Desktop Defenses

MANAGING PATCHES

You probably realize that in order for computers to function and be useful to us humans, they need software. Examples of software include the following:

1. Operating systems such as Windows 7 Professional, Windows Server 2008, and Linux.

2. Network services such as file and print sharing, database and web services.

3. User applications such as Microsoft Word, Adobe Acrobat reader, Adobe Flash Player and many more.

What happens when a bug (bad code) is found in the software AFTER it is released? We may have to live with it for a while and maybe even risk being attacked if the bug creates a vulnerability that an attacker can exploit.

Bugs are often found and reported by the users of the program. After this happens the developer(s) of the program will create a fix for the bug. This fix is called a **patch** and they can be downloaded individually or in an update.

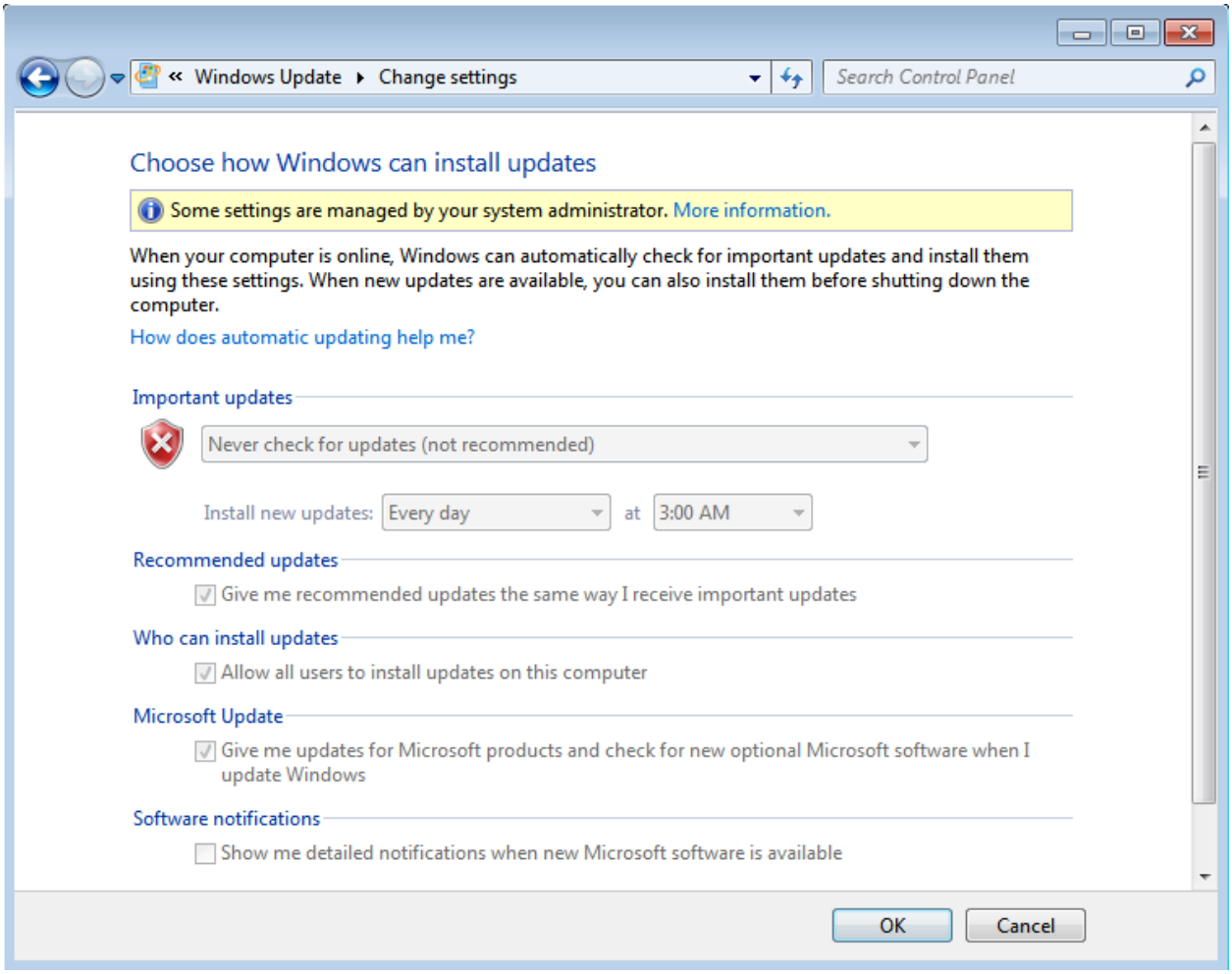
MANAGING PATCHES THROUGH UPDATES

If you let your operating system automatically update your system the update process becomes, well, automatic. This is the easiest way to get your system updated because you don't have to be reminded :>)

But, there are other options!

To view these options in Windows 7 Professional, click **Start -> Control Panel -> Windows Updates -> Change Settings**.

Note: If you are on one of NTC's lab computers, you will likely not be able to change these settings on the host operating system; you will be able to change these settings on your virtual operating system, however. See image below.



Microsoft releases patches on the second Tuesday of every month - unless a patch is meant to fix a serious illness like a security vulnerability, then it is released immediately.

By using **Windows Server Update Services (WSUS)**, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network, thus controlling the consumption of valuable network resources.

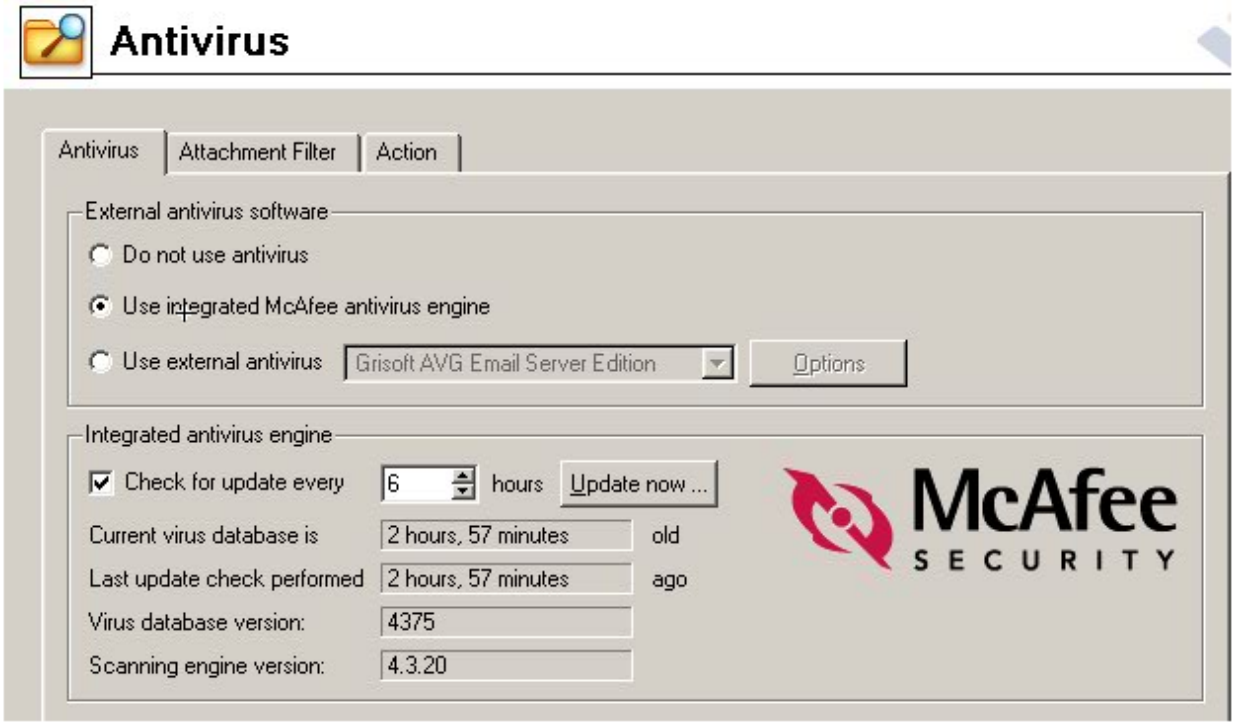
ANTI-VIRUS SOFTWARE

If properly managed, attacks can be blocked with antivirus (AV) software. AV programs can scan your disk for virus infected files and can be programmed to scan incoming files such as downloads, emails, etc.

AV ENGINES

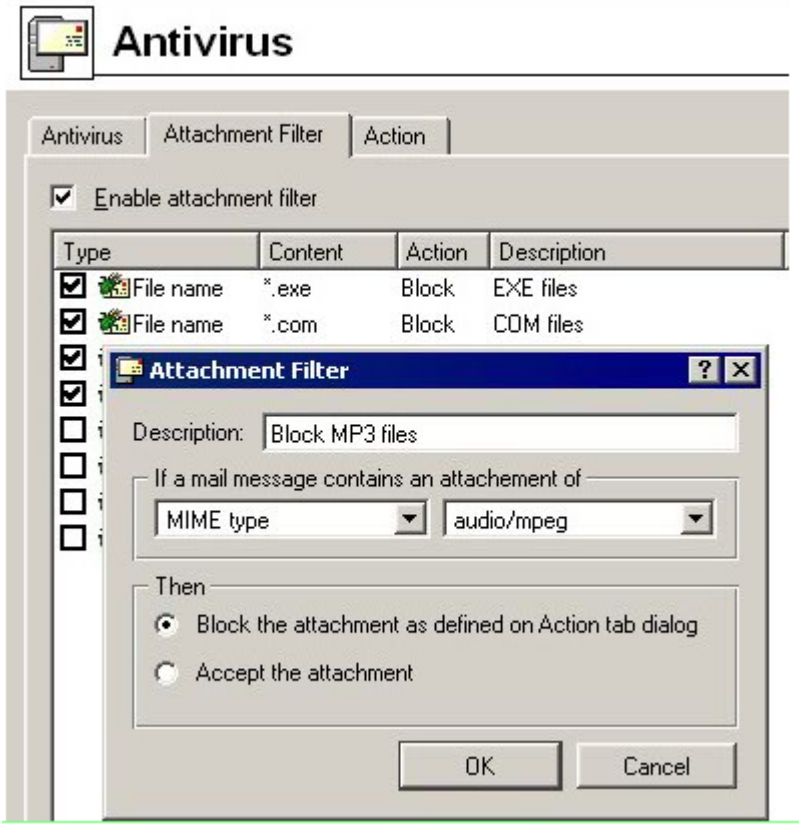
In order for an antivirus solution to be affective, the software needs to know what to look for. Viruses have a signature, a certain look to the code. Antivirus software looks for this signature and when found will address the situation as it is configured to do so. Antivirus software is only as good as its' signature dictionary (database).

The image below represents an example of an antivirus agent configured to obtain a new signature file from an external source.



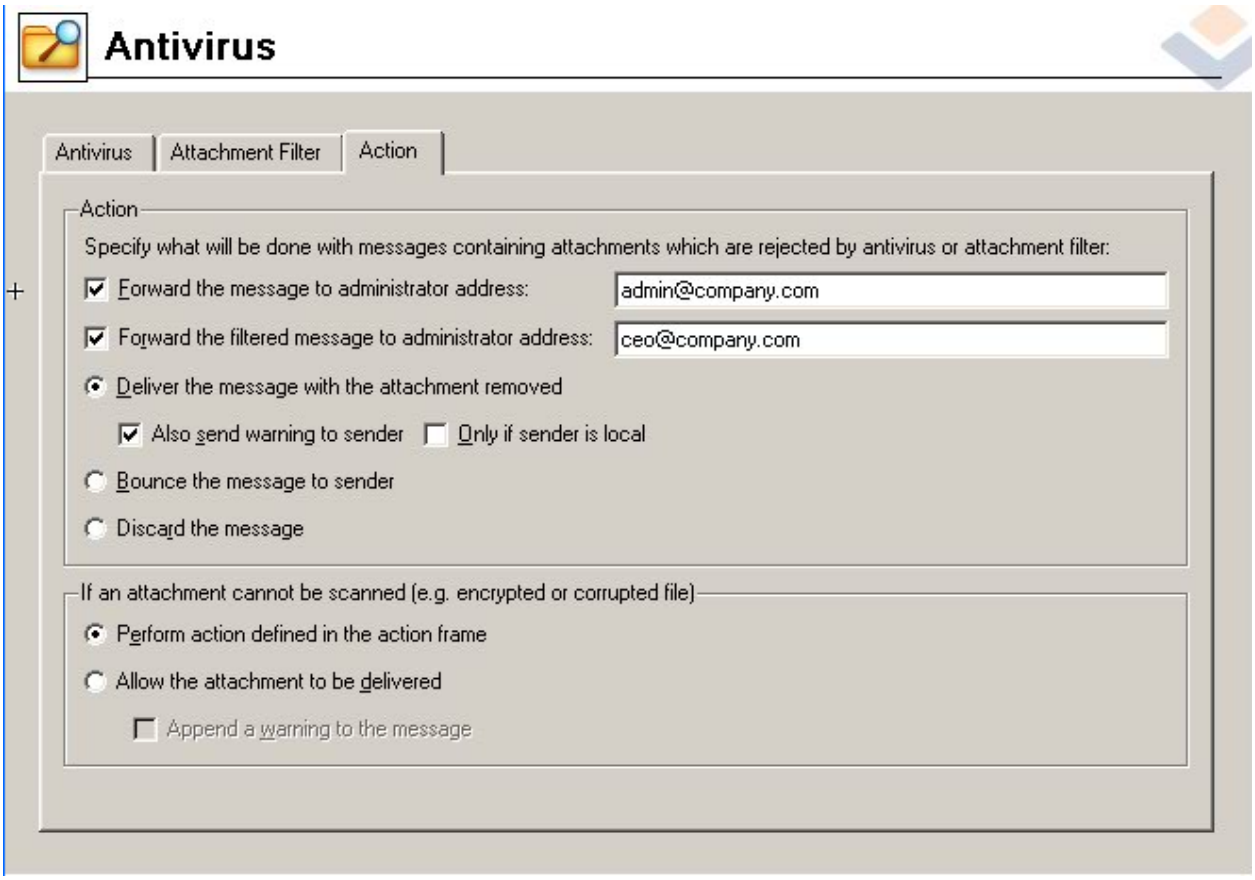
CONTROL ON INPUT FILES

You can configure antivirus filters to block certain file types known to carry viruses, as shown in the image below.



ADMINISTRATOR CONTACT

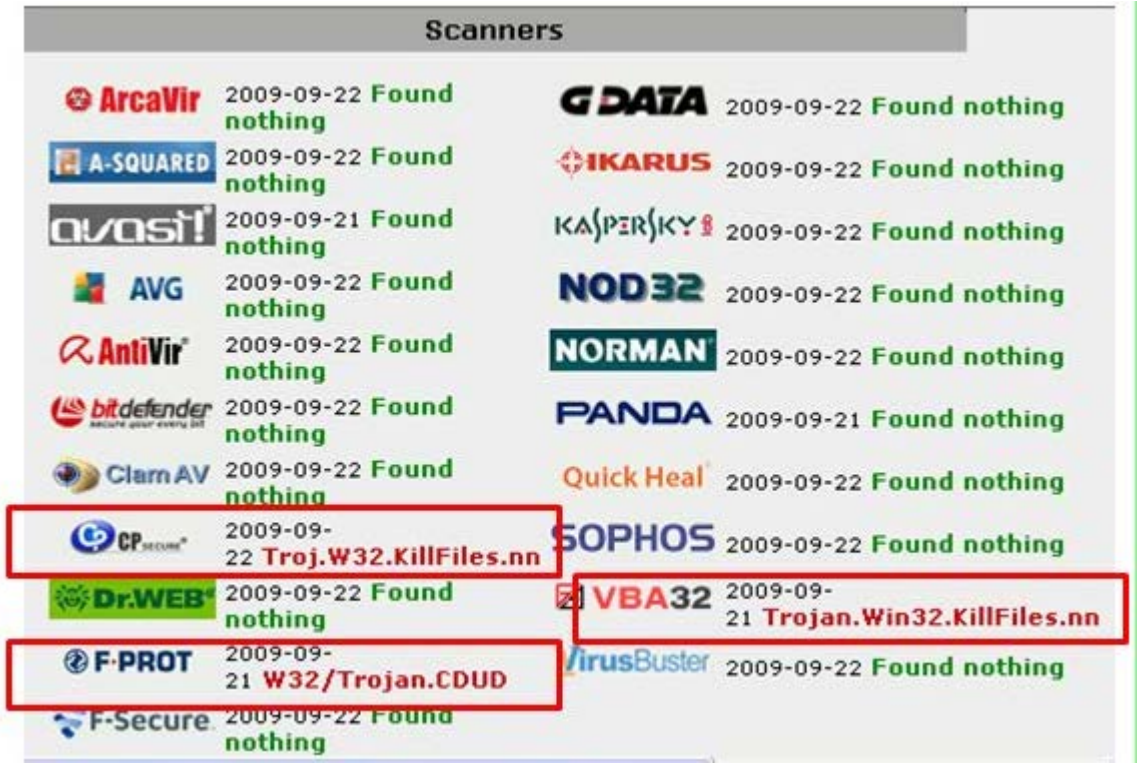
You can have the antivirus software contact the security administrator when appropriate, as shown in the image below.



ANTIVIRUS SOFTWARE PACKAGES ARE NOT ALL CREATED EQUAL

What you have installed on your computer may not look for all bad things. Commercial antivirus software that works at the enterprise level is more expensive, but may do a better job of looking for viruses such as Tojans, worms, and macro viruses that freeware would not detect.

See for yourself in the image in the image below.



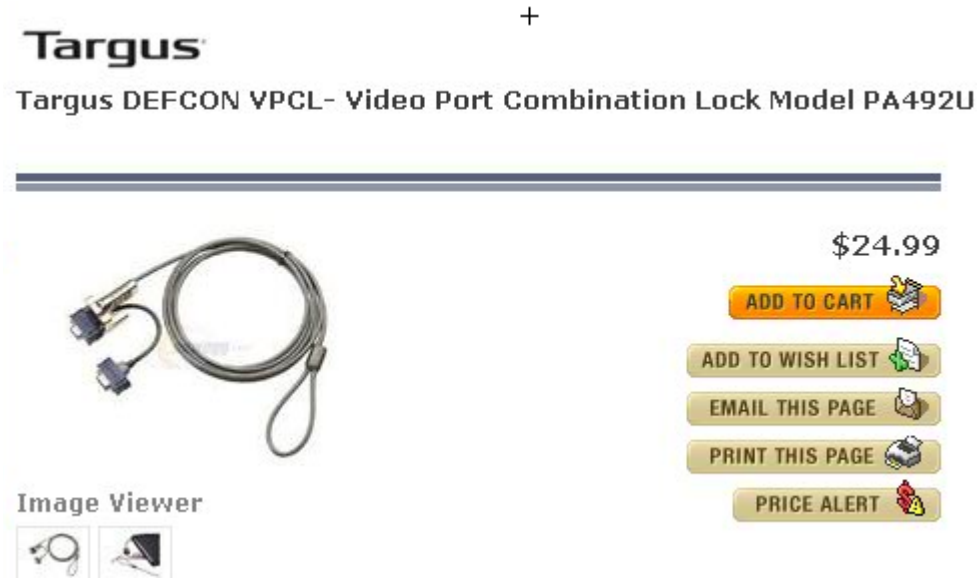
BUFFER OVERFLOW PROTECTION

When a software program is not designed right it can give way to an attacker and allow access to the computer that the program is running on. The means by which this is done is with a **buffer overflow** attack. This is when an attacker purposely pushes the program to the limits of its memory capabilities to allow the attacker to overwrite data that controls the program execution path and hijack the control of the program to execute the attacker's code instead of the process code (the code the program would execute if uninfected).

PROTECTING AGAINST THEFT

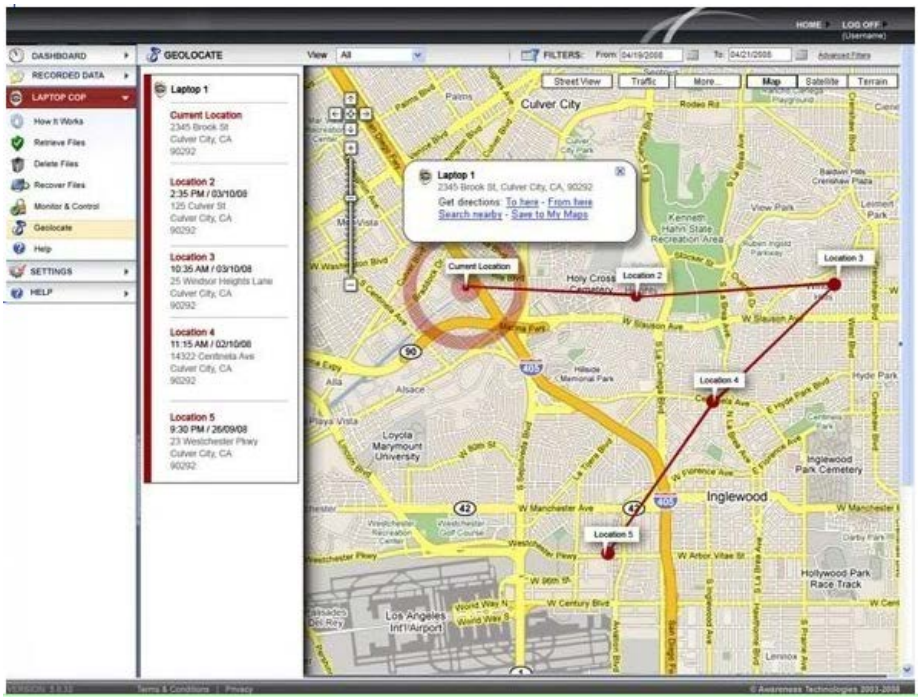
LOCK YOUR LAPTOP!

There are simple, inexpensive device locks on the market to keep the honest folks honest. See image below.



SOFTWARE TRACKING

There is software available that will help you track stolen phones or laptops. For laptops check out www.laptopcopsoftware.com



CREATING DATA BACKUPS

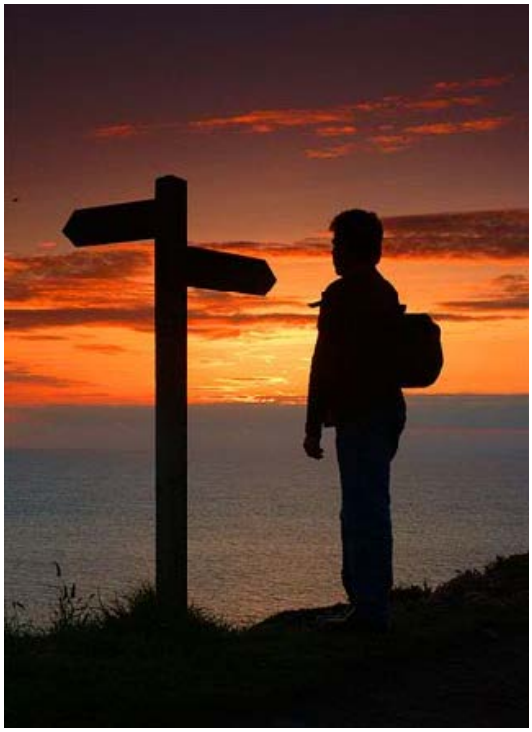
It is essential that the information stored on your hard drive be backed up onto other digital media and then stored in a secure location.

The reason for this is to minimize losses should your data get lost (stolen, corrupted, burned, soaked, deleted, whatever).

FOUR BASIC BACKUP DECISIONS

There are four basic decisions to make regarding backups and they are:

1. What information should be backed up?
2. How often should backups be made?
3. Which device type should backups be made to?
4. Where should the backup device be stored?



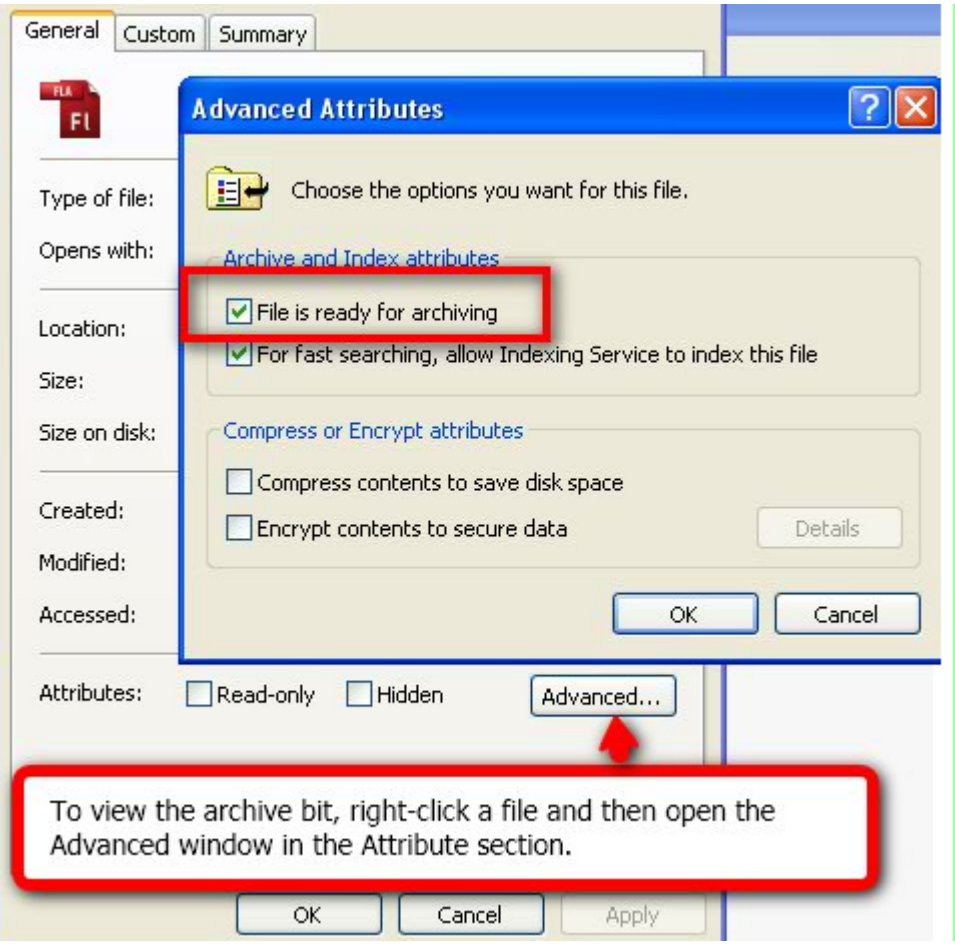
WHAT INFORMATION SHOULD BE BACKED UP?

User files or all files?

For a personal computer it is not always necessary to backup the entire hard drive. Backing up only your personal files such as photos, work documents, school work, financial information, etc., is adequate as long as you are able to restore the system and application programs by reinstalling them from CD or DVD.

Corporations typically have a backup policy that includes a **full backup** (all files) once per week followed by partial backups of only the files that get changed during the week.

Backup utilities allow this to happen because of a special file archive bit that informs backup utilities whether the file was changed or not since the last time the backup archive bit was turned off by the backup utility (such as during full and incremental backups).



There are three main, universal backup types that are performed and these are:

Full backups: Copies all files selected to be backed up regardless of the archive bit setting and will clear the archive bit of all files that get backed up.

Differential backups: Copies all files changed since last full backup (files with the archive bit turned on) and does not clear the archive bit after files get backed up.

Incremental backup: Copies all files changed since last full or incremental backup (files with the archive bit turned on) and will clear the archive bit of files that get backed up.

HOW OFTEN SHOULD BACKUPS BE MADE?

Corporations backup their data nearly every night. A full backup is made usually on a Friday or a Saturday night. The rest of the week either an incremental or a differential backup is made (this depends on whether they want a quick backup or a quick restore).

Corporations do not depend entirely on backups, however. Most use RAID technologies. RAID stands for Redundant Array of Independent Disks. This basically creates data redundancy on the hard drives, enabling the ability to instantly recover lost data due to a drive failure. RAID does not enable the corporation to recover deleted or corrupt files, backups are required for this.

WHICH DEVICE TYPE SHOULD BACKUPS BE MADE TO?

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp2/m25-backupdevices.html

WHERE SHOULD THE BACKUP DEVICE BE STORED?

Everyone would agree that backups need to be made. If the backups are for a corporation, these backups should preferably be made on portable digital devices such as tapes and then stored off site, preferably in a fire proof vault.

Personal backups at home are typically not stored offsite, but still could be - perhaps at grandmother's house. They should be clearly labeled with a date, time, and contents.