10 computer and LAN security rules

No matter how good a security solution is, if the device and software are not properly set up, the risk is always lurking.

No matter how good a security solution is, if the device and software are not properly set up, the risk is always lurking.

There are a series of solutions for network and computer protection such as virtual private network (VPN), intrusion detection system (IDS), intrusion prevention system (IPS), biometric ., but the object is infinite, and our ability to invest is finite.

Perhaps the weakest point in computer and network security is human factor. And no matter how well equipped you are, if the device and software are not properly set up, the risk is always lurking.

This article provides 10 rules to protect computers and LANs: the first 5 rules apply to all computer users; The next 5 rules are for small businesses.

1. Back up valuable data

It sounds extreme, absolutely secure computers are off. When you turn on your computer, the likelihood of losing data will increase, even when you're not connected to the internet. A hard drive is one of the weaknesses of a computer and a hard drive is a possibility. Or you may accidentally delete the data file. Therefore, the first rule is to backup data, use CD, DVD, hard drive or other storage media.

2. Install and update antivirus software regularly

About ten years ago, the chances of being infected with the virus were quite low because few people had access to the Internet and the storage facilities were not as diverse as they are now. The main source of infection is the exchange of floppy disks and pirated software. But now most people use Windows, the virus spreads at the speed of light, and in half a day the world may be threatened.

Viruses and worms are codes that attach files that can be reproduced to spread, usually executable files (exe) or macros, although recently detected viruses in the image file (jpg). Viruses can be harmless or really destructive, so it is imperative to equip an antivirus program and it must be updated regularly or otherwise useless.

3. Remove unnecessary files, programs and services

By default, Windows will install many unnecessary files, programs, and services that cannot be removed with the Add / Remove Programs in Control Panel. These unnecessary files pose the risk of insecurity, which can be exploited by intruders. In an office environment, some useless default programs: who needs to play games (Freecell, Hearts, Solitaire .), send instant Messenger .?

To avoid unnecessary risks and also to speed up the operating system, you should install only what you need. To remove unnecessary programs, you can use specialized tools like nLite of Nuhi (freeware) or xplite of LitePC. But be careful to avoid deleting important files.

4. Update the operating system

Current Windows updates are needed. Attackers often use weaknesses in operating system security to exploit weaknesses. Updating important operating system patches is a way of securing, fixing holes and closing unsafe doors. An easy way to check for updates for Windows is to go to Windows Update in Internet Explorer, but if you manage multiple computers, you can use a more powerful tool, such as MBSA (Microsoft Baseline Security Analyzer), a typing tool. Free weaknesses for Microsoft platform.

If the LAN has only a few computers, updating is not a big deal, but for companies with large computer systems, it is not an easy task. However, network administrators have the ability to update computers quickly and efficiently, such as using free SUS (Microsoft Software Update Services) or dedicated patch management tools like Ecora Patch Manager, HFNetChkPro or UpdateEXPERT.

5. Install a firewall and configure it correctly

When connected to the outside world, the most important device should be a personal firewall. Don't go anywhere without it. Personal firewalls protect the assets of computer users and businesses, and ensure secure connection to the Internet and between networks. There are many types of firewalls: software or applications, single or multi-function functions such as VPN, antivirus, IDS, content filtering ., some even introduce an all-in-one solution (Proventia-G of ISS, currently distributing in Vietnam through Misoft - PV).

For individual users, first use a Windows XP firewall or install a freeware / shareware firewall such as ZoneAlarm, Kerio Personal Firewall, Sygate Personal . Businesses should choose the right firewall for their needs. . Choosing a firewall for business is not easy, as there are very few testing standards for evaluating firewalls while these models change frequently.

6. Close all access ports

Suppose you have a LAN with several computers, people can access every computer on the network, so anyone can easily steal valuable data with a USB drive. To avoid the risk of data loss from external storage media, you need to protect computer ports such as USB, serial port, infrared, Bluetooth, CD drive, DVD drive or floppy drive if available. The network administrator is responsible for managing and granting access to those ports. There are software to do that, like DeviceLock from Smartline.

7. Set BIOS password

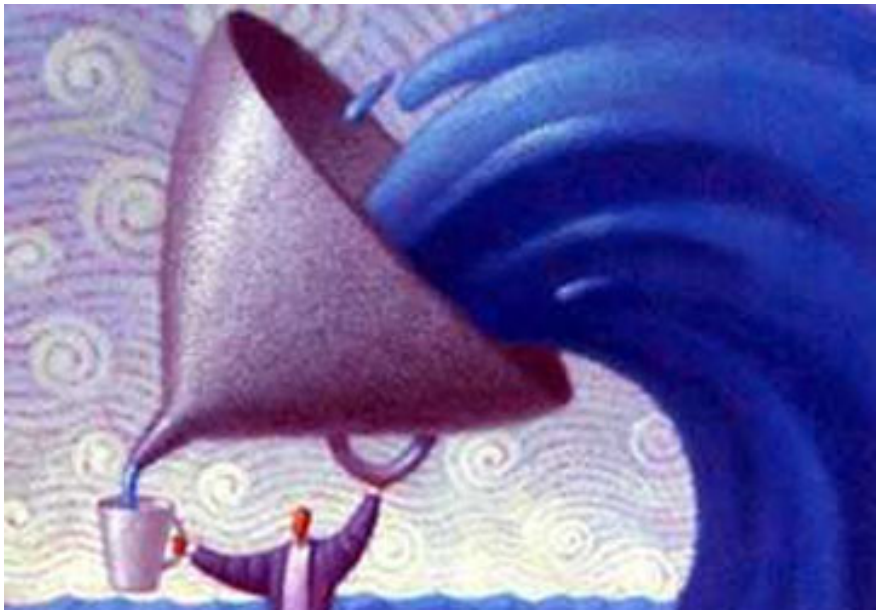
Another risk is accessing the BIOS on the board. Password should be set to lock BIOS. Set the first boot device to be the hard drive. If you access the BIOS, with a bootable CD and a few other tools, a computer savvy person

can steal the administrator password for computers on the LAN.

8. Set the rules for GPO

Employees using computers should not be allowed to install or run software, because they can download potentially dangerous programs. Windows server operating systems have a powerful tool to manage user rights as GPOs (Group Policy Objects). With this tool, you can set up network management and security policies, set up rules: password complexity, screensaver, applications that are allowed to run. Group Policy in GPOs have a great impact on users, so check carefully before doing so.

9. Use content filtering software for HTTP, FTP and SMTP



Networking has many advantages, promoting correspondence and information, but it also brings unwanted content to employees. Harm is a waste of time, leaving the network exposed to potential risks and bandwidth costs. Therefore, content filtering solutions must be applied.

10. Use anti-spam software

Go to some websites and sign up to receive newsletters or new information ., a few days later you will receive dozens of spam (spam). Anti-spam software is becoming necessary and should be installed to avoid wasting time and unwanted emails.

The above rules are not mandatory, they reflect the writer's points that are important to preserve computers and LANs. In fact, the first problem you have to answer is knowing what you need to protect, how to prepare to protect the data; Small businesses decide how to create a level of freedom for employees. The protection for computers and LANs depends on many factors: investment, time, level of protection. Therefore, it seems impossible to have a 100% secure network. You must choose priorities for protection.

You finished reading the article "**10 computer and LAN security rules**" 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.

© 2019 TipsMake.com