

10 things you can do to protect your data

When you think about it, the most valuable thing on your computer or network is the data you create. After all, that data is the reason for having the computer and network in the first place—and it's the bits and bytes that make up that data that are your first priority when putting protective strategies in place. Operating systems and applications can always be reinstalled, but user-created data is unique and if lost, may be irreplaceable.

Some data is also confidential; not only do you not want to lose it, you don't want others to even view it without authorization. Exposure of your social security number, credit card, and bank account information could subject you to identity theft. Company documents may contain trade secrets, personal information about employees or clients, or the organization's financial records.

Let's look at some ways to protect your all-important user data from loss and/or unauthorized access.

1 Back up early and often

The single most important step in protecting your data from loss is to back it up regularly. How often should you back up? That depends—how much data can you afford to lose if your system crashes completely? A week's work? A day's work? An hour's work?

You can use the backup utility built into Windows (ntbackup.exe) to perform basic backups. You can use Wizard Mode to simplify the process of creating and restoring backups or you can configure the backup settings manually. You can also schedule backup jobs to be performed automatically.

There are also numerous third-party backup programs that can offer more sophisticated options. Whatever program you use, it's important to store a copy of your backup offsite in case of fire, tornado, or other natural disaster that can destroy your backup tapes or discs along with the original data.

2 Use file-level and share-level security

To keep others out of your data, the first step is to set permissions on the data files and folders. If you have data in network shares, you can set share permissions to control what user accounts can and cannot access the files across the network. With Windows 2000/XP, this is done by clicking the Permissions button on the Sharing tab of the file's or folder's properties sheet.

However, these share-level permissions won't apply to someone who is using the local computer on which the data is stored. If you share the computer with someone else, you'll have to use file-level permissions (also called NTFS permissions, because they're available only for files/folders stored on NTFS-formatted partitions). File-level permissions are set using the Security tab on the properties sheet and are much more granular than share-level permissions.

In both cases, you can set permissions for either user accounts or groups and you can allow or deny various levels of access from read-only to full control.

3 Password-protect documents

Many productivity applications, such as Microsoft Office applications and Adobe Acrobat, will allow you to set passwords on individual documents. To open the document, you must enter the password. To password-protect a document in Microsoft Word 2003, go to Tools | Options and click the Security tab. You can require a password to open the file and/or to make changes to it. You can also set the type of encryption to be used.

Unfortunately, Microsoft's password protection is relatively easy to crack. There are programs on the market designed to recover Office passwords, such as Elcomsoft's [Advanced Office Password Recovery](#) (AOPR). This type of password protection, like a standard (non-deadbolt) lock on a door, will deter casual would-be intruders but can be fairly easily circumvented by a determined intruder with the right tools.

You can also use zipping software such as WinZip or PKZip to compress and encrypt documents.

4 Use EFS encryption

Windows 2000, XP Pro, and Server 2003 support the Encrypting File System (EFS). You can use this built-in certificate-based encryption method to protect individual files and folders stored on NTFS-formatted partitions. Encrypting a file or folder is as easy as selecting a check box; just click the Advanced button on the General tab of its properties sheet. Note that you can't use EFS encryption and NTFS compression at the same time.

EFS uses a combination of asymmetric and symmetric encryption, for both security and performance. To encrypt files with EFS, a user must have an EFS certificate, which can be issued by a Windows certification authority or self-signed if there is no CA on the network. EFS files can be opened by the user whose account encrypted them or by a designated recovery agent. With Windows XP/2003, but not Windows 2000, you can also designate other user accounts that are authorized to access your EFS-encrypted files.

Note that EFS is for protecting data on the disk. If you send an EFS file across the network and someone uses a sniffer to capture the data packets, they'll be able to read the data in the files.

5 Use disk encryption

There are many third-party products available that will allow you to encrypt an entire disk. Whole disk encryption locks down the entire contents of a disk drive/partition and is transparent to the user. Data is automatically encrypted when it's written to the hard disk and automatically decrypted before being loaded into memory. Some of these programs can create invisible containers inside a partition that act like a hidden disk within a disk. Other users see only the data in the "outer" disk.

Disk encryption products can be used to encrypt removable USB drives, flash drives, etc. Some allow creation of a master password along with secondary passwords with lower rights you can give to other users. Examples include PGP [Whole Disk Encryption](#) and [DriveCrypt](#), among many others.

6 Make use of a public key infrastructure

A public key infrastructure (PKI) is a system for managing public/private key pairs and digital certificates. Because keys and certificates are issued by a trusted third party (a certification authority, either an internal one installed on a certificate server on your network or a public one, such as [Verisign](#)), certificate-based security is stronger.

You can protect data you want to share with someone else by encrypting it with the public key of its intended recipient, which is available to anyone. The only person who will be able to decrypt it is the holder of the private key that corresponds to that public key.

7 Hide data with steganography

You can use a steganography program to hide data inside other data. For example, you could hide a text message within a .JPG graphics file or an MP3 music file, or even inside another text file (although the latter is difficult because text files don't contain much redundant data that can be replaced with the hidden message). Steganography does not encrypt the message, so it's often used in conjunction with encryption software. The data is encrypted first and then hidden inside another file with the steganography software.

Some steganographic techniques require the exchange of a secret key and others use public/private key cryptography. A popular example of steganography software is StegoMagic, a freeware download that will encrypt messages and hide them in .TXT, .WAV, or .BMP files.

8 Protect data in transit with IP security

Your data can be captured while it's traveling over the network by a hacker with sniffer software (also called network monitoring or protocol analysis software). To protect your data when it's in transit, you can use Internet Protocol Security (IPsec)—but both the sending and receiving systems have to support it. Windows 2000 and later Microsoft operating systems have built-in support for IPsec. Applications don't have to be aware of IPsec because it operates at a lower level of the networking model.

Encapsulating Security Payload (ESP) is the protocol IPsec uses to encrypt data for confidentiality. It can operate in tunnel mode, for gateway-to-gateway protection, or in transport mode, for end-to-end protection. To use IPsec in Windows, you have to create an IPsec policy and choose the authentication method and IP filters it will use. IPsec settings are configured through the properties sheet for the TCP/IP protocol, on the Options tab of Advanced TCP/IP Settings.

9 Secure wireless transmissions

Data that you send over a wireless network is even more subject to interception than that sent over an Ethernet network. Hackers don't need physical access to the network or its devices; anyone with a wireless-enabled portable computer and a high gain antenna can capture data and/or get into the network and access data stored there if the wireless access point isn't configured securely.

You should send or store data only on wireless networks that use encryption, preferably Wi-Fi Protected Access (WPA), which is stronger than Wired Equivalent Protocol (WEP).

10 Use rights management to retain control

If you need to send data to others but are worried about protecting it once it leaves your own system, you can use Windows Rights Management Services (RMS) to control what the recipients are able to do with it. For instance, you can set rights so that the recipient can read the Word document you sent but can't change, copy, or save it. You can prevent recipients from forwarding e-mail messages you send them and you can even set documents or messages to expire on a certain date/time so that the recipient can no longer access them after that time.

To use RMS, you need a Windows Server 2003 server configured as an RMS server. Users need client software or an Internet Explorer add-in to access the RMS-protected documents. Users who are assigned rights also need to download a certificate from the RMS server.
