simply staying safe

The Flying Doctor's guide to protecting your valuable computer data with practical precautions and back up strategies

Simply Staying Safe

Computers are more and more an essential part of our lives. So when they stop, it's as if the electricity has failed: panic!

Take some simple steps to protect yourself against your computer being invaded and against losing your valuable data.

Contents

Don't catch a virus

I've got the same protection on my computer as my friend, but he is always getting viruses. Why? Because we act differently.

Computer security is part technology, part attitude.

If you are sensible then you have little to fear.

Technology

Consider using browsers and email programs that are not Microsoft. Microsoft has fine products but other packages, like the Firefox browser and the Thunderbird email client, are less popular targets for virus writers.

Firewalls

A firewall is like the front door to your house. It stops people coming or going unless you allow them.

Big computer networks have hardware firewalls and experts to manage them. Smaller setups like the self employed and individuals use software firewalls installed on their PCs.

A software firewall like Zone Alarm or Sunbelt (both have free versions) or those from McAfee or Norton will monitor internet activity and whenever a program tries to communicate in or out it will ask you for permission. You can tell it to remember your answer and so it gradually learns, asking less and less often.

Zone alarm: search for 'zonealarm free' in google or browse to
http://www.zonealarm.com/store/content/catalog/products/sku_list_za.jsp?dc=56

Sunbelt: search for 'sunbelt free firewall' in google (Kerio is the old name) or browse to

http://www.sunbelt-software.com/Home-Home-Office/
Sunbelt-Personal-Firewall/

If you are doing something and you expect your computer to be communicating across the internet and network, then if your firewall tell you that your computer is accessing the internet, you would feel comfortable answering 'yes'.

On the other hand, if you don't recognise the program or the firewall window pops up unexpectedly, then it's best to answer 'no'. This is especially true for external computers and programs trying to access your computer. Just say 'no'.

Anti-virus

The purpose of anti-virus programs is to stop programs that have got past the front door from smashing your house up. So an anti-virus program sits behind a firewall.

There are many anti-virus programs, from AVG (free) to Sophos, Symantec and others at various prices.
AVG :
http://free.grisoft.com/

Anti-virus is simpler than a firewall as it knows what to do. So you will just see messages from time to time telling you that the anti-virus program has intercepted a virus. What you need to do is to keep it up to date. Most programs have a method of automatic updating over the internet and you should select this. If you can't then check for updates at least twice a week.

In all cases, run a full virus scan at least weekly.

Spyware

The final type of preventative software is anti-spyware. Spyware are small programs that report back over the internet or cause your computer to dial strange numbers. It's like having a spy hidden in your house, reporting back about your behaviour and secrets. Most anti-spyware products are free. Spybot is very good, as is Adaware. Microsoft also offers a free program called Microsoft Defender. Search for them on Google. You can set most of them to keep a watch and prevent some spyware installing on your machine. It's still worth running a scan every week.

What I find most interesting is that the various anti-spyware programs all find slightly different issues. So it's worth scanning with at least two of them.

Cookies

Cookies are a blessing and a curse. They are small files that web sites put onto your computer. Often these are really helpful, remembering your preferences or password between visits.

However, some times they do more than this. The cookie cannot access your data and open it up to others, but it can tell people who you are and what you have been doing. So you may want to remove the ones that aren't helpful to you.

Cookie Monster is a very good tool. You can decide which cookies to keep and which to delete. Download it from: http://www.ampsoft.net/utilities/CookieMonster.php

Attitude

This is probably the crux of the matter. You must be alert.

The main routes of viruses into your computer are emails and instant messaging.

So, first turn off instant messaging programs.

Now review your approach to emails. Be suspicious. Ask yourself:

> does the title look strange? Most emails with viruses use poor English
> if it is 're:xxx' then do you remember sending 'xxx'?
> does it seem to be from you?
> do you know the sender? Even if you do:
>
> > does it look strange like the ideas above? Many viruses spread by emailing themselves to people in an infected computer's address book. It is better to check with the sender before opening it than risk an infection.

If any of the above, or anything else, makes you suspicious then do not even open the email. Delete it. Most emails like the above are spam, but some are harmful. If you open the email, then a virus can infect your computer. And a spam sender can see that you have opened the email, which tells them that you email address is valid and you will just gets tons more.

In the same way, do not reply in order to unsubscribe. It just encourages them to send more.

A problem that I've been seeing more and more recently is emails claiming to be undeliverable emails that you have sent. If it is from a source you don't recognise or the subject seems unfamiliar, then just delete it. If you *had* sent it, you'd recognise it!

Other sorts of email don't have a virus but are trying to get you to do something:

Phishing emails

These are emails that purport to come from an on line bank, PayPal or whatever. They look very realistic. What they want you to do is to reveal your security details. No bank will ever ask you to do this. While the sender's address may look like the bank's, these are very, very easy to forge.

Delete them straight away and never, ever, click on a link.

419 emails

These are called '419' after after a formerly relevant section of the Criminal Code of Nigeria that they are breaking. Follow the old adage that 'if it looks too good to be true it probably is'

These fraudsters are trying to get you to reveal you bank details so that they can apparently pay in a large sum. All they in fact do is to remove all your money. Similar emails tell you that you have won a lottery somewhere (even though you haven't entered) or that they want you to act as a funds transfer agent.
Stay well away from these.

There is also software that claims to be helping you but is the exact opposite. Anything window that pops-up suddenly telling you that your computer may be infected should be closed. Any true alter will have the name of your firewall, antivirus or anti-spyware program. It also won't flash or have gaudy colours.

A new variation is an alert in the System Tray (where the clock is) that invites you to download 'the most effective anti-spyware' or a similar advertisement. What they actually do is download viruses and other problems.

Don't take up the offer. Use the tools that you know and trust.

Replying to emails

The problem with replying to emails is that it proves that your email address is active. Now, in most cases this is not an issue. However, if you received a spam email, all that happens is that you get even more emails! Especially if you reply to an unsubscribe email address or web link.

It's also a good idea not to set up general autoresponders when you go away. If you don't know what an autoresponder is, then you don't use one and everything is fine. If you do and set one up, then all the spam you receive will be replied to. See above.

If you do have to, then only set it up to reply to email addresses you know.

How can I tell if I have a virus or spyware?

The majority of computer problems are caused by hardware or software problems. Most viruses will announce themselves.

If you are getting lots of pop-up windows advertising things, then you may well have spyware.

Run your spyware removal tools.

If the computer is very slow, then spyware is probably clogging up your system and again your spyware tools can remove most of them. If you know what you are doing, use Task Manager to see what program is using up all your CPU time. Then look up the program on google and get advice on how to remove it. Just to show that even this has risks, most of the sites offering help or free scans are just trying to sell you software. I can't recommend a site that is guaranteed to be free of scams, but look at a few results, such as forums, that aren't selling things to you.

Removing programs can have serious effects, so don't do this unless you are confident.

A virus is indicated by a pop-up window from your anti-virus system, files disappearing, or other problems.

First run a full scan with your anti-virus. This may remove the problem. If you know what the virus is, then use another computer to look up removal instructions and follow what they say.

If you are not confident, then ask someone who knows what to do.

But most of all **don't panic**

Backups

Why backup?

We want to back our computer in case:

- we accidentally delete a file;
- we want to go back to an earlier version;
- the hard disc fails.

What should I backup?

In short anything irreplaceable. There are three ‘types’ of data backup and recovery:

- **Reinstallation**. This applies to programs: if you have the program discs then the program can be put back on your computer. So there’s no need to make copies. If you don’t have the discs for an installed program, then there are ways to create copies. Please ask us.
- **Archiving**. Files that don’t change, such as digital photographs just need a copy that you can put back on. Copying to CDR/DVDR is ideal.
- **Backing up**. Files that change frequently need to be backed up on a regular basis. This can include letters, spreadsheets, emails and contact lists. This document concentrates on this category.

When should I back up?

Ideally, every time you make a change. Yet this is too onerous and costly. As a rule of thumb, a backup needs to be recent enough that you can get back near enough to the current position from it to be cost-effective. The more vital the data is to you, the more frequently you should back it up.

For example, many people backup weekly. If your business depends on your computer, then do it more frequently.

What types of backup are there?

There are two main types:

- **Incremental backup**. This just backs up those files that have changed since the last backup. Keeps space to a minimum, but you have to find the right backup that has the file
- **Full backup**. Backs up everything in the list. As storage is so cheap these days, we recommend this for ease of use.

What should I backup to?

Something that's not going to fail when your disc does. For example, CDRW. Flightbyte uses these and also has a second hard disc for daily backups.

How many backups should I have?

It is conventional to have a 'grandfather-father-son' set of backups. For example, a set of CDRWs labelled A, B, C that are used in a cycle: A, then B, then C, then A again...... Thus you can go back to three backups ago in case a problem was not discovered recently. E.G. a virus might have infected a file before the last backup, so you would need one earlier.

We recommend recording to rewriteable CD or DVD as a backup medium. For frequent, automated backups, you can use a second hard disc.

Some go as far as to take a periodic backup to CDR and store it off site in case their office burns down or the computers are stolen.

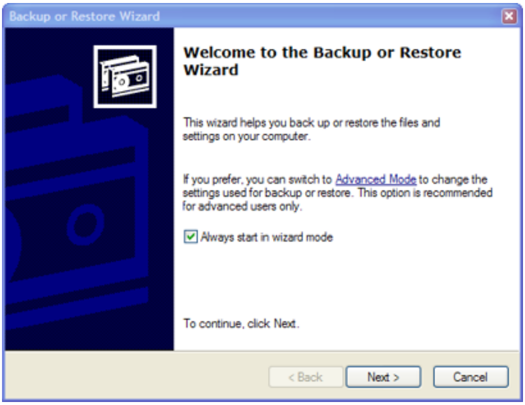
Where do I find backup software?

If you use a PC, then software to backup is included in Windows. It is also available commercially and with DVD recorders.

You can also just copy the files using windows explorer, but dedicated software makes the task easier. For example, you can save a standard backup list.

Using Windows Backup

Go to Start|All Programs|Accessories|System Tools|Backup. If you can't see one of these but can see '︾' then click on this to show a complete list of options.



Welcome to the Backup or Restore Wizard

This wizard helps you back up or restore the files and settings on your computer.

If you prefer, you can switch to Advanced Mode to change the settings used for backup or restore. This option is recommended for advanced users only.

☑ Always start in wizard mode

To continue, click Next.

I can't find backup

If you are using Windows XP home, then backup is not installed as standard.

If you have an XP install CD:

1 Insert the CD Rom and navigate to CD-ROM Drive:\VALUEADD\MSFT\NTBACKUP

2 Double-click the Ntbackup.msi file to start the wizard that installs Backup

3 When the wizard is complete, click Finish.

If you don't have a CD:

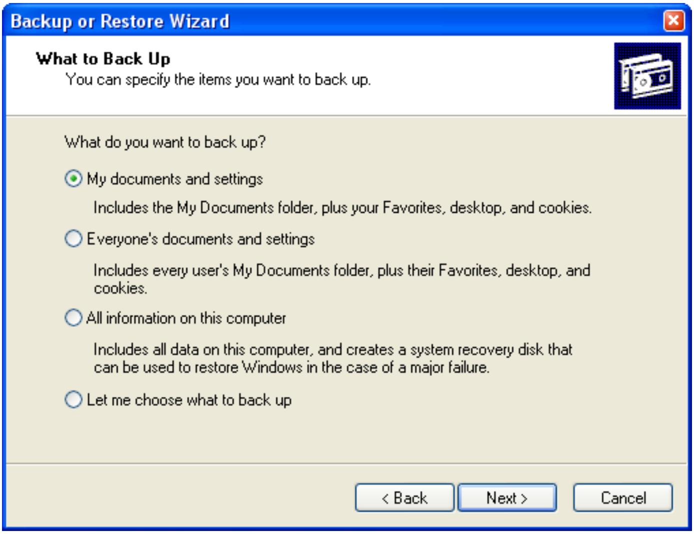
Search the internet for 'ntbackup.msi download' and download a copy. Then follow steps 2 and 3 above.

Start backing up

Click next and select backup files and settings.

Then select the option that you want. The top option is simplest but may not back up your email unless you have them stored in the ‘my documents’ folder.

If you use Outlook Express, see the appendix on how to change your mail file location.



Backup or Restore Wizard

What to Back Up

You can specify the items you want to back up.

What do you want to back up?

● My documents and settings

Includes the My Documents folder, plus your Favorites, desktop, and cookies.

○ Everyone's documents and settings

Includes every user's My Documents folder, plus their Favorites, desktop, and cookies.

○ All information on this computer

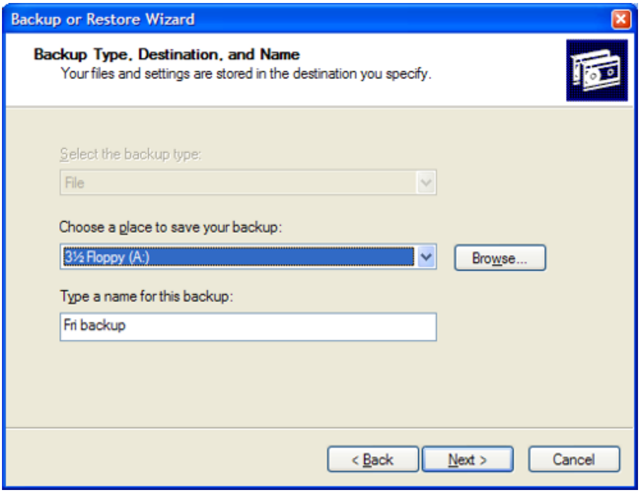
Includes all data on this computer, and creates a system recovery disk that can be used to restore Windows in the case of a major failure.

○ Let me choose what to back up

The bottom option will let you choose the files to backup. You may not wish to backup music or photographs that you have archived, for example.
Click ‘next’.

The next screen is where you select the destination drive and a name. Don’t choose the same drive as the data that you are backing up!

The next screen confirms your choices. There is an ‘advanced’ button for more choices. This is where you can schedule the backups to happen automatically. Click it if you wish to schedule backups. Otherwise click OK and you are done.



Backup or Restore Wizard

Backup Type, Destination, and Name

Your files and settings are stored in the destination you specify.

Select the backup type: File

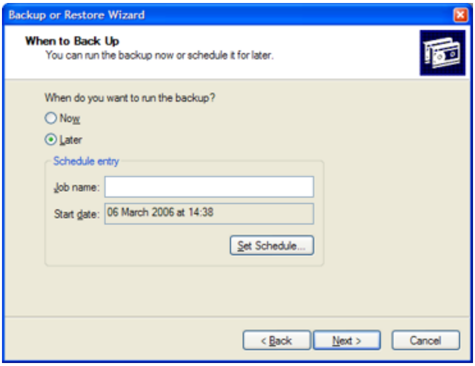
Choose a place to save your backup: 3½ Floppy (A:)

Type a name for this backup: Fri backup

To schedule backups, accept normal backup on the next screen and verify data on the next. Finally choose if you are going to add the backup or replace any with the same name. Choose the latter if you are creating a routine backup and store each backup on different CDs, etc.

You can run the backup now or later. To create a regular backup, choose 'later' and give it a name.

Now 'set schedule'.



Backup or Restore Wizard

When to Back Up

You can run the backup now or schedule it for later.

When do you want to run the backup?

○ Now

● Later

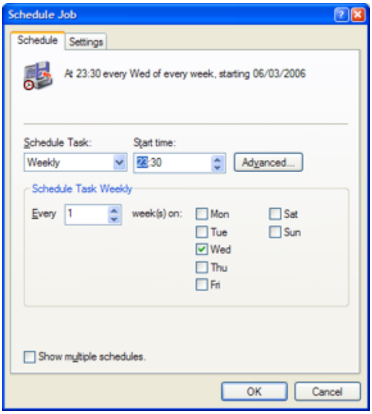
Schedule entry

Job name:

Start date: 06 March 2006 at 14:38

The standard Windows Task scheduling screen appears and you can select your options. For example you may wish to have a backup every Wednesday that runs at 23:30. Understand that we have set the system to overwrite any previous backup with the same name. So, if you set it to run every day, you will only have access to the last day's backup. You should set a weekly backup for every Monday, Tuesday, Wednesday, Thursday and Friday by running through this procedure again and using a different file name for each.

Finally press OK and enter your login password when prompted.



Schedule Job

At 23:30 every Wed of every week, starting 06/03/2006

Schedule Task: Weekly

Start time: 23:30

Schedule Task Weekly

Every 1 week(s) on:

□ Mon
□ Tue
☑ Wed
□ Thu
□ Fri
□ Sat
□ Sun

□ Show multiple schedules.

Outlook Express files

OE puts its files in various locations. Which are hard to make part of your automated backup strategy. Here is how to change the file locations:

Changing Outlook Express mail files location

This works for Outlook Express 6 and may for other versions

Do this through Outlook Express, not by manually moving files.

1 Create a new folder in Windows Explorer where you want OE to store your files. Ideally this will be somewhere in 'My Documents'.

2 Open OE and click Tools| Options| Maintenance| Store folder, then click the Change button. Browse to the new folder and click OK. Close the dialogue, then close OE. When you re-open OE, it will automatically move the store to its new location.

Changing Outlook Express address book location

Only do this if you are comfortable with editing system files.

A In Outlook Express, open the Address Book and click Help| About Address Book to fond where your address book is located.

B Close OE, any open message windows, and the Address Book.

C Cut and paste the *.wab file to its new location: probably the same location as the mail files location above.

It may be that you cannot see the original folder or the destination folder.

If so , in Windows Explorer click tools|folder options|view and under the 'Hidden files and Folders' folder select 'show hidden files and folders'

D Now click Start|Run, enter Regedit in the ‘open:’ box, press OK and navigate to this key:

```
\HKEY_CURRENT_USER
   \Software
      \Microsoft
         \WAB
            \WAB4
               \Wab File Name
```

E Click Registry| Export and save the selected branch to your desktop as "WAB.reg". You can then restore the current location if you have a problem, simply by double-clicking the saved WAB.reg file.

F In the right-hand pane, right-click on (Default) and click Modify, then carefully enter the full path *and* file name of your relocated *.wab file. Eg 'c:\my documents\emails\xxx.wab'

G Close Regedit and open Outlook Express to make sure everything is there.

Glossary

CDR	A recordable CD. Secure archive storage.
CDRW	A rewritable CD that can be erased and re-recorded. Good for repetitive use.
DVDR	A DVD that can be recorded. Secure and holds 7-8 times as much as a CD. Comes in + and - formats. Check your drive.
DVDRW	A rewritable DVD. See notes above about formats.
DVDRAM	A temporary form of storage. Not recommended for backups.
External disc or HDD	A separate hard disc that can be plugged into your PC, usually by USB. Data can be transferred to it and then the unit can be removed.
Flash Disc/memory	A form of stable memory for short-term storage. Used in digital cameras and MP3 players. Not recommended for backups.
Nero	A popular backup software package supplied with DVD recorders.
Online backup	Using the internet to back your data up to a remote location. Secure but a little slow and charges continue.
Tape	A form of external storage with massive capacity backup system for large computer systems. Slow but cheap and effect. ive. Probably not required by most PC users as other media drop in price and increase in capacity.

Price:

UK	£7.97
USA	$15.46
EU	€11.76

the flying doctor

the GP for your PC

12 Yeftly Drive
Littlemore
OXFORD
OX4 4XS

+44(0)1865 748197

info@theflyingdoctor.biz
www.theflyingdoctor.biz