

By Scott Lowe

---

There are a lot of reasons to make sure that your laptop stays secure -- both from a physical perspective as well as a software/data perspective. From the physical side, laptop theft isn't generally considered a positive event -- at least from the victim's perspective. From the data side of the equation, however, losing the wrong laptop can cost your company much more than the cost of laptop. Imagine the public relations fallout if your company loses a laptop containing private information about all of your customers.

This 10 Things describes steps that you can take to protect your laptop. Not all of the steps will necessarily apply to you, but they should all be considered in any comprehensive protection plan.

## 1

### Encrypt the hard drive

Scenario: You're in the airport and you lose your laptop or it's stolen. Said laptop contains your entire customer database along with personal information about each of them. Voila! Instant public relations incident -- except it is not the kind of PR that you want. Protect yourself from this kind of problem by encrypting your laptop's hard drive.

If you're using Windows Vista, consider using Vista's BitLocker drive encryption software. If you're using Windows XP or another operating system, there are a number of third party full-disk encryption products available on the market.

Although you can use EFS (Encrypting File System) to achieve a similar goal, full disk encryption provides better protection as everything on your disk gets protected and you don't have to worry about saving files to a particular location.

For more information about hard drive encryption, see the following TechRepublic resources:

- [The Top Ten Myths About Full Disk Encryption](#)
- [BitLocker Drive Encryption: Value-Add Extensibility Options](#)
- [Managing Enterprise Risk With Full Disk Encryption](#)
- [Secure your hard drive with Windows Vista BitLocker](#)
- [Become familiar with Windows BitLocker Drive Encryption](#)

## 2

### Install tracking software

Protecting data is extremely important but if your laptop is lost or stolen, you probably want it back. To this end, install software on your computer that tracks its location should it ever be lost or stolen. Most laptop theft recovery software installs to an undetectable location on the laptop and the software cannot be erased from the system.

Each time the computer connects to the Internet, it reports in with the software manufacturer. In the event that the computer is reported to the recovery software company as stolen or missing, the company tracks down the physical location of the laptop and then notifies the authorities. In many cases, the hardware is actually recovered. However, even if the laptop is recovered, you can't be sure that the thief didn't compromise your data.

Some tracking software includes the ability to remotely delete information from the laptop as well. This feature can be a lifesaver if a laptop with sensitive information is stolen. With this capability, you'll be able to delete potentially sensitive information before it falls into the wrong hands.

Here are a couple of TechRepublic resources to aid you in making the justification for tracking software:

- [Remote Laptop Security: Implementing a Laptop Theft Solution](#)
- [Lesson learned in laptop theft](#)

## 3

### Install antivirus and antispyware software

The two pronged antivirus/antispyware software blaster will do far more to protect your assets than a single application that handles only virus-busting. These days, spyware is probably a worse problem for many organizations than viruses were in their heyday. Many spyware infestations install keylogging software and other kinds of monitoring software designed to gain access to private information. Laptops can be especially vulnerable to spyware since they often spend time outside the organization's protective firewalls.

- [SolutionBase: Controlling spyware with McAfee Antispyware](#)
- [Investigating Windows Vista's built-in spyware Defender](#)
- [TechRepublic Pro Fast Facts: Antispyware Report](#)
- [SolutionBase: Stopping spyware with Trend Micro Anti-Spyware Enterprise Edition 3.0](#)

## 4

### Tie down the machine with a lock (hardware or software)

Even those employees that are issued laptops don't always carry them every place they go. As such, there are times when laptops are sitting in employees offices, in hotel rooms, at home, etc. There are numerous documented cases of laptops containing sensitive information being stolen from homes, airports, hotels, and even people's offices. If you're traveling or using a laptop at home, consider taking a security cable and lock (such as a Kensington lock/cable combination) with you that you can wrap around a table leg. Although a solution like this will not completely prevent laptop theft, most thieves go after easy targets. Any roadblock you can put up will deter would-be thieves.

- [Cable locks keep laptops on a short leash](#)
- [Laptop Alarm software download](#)  
Laptop Alarm is software that sets off an alarm on your laptop when the A/C adapter is unplugged. If someone tries to steal your laptop, they'll have to disconnect the power, after all.

## 5

### Install a software firewall

A software firewall goes a long way toward protecting a system. Such software keeps unwanted traffic away from your computer. However, not every system necessarily needs a software firewall. If you need to pick target systems on which a software firewall will be used, seriously consider laptops in your plans.

As I mentioned before, laptop computers often spend time outside your company firewall, meaning that they lose the important protection of those devices. Especially if you're out in the wild using an unsecured wireless network, a firewall will help to keep your computer from being subject to attack.

Some TechRepublic resources:

- [SolutionBase: Take a look at the Windows Vista Firewall](#)
- [Determine your need for client firewall software](#)
- [Learn the pros and cons of Windows Firewall](#)
- [Configure the Windows XP firewall after Service Pack 2](#)

## 6

### Stay current with updates

Even though they come frequently and can be a hard to keep up with sometimes, staying current on all of your installed software is critical. A number of patches are designed to correct bugs that result in vulnerabilities that can be exploited. Implement an automated system such as WSUS or, at the very least, configure your laptop for automatic updates so that patches are applied as they become available.

- [SolutionBase: Configuring Windows XP for Windows Update and Microsoft Update](#)
- [Learn how Windows Server Update Services \(WSUS\) makes Windows Server 2003 patch management easier](#)
- [Study: Unpatched PCs compromised in 20 minutes](#)

## 7

### Use a strong password

Passwords remain the most common way to secure resources, including laptop computers. Again, since laptops are often in the wild, it becomes even more important to use a strong password to lessen the risk that a local account is compromised. Make sure that all local accounts are appropriately secured, including the local Administrator account.

- [Hold your own user seminar on creating strong passwords](#)
- [Strengthen passwords for better security](#)
- [Help users create complex passwords that are easy to remember](#)

## 8

### Use wireless networks carefully

Wireless networks are everywhere -- from Barnes and Noble to Starbucks, and even McDonalds. In most of these cases, even though you often have to sign up to use the connection, the wireless service is insecure meaning that anyone within range of your laptop can pick up everything you see, do and type. Obviously, this is not good.

If you're working from one of these locations and find it necessary to work on something sensitive, try to connect to your organization's VPN service and do your work via that connection instead. With the right kind of VPN in place, traffic between your laptop and your organization's network will be encrypted. If information security is a critical concern, only use wireless networks that are secured with WPA or WPA2. This isn't a perfect solution, but is much better than using only WEP.

- [WPA wireless security offers multiple advantages over WEP](#)
- [SolutionBase: Protect your wireless network with WPA](#)
- [10 things you should know about securing wireless connections](#)

## 9

### Disable Windows services you don't need

Every service that runs on your laptop increases the attack surface of your computer, especially services that listen on particular ports. To help further protect a roving laptop, disable any services that you don't need to do your job.

TechRepublic has a number of resources available to help you complete this step:

- [Windows Vista services that can be disabled](#)
- [Windows XP services that can be disabled](#)
- [How do I... Disable services in Windows Vista?](#)
- [Video: Disable and enable Windows XP services](#)
- [Tech Tip: Shut down unnecessary services](#) (For Linux users)

## 10

### Make sure your laptop is insured

This one is easy: When all else fails and your laptop is stolen, you will probably need to replace it.

- [Is your laptop insured?](#)



## Additional resources

- **Subscribe to TechRepublic's [Downloads RSS Feed](#) [XML](#)**
- Sign up for TechRepublic's [Downloads Weekly Update newsletter](#)
- Sign up for TechRepublic's [Security Solutions](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)

## Version history

**Version:** 1.0

**Published:** September 12, 2007

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team