The Facts

- The number of people who engage in this silly and hurtful activity is very small.
- **There are far more good messages than bad. Don't let this spoil the internet for you**.
- People who send viruses or malware are breaking the law. Report it when you can.
- **By reporting this and asking for help you are not only proving you are a responsible internet used, you are making the web safer for all of us**.
- There are simple steps you can take to stop this happening, and for dealing with it should it ever happen again.
- **We can beat the email scammer**.
- Every adult in your home needs to read this leaflet.
- **Tell your friends if you think there are scam emails about.**
- Remember, talking about it is the first step to making it stop**.**
- Ask your parents to install Internet **Explorer 8 with Zip it, Block it, Flag it** buttons. Then **YOU** are in charge.
- **Together, we can make everyone in East Sussex E-Safe**.
-

Further information

You may find these sites useful.

The UK Council for Child Internet Safety. (UKCCIS)

http://www.dcsf.gov.uk/ukccis/

Microsoft Windows Parental Controls

http://windows.microsoft.com/en-GB/windows-vista/Kids-online-A-parents-guide-to-monitoring-computer-use

The Child Exploitation and Online Protection website (CEOP)

http://www.ceop.gov.uk/

The Byron Report (An investigation into online safety for children and young people by Dr Tanya Byron)

http://www.dcsf.gov.uk/byronreview/

Parent's centre (A government resource for parents who want to know more about e-safety.)

http://www.parentscentre.gov.uk/usingcomputersandtheinternet/

Odd Emails

What they look like
What to do
What NOT to do

East Sussex County Council

eastsussex.gov.uk

What are "odd emails"?
They can take many forms. They tend to take two main forms.

1) From people you know. This type of email comes from a person who you know in the real world, but it usually offers you something, or suggests that clicking on an enclosed link will help your computer or protect you from a problem. **It Doesn't**
2) A blank email with an attachment. These usually are blank, or have a few meaningless words in them, but they have an attachment which is usually quite small. It is very tempting to click on the attachment to see if it helps you understand what the email is about. **It won't. Don't do it.**

Why do people do this?

Some people think that planting a virus on your computer is funny. Others have a more sinister intention and they want to be able to access your PC remotely, or harvest information from it. They can get access to anything – your bank details, bank details of others who use your computer and maybe addresses too. They use this information to rob you, or set up a false identity.

How do I beat this?

There is no doubt that using an email system like Outlook or Outlook express is the best way. Web-based email like Hotmail is full of problems and offers little in the way of protection. You should configure your email browser to have a "Preview pane". This allows you to look at the contents of an email without opening it. You will soon learn to tell what the suspicious ones look like. **And never EVER open an attachment unless you are certain it is ok.** If it comes from a friend, it is worthwhile phoning or texting them to ask if they have sent you an email with an attachment. **It is very easy indeed to copy someone else's email address.**

Anything else?

Yes. You must make sure you have a good quality anti-virus, firewall and anti-spyware/malware system installed, updated and running. You need one that offers real-time scanning. Sometimes, on older computers, installing this software slows them down. Sometimes it is tempting to only install anti-virus. **It is not enough.**

So which one should I use?

We cannot give you product advice. Let's just say that some are far more well known than others. Schools use MacAffee. It is not the only product out there and there are "free" ones. The problem with freeware is that it may or may not have the latest virus definitions, and it may or may not update often enough. Virus activity seems to come in waves. At times, it is not impossible to have 20 updates a day! The important thing is that you **have** a good quality product, that it is installed on **all** the computers in your home, and that it is set to update and install updates automatically. **(Windows should also be set up to download and install updates automatically)**

How do I know if I have got a virus?

This is difficult to answer, but if your computer suddenly starts working very slowly, or if there is a large amount of hard drive activity, then this might indicate a problem. Similarly, if you start to see odd characters on your screen, or your keyboard starts acting up, this may mean you have spyware, malware or a virus.

So what do I do if I think I have?

1) Run a **full system scan** using your anti-virus product.
2) If you use Windows, download and run the Windows Malicious Software Removal Tool. http://www.microsoft.com/en-us/download/details.aspx?id=16

I have a Mac. What do I do?

Macs seem less susceptible to viruses that Windows-based PCs, probably because Windows became established more quickly than the Mac system did. Talk to your local Apple store or check online. There are products out there, but you will need one that suits the Mac that you are using.