

Lambda Computing PC Health Tips

Back up your data regularly.

Backup your data at least once a week to a separate hard disk drive.

Keep your computer healthy and protected

Use up-to-date antivirus software and a personal firewall to ensure PC wellness.

Be careful with email

Do not open any email attachments that have been sent by someone you don't know, or click links in spam emails. Over 80% of all viruses are spread via email attachments.

Be careful with your personal information and passwords

Never give away your bank numbers or other personal info to sites you don't trust, or send them by email to an unknown recipient. Note: Banks never ask you to send account details by email!

Choose your passwords carefully. Your passwords should be at least 10 characters long and include lower and upper case letters, numbers, and special characters.

Be careful when using chat rooms

Never accept attachments from strangers in online chat systems, such as IRC, ICQ, or AOL Instant Messenger.

Do not download files from unknown locations

Downloading files from the Internet is risky. If you are not completely sure that the source is safe, do not download. If you do download, make sure you have set the PC to scan file downloads by enabling web traffic (HTTP) scanning.

Be careful with your credit card information

Be careful with sites that ask you to give your credit card number. Not all sites can be trusted. There are sites that collect credit card information for criminal purposes.

Viruses

Viruses are programs that, once opened, almost always cause harm to the computer. Viruses enter computers most often through email attachments or files downloaded from the internet. They can also be placed on websites, and they enter your computer when you visit such a site. New viruses are released onto the internet every day, and the methods for spreading them are increasing constantly.

Trojans

Trojans are software disguised as normal programs which can actually damage your computer without your knowledge. A typical example of a trojan is a computer game that deletes files from the user's computer while the game is running.

Worms

Worms spread from one computer to another faster than viruses and can be divided into two main categories:

- Network worms try to infect computers that are connected to the internet and do not have the latest virus definition updates installed.

- Email worms usually forward themselves to the addresses stored in your address book and often include information or documents gathered from your computer in the messages.

Spyware

Spyware is software that tracks user information and sends it to third parties without your knowledge. Spyware can collect information about your web browsing behaviour, for example, targeted advertising. It can also gather information about your email addresses, passwords and credit card numbers.

Spyware applications can be installed on your computer without your authorization or knowledge as a part of some other software you install.

Note: Public and shared computers are appealing targets for spyware. Do not use personal information or passwords on such computers.

Riskware

Riskware is not, technically speaking, a type of malware. It refers to any program that does not intentionally cause harm but can be dangerous if misused, especially if set up incorrectly. Examples of such programs are chat programs (IRC), or file transfer programs.

If you have installed such a program, it is less likely to be harmful. If riskware is installed without your knowledge, it is most likely installed with a malicious intent and should be removed.

The difference between riskware and malware is that malware is specifically designed to damage your computer.

Rootkits

Rootkits are typically used to hide malicious software from users, system tools, and antivirus programs.

Adware

Adware (short for “advertisement software”) is a software program that displays advertising material in your web browser. Some adware programs collect information about your browsing habits and computer use. Based on that information, they automatically download advertising material on your computer and display it. Some adware programs are installed together with other software programs.

Spam

Spam includes any unsolicited email that is sent in great numbers to people. Spamming slows down email systems and clogs email inboxes.

Spam can also be spread by email worms. Although the contents of a spam message may seem very appealing, you should never forward spam messages.

Phishing

Phishing (pronounced “fishing”) is a scam technique used to steal personal information. It uses false email messages that appear to come from legitimate businesses and that link to false, but genuine-looking web sites. These authentic-looking messages are designed to fool people into giving away personal data, such as bank account numbers, passwords, and credit card and social security numbers.

Note: Banks never ask for your bank account numbers or passwords by email.

Botnets

A botnet is a network of bots. A bot, or zombie, is a computer infected with malware that makes it possible to use the computer remotely, such as for sending spam. With that remote access, a malicious user can connect all such bots into a powerful network and use it for criminal activities.

A computer or a network that is used in a botnet may become noticeably slower for no apparent reason.

Windows Updates

Windows Update is a program used to update the Windows operating system.

If you do not install the critical Windows Update files immediately after they are released, your computer will be compromised by a worm that takes advantage of vulnerabilities in Windows. The easiest way to make sure you do all the necessary updates is to set your computer to download the updates automatically.

Instructions for setting Windows Update to download updates automatically

Configuring Windows XP with Service Pack 2 for Automatic Updates

1. First, go to the Control Panel. This can be reached by clicking on the Start button, most often found at the bottom left of your screen, and choosing either Control Panel or Settings and then Control Panel.
2. Choose Security Center. This will show up regardless of your Control Panel display choices.
3. When the Security Center appears, look to the bottom section, under Manage security settings for: and choose Automatic Updates.
4. If your machine stays on all night, choose Automatic. If not, choose Download updates for me, but let me choose when to install them. If you choose the second, you must be on the lookout for warnings appearing on the taskbar calling for your attention. When you are informed that updates are ready to install, you must do so.
5. Click OK at the bottom of the window to finish.

You must run Updates even if you do not engage in risky internet activities. This applies to each and every user of any Microsoft Windows Operating System. Microsoft will identify security holes and hackers will use those announced holes to get into your system if you have not used Windows Update.

You will get infected if you neglect to update your operating system when the updates become available. You must do this when the updates become available. No t when it's convenient, but when they become available.

For information on current threats and alerts:

AclS Alerts: <http://www.columbia.edu/acis/>

CERT's Advisories: <http://www.cert.org/advisories/>

Microsoft Security Bulletins for Microsoft Products: <http://www.microsoft.com/security/bulletins>

Resources for Secure Computing

The following list contains links to sites that help you protect your computer and keep you informed of the latest security-related news and tools.

- http://www.cert.org/tech_tips/home_networks.html

CERT's guide to Home Network Security.

CERT is part of the Software Engineering Institute (SEI), a federally-funded research and development center operated by Carnegie Mellon University. CERT researches the causes and prevention of system security vulnerabilities and the improvement of system security, publishes information about security issues on its Web site, and develops information and training to incident response professionals and system administrators.

- <http://www.microsoft.com/technet/security/bulletin/notify.asp>

Free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. AcIS strongly recommends that you subscribe to this list.

- <http://www.microsoft.com/security>

Microsoft's "Get Secure and Stay Secure" campaign . This site contains general information about Microsoft's support of security issues.

- <http://www.microsoft.com/technet/security>

Microsofts' TechNet Web site. Contains links to security bulletins, the latest security news and technical information, discussion and chat groups, and troubleshooting tips and advice.

- <http://www.securityfocus.com/microsoft>

Contains security-related news, existing vulnerabilities, tools, and mailing lists.

- <http://www.microsoft.com/technet/security/current.asp>

Using Windows Update for Windows XP 7 Microsoft's toll-free security support line.

- <http://www.microsoft.com/technet/security/tools/w2kprocl.asp>

Windows 2000 Professional baseline security checklist.

- <http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp>

Windows 2000 Server baseline security checklist.