Protect your laptop safely from thieves

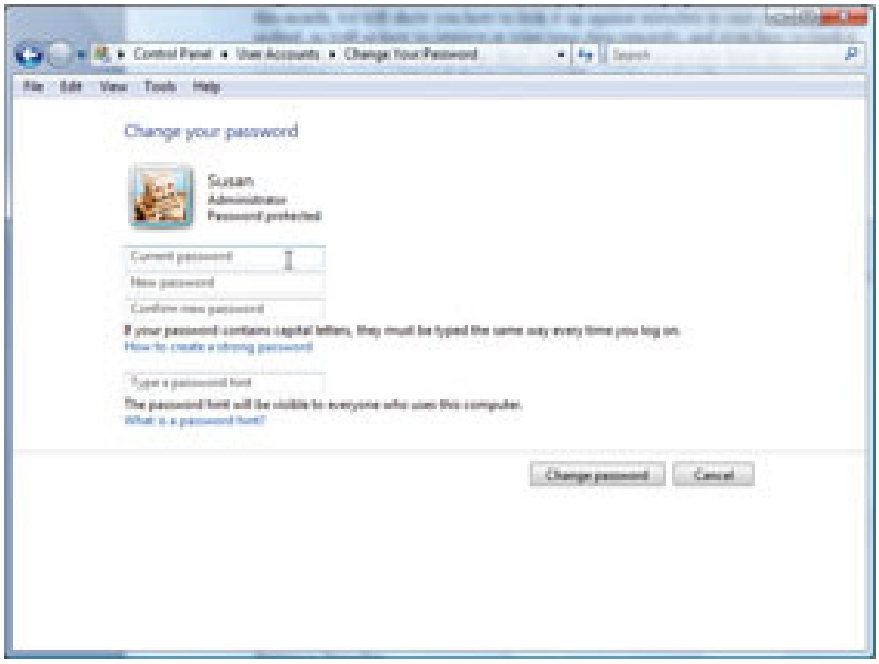
You must be worried about losing your hard drive, this is probably the most valuable component on your laptop. The first reason most people complain is that they have put all their 'lives' on their laptops from software, photos, letters

Laptops of the table can be stolen anywhere and anytime. When you are in a coffee shop or at the office itself, just take your eyes off the laptop for a moment and it is most likely stolen.

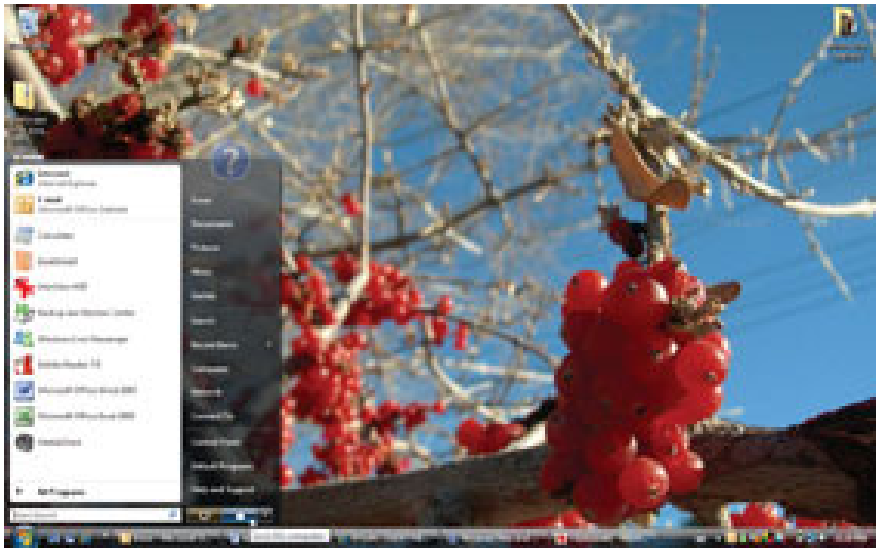
You must be worried about losing your hard drive, this is probably the most valuable component on your laptop. The first reason most people complain is that they have put all their "lives" on their laptops from software, photos, emails, documents, projects and many other precious things categorized and Stored on a laptop, it is very difficult and takes a long time to be retrieved and downloaded.

There are many security software options for computers. We show you how to prevent eavesdropping when you are using a public wireless network, how to lock your laptop in front of annoying people, how to recover, clean or monitor your data how remote

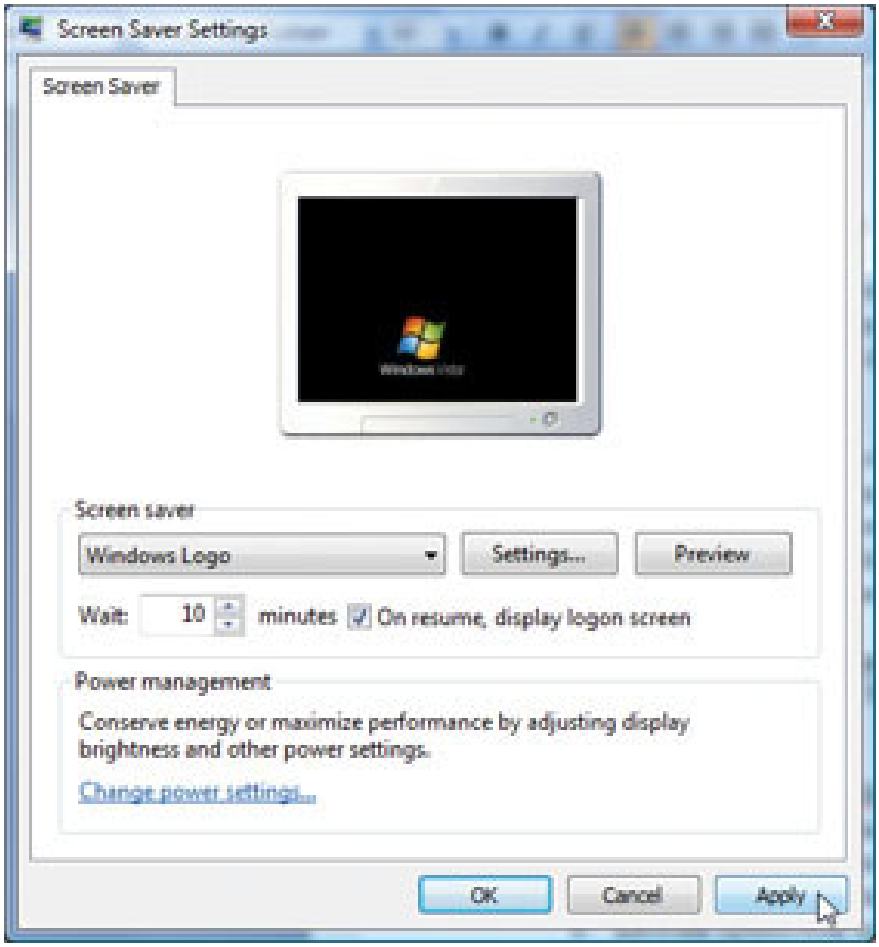
1. A secure password should be at least 8 characters long and should have a combination of uppercase and lowercase letters, numbers and symbols. You should not get a full word or your name as a password. At **Control Panel** , select **User Accounts** , **Change Your Password** (on Vista, press Ctrl, Alt, Del).



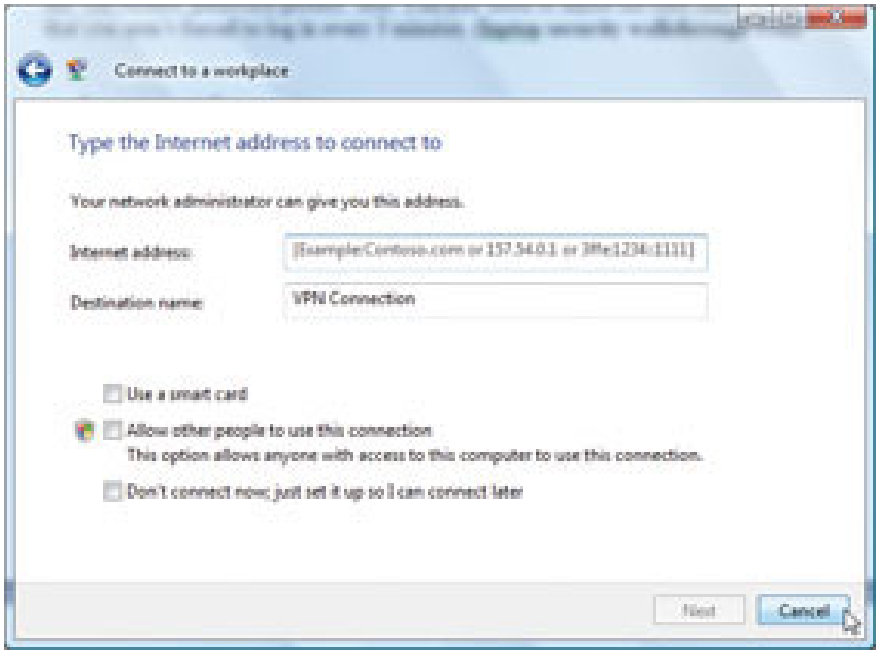
2. Protect yourself from 'unforeseen' information thieves - You don't want curious colleagues to peek at the computer when you leave the laptop during the break. On Vista, select the **Start** button and then click the lock icon. On XP, select **Start** , **Log Off** to return to the password entry screen.



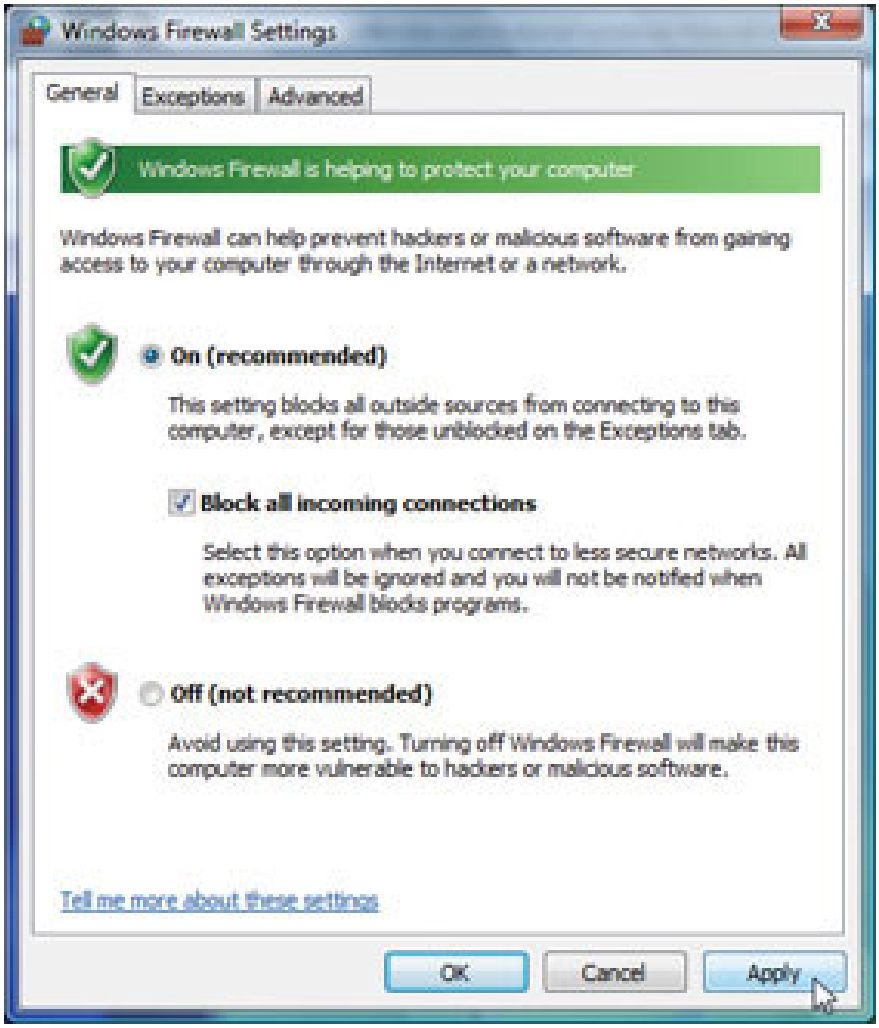
3. Password protected screen standby mode. At **Control Panel** on Vista, select **Personalization** , **Screen Saver** and then click ' **On resume, display logon screen** '. At **Control Panel** on XP, select **Display Properties** , **Screen Saver** and then click the ' **On resume, password protect** ' checkbox. You will need to adjust the timeout.



4. If your workplace has a private virtual network, you can use this network to securely send encrypted data over the Internet. At **Control Panel** on XP, select **Network and Internet Connections** (or **Network and Sharing Center** on Vista), ' **Create a new connection** ' (' **Connect to a workplace** '), then Follow the step-by-step instructions.

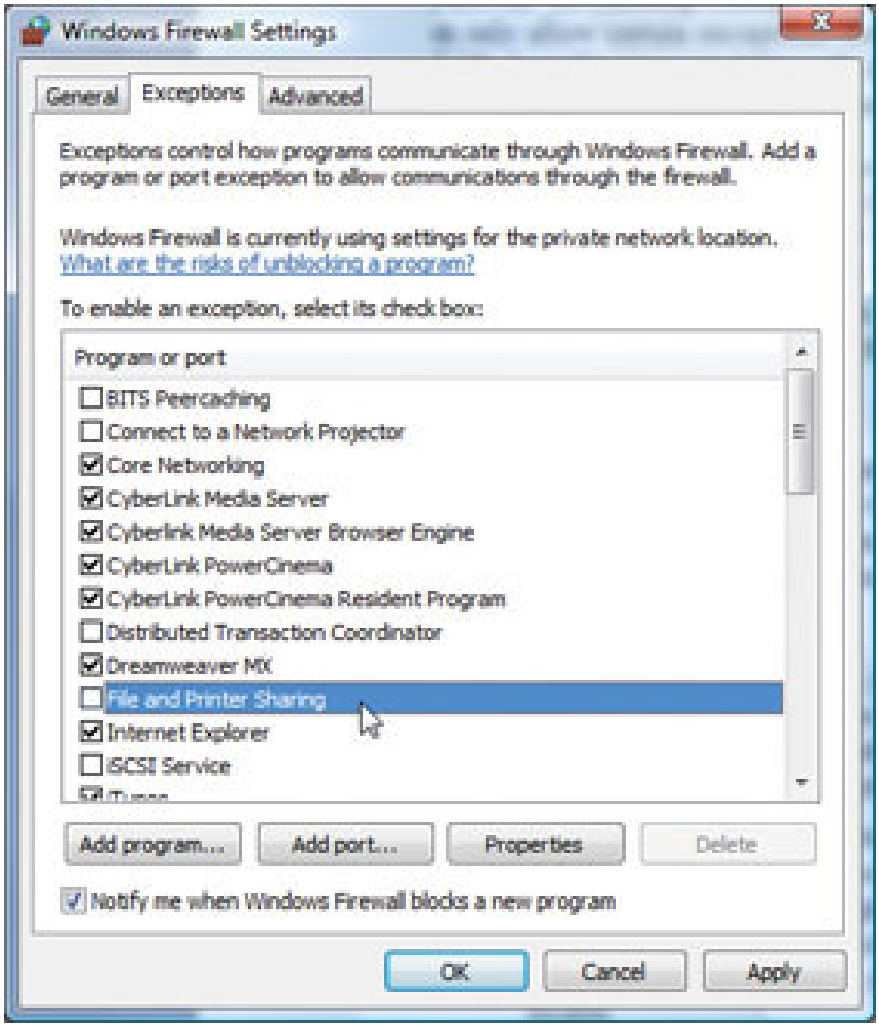


5. Make sure you use fire software in the right place and effectively at public Wi-Fi spots. Select **Start** , **Control Panel** , **Windows Firewall** . Click **Change Settings** and then select ' **Block all incoming connections** ' (Lock all **incoming connections**). Installing a second firewall, such as Firewall Pro, is a good idea.



6. When you connect to Wi-Fi at a public place, be sure to check if the connection point is dangerous. Hackers often create fake Wi-Fi connections in hotels or airports in order to trick users into accessing those connection points. Thereby the attacker can capture the information you send over the network.

7. Turn off shared files when they are not in use. XP SP2 will set this mode to default. You can do this by selecting **Control Panel** , **Windows Firewall** , and **Exceptions** and make sure ' **File and Printer Sharing** ' is not selected. On Vista, select **Change Settings in Windows Firewall** , select **Exceptions** and do the same for Windows XP.



8. Turn off wireless cards if they are not used. You can turn it off with the physical buttons available on your computer or turn off on XP by right-clicking on the wireless connection icon in the Taskbar and selecting **Disable** . On Vista select ' **Manage wireless networks** ' in **Network and Sharing Center** , right-click on the wireless connection icon and select **Disable** .

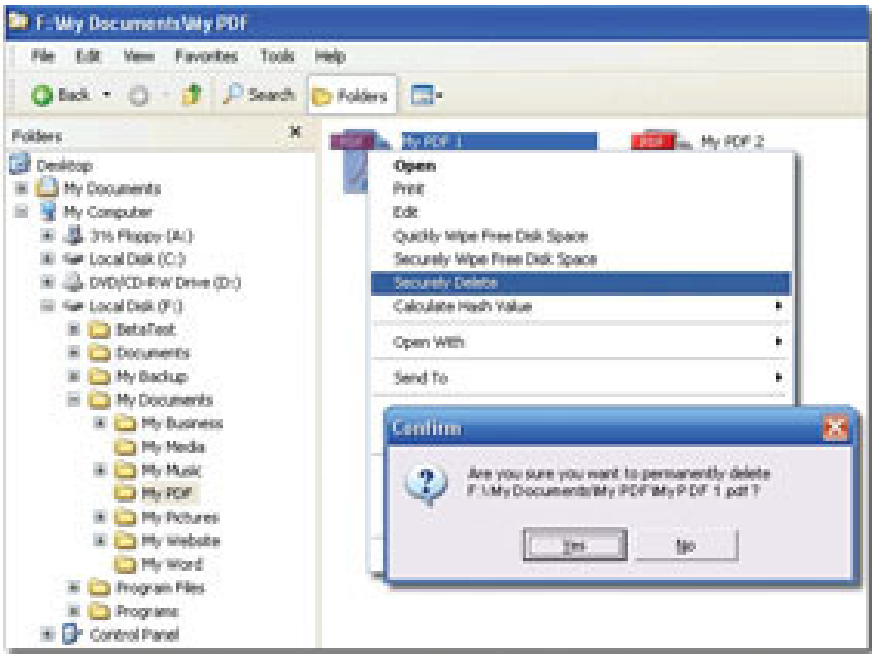
9. Beware of browsers that allow to save information for later reuse. What is convenient for you is even more convenient for laptop thieves. To delete Internet Explorer cookies, select **Tools** , **Internet Options** , **General** . Then under **Cookies** , click **Delete** . Select **Yes** to confirm, **Close** , and finally click **OK** .

10. Store your personal documents securely on your hard drive.**Safe One** allows to create 1GB safe for your files. These files can be password protected (Safe One will help you create secure passwords), a picture password or device lock such as USB key, mobile phone or camera.

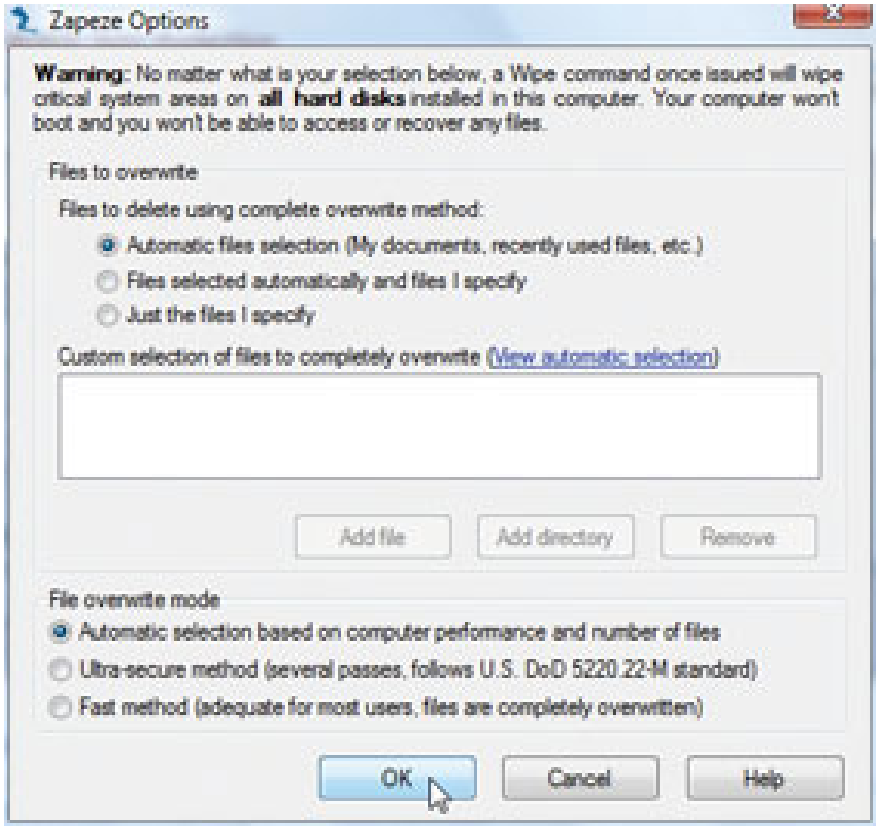
11. You can easily encrypt special files and folders on XP and Vista. Select **Start** , **All Programs** , **Accessories** , **Windows Explorer** . Right-click on the file you want to encrypt, then select **Properties** . Under the **General**

tab, select **Advanced** , then select ' **Encrypt contents to secure data** '. To cancel encryption, clear the check box.

12. A laptop thief with a lot of techniques can identify and easily access the files you have deleted. **DeleteOnClick** is a free utility that allows you to securely delete data just right-click on the Windows menu. This utility will also save disk space.



13. **Zapeze** is a service that allows you to delete remote files if your laptop is online. The benefit of this service is that you do not need to secure data before losing a laptop, you can protect them later when clicking **Destroy** .



14. You have a lot of opportunities to find your lost laptop when you join the computer tracking service - When online computer thief sends a message to this service. You can try it with **Steganos AntiTheft** (part of Secure Traveler) or **Absolute Laptop Theft Recovery** .

You finished reading the article "**Protect your laptop safely from thieves**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.