Some common data security measures

Data protection is extremely essential, because data is the most important asset of users on computers. It can be said that the need to use computers and networks comes from data.

***Network management* - Data protection is essential, because data is the most important asset of users on computers. It can be said that the need to use computers and networks comes from data.**

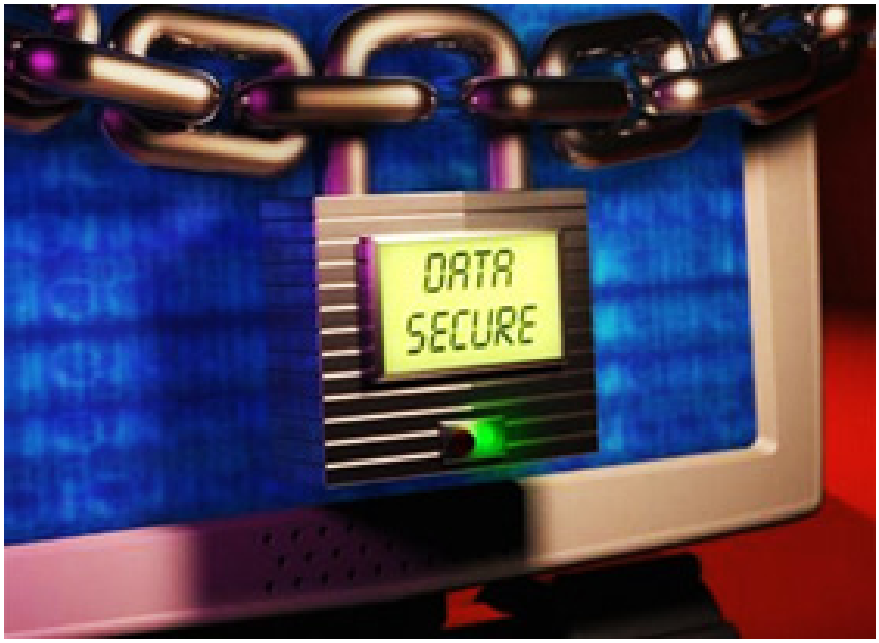
Usually when deciding to choose a method of computer protection, the data plays a prerequisite. The operating system and applications can be reinstalled, but the user data created by the user is unique, if lost, nothing can be replaced, can even cause great damage. for individuals and organizations. There are many objective and subjective causes of data loss such as system errors, viruses or mistakenly deleting. In addition, some data is very confidential, it is important that we not only want to lose it, but we don't want others to see it without permission.

In this article, we will share with you some ways to protect data on your computer, depending on the level of importance and specific conditions that you can choose the appropriate method for your data. .

Backup data promptly and regularly

The most important step in protecting data from misplacement is to perform regular backups. How long do we need to perform backups? This depends on how much data will be lost if the system is completely knocked down. We can do backups weekly, daily, or hourly.

1. Some common backup errors



We can use the backup utility built into the Windows operating system (**ntbackup.exe**) to perform basic backup processes, in addition, **Wizard Mode** can be used to simplify the creation and restore process. Restore backup files, or manually configure backup settings and schedule backup tasks to automate this task.

In addition to the above tool, there are many other third-party backup tools with more advanced options. No matter which tool we choose, storing a backup copy of the backup file is important in case the tapes / discs containing the backup file are destroyed along with the original data. There is now a very effective method that we can use to store backup that backup is online backup.

Apply shared security and file level security

For data security, the first step is to install the license for files and folders. If you are sharing data over the network, we can install sharing licenses to control which user accounts can or cannot access these files over the network. With Windows 2000 and Windows XP, we perform a license installation by clicking the *Permissions* button on the *Sharing* tab of the *Properties* properties window of the folder or file.

However, shared-level licenses will not be valid for users who are using shared data storage computers. If the computer is used by many people, we must use file-level licenses (also known as NTFS licenses because they only appear on folders and files stored on NTFS-formatted partitions). . File-level licenses, installed in the *Security* tab of the *Properties* properties dialog, are more secure than shared-level licenses.

In both cases, we can install a license for a user or group account, and can allow or deny multiple access levels different from read-only to full access. .

Set password to protect documents

Some applications, such as Microsoft Office and Adobe Acrobat, allow us to set passwords on many different documents. To open these documents we will have to enter the installed password for them. In Microsoft Word 2003, to set a password for a document, go to Tools | Options and then click on the Security tab. We can set the password to open this file and set an anti-editing password. Also we can install the type of encryption used.

1. How to lock the folder with a password with the file command * .BAT

Some compression software such as WinZip or PKZip also supports compressed file encryption.

Use EFS encryption

Windows operating systems from Windows 2000 to Windows 10 are supported with **Encrypting File System** (EFS). We can use the encryption method that integrates this license platform to protect individual files and folders stored on NTFS formatted partitions. The operation of encrypting files and folders is very simple, just click on the *Advanced* button on the *General* tab of the *Properties* properties page. Note that we cannot use the combination of NTFS and EFS encryption.

1. How to encrypt files and folders with EFS on Windows 10

EFS uses a combination of symmetric and asymmetric encryption for both security and execution. To encrypt files with EFS, the user must have an EFS license, which can be created by a Windows Certification Authority, or a self-signed license if there is no Certificate Authority on the network. EFS files can be opened by user accounts that have encrypted them, or by a dedicated recovery agent. With Windows XP or Windows 2003, we can also assign other authorized user accounts to access encrypted files using EFS.

Note that EFS is used to protect data on the drive. If you send an EFS encrypted file over the network and someone uses a Sniffer to steal, they can read the data in this file.

Use disk encryption tool

In some versions of Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2, there is a powerful disk encryption tool called BitLocker. By default, this tool uses AES (Advanced Encryption Standard) encoder operating under CBC (Cipher-Block Chaining) mode.

1. How are BitLocker and EFS different?

In addition, we can use many other third-party disk encryption tools to encrypt the entire drive. When encrypting the entire drive, users will not be able to access the data in it. Data will be encrypted automatically when written to this drive, and will be automatically decrypted before being loaded into memory. Some tools can create invisible storage areas inside a partition, then act as hidden drives inside a drive. Other users can only see data in the external drive.

These disk encryption tools can be used to encrypt removable drives. Some allow you to create a master password with lower-level extra passwords for other users, such as Whole Disk Encryption, Drive Crypt, etc.

Take advantage of Public Key Infrastructure

A **Public Key Infrastructure** (PKI) is a system that manages Private Key and Public Key folders, and digital licenses. Because the Key and license are issued by a trusted third-party tool, the license platform is secure, which the system provides is quite strong.

We can secure the data we want to share with others by encrypting this data with a Public Key and a shared person. All users in the network will see this data, but only users with Private Key corresponding to Public Key can decrypt.

Hide data with Steganography encoding

Steganography is a type of encryption that creates hidden email in which only senders and recipients know the existence of this email.

We can use a Steganography application to hide data inside other data. For example, we can hide a text email in a .JPG image file or an MP3 music file, etc.

Steganography does not perform email encryption, so it is often used with encryption software. First the data will be encrypted, then hide it inside another file with a Steganography software.

Some Steganography-style encryption tools require the exchange of a secret Key, while others use Private and Public cryptographic keys. A good example of Steganography software is StegoMagic. This is a free software that encrypts email and hides them in .TXT, .WAV, or .BMP files.

Protect data sent by securing IP

Our data can be stolen by hackers while transmitting over the network with a Sniffer software. To protect data while it is being transmitted over the network, we can use Internet Protocol Security (IPSec), however both the sending system and the receiving system must support IPSec. Since Windows 2000, Windows has built-in support for IPSec. Applications do not have to recognize IPSec because it operates at a low-level network model.

Encapsulating Security Payload (ESP) is the protocol IPSec uses to encrypt data. IPSec can operate under tunnel mode to provide protection at the gateway, or in transmission mode to provide protection when data is being transmitted. To use IPSec in Windows, we must create an IPSec policy, select the authentication method and the IP filters to use. To configure IPSec settings, open the *Properties* properties window of *TCP / IP* on the *Options* tab of *Advanced TCP / IP Settings* .

Secure data transmitted via Wifi network

The data that we send over Wifi networks is more vulnerable than when sending via an Ethernet network. Hackers do not need to physically access the network or devices on it, any laptop user who has Wi-Fi enabled and a powerful transceiver antenna can steal data or break into the network. and access to data stored on that network if the WiFi access point is not configured securely.

1. Secure WiFi from basic steps

We should only send and store data for encrypted Wi-Fi networks. To encrypt the Wifi network, it's best to use WPA / WPA2 in conjunction with AES instead of Wired Equivalent Protocol (WEP).

Use Rights Management to maintain control

If you need to send data to other users but we are worried about protecting this data when it is no longer on our system, we can use **Windows Rights Management Services** (RMS) to check it. Control the behavior of the recipient for the data they receive. For example, we can assign permissions so that the recipient can read the received Word document but cannot edit, copy or save this document. In addition, we can block the recipient from forwarding the email we send, or set the expiry date for the email or the document so that the recipient cannot access it after that time.

To use RMS, we need to configure Windows Server 2003 as an RMS server. Users need to use Internet Explorer or install client software to access RMS-protected documents. Authorized users need to download a license from the RMS server.

Hopefully some of the above solutions can make your computer and data safer in this age of cyber security.