Simple Ways To Protect Your Computer

Getting software to protect your computer is unfortunately a must these days. Yet before that point, there are a number of simple things to do to protect your PC...

- **Ensure your computer is updated.**

  The software your computer operates on already has some in-built protection; crackers and fraudsters often try to break through this software to exploit weaknesses and Microsoft is permanently upgrading its software to prevent them in a cat and mouse game.

  Updates are available from Microsoft's dedicated website, but it's easier to set your computer to download them automatically. Just go to Control Panel and click the 'System' icon, then go to the Automatic Updates section where you can toggle the latter on or off.

- **Turn your PC off!**

  Another easy tip to reduce the risk of crackers accessing your PC is to disconnect from the internet or, even better, turn it off when it's not in use, saving energy too. While your PC's on and after you've been browsing is a prime time for malware attacks.

- **Don't open unknown e-mail attachments.**

  The majority of web crime happens via email, so be on guard when checking yours. Don't open any attachments you're not expecting, or click any random links you find in the text (If you're unsure of a site's veracity, whack the link into Google and see what comes up; it may be listed as a bad 'un.

- **Only download software from trusted websites.**

  If you're looking for a piece of software, find out who makes it first and then go to their site to get it. For smaller free/shareware programs, try using big sites like cnet's Download.com rather than just getting them from anywhere that shows up.

- **Use different passwords for different sites.**

  It may seem obvious, but don't use the same login for lots of sites, because then if one falls into the wrong hands, your whole online life is up for grabs. It's a nightmare to remember lots of different ones, so why not take one and just add a few letters to it related specifically to each site you're logging into?

The banks say 'if you don’t have it, you could be liable'

If you’re not protected and someone uses your computer to get passwords or access your bank account or other financial products, you may find it harder to get a refund.

While the burden of proof's on the bank to prove you didn’t act with care, it's best to be safe.

Know thy enemy: The main threats

Threats to your computer come in different guises with various funky names. Collectively they're considered *malicious software*, abbreviated to 'malware' in security parlance. The main types are as follows:

- **Viruses.** *Hidden programmes which wreak havoc.*

  These are transmitted via websites, e-mail attachments, directly over the internet, or via any other removable media. They hide in applications or files and spread from computer to computer, generally wreaking havoc wherever they get the chance to.

- **Trojans.** *Bugs within harmless looking files.*

  Trojan (horses) are hidden within a file that looks harmless, like a picture of a celebrity, aiming to trick the user into installing the malicious software like spyware or adware on the computer.

- **Worms.** *Can drill in via open web connections*

  Worms take advantage of any open Internet connection, to try and sneak in and replicate on the computer. Once loaded, they often start to send spam email from your computer without your knowledge.

It's often about big, organised crime.

It's a common misconception that producing computer viruses is the sole domain of angst-ridden one-man-bands with little to do, showing off to their equally reclusive peers. Whilst there may have been some truth in this at the beginning, and of course it still happens, these days it's often about big criminal business. Some of the reasons it happens include...

- **Stealing your information.**

  Cracking into your computer can reveal a breadth of information about you, possibly including bank details for ID fraud or just directly taking your cash.

- **Grabbing your e-mail contacts.**

It may be a programme looking to grab all the e-mails in your contacts e-mail data in order to find real addresses to sell to spammers. These people may well then be e-mailed from your address.

- **Utilising your computer to threaten websites.**

  Some viruses can allows your computer to be controlled in order to create a DDOS attack. This is where a website (or even a country's whole domain e.g. Estonia's .ee domain) is closed down due to simulated use by billions of simultaneous users. This can be for political reasons, ransom, to close down competitor sites or just for 'sport'.

  Many of the people whose computers cause this are unaware it's happening, as viruses are controlling their web connections. This site was hit by just such a DDOS attack, the irony being some of the people who were denied access for three days could've been contributing to the closure by hidden viruses on their system.

Free Anti-Virus Software

Pay for anti-virus software from the biggies Symantec/Norton or Mcafee and it'll cost roughly £50 per year. Yet you can also take advantage of a variety of decent free programmes... Bear in mind most free anti-virus programmes do not support real time protection which means they will only delete viruses on the system but will not alarm to a real time threat.

- **Microsoft Security Essentials.**

  Launched earlier this year, Microsoft's security essentials package has gone from strength to strength since coming out of beta testing. The package is completely free to users of 'genuine Windows machines' - ie it'll verify your copy - and three versions are available, for XP, Vista, and Windows 7.

  The software's unobtrusive and provides quick, and increasingly comprehensive protection from viruses, trojans, rootkits, and spyware. While Antivir below provides marginally better cover in tests, most casual Windows users won't go wrong with the firm's own offering, since it feels and operates like part of the regular operating system rather than an added extra.

- **Avira Antivir.**

  The free anti-virus software of choice for techies, Antivir's won many tech publications' free antivirus round-ups by providing both the most thorough software protection and the fastest. Yet the reason it doesn't top our list is that it's slightly less user-friendly than the Microsoft offering, with some of the settings requiring some technical knowledge to get right. Yet if you've the knowhow, it'll do everything you want it to.

- **Avast! 4.8 home edition.**

  Alwil's Avast! home edition offers great detection of known malware, but it's usually beaten by Antivir in tests. The latest version's a good all-rounder, providing all the features you'd get with a paid-for program, but its interface still isn't the best on offer.

- **AVG Free.**

  AVG has a long history, and has been through loads of modifications to provide a better service on its way to the current version, AVG 9. It's protection is reasonably thorough, though it doesn't offer any real tech support.

  AVG's quite unintrusive, doesn't use too many resources, and will regularly auto-update. It includes LinkScannner - real-time threat detection which checks links out when you're surfing the web (Firefox and IE only), and marks unsafe ones with red flags so you know not to click them. LinkScanner is also available separately as a sub-1MB sized plugin for those who already use another anti-virus suite.

Whichever of these you choose, there's one important warning...

Hackers develop new bugs constantly. All these free anti-virus services offer regular updates, if you don't download them, you're not protected.

Yet it's not just about how up to date your software is. If you're not using it, what's the point? Try to fit in a full 'on-demand' scan (that is, one where the virus scanner flicks through all the files on your hard drive) once a week. This should make sure nothing slips through the net.

Cloud-based anti-virus tools

The growing trend towards web-based applications where all the processing happens online and then gets delivered back to you is now properly entering the realm of security. While it may seem counter-intuitive given that the threats are online too, one tool yields particularly impressive results (assuming you've an always-on broadband connection):

- **Panda Cloud Antivirus.**

  Panda's paid-for software comes highly rated, and this totally free, no nag-screen online antivirus product clearly draws on the same expertise. In fact, in some tests, Cloud Antivirus detected even more threats than the top-performing Antivir software above.

  As it's cloud-based, all the number-crunching happens online, so it's light as a feather on system resources and there's no need for update downloads. In all, the only drawback is that it's only recently come out of beta.

A note for those with new PCs

Often companies throw in free anti-virus programs hoping you'll subscribe to them out of convenience once the free trial ends. By all means take advantage of the free offer, but then ditch and switch to a free version when it expires. Make sure you uninstall the trial too; it may interfere with the new virus scanner, and even if not it'll certainly slow down your PC.

Note for Norton users only: It can be a bit of a pain to get rid of all Norton AntiVirus's components from your machine. If you're having trouble doing so, try Symantec's own Norton Removal Tool, which is designed to solve this very problem.

Mac Anti-Virus software

As viruses are a relatively new worry for Mac owners, there are far fewer free programs available. There are still a couple worth checking out though:

- **PC Tools iAnti-Virus.**

  Offering simple bloat-free scanning in real time, this PC Tools offering covers all the basics quite well, and doesn't hog system resources too much either. Whilst it lacks the scope of paid-for programs from the usual suspects, it nonetheless offers a range of scanning options, and will auto-update itself whenever necessary.

  However, it's worth noting it only looks for viruses and malware specific to the Mac platform; PC viruses will slip by undetected, which won't be a problem for you, but could cause trouble for PC-owning friends should you unwittingly email some malware to them.

Free Firewall software

Anti-virus isn't the only protection your computer needs. If you don't have a Firewall, you're leaving all your files and sensitive information vulnerable. Therefore its important to get one. To help explain this, let me use a simple analogy.

If anti-virus software's the border patrol checking to see what's allowed in, a firewall's the border fence stopping all the bad stuff coming in in the first place.

Got a router?

Thankfully most of us use a router to connect to the web nowadays rather than just a modem. I say thankfully because routers have built-in firewalls which deal with incoming connections before they hit your PC, and outgoing connections before they hit the web after leaving your machine. Ensure yours is turned on and set to a high enough level of security. Consult the manual or search online for the make and model number if you don't know how to check.

Whilst you're there, check your router password has been changed from its default; you'd be surprised at how many connections are hacked simply because the password hasn't been changed. Spend a little time and get your settings right here, as router firewalls afford a higher level of protection than software ones.

Windows Firewall.

Windows XP, Vista and 7 have a firewall built-in, which should be sufficient for most people (especially those who've already got router firewalls), though do make sure it's switched on and your copy of Windows is up to date. The firewall can be set on low, medium & high levels of protection.

If you have the Windows firewall set on a high level of protection, it's likely you'll need to spend some time tweaking its settings in Control Panel to stop it becoming a nuisance. By default, it'll stop you downloading files over MSN messenger, and it'll block a whole load of programs which download from the web.

Alternative Free Firewall Software.

If you want better protection, are having problems with Microsoft's firewall, or just want more flexibility, consider these free firewalls too:

- **Outpost Firewall Free edition.**

  Agnitum's Outpost Free Edition offers the ideal combination of top protection and good user-friendliness. It's a totally free product so there are no nag screens to contend with, and it comes highly rated by numerous tech sites.

- **Online Armour Personal Firewall.**

  Publisher Tall Emu's Online Armour firewall has been proved very efficient in tests, even outperforming some big-name commercial equivalents. It's light on resources, and heavy on security, so well worth checking out.

- **Comodo Personal Firewall.**

  It's totally free to use but you will need to register and activate the licence by e-mail within 30 days of installation. Whilst Comodo outperforms many similar offerings, it can be pretty intrusive, especially if you just want a firewall that does it's job no questions asked. Tech support is available via email, but not by phone.

Adware and Spyware

There are two more commerical types of software that you can find on your computer. Often legitimate developers will design programmes which incorporate useful functions, but unbeknownst to you either provide them with information about you or try to sell you things. They fall into two main categories:

- **Adware. Software that tries to sell you things.**

  Adware is software which sneaks onto your machine and opens up pop-up windows which sell you things, often but not exclusively gambling sites. It's easy to think of these as being related to the site you were visiting, yet often it's because a programme's snuck itself on your computer. If you've closed your browser and yet pop-up windows still appear on your desktop, chances are you've been infected.

- **Spyware. It tracks what you do.**

  Spyware is a more dangerous, less noticeable type of software which covertly grabs information from your PC and sends it back to its leader in out in the cyber-ether. Owing undoubtedly to their potential for criminal moneymaking, malicious spyware programs have become much more advanced in recent years, to the extent that some of the top spyware removers of yesterday can no longer cope. Luckily, there are some new pretenders to the mantle.

Some spyware can be legitimate...

There are a couple of legit spyware programs too; Google's desktop (if you allow it to) can send info on what you've been searching back to Google, and Alexa's toolbar can do the same. In both cases the aim is to monitor your computer to help develop their own product and data about people's searching habits.

Whether you allow this depends on your view on how you want the information to be used. Its mostly harmless but does mean someone, somewhere has access to your searching habits.

Basic anti-adware/spyware measures:

To put your mind at rest you'll need to download some extra software, but in the meantime there are a couple of basic things to do:

- **Use a pop-up blocker.**

  If you presume you're being troubled by adware, use a pop-up blocker to alleviate the symptoms while you find a solution. Do be aware though, that not all pop-ups are bad; some sites open new windows in this way - if you want to see them, hold down CTRL while clicking the link.

- **Be careful when downloading.**

  The usual way for ad/spyware programs to get on your machine is by attaching themselves to other things you download. Thus, check the veracity of download sources before getting files.

- **Delete programmes you don't use.**

  Use the add/delete function on your Control Panel to get rid of any programs you don't need anymore; they may be corrupted.

Free Ad/Spyware software removal

Spyware removers work by comparing what's on your machine to a list of known offenders. As ever, the top anti-ad/spyware programs are commercial, but that doesn't necessarily mean you need to buy them. Try these first:

- **A-squared Free edition.**

  Boasting awards aplenty, EMSI Software's A-squared free edition lacks the background scanning facilities of its commercial big brother, Anti-Malware, yet still packs in almost all its most useful functions. It's user-friendly with daily auto-updates, and has received excellent user feedback. Thanks to bazzlad for posting it in the forum discussion.

- **Malwarebytes' Anti-Malware free edition.**

  Whilst the free version doesn't provide real-time protection or scheduled updates, Anti-Malware is still powerful enough to make a big difference, and as a lightweight program it's pretty quick too.

- **Ad Aware 8 free edition.**

  Ad Aware's great at detecting and removing malware, and this version works even faster than previous ones. On the downside though, most of its features are locked in the free version, meaning that if you make it your primary tool, you won't be fully protected.

- **Spybot - Search & Destroy.**

  Spybot's been going for a while, and while it has a pretty long list of features, it's always received mixed feedback. It's fairly processor-hungry, so if your machine's already quite slow it'll be an unwelcome addition.

- **Spyware Doctor 2010 free edition.**

  The commercial version of Spyware Doctor is one of the best-perfoming anti-ad/spyware programs, yet the free trial version comes with numerous restrictions, and only offers real-time protection, no scanning etc.

Dealing with spam email

Want dodgy viagra or a fake watch? Want to invest in non-existent shares or visit fraudulent pornography sites? Or do you just want to click on a fake email from your bank to have your password stolen You may think it unlikely anyone would say yes, but if that were true, they wouldn't bother sending out the e-mails.

For the rest of us, spam is time consuming to wade through and potentially dangerous. Sadly, while you can register to stop junk mail or phone calls the same isn't true with spam e-mail. Yet there are a number of things you can do:

- **Use your e-mail provider's filtering.**

  Most big e-mail clients such as Google, Hotmail and Yahoo have their own filtering system to stop spam. Check your settings and make sure the filter is switched on.

- **Use rules in your e-mail software.**

  If you download your e-mails to a computer eg using Microsoft's Outlook - you can create rules to stop common spam by entering key words, e.g. VIAGRA, so those e-mails are automatically filtered. The only problem with this is that spammers try to beat it through mis-spelling words or using numbers in place of letters (i.e. V14GRA), so you'll have to block out other combinations too.

- **Never post your e-mail address in a public forum.**

  Only give out your e-mail address to people you know and don't post it on public forums or chat rooms (including this site's). Spammers often use software robots, or 'bots', to read all forums, store any e-mails and spam them.

- **Be careful what you agree to.**

  When signing up for free offers or sites, be careful what you agree to. All sites should have a privacy policy which declares what they will do with the info they collect. If they don't have one, steer clear!

- **Use a spare e-mail address.**

  Having a second e-mail address can be handy for special offers, newsletters or freebies if you don't want to clog up your proper e-mail address. Google's Gmail is especially useful for this, as at a later date if you change your mind and want those e-mails direct it can auto-forward them.

Yet do remember, Blocking spam's by no means an exact science, and thus important e-mails may also be blocked. For example, the term ‘mortgage' is commonly filtered out as spam, so you could miss an important note from your broker. And especially...

Do you get the free weekly MoneySaving e-mail? Please ensure it's in your 'accepted list'. The nature of freebies, money, mortgage & debt info means it's commonly hit by spam filters.

Free Anti-spam Software

Pro-level spam filtering programs can be really awkward to set up for casual users, so I've chosen a couple of simpler ones:

- **Mailwasher.** Rather than filtering through all your emails itself, Mailwasher works by allowing you to preview emails whilst they're on the server, so any nasty ones can be deleted before they make it to your machine.

- **Spamihilator.** Also free, Spamihilator runs in the background and claims to recognise 98% of spam which it moves to a recycle bin. You can teach its filter what to look out for, and thus tune it to your needs. Hasn't been updated in a while though...

Free Back Up Software

We've all had moments of horror (even in this very office) where due to hardware failure, power cuts or just plain ol' silly mistakes, precious documents disappear. As more and more of our lives are committed to the digital domain, backing up data is becoming more and more important, and since there are ways to do it free, you'll only have yourself to blame if you don't.

What to back up?

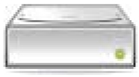
A good way to think about it is if your PC shut down tomorrow and didn't switch back on again what files would you miss most? These are the ones you should be backing up as a minimum.

Ways to back up:

- **Use Online Storage.**

This is a growing sector, and thus as companies compete to gather custom, there's loads of free space up for grabs. US site Adrive offers a mammoth 50GB free, making it the leader in terms of allowance. Others include Windows Live Skydrive (25GB), and Humyo* (10GB).

There are a couple of downsides to using these though; aside from the obvious worry about handing your data over to a third party, uploading's often painfully slow, and you'll have to log-in intermittently lest they think you've disappeared and strike your files from their servers.

- 

  Use Hardware.

  If you'd rather keep more tangible copies of your files, then the options are either storing them on CDs & DVDs (obviously you'll need a CD/DVD writer), or for larger amounts, on an external USB hard drive. As technology marches on, the latter are getting increasingly cheap; 1TB for around £60 is increasingly common.