

Should You Use the Business Center PC?

Many hotels offer business centers with computers and printers. Some hotels provide these amenities free of charge while others charge a fee. Regardless, the actual cost can be quite high if you are not careful.



Randy Abrams

The hotel business center computer (or a cybercafé computer) presents serious security and privacy risks. From a security standpoint you risk having data, including usernames and passwords stolen, and you may risk the infection of documents stored on USB drives. From the perspective of privacy, data may be intercepted and you may not realize what data you leave behind.

In two hotels I discovered interesting information in the temporary files directories of the business center computers. I'm sure I would find a lot more if I checked more than once every couple of years. In a New Zealand hotel I decided to look at what might be in some temporary files on a computer in the business center. I came across what appeared to be a private document that had to do with US government cyber-security officials and some people in New Zealand. The document had a .tmp extension but simply renaming it to .doc made it quite readable in Word. Since the document was marked "Confidential" I stopped reading it and deleted it. I probably deleted a secret spy drop! In a Dublin hotel I discovered the business center computer was infected with a macro virus and some people had recently used the computer to modify their documents. Business center computers are frequently unsupervised and often not well managed - a hardware or software based key logger can be installed quickly and easily, enabling the theft of passwords and other data.

Public computers are fine for games. These computers can be used to compose and print information that is not confidential — or not intended to remain confidential. You might use a business center computer to check in for a flight — as long as you are comfortable with unknown people knowing some of your travel details. Unless you can use a VPN, you do not want to use these computers for private email or to connect to your corporation. Any documents you work on may be left in temporary files on the hard drive and then can be recovered quite easily by unauthorized people. Your privacy and security are better protected by using your own laptop. There are some risks with using your own laptop, so come back next month for "Why does my Coffee Smell like Data?" as I discuss the dangers and protective steps you should take when using wireless internet.

As always, feel free to send questions or comments to askeset@eset.com



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.