The Facts

- Exploitation happens. You can make sure you are not part of it.
- **Listen to your inner voice. If it doesn't feel right, then it probably isn't.**
- Any decent, reputable company will understand if you don't want to talk to them on the phone.
- **Most fraudsters won't and will quickly become angry, threatening or abusive**.
- Remember, once a photograph, movie or image of you is online, it is there forever.
- **If you think someone else knows about any bank account you may have, tell your bank. They can help you stay safe**.
- No bank will ever ask you to visit a website to confirm your details. It just doesn't happen like that….EVER.
- **Your personal information is highly valuable. People need a very good reason to ask for it.**
- You have the right and the ability to control how much information you give to others or put onilne. The more you think about this the more empowered you become and the more safe.
- **Don't let the exploiters win!**

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.education.gov.uk/a0076277/the-byron-reviews

Parents Protect (An online source of advice for parents and carers.)

http://www.parentsprotect.co.uk/internet_safety.htm

What is "online exploitation"?

And what does it mean for me?

East Sussex County Council

eastsussex.gov.uk

What is “online exploitation”?
This is term that covers a very wide range of behaviours. It may mean, for example, trying to get money out of you by playing on your sympathies, or by frightening you. It can also mean making you do things online that others will later use.

Who does it?
The short answer is “anyone”. Some people may ask you for money who are perfectly genuine, and who may well represent the charity or organisation they claim to, but others are out to con money out of you and anyone else.

What sort of things do they want?
Your bank details for one! You may think you are giving some money to a good cause, but the moment you give out your bank details, there is nothing to stop them taking as much money as they can from you. Some people want you to send pictures of yourself, or may ask you to do things on a webcam that you feel embarrassed or uncomfortable about. This is also a form of exploitation. Others will want your contact information, usernames, passwords, that kind of thing.

How do I know?
There is one thing that is a dead give away. If you ever get an email from a Bank or Building society telling you that your account has been frozen because of a security issue, you can ignore it. No bank will ever contact you in this way and they will never ask you to go to a website to “confirm your details”. It can be scary to get an email like this, but each and every one of them is a fake. Sometimes, you may be told you have won some money, or a prize. (You cannot win a competition you never entered!) Sometimes you may get an email from a foreign country asking you to help with distributing money and offering you some in return. Again, these are always fake and, tempting though it may be, all they want are your personal details so they can either assume your identity or take your money.

What IS identity theft?
It is when someone pretends to be you. To do this, they have to know pieces of information about you. If they know the right pieces of information, they can take out loans in your name, run up bills and even create a bank account and then run up an overdraft. Your personal information is private.

I’ve heard about phone calls like that.
Yes, sadly, this happens too. Some people phone up, pretending to be, say, the gas company, and ask you for some “security information” such as your home address, or postcode, or even your date of birth. They may even ask for several things. One way of looking at this is that they phoned you! They should know who you are and you do not have to tell them anything. The best way forward is to just put the phone down, but if you must talk to them, try asking them to prove who they are. They will soon cut the call off! Also, another indication is that if you do not give them the information they want, they very quickly become angry or threatening. If that happens, you can be sure that it is a hoax call. No utility company, bank or building society would ever ask a child for such details. Ever!

So what should I do if I get a call like this?
First, never give any information whatsoever to anyone on the phone. If they are who they say they are, they will understand this and phone back later. Then, always tell your parents or carers that you have had the phone call.

What if I have got a lot of personal information like this on my social networking site?
Then you might want to consider taking it off. There is no legal requirement for you to post everything, (or indeed anything) about yourself online. You cannot have a loan under the age of 18 anyway, so up until then, they can’t use that information. However, people sometimes keep it for a long time, so you might want to think about taking it down now.

Do people really behave like that?
Yes, sadly, they do. And even more sadly, every year people fall for it. Usually the young, very old or the vulnerable. These people do not care who they hurt. All they want is your money or your identity.