- **Avoid free online offers of programs to rid your hard drive of viruses and shred your history completely. It will probably install spyware or infect your hard drive.**

- **Do not open attachments on emails that you are not sure of.**

- **Delete *en masse* all your junk or spam emails from their folder. However, first check that you have not had any real or genuine emails arrive in the junk or spam file.**

- **Trojans can appear as pictures, videos, music etc. in Windows, so take care when you click that nothing downloads.**

- **Always check that the padlock icon is visible at the bottom of a website's screen if you are going to make a purchase – this is a sign of a secure transaction.**

- **On mobile devices such as PDA units and smart phones, use one of the many secure electronic wallet/safe programs to protect sensitive date such as passwords/pins etc.**

What else can be done to protect the computer user online? There are a number of other forms of protection that are in use to protect the shopper or Internet surfer.

There will be a growing number of securities that will no doubt be put into place to try and help. For example, some card companies allow you to set up a second on-line password once you are making a purchase. This is intended to stop someone with your card, or card details, from using it on-line as they need this second password also.

It is up to the card holder to decide if they wish to register for this extra security when they first use the card or at a later date. Once selected it will be necessary to use it each time. It is recommended that if your card provider uses this system that you take advantage of it.

A second and far stronger system is also in limited use, although unfortunately not at the present moment in the UK except on an inter-commercial level. It is, though, in much wider use in some European countries.

The card holder is issued with a plug-in hardware box that connects to the computer. Each time the user connects to, say, a bank web site; a different second password is used in a sequence only known by the bank's computer.

Alternatively, the user may be given a simple scratch card. Each time the user logs onto their account, they scratch off the next panel to obtain their second password. If a panel is removed by a third party, the user is made aware.

Unfortunately, this system is seen by many as adding to cost and needing more administration, though one can see how it would improve security greatly.

Fingerprint recognition is now being employed more and more from mobile phones and shop tills to banking. It is far cheaper than second password security, though there are still a few problems to overcome. Iris technology will probably also have a similar role in the very near future.

Temporary e-mail addresses: Also called disposable email addresses. As stated earlier, it is well worth making full use of the short-life email addresses that are available and free. A Google or other web search will show many providers of these useful tools.

Not only do they stop spam in its tracks, but they provide you with a vital defence from criminals. You have a set lifespan for the email address, or you can have one that you can kill at any time you choose.

This allows you to complete a task in hand, for example, a purchase or a communication with a person or organisation. However, after this task is completed you may have good reason that the person cannot use the email for future follow-ups. This is the simplicity of the temporary e-mail address.

Other e-mail addresses: You may also want to make use of other email addresses to protect yourself. You may want to use an online email address such as Hotmail and use it only for a single intended purpose.

For example, if you enter a lot of on-line competitions you may have one dedicated just for that purpose. It will without doubt attract a lot of spam, as well as being picked up by fraudsters wanting victims to approach. You would consider all non-competition communication in this inbox as probably fake or dangerous, though quarantined.

You may set up a number of such email addresses for different purposes, should you get swamped out with spam etc., and it is simply a matter of ending the account.

A warning about links and displayed email addresses. It is vital to understand that just because we can see an address we know to be correct on display on a web page, does not mean that we actually believe it to be what it proposes to be.

Most of us will have received phishing emails trying to trick us to reveal our personal details such as bank accounts password etc.

They normally try to worry people by giving them a concern, e.g. account suspended, attempted log in by third party etc. and the need to correct this information by clicking on a link and providing the information that they want.

The link is, as we can see, a correct e-mail address, and as such some may be tempted to click on it. **DON'T**, ever. Look below how easy it is to redirect an e-mail to another address. This is using Outlook Express, though all other email applications can be adjusted also.

How to fake source of email:

In Outlook Express click the TOOLS menu
Click ACCOUNTS tab
Click MAIL tab
Click on default email account
Click PROPERTIES
Click on GENRAL tab
Find section titled USER INFORMATION (your details should be in the box)
Delete this information and put in false details
Click OK followed by close

Now send yourself an email. It will appear to have come from someone with the false information that you placed in the box. Repeat these steps to correct the settings for your email.

It is also just as simple to change the outgoing email intended for the address shown on the link to go to any other inbox. It would, though, possibly be irresponsible to print how to do this, should somehow someone come across this information who had less than virtuous ideas.

Should you have any concerns as to the contents of an email received, etc., always use the email address you know to be correct that you have on printed documents etc., and that you physically type into the browser window.

If you study these phishing e-mails you will almost always find many clues (99.99% of the time) that show it to be a fake. The following are just some of the clues:

- **You have no connection with the source, e.g. do not bank with them, have not entered the lottery you have 'won'.**

- **They call you 'dear customer', not your correct name and title.**

- **They are full of spelling mistakes with poor grammar.**

- **They follow a foreign speech swing, showing they are from Africa, Asia etc. You simply see, almost hear the accent of the foreign person.**

- **The start by quickly trying to instil fear (that you are at risk etc.) or joy (you are about to come into money).**

- **They try to instil trust by signing with a title, such as Doctor, Chief, Rev, etc.**

- **You do not know them, and they do not know you, despite offering you a vast sum of cash etc.**

- **The logos on the web site are poor quality, links do not respond etc.**

These are some of the examples. If you take time to look, you will spot many – it is often simply studying what comes and, if you are not happy, send it on via a phishing link on your browser.

Hijacked Internet accounts: This can be a real problem depending on the account in question and the resourcefulness of the fraudster.

A simple example would be the takeover of an eBay account. Without any doubt, eBay is massive. It is a worldwide empire that is the world's greatest marketplace, to coin their own term.

It has also had many scams played against its members in an amazing amount of ways. This is not saying that eBay is a security threat. It is simply so massive that, pro-rata, it will have many such scams.

In fact, eBay take security so seriously that it is probably one of the most secure sites to use if care is applied. eBay is constantly bringing in new security measures to thwart possible future security threats so that they make it hard for the scammer to achieve their intended goals.

That said, the people at eBay are only human, and scams will continue and new ones will be born on a continuing basis. One of the hardest to deal with is account takeover. This is where the criminal has enough information of the eBay member to use their identity and take payment for non-existent goods in the name of the member.

The money, often via Paypal or similar, is funnelled into another bank account before the thief disappears. She/he does not simply disappear with your money, but often with many more members whose accounts have been hijacked at the same time.

If the thief knows something of your lifestyle, e.g. when or how often you access eBay, or when you are on holiday, all the better. This means they may run the scam in your name over a longer timescale, knowing you are less likely to spot them.

However, it is simplicity itself to find countless eBay accounts that are active, but have never been used for many months and equally many years. This allows a virtually undetectable account takeover.

Even the account of someone that is active can easily be targeted. Once the criminal is logged into an account such as eBay they often simply change the password and lock out the person whose account it really is.

Often the person locked out does not realise what is going on. They simply think that they have a simple technical difficulty that will soon rectify itself if left alone, this is the apathetic or 'it should sort itself out' attitude.

To access the account of others is not too difficult to those who do not give up easily. They have the user name of the individual, as this is common knowledge and displayed for all to see.

The email address is almost as easy to find, as many openly show this, and it is available from many other sources other than eBay. The password is the only one that needs some work to reveal, but as we have seen this is often just a matter of time with the methods available.

With this information the criminal can enter an eBay account and take a number of courses of action. One may be simply to use eBay to access a linked Paypal account. Often more than half the time the password is the same one as used on eBay, and the only other requirement is an email address that the thief has anyway.

Now they can take over the Paypal account, within minutes adding another bank account and emptying the funds in the Paypal account into the bank account. They can receive payments into the account for goods they do not send or even have before also sending the money to their account. They can remove limits set up to control how much money can be taken from the account, and many other devious schemes are employed.