

This page printed from: http://www.kiplinger.com/news/XmlStoryResult.php?storyid=20040617670.4_6f840009e5bfe6f9

All contents © 2004 The Kiplinger Washington Editors