Phone and Email Scams - more

There are a growing number of scams being reported, using phone calls, Emails, text messages (SMS) and web sites.

These all have one or more of these aims:-
1) To get you to give them your phone number or Email address, which at the very least will be sold to get you lots of scam phone calls and/or emails.
2) To obtain money from you by fraud.
3) To obtain personal information which can be used to obtain money from you or 'steal' your identity, which can be VERY serious.

Remember:-
A) If you did not initiate the contact then you have no idea where it comes from.
B) The originating email address or phone number can very easily be falsified and the scammers are getting 'better' at doing this convincingly.
C) Email addresses get 'harvested' regularly when email servers get 'hacked'. This appears to happen more often for web-mail addresses, i.e. hot-mail, g mail, yahoo, BT etc. as many thousands of addresses can be obtained from one computer mail server.
D) Your computer does NOT send out data to ANYONE about the speed it is running at or any viruses it may, or may not, have.
E) Your router (hub) does NOT send out data about your internet/broadband connection state or speed.
F) Anybody can put anything they like on a website and many people can falsify (hijack) web addresses so that you are not on the site you think you are.
G) All of these can apply to text (SMS) messages.

How you can help others when you send emails:-
A) Always put a meaningful title/subject for your email, preferably several words. I know it can be tempting if you are in a hurry to just put 'Hi' or some such but this makes it very difficult for people receiving it to decide if it is genuine.
B) Always add photos as 'attachments' and never 'in-line' as in-line items are automatically opened.
C) Don't put web addresses in an email unless there is no other way of doing it, and if you have to ALWAYS mention it in the text.

How you can help yourself when you receive an email:-
A) Ensure that your email programme does not open an email until you double click on it. This is especially important if there is an attachment. This can usually be done in an 'options' menu which is often listed under 'tools', but different email systems can do things differently or not at all.
B) Ensure that you have set appropriate programmes to open common file types with. This will help protect you if an attachment is not what it seems to be. This can also be done in an 'options' menu which is often listed under 'tools'.
C) Set windows NOT to 'hide extensions of known file types'. This makes it much more difficult for an attachment to appear as something it is not, and can be done from the 'Control Panel' under 'Appearance and Personalization', click on 'Folder Options'.