THE HELPFUL BOOK COMPANY

Staying Safe on the Internet

8th Edition
(Covers PCs, Laptops, Tablets & Smartphones)

By Tim Wakeling

Intro – What are the Risks?

It seems like computer viruses are always in the news. And now there are plenty of other nasties on the Internet, such as spyware, ransomware, spam and dodgy websites that nick your credit card details.

You need to be careful. It's not just PC's you need to be careful on though – smartphones and tablets can be affected too. If you understand what some of the different risks are and what to do about them, you're much less likely to be attacked by a virus or spyware or whatever. And if you are, you'll know when it happens and you'll know how to do something about it.

I've written this little booklet as an introduction to Internet Safety. I'll explain a bit about the main risks and I'll tell you what you can do to guard against them. I hope you find it useful!

Tim Wakeling

Viruses

What's a virus?

A virus is a program that automatically passes itself from computer to computer. They usually do nasty things to the computers they "infect" along the way. For example a virus might send itself on via email to other people in your email address book, then corrupt all your work on the hard drive.

How can you avoid them?

Most viruses travel in email attachments. So if you get an email from someone you don't know with an attachment, don't open it. Even when you get an attachment from someone you do know, check it's genuine. If it says "Here are those photos of us in Blackpool that I promised you" and they did say they'd send you the photos, then it's likely to be fine. If it just says "Important files - read at once" then you should check whether that person really sent them or whether their computer is infected.

The other part of avoiding viruses is to have anti-virus software (see

below). Once you've bought some and installed it on your PC, or downloaded a free anti-virus app on to your tablet or smartphone (see below for more), you need to keep it up to date so it can recognise and get rid of new viruses. You need to set it to update itself through the Internet.

Then it:

1) Scans emails to check for viruses.
2) Watches which files certain programs are accessing and checks whether any are viruses.
3) Checks any disks you put in the PC.
4) Can check the whole of your PC is safe.
5) Gets rid of any viruses it finds for you.

Which anti-virus software should I choose?

If you have a computer running Windows 10, 8 or 8.1, you don't need a separate one because it comes free with the new version of Windows Defender , which is an anti-virus program as well as an anti-spyware program (see page 5 for more on anti-spyware programs).

If you have Windows 7, there are a few to choose from, and basically they all do the same job – protect you from viruses. Some can provide extra protection, for example against spam emails. Norton and McAfee are probably the best known brands of anti-virus software that you can buy, and they're both pretty good.

When you buy your PC, you may have either Norton or McAfee already installed on a trial basis. If so, you can use this for the trial period and then decide whether you want to pay to continue using it, or to swap to something else.

There are a few free anti-virus programs available too – for example Avira and AVG. They're free for home use, but you have to pay if you're a business or if you want extras like spam protection. But as far as virus protection goes, in my opinion they're as good as any. You can download them from the following websites:

Avira: www.avira.com
AVG: www.avg.com

If you've got an iPad or an iPhone then you don't need anti-virus software. There are a couple of reasons for this. One is that all the apps on the App Store are checked by Apple to make sure they're not infected with anything nasty, so you know they're OK to download. The second is that iPads and iPhones don't allow unauthorised programs, like viruses, to work – every program has to come from the App Store. So this means that even if someone emailed you something dodgy, the operating system that controls them won't let it install on the device. (The big anti-virus companies do sell security apps for the iPad and iPhone, but these protect your information if your device is stolen, rather than protect it from viruses.)

There's quite a lot of debate at the moment about whether you need anti-virus software on Android tablets and smartphones, e.g. ones made by Sony or Samsung. Google also check all the apps on the Google Play Store to make sure they aren't infected, and there are various in-built protection measures. If you stick to only downloading apps from the Play Store you should be fine, but Google's checks aren't foolproof, so if you want to err on the side of caution you can install a free anti-virus app. The anti-virus apps also usually have some handy extra features, such as being able to wipe your personal data from them if your device is stolen. A free app I'd recommend for android devices is the Avast app. To download it, just go to the Play Store, search for 'Avast antivirus' and tap on 'Install'.

What settings do I need?

The virus definitions (the info that tells it how to spot each different virus) need to be kept up to date – most software has a setting to automatically check for updates when you're on the Internet.

Set it to scan all incoming emails.

Set it to scan your whole computer, tablet or smartphone regularly. For example, you could set up a schedule where every Monday at 9 am it starts off a scan of every file on the computer. If your computer isn't on at that time, it should start the next time you turn the computer on.

Spyware

Spyware is nasty software that installs itself on your computer while you're browsing the Internet. Some **installs itself** without your permission and some pretends to be something useful so **you choose to install** it.

There are two nasty things Spyware does:

The fairly nasty kind (also called "Adware"):

Adware watches what websites you visit and pops up adverts for things that it thinks you might buy. Some types will try to connect to the Internet when you're doing something else.

Others pop ads up even while you're not on the Internet. Irritating!

The REALLY nasty kind:

These programs steal your money. For example, one type keeps track of what keys you press on different websites and when you type in your credit card details, they send them off to whoever wrote it.

3 steps to avoid Spyware:

1) Don't install software you download from the Internet unless you're confident it's genuine.
2) If you do download software from the internet, **read the agreement**. Many of them actually say that they'll pop-up ads (that way they're legal). Look near the end. That's often where they mention it.
3) **Make sure you've got spyware protection software**. If you have Windows 10, 8 or 8.1, you'll already have the new Windows Defender installed, which is both an anti-virus and an anti-spyware program. If you have Windows 7, it comes with the previous version of Defender installed, which is just an anti-spyware program (so you also need anti-virus software, see page 3).

Ransomware

Ransomware is a nasty piece of software that either locks you out of your device or encrypts all your files so you can't read them. Some ransomware even pretends to be from local law enforcement agencies, claiming that you've been caught doing something illegal online and your device has been locked. You can only get your files back by paying ransom money.

How much the scumbags demand varies - it might be £100 or it might be thousands, and they often demand that it's paid by something like bitcoin (a digital currency that's hard to trace) or by sending gift vouchers for iTunes or Amazon (which can be resold on the black market - nothing to do with Apple or Amazon). And if the unfortunate victim does pay up, there's no guarantee they'll get their files back. Sometimes they do, sometimes they don't.

Since 2012 ransomware has been on the increase. Some of the bigger ransomware attacks have made the headlines, for example, an attack in May 2017 affected over 230,000 computers in 150 countries, including many computers in the NHS. But despite the media coverage, ransomware isn't that common. Even though the chance you might be affected is very small it can have serious consequences, so it's a good idea to take some steps to protect yourself.

What can I do to protect against ransomware?

The main thing is to protect your device with anti-virus software (which also protects against ransomware) - see page 3.

The second thing you can do is follow some sensible rules to prevent ransomware getting on your device in the first place:

1. Keep your device's software up to date (that's Windows for computers, iOS or Android for phones or tablets).
2. Don't open attachments in emails from people you don't know.
3. Stay away from dodgy websites (e.g. ones for downloading pirated films or adult content).
4. Only install software downloaded from the internet if you're confident it's genuine.
5. Ignore any phone calls you get from someone claiming to be

from Microsoft or BT, – see page 12.

6. The final thing you can do is to keep a backup of all your important files. That way, if the worst happens and your device is held ransom, you don't lose everything.

Some anti-virus programs, anti-spyware programs & so on have very confusing names

Sometimes the names of programs designed to protect you against all these nasties actually have names that sound like you'd want to run a mile from them. The best example is a program called "Adaware" – a program designed to protect you from adware (which is bad). "Adaware" does have an extra "a" in it, but you have to be concentrating to spot it. At first glance it looks like it's just adware itself, so people are naturally wary of installing it.

Similarly anti-virus programs are good – they protect you from viruses, which are bad. And the same goes for spyware. Spyware is bad, but an anti-spyware program is good.

Most of the makers have the sense to include the word "anti" in their product names, so it's clearer what they do. Luckily the program Adaware is better than the name and does quite a good job of keeping you protected from Adware.

Fake anti-virus or anti-spyware programs

Here's what can happen: You're happily checking the weather forecast on the internet (or whatever else you do on there) when a new window pops up. The message says something like "Your PC may be infected with a virus. Would you like to scan your PC: Yes or No"). Sometimes it'll say your PC is corrupt or ask if you'd like to download

spyware protection – something along those lines.

At this point lots of people click on "yes". But it won't scan your PC, recover it or download spyware protection. It'll either take you to a very dodgy website or (more likely) download a program called something like SpyShredder or WinFixer… that actually is spyware or a virus itself, despite the name.

Now you know this, you won't fall for pop-ups like these and you'll click on "no". But the bad guys are cleverer than that.
On most of these pop-ups nowadays, the no button does exactly the same as the yes button – ie downloads the virus.

You might try clicking on the cross in the top right hand corner, to close the pop-up window. But some of the really clever villains can make that act like clicking yes. I honestly don't know how. Even if I was a baddie, I wouldn't be able to do that. But they manage it somehow.

But there's one trick that they can't beat

If you hold down the Alt key & tap the F4 key, that closes the current window. It's a useful shortcut anyway – it works for any program. But it's crucial here – it's the only thing they can't get around (because it's not clicking on anything with the mouse). So if one of these messages pops up, hold Alt, press F4 & you're safe.

And don't download any anti-virus or anti-spyware programs that you don't know are genuine. Especially if they're free. There are genuine free ones (see page 3), so don't be put off, but check it's recommended by someone you trust first! And if you've already got anti-virus and anti-spyware on your PC, just ignore any other programs. You don't need two.

You can also get fake anti-virus programs on Android tablets, smartphones, iPads and iPhones but Google and Apple have been removing the fake ones and updating their security checks to stop any new ones from being added to the app stores.

Spam

Spam is "junk email" sent out to thousands of email addresses to try to sell you junk. Once you get onto a spam list you can end up with dozens of emails every day, which clog up your inbox. See pages 10-13 for more about how to spot common scams and avoid getting caught out.

Three things about spam:

1) Although some "spammers" guess random email addresses, most get them from you entering your address somewhere on the web. So be careful about giving it to dodgy websites.
2) Some people do actually reply to spam — that's why spammers carry on. Even if it sounds like a good offer, please don't. It only encourages them.
3) Some spam says "email us to stop messages from us". Don't. They'll know you read your email and send you even more. *By the way, there are lots of perfectly reputable email newsletters (like my own), and if you've signed up for one of those, they'll also give you the choice of opting out. That doesn't mean they're trying to trick you – it's just fair to give you the chance to opt out. My point is just to check whether it's an email you've asked for – if it isn't, then don't reply to it, even to unsubscribe.*

Three ways to stop spam, but only one I'd recommend:

1) Buy a spam filter program. *(I don't like using these myself, because they can also filter out real emails that you wanted!)*
2) Use an Internet Service provider that filters spam out for you. *(These tend to have the same problems as "bought" spam filter programs, although most ISPs have them, so you might be stuck with it anyway.)*
3) "The webmail trick" *(this is the one I'd recommend)*:

As well as your normal email, set up a free webmail account. Then only give your main email address to people you really trust. If you need to enter an email address on the web (for example to get a free download) you give your webmail address. Then if you start getting too much spam, close your free webmail account and start up a new

one with a different email address. Let anyone who matters and who has your webmail address know, and Bob's your uncle.
Back to no spam (or next to none).

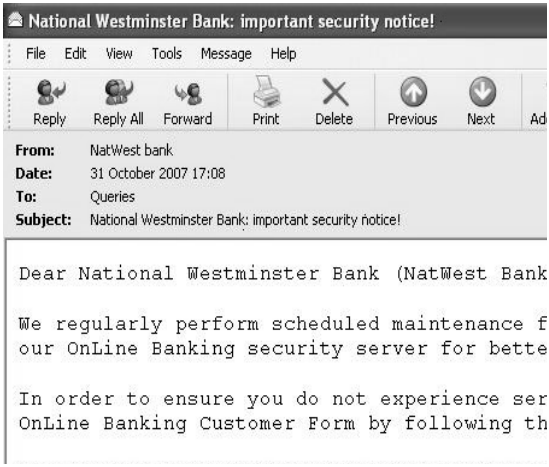
Common Scams (including "Phishing")

Scams are worse than your ordinary "junk mail" spam (see page 9). They don't just offer a product to buy, they try to con you out of money.

They try to get you to give personal information (generally bank details or passwords to your accounts with online shops) which they can then use to steal money from you. This type of scam is sometimes known as "phishing" (pronounced "fishing"), and there are two main types:

1) Fake emails from Banks, eBay, etc

The first type is an email claiming to be from eBay, PayPal or some bank or other. It'll look realistic and seem to be from the right email address:

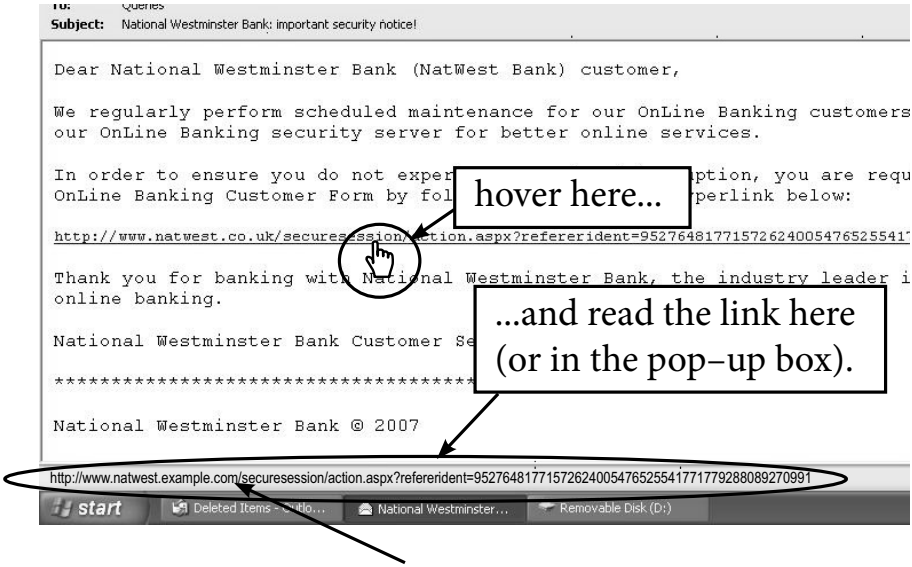


They say that there's a problem with your account and it won't work any more unless you update your details. Then they give you a link to click on. It'll actually take you to a fake website, they'll ask for your bank details or password and they'll use it to steal your money or buy things pretending to be you so you get the bill later on.

What to do: The simple rule is if you get any email asking you to confirm your personal account details, don't click on any links in that

email. Banks use the post to send out anything like this, not email. In any case, if you think it might be genuine, go direct to the real website by typing their address into the address bar of your web browser – then you know you're going to the right place and you can check up on your account safely. Or find their customer service email address from their website and ask them.

Another trick (although this only works if you're using a mouse, not with a touchscreen): You can check where a link is going to take you, without clicking on it. Hover over it with your mouse pointer (remember not to click!), and it tells you the website address at the bottom of the email window, or in a little pop–up box:



Notice that it says "www.natwest.example.com" – not "www.natwest.com". It's the bit just before ".com" that's important. Clicking on this link takes you to the "example" website, where there's a page named "natwest" – it won't take you to the Natwest website at all.

As I said before, it's always safest to avoid clicking on links in emails – just type in the website address yourself.

PayPal and eBay have email addresses for reporting these kinds of emails: spoof@paypal.co.uk and spoof@ebay.co.uk – just forward the dodgy email to them. Or if you get emails through Hotmail or

Outlook, you can click the 'Junk' button at the top, then on 'Phishing scam', where you can report the scam.

2) Sob Stories

The second is an email saying that the sender has had to leave a corrupt country and has lots of money which they can't get out.

If only they could go via a British bank account, they say, they could get the money that is rightfully theirs and wouldn't have to live in poverty. They'd be so grateful to you if you'd help that they'd pay you 5% of the millions of pounds they want to transfer via your account for a few days. Of course, once they've got your details they'll actually use them to steal your money. Sometimes they send a more vague email the first time and then will ask for your bank details later on if you reply.

There are variations on this – sometimes they ask you to pass on their money to a charity, and as a thank you you may keep a percentage of the funds – but it amounts to the same thing.

What to do: Don't reply, even to say you're not interested. It just tells them that you read your email. Then they'll send you even more junk.

Phone Scams

Another type of scam comes in by phone – and it can be very convincing. You get a phone call saying it's from Microsoft (or an anti-virus company) and they've noticed that your computer isn't protected and it's at risk. They might talk about a new virus that's out that can damage the actual physical bits of your computer.
It's sweeping around and will catch anyone not protected – so you'd best pay now by card and they'll install the protection on your PC over the internet for you.

To try to make you even more likely to say yes they might say that if it does attack your computer, it will cost (say) £200 to put it right again – but the protection is only £70 (or however much they want to say that day). This is a scam – it's not true. They'll charge your card for the £70 (or however much) and then sell on your card details.

They might ask you to install something on your computer, too – most likely some sort of virus.

Microsoft don't phone people like this – and in fact they wouldn't even know who to phone, since they don't normally sell Windows directly to you. The same goes for anti-virus companies.

The best thing is just to put the phone down – if you like you can tell the police, although they do already know about it and are trying to catch the people behind it.

It's worth knowing about in advance as some of these crooks can be very persuasive and can sound very convincing. But once you know in advance it's a scam, you won't be taken in.

Emails about Viruses that don't really exist

This isn't quite spam – but it still comes in via email.
What happens is this:

1. Some rotter writes an email saying that Microsoft, IBM, Norton or some other well-known company has just discovered a new virus.
2. They say it's the worst one ever. Often they'll say things that are impossible, like it'll physically destroy your PC. Or just that it'll delete all your files.
3. They tell you how to spot it.
4. They ask you to send the email to as many people as possible, so everyone knows about this new virus.
5. They send the email to everyone they know. They send it on to everyone they know… and so on, until it gets to you.

It sounds plausible – and it will come from someone you know. But the virus is completely made up.

These emails fall into two types:

The first type say that the virus is an email titled such-and-such, or with an attachment labelled so-and-so. There's no such email, so the only thing you lose is that you waste time checking to see if any of your emails are like this. The people who do this are small-time rotters, doing it for a laugh.

The second type tells you to check something on your PC, and if you find a particular file, they say you have the virus and must delete it. The file is actually a part of Windows and by deleting it, you'll stop your PC from working properly. The people who create this type are out-and-out rotters who delight in causing pain and frustration.

If you get an email like the above, ignore it. If you're nervous, just make sure your anti-virus software is up to date (see pages 2-4) with the latest "virus definitions". But I've NEVER seen one of these emails that's genuine AND up to date, so don't worry too much. Just delete it.

What's a "firewall"?

A firewall is another level of protection against nasties on the internet. It stops other computers accessing yours over the internet without your permission.

Do I need a firewall?

If you have an Android tablet or phone or an iPad or iPhone then no – you don't need a firewall as long as you only download apps designed for your device and get them through the store on your device.

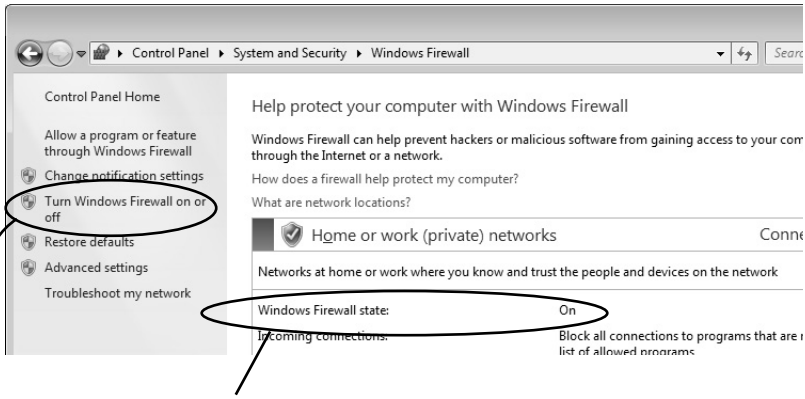
If you have a Windows computer or tablet then yes (but only one – see the next page). You should already have a firewall as part of Windows. To check it's turned on:

In Windows 10, type "firewall" into the search box on the taskbar and click on "Check firewall status" in the search results.

In Windows 8 or 8.1, on the Start screen, either start typing "firewall" or on a tablet, swipe in from the right and click on "Windows Firewall" in the search results. (If you've got Windows 8 you might have to click on 'Settings' first.)

In Windows 7, click on the Start button, then on Control Panel, then click "System and Security", then "Windows Firewall".

However you get there, you should see a screen like this:



If it says it's turned on, great. If not, click "Turn Windows Firewall on or off" and follow the instructions to turn it on.

My anti-virus software has a firewall with it. Should I install it?

You can if you like – BUT... *only if you turn off the Windows Firewall first*.

If you get a firewall with your anti-virus software, it may well be even better than the Windows one, so there's no harm in using it if you want. But you should only use one, not both. Two firewalls could interfere with each other and leave your computer as vulnerable as if you didn't have a firewall at all. Not a good idea!

If you'd rather have, say, your Norton one running, just turn the Windows Firewall off. To do this, follow the instructions above for how to change the settings, but select the options to turn it off instead of on.

It probably doesn't make a great deal of difference which one you use, just remember the golden rule:
only have one firewall running at any one time.

A Few Other Precautions

Internet Security Settings

In later versions of Windows there are quite sophisticated security settings that you can set as high or low as you want.

In Windows 10, type "internet options" into the search box on the taskbar and click on Internet Options in the search results.

In Windows 8/8.1, search for "internet options" from the start screen (just start typing and the search box appears), then click on Internet Options in the results. If you've got Windows 8 you might have to click on Settings first.

In Windows 7, click on the Start button, then on Control Panel, then choose Internet Options (you might have to click on Network and Internet in the Control Panel first).

In the window that comes up, click on the Security tab.
Here you can choose a level of security between medium and high.
I find the highest security setting can be a bit over-eager – it tends to give me warnings all over the place, for no good reason. I usually keep security set to medium-high, which is pretty safe without being annoying.

Protecting the kids

If you're worried about any children using your computer, tablet or smartphone too much, or using apps that you think are unsuitable, you can restrict their access. This involves setting up a user account for them, then once you've done that you can restrict the time they use it for and what apps/programs they can open.

To do this in Windows 10, open the Settings app by clicking the Start button then on the cog icon in the menu. In the app, go to "Accounts" then "Family & other people".

In Windows 8/8.1 and 7, go to Internet Options (as described above)

where you'll find a "Parental Controls" or "Family Safety" option in the Content tab.

For iPads, iPhones, Android tablets and Android phones, you can't control what websites can be viewed. Your only option there is to prevent the use of the browser at all (ie "No web searching while you're using Grandma's tablet!").

You can do this by setting restrictions on your tablet or phone, and choosing which apps can or can't be used. You can also make sure that no new apps can be bought without a password if you like.

On the iPad/iPhone, this is all lumped together in "Restrictions", which you get to through Settings, then General, then Restrictions. You can then enable restrictions, set a passcode and choose what features and apps you want to be allowed and what you don't.

On Android devices, there are two separate steps. First, open the Google Play Store app. Tap on the three lines in the top left and then tap on Settings. Then under User Controls you can chose to password protect any purchases and set a limit on the maturity level of the apps that can be downloaded (the maturity level bit isn't 100% accurate, by the way).

Second, go to the Settings app on your device, choose Users, and set up a "Restricted User Profile". This lets you enable/disable most of the apps on the device, including Chrome, the web browser. You'll need to password protect your main account, so that children can easily access the restricted account, but need your password to get at your main account that lets you do anything.

Buying Online Safely

I've got two pieces of advice about shopping online safely.

First, make sure the company is genuine. M&S aren't going to nick your credit card details and run off to the Bahamas, but some dodgy guy might. This is no different from buying in a shop or over the phone, really. One tip is to check the website has a phone number and physical address listed. If it doesn't, why are they trying to hide?

Second, check the website is what's called "secure". That means someone else can't hack into it and steal your credit card details while you pay. Otherwise, even if the company is genuine, someone else could get your details. Luckily, it's easy to check. Up in the top of the

screen, where it says http://www.thewebsiteyoureon.co.uk, it should say **https:** instead of **http:** (The s stands for secure. It only needs to say it while you're putting the payment in, not when you're looking at the rest of the site.)

Common Sense

By far the most important thing is to **use your nonce**. If a web page looks shady, close it down. If an email seems to be doing strange things, close it and use your anti-virus program to scan your PC. If you hear about a particularly bad virus on the news, make sure your anti-virus is up to date.

5 more common-sense points

1) Don't give out credit card details unless you're comfortable it's a genuine company.
2) If your PC, tablet or smartphone starts acting strangely, disconnect from the Internet and run a full virus scan.
3) Don't respond to spam email.
4) If you do get a virus, disconnect from the internet until you've got rid of it, or you might spread it around.
5) If you randomly get a pop-up asking for personal details or for you to allow your computer to download something, don't.

One last thing...

Don't let all this put you off using the Internet. There's a tremendous amount of really useful, fun and interesting stuff out there. Think of the risks a bit like crossing the road: running across without looking is dangerous but if you follow the basic precautions, you'll be fine.

Above all, have fun!

What all the jargon means

Adware	A type of spyware that shows adverts on screen based on what websites you've visited. Sometimes a mild pain, sometimes there are so many adverts your PC becomes unusable until it's cleared up.
Definitions	For example virus definitions or spyware definitions. They're the info that your security program uses to spot a particular virus or spyware.
Firewall	A programs that stops other computers getting into your PC across the internet without your permission. Especially important to stop your PC becoming a zombie (see below).
Keystroke logger	A type of spyware that reports back all the keys you press, which might include passwords or credit card details – which is why on some sites you use menus to select letters from a password or the expiry date of your card. That way a keystroke logger can't tell what it is.
Malware	Any type of software designed to cause damage, including spyware, viruses, ransomware, worms... Short for malicious software.
Phishing	Pronounced fishing. Emails or websites that try to trick you into giving personal details – your passwords or card details.
Spyware	Software that watches what you're doing on your computer and reports back to the person who wrote it. Usually with unpleasant intent.
Ransomware	A nasty piece of software that either locks you out of your device or encrypts all your files so you can't read them. You can only get your files back by paying ransom money.
Trojan	A program that looks like you want it (eg a handy program to play music) but that also includes something you don't want (eg a virus or spyware).
Virus	A program that passes itself from computer to computer, usually doing harm on the way.
Worm	A bit like a virus but different in technical ways. Real techies get annoyed if you call worms viruses and vice versa. But they're both bad news.
Zombie	Your PC becomes a zombie if someone else manages to take control of it over the internet. You might not notice as they'll only use a part of its power. But they might use it for sending spam – which is why it's so hard to track down spammers.

www.helpfulbooks.co.uk

CSFB08A
1217