



Ask Bob Rankin

Need expert tech support? Ask Bob about Computers or the Internet!

Google Custom Search

Ask Bob!

(Enter search keywords, or ask your question.)

Recommended: [The Top 20](#) [Free Anti-Virus](#) [Free Faxing](#) [Magic Jack](#) [Free Credit Reports](#) [Faster Windows](#) [Free Online College](#) [Free Satellite TV](#)

Securing Your Laptop

Category: [Laptops](#) [Security](#)

The mobility and convenience that laptop computers provide has made it imperative for users to take steps to secure their laptops, and the data stored on them. There are several simple things that you can do to keep your laptop safe. Read on to learn how to protect your laptop from theft, snooping and data loss...

Share This 49

Build a Website: Web.com®

Web.com/BuildWebsite
10,000+ Templates for Your Website. Free Domain & Hosting. Start Now!



Sony® VAIO® T Series

store.sony.com/VAIO
Great Deals on T Series Laptops 3rd gen Intel® Core™ i7 processor.



Track a Stolen Computer

LoJackforLaptops.com
Track Down Your Stolen Computer LoJack for Laptops. Official Site.



AdChoices

combination or key lock device, and attach to the security slot found on most notebook computers. Expect to pay about US\$40 for a high-quality laptop security cable. A determined thief with a bolt cutter could foil this device, but it certainly makes it a lot harder to grab and run.

Another physical security device that you can add to your laptop is a theft protection tab. This tab is used to identify the owner of the computer and to prevent people from trying to resell your stolen computer. If this tab is removed then it leaves a permanent acid "tattoo" on the laptop, and in some cases it can also damage the LCD. These security tabs are available from [STOP](#) for about \$25.

Biometric devices can also be used to ensure that if your laptop is stolen, it can't be used by someone else. Biometric devices include fingerprint scanners and retinal scanners. These devices can be added to just about any laptop. The fingerprint scanner comes standard on some Toshiba laptops. I expect that in the next year or two, we'll see more mobile devices using facial or voice recognition. If you have a smartphone running the latest version of the Android operating system, you can try out the face recognition feature now.

Security Software

Front Door Software's [Retriever](#) software can help to get your laptop back if it's lost or stolen. Retriever displays ownership information at startup, and can also report tracking information to the owner if the laptop goes online. Also, if your laptop is stolen, you can login to the Front Door website and enter a lockdown code that will help to protect your information. You can even send a personal message to the thief, or cause an audible "This laptop was stolen!" alarm to be played. Retriever works on Windows, Linux, and Mac OS X. The software has a free Basic version, and a Deluxe version with a 90-day free trial. Deluxe costs \$30 for 3 year license.

[LoJack for Laptops](#) is another software-based laptop recovery product. This company provides you with a Theft Recovery Team that's actually a licensed private investigation agency. They will work with local law enforcement and Internet Service Providers, using information sent from the stolen computer, to assist local police in recovering your computer. They claim that 3 out of 4 stolen computers with LoJack for Laptops are recovered. LoJack for Laptops costs \$29/year.

[Laptop Sentry](#) is an offering similar to Frontdoor and LoJack, but with one unique feature. It automatically backs up your files to cloud storage so you'll never lose your data. You can track and control your laptop remotely as well as recover, delete, and encrypt files.

And of course, there's always the "inside job" that nobody sees coming -- the threat of hackers and snoops that attack through viruses and spyware. Every laptop should have an up-to-date anti-virus and anti-spyware software package installed, to identify and remove malware from your system. Read my companion article [Should I Buy Anti-Spyware or Anti-Virus Software?](#) for my recommendations to keep your computer safe from viruses, spyware and other threats.

File Encryption

File encryption is used to protect your data from hackers, thieves and others who may access your computer without permission. Windows Vista, Windows 7 and Windows 8 have [BitLocker](#), which can be used to encrypt an entire hard drive. Other options for encryption are [PGP Whole Disk Encryption](#), and the free [TrueCrypt](#) software, which can encrypt a hard drive partition, USB flash drive or external hard drive. Both PGP and TrueCrypt work on Windows, Mac and Linux systems. Learn more about the pros and cons of encryption in my related article [Should You Encrypt Your Hard Drive?](#)

Password Security

In addition to physically securing your laptop and protecting your computer with security software, you also need to take steps to protect your laptop with strong passwords. While it is important to set up a user account password for your laptop you will also want to set up a power-on password. These passwords will prevent unauthorized people from logging in to your computer, or accessing it by using a boot-up disc. To create your and power-on password you will need to enter your BIOS security set-up menu. This is usually accessed by pressing the Del, F1 or F2 key while your computer is starting up. Try to use passwords that include a combination of at least eight letters and numbers, and stick to a password rotation schedule that changes your passwords on a regular basis. Make sure you remember the passwords, or you'll lock yourself out!

Here's one other point on passwords, particularly relevant for travelers. If you allow your web browser to store your passwords, and your laptop is stolen, you've given away the keys to the kingdom. Roboform and similar tools can keep all your passwords handy, but with the protection of a master password. See [Is Your Password Hacker-Proof?](#) for more information on password strategies.

Keeping Your Laptop Safe

Here a few more practical tips you can use to secure your laptop and your data.

Consider using free [Portable Apps](#) that can be loaded on a USB flash drive. Using this approach, all your software and your personal files never need to be stored on the laptop's hard drive. This has the additional advantage that you can plug the flash drive into any available computer, and work without fear of leaving behind any personal data. Just be sure that the drive and the laptop don't travel together in the same bag.

If you'll have Internet access while traveling, an even better solution might be cloud-based apps and storage. By managing your email, documents and other tasks with free cloud-based services, all your data is stored online, and you don't need to carry a flash drive that could possibly get lost or stolen. See [Seven Free Cloud Services You Should Try](#) and [Free Online Photo Editors](#) to get an idea of all the tools available.

To keep your laptop as safe as possible you will want to combine physical, software and use password strategies. While not all of the above security methods are applicable, practical or necessary for all laptop users, it is still important to understand what your security options are so that you can alter your security strategies as your computer use evolves.

What strategies do you use to keep your laptop safe? Post a comment below...

Laptop Security Tips

Over half a million laptops are stolen every year, from cars, coffee shops, offices, campuses, and hotel rooms. Keeping your laptop or netbook safe involves a combination of common sense, physical security devices, and software strategies. Let's start with devices that make it harder for your portable computer to be carried off by someone else.

Physical security devices are used to keep your laptop from being stolen or used without your authorization. The most basic physical security device is a laptop security cable. This cable connects to your laptop and secures it to a non-moveable item in your office, hotel or conference room. For example, you can connect your laptop to your desk, or the leg of a conference room table.

The cables

usually have a



SUPERCHARGE
YOUR SYSTEM TODAY!



\$77.99 BUY

m4 60GB/s 2.5-inch SSD
21x faster than HDD



m4 SSD



V4 SSD



ADRENALINE

FREE SHIPPING
FREE COMPATIBILITY TOOLS

crucial.com

Deface the equipment.



Reveal the invisible "Stolen Property" tattoo.

