The website getsafeonline.org aims to provide computer users with free, independent, and user friendly advice so you can use the internet safely, securely and with confidence. Please take the time to browse through the information which will tell you how to protect your PC, how to avoid on-line scams and much much more. We have picked out some basic advice below but please access the website for more detailed information.

Follow these tips for online safety

Be aware of online fraud, identity theft and scams
Use anti-spyware
Use anti-virus software and update it regularly
Use firewall software
Use the latest version of your computer´s operating system
Keep your software up to date
Protect your computer against theft and damage
Block out unwanted emails
Protect your wireless network

Online fraud, identity theft and scams - There are so many scams on the Internet that you really need to be very wary. Here are some examples.

Spammers - These are people who really don´t care how they get hold of email addresses. The more they have the more spam emails they can send or they sell them on to other spammers. They will do anything to get access to your contact lists. Here are some key rules that you need to follow.

DO NOT forward emails that say “forward this on to '10' of your friends, sign this petition, or you'll get bad luck, you'll see something funny on your screen after you send it.....” These almost always have an e-mail tracker program attached that tracks the cookies and emails of those people you forward it to. The host sender is getting a copy each time it gets forwarded and then is able to get lists of 'active' email addresses to use in SPAM emails or sell to other spammers.

DO NOT forward emails that ask you to add your name and forward on to others. This is similar to a mass letter sent years ago that asked people to send business cards to a little kid in Florida who wanted to break the Guinness Book of Records for the most cards. All it was, and all any of this type of email is, is a way to get names and tracking information for telemarketers and spammers.

DO NOT forward emails that warn of other hoax emails. Get familiar with www.snopes.com and
www.truthorfiction.com
for determining whether information received via email is true/false or fact/fiction. If in doubt

about anything just delete the email if it is really genuine the person who sent it will contact you again.

Phishing - Another example of a form of fraud is known as "phishing"

Barclays, Lloyds TSB, MBNA, Natwest, Citibank and even the Bank of England have been affected by phishing. Customers were sent emails saying that the bank was making technical changes. There was a link to go to a page where customers were prompted to enter their account details. Some customers received emails saying their accounts would be cancelled due to a new security measure unless they went to a site and entered their details. The fraudsters set up “spoof” email addresses that look like they could credibly belong to the institution. Once they have received account details, they siphon money out via “mules” – people with UK accounts – to their own accounts abroad. These scams are believed to be run from Eastern Europe. In another case an email supposedly sent from the Bank of England urged people to download anti-virus software.

Other common scams are shown below but there are hundreds of other examples. Use the websites www.snopes.com and www.truthorfiction.com to check out new scams which are being created every day - the message is be on your guard!

Fraudsters send emails to people telling them they can release a fortune that is tied up in an African bank by allowing them to transfer the money into the person’s account. In return, the person will be given a share of the profits. Another variation on this is an email supposedly from the widow of a high-ranking Nigerian official pleading for the recipient to help her access her late husband’s money. Again, the recipient is asked for their bank details.
The catch with these scams is, of course, that rather than money going into the person’s bank account, the fraudsters clean out them out using the details sent to them.

Lottery and prize draw wins. Emails are sent out to people telling them they have won a lottery or prize draw and they need to send a payment for “administrative” or some other purpose in order to claim their winnings. Of course, there is no prize...