



Lock down Your Laptop Smart Card

20141029

Creating a Windows Login Password

Lock your laptop by making sure that your Windows user account is set up to require a password on log-in. A log-in password won't protect against an even semi-competent hacker, but it could easily be enough to dissuade unsophisticated criminals from snooping through your files after stealing your laptop.

In Windows 7, just hit **ctrl-alt-del** and select Change Password, the fourth option down. After that's set, head to the Power Options in the Control Panel, click **Require a password on wakeup** in the left-hand pane, and click the radio button next to **Require a password**.

In Windows 8, just search for "Users" to open up the Users menu in your PC Settings. Here you'll find options to both change your password and require users to log in when they wake the PC.



Encrypt Your Data

As mentioned above, a user account password won't protect your data from a determined snooper—they're easily cracked, or the thief can simply plug your hard drive into a different computer in order to access your files directly. If you travel and have any files on your computer that you simply don't want anyone else to see, you should use full disk encryption to keep them safe.

Because the strength of encryption is pretty much entirely dependent on the strength of your password, now would be a good time to talk about good password practices. You've probably heard it before, but a password can be easily cracked if it's too short or simple, or if you use the same one across multiple services. For the rest of your security measures to be effective, make sure you're following these three simple rules:

1. Use a password that's at least 12 characters, featuring a mix of lower case and upper case letters, as well as symbols and numbers.
2. Don't re-use passwords, especially for sensitive accounts, like your Windows logon, bank account and email account.
3. Change your password frequently. Every 6 months for important passwords, at the minimum. A free password manager like [Keepass](#) can make it a lot easier to follow the above rules. Again, make sure you choose a strong master password.

Bitlocker



Even without knowing your Windows password, intruders can easily gain access to files and passwords stored by Windows and other programs on your computer. They can do this by booting into their own operating system (Windows or Linux) from a special disc or USB flash drive. After doing so, they can access your hard drives just as you can when you're logged into Windows.

The only way to protect your data completely is by using encryption. You can encrypt select files, but to protect your system files and saved passwords, you must encrypt your entire hard drive. This operation takes more time and effort than encrypting select files does, but it offers more security—and it's great for laptops and netbooks that can easily go missing.

BitLocker offers protection for all of your personal files and documents, as well as for all of the system files and cached or saved passwords on your drive. Though Microsoft includes BitLocker with Windows Vista, Windows 7 Ultimate or Enterprise, and Windows 8 Pro or Enterprise, the feature isn't enabled by default. To activate it, you must manually enable it in the 'System and Security' Control Panel.



Lock down Your Laptop Smart Card

To support this simple encryption process, however, your computer must meet a few stringent software and hardware requirements. To start with, your drive must have two NTFS drive partitions: a system partition (which contains the files needed to start your computer), and an operating system partition (which you should have already, and which contains Windows and your personal files).

If the system partition is not already available, BitLocker may try to create it for you automatically, but sometimes it may not have enough available drive space to do so. In addition, your computer must have a motherboard with a compatible Trusted Platform Module (TPM) microchip, and the BIOS should be TCG (for Trusted Computing Group) compliant. Having a TPM microchip isn't mandatory, but without it the configuration and usability are more complicated.

If you don't understand the requirements, don't sweat it. To see whether your system meets them, simply open BitLocker: *Click Start, Control Panel, System and Security, BitLocker Drive Encryption, Turn on BitLocker.*

If your computer doesn't meet the requirements, it will let you know. If you get an error message about not having a TPM device, it's possible that your PC does have one that isn't enabled in the BIOS. Try checking your PC's BIOS setup menu at boot for any mention of TPM support. Otherwise, consider using a third-party encryption program, such as DiskCryptor, instead of using BitLocker.

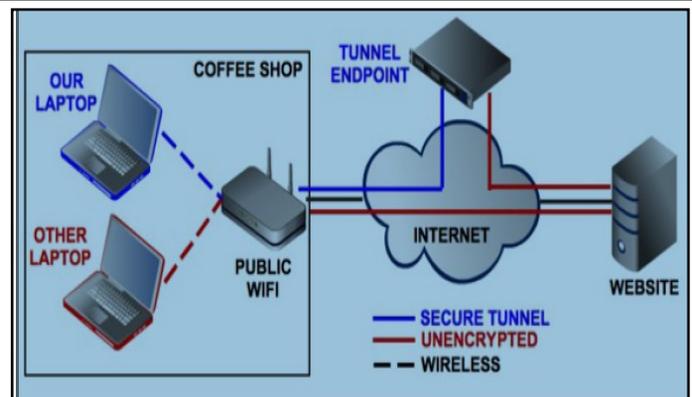
Use a VPN on Unsecured Wi-Fi Networks

This diagram shows the difference between an unencrypted and a VPN-secured Internet connection.

Unsecured Wi-Fi networks present a major threat to your system's security on the road. You don't know who else is sharing the network, potentially intercepting and recording packets wirelessly sent by your computer. Basic HTTPS web security does a good job of protecting data sent across the internet, but you are essentially at the mercy of the receiving site's security protocols. If you're transferring sensitive data, the sensible solution is to always use a virtual private network.

With a VPN, traffic originating from your laptop is encrypted, then sent to a third party server, where it can safely be forwarded on to the World Wide Web at large, safe from prying eyes. There are lots of options for connecting to a VPN. Your company may provide one for you to use, or you can set up your own VPN server at home. For most people, the easiest option will be to use a web-based VPN, many of which offer a limited free service, and low-price monthly rates for heavier users.

Easy-to-use programs such as Firesheep make it easy for snoops to see what you're writing in your e-mail messages, posting to your Facebook page, or buying online. But with a VPN, you can surf the Web through that virtual tunnel, away from prying eyes, and your Internet traffic is encrypted. Whether you just want to access Wi-Fi networks on the road without potentially exposing your activities to nosy strangers, or whether you need to enable a team of remote employees to handle business securely on the Internet, you can find a VPN to fit your needs.



VPN for Beginners

Numerous VPN providers, including Banana VPN, Black Logic, LogMeIn Hamachi, and StrongVPN, have started offering their services for a fee, generally from \$15 to \$20 a month.

Is the privacy factor alone worth the effort? Yes, but VPNs offer other advantages as well. For example, if you're in Canada, ordinarily you can't watch a U.S. TV show on Hulu. But you can access the show if you use a VPN to obtain a U.S. IP (Internet Protocol) address.

Some VPN providers offer another benefit: anonymous Web browsing, which allows you to roam the Internet without being tracked. If your ISP blocks some applications, such as Skype or other VoIP (Voice over Internet Protocol) applications, you can use a VPN to get around the restrictions.

These VPN services may sound exactly like what you need. Beware, however: Not all services are created equal. If a service doesn't have enough VPN servers-- technically, VPN concentrators-- to support the number of customers, you may experience poor Internet speeds or be unable to make a connection at all. So, before subscribing to a VPN service, look into what its customers say about it. Better still, if the company offers a free test period, take advantage of it before paying money for a service that may not meet your needs.



Lock down Your Laptop Smart Card

20141029

VPN on Your Router

Besides paying \$15 to \$20 a month to a VPN subscription service, you might be able to install a VPN server into your router using open-source, alternative router firmware such as DD-WRT and OpenWRT. This firmware will allow you to use many, but not all, Wi-Fi routers and access points as VPN endpoints.

Before flashing your Wi-Fi hardware with any alternative firmware, make sure that it's supported. The last thing you want to do is to "brick" your wireless device--rendering it useless--just to set up a small VPN. Be sure to consult the [DDWRT](#) or the [OpenWRT](#) supported device lists. As these lists are all works in progress, check back often if you buy a brand-new router or access point. If you'd rather not take your hardware's life into your own hands, some routers, such as Buffalo Technology's WZR-HPG300NH AirStation Nfinity Wireless-N High Power Router, come with DD-WRT already installed.

VPN Server Software

Some desktop operating systems, including Windows (from XP) and Mac OS X, include VPN server software. Granted, these are very simple VPNs, but they may be all you need. Of course, the Windows Server family comes with more-sophisticated VPN setups. If you're running all Windows 7 clients and Windows Server 2008 R2, you may also want to consider using DirectAccess, an advanced IPsec VPN that runs over IPv6 on ordinary IPv4-based LANs and the Internet.

If you don't choose to use DirectAccess but opt for Microsoft's older VPN technologies, Windows Server 2008 R2 has a helpful new feature: VPN Reconnect. Just as the name suggests, it will try to connect VPN sessions automatically if they're interrupted by a break in Internet connectivity. This function can be handy for users with spotty Wi-Fi connectivity, since they won't need to manually reconnect with the VPN after they reestablish a network connection. Most popular routers, such as the Linksys WRT160NL, make it easy for a VPN connection to work through the firewall.

Another way to add a VPN to your small network is to install VPN server software yourself. The best known of these is OpenVPN, which is open-source. It's available in versions for almost all popular desktop operating systems, including Linux, Mac OS X, and Windows. If setting up native OpenVPN sounds a little too technical for you, you can run it as a VMware or Windows Virtual Hard Disk OpenVPN virtual appliance. With this arrangement, you'll have a basic VPN up and running in minutes. But OpenVPN is far from the only VPN software out there. Other programs worth considering are NeoRouter and Tinc.

Sources

<http://www.pcworld.com/article/2025897/a-road-warriors-guide-to-locking-down-your-laptop.html>

<http://www.pcworld.com/article/242617/how-to-use-bitlocker-to-encrypt-your-hard-drive.html>

<http://www.pcworld.com/article/236006/KeePass.html>

<http://www.pcworld.com/article/223044/vpns-for-beginners-to-experts.html>

http://www.dd-wrt.com/wiki/index.php/Supported_Devices

<http://wiki.openwrt.org/toh/start>