SCHOOLS ICT

High Risk Questions

E-Sussex, E-Safe

Safeguarding all children in East Sussex all the time

East Sussex County Council

Provided by East Sussex County Council

In the world of Social Media, texting, and instant messaging, there is a wealth of opportunity to stay in touch, share important events and information, and also, unfortunately, to come into contact with unsavoury people who may have highly dubious intentions.

Most messaging systems, be they on social media, or stand-alone messaging allow “contacts”. This is a list of people who can send you messages. Sometimes you have control over this, and sometimes you don’t.

There are two kinds of contact – people you know in the physical world, and people you have never met and therefore don’t know in the physical world.

What’s the problem – I like meeting new people?

The problem is that it is easy to set up a completely false profile online. Unless you know someone in the real, physical world, you have no way of knowing they are who they say they are. We have seen middle aged and elderly men pretending to be 14 year old girls; we have seen women pretending to be men; we have even seen individuals pretending to be companies such as Facebook.

So, what questions should I not answer?

Anyone who has the right to personal information, already has it. Family and friends, for example. So, anyone asking your age, sex, location, where you go to school, where you go at weekends, what clubs you go to are asking for personal information to which they are not entitled.

And it doesn’t end there. Questions about what you have in your home should also be avoided. For all you know, a thief already knows where you live, now all they need to know is what you have that might be worth stealing.

Really?

Oh yes! Thieves have now reached the electronic age too. Why wander about a town trying to look into people’s windows, when you can try and get them to tell you, online, what you have in your home.

For this reason, never respond to official-looking inquiries of this nature. Your Local Authority, for example, will never email you asking such questions, and neither will insurance companies. (There have been scams where people have been approached by what looks like insurance companies offering unbelievably low quotes which turned out to be a team of thieves.)

How do these questions appear?

Language has changed, and acronyms are all the rage. Here are just a few:-

ASL? = Age, Sex, Location. Someone wants to know how old you are, what gender you are and where you are. Anyone who has the right to this information already knows it.
WC? = Have you got a webcam? Again, anyone who has the right to this already knows, but this is also used by people who may try to encourage you to do more than just talk to them online.
WMM? = Wanna Meet Me? Sometimes you see **MM@** (Meet Me At….) NEVER agree to meet with a stranger.

There are more, and it is worthwhile making a list of questions that you will never reply to.

Remember, online, there is NO need to respond to a question. You have the right to ignore it.

Any question that gives personal information or location information about you should not be answered.

And that applies to questions about your friends too.

It's not a question of not trusting people, its more about just being on your guard.

If you are a parent or carer….

Encourage your children to make their own list of No Response questions, but bear in mind that sometimes they may be tricked into giving information away. If that has happened, make it OK for them to tell you – now is not the time for an angry response – then you can plan accordingly.

For example:-

Scenario.
"Jessica" is 15, she has been chatting with someone online and has told this person that she goes swimming every Saturday afternoon. She has also told the person the town where she lives. It has a public swimming pool.

It's too late to take the information back, but what you could do, is to go with her for a few weeks. Just be there and watch. You could also alert the pool that this contact has been made and you are worried.

Scenario

Billy has been using Facebook since he was 9. He set it up without his parents knowing and he is very proud of having over 1000 “friends”. On his 12th birthday, he was given a bank account and it came with a bank card.

Billy thought this was great and published “Got my own bank card” in his Facebook status. One of his “friends” then started a game with Billy to guess the numbers on the card. After a few weeks, Billy realised he had given the whole number, expiry date, and CVC number away!

Billy didn’t tell his mum or dad, because he thought they would be cross.

When Billy’s bank statement arrived, a lot of purchases had been made.

Outcome

Billy’s parents contacted his bank who were able to recover most, but not all of his money. They said that Billy had broken the terms of use of the account by giving the number away in this way. Billy was lucky that he got most of his money back.

Key Points:

- Children are highly technically aware, and can set up accounts on social media with no assistance whatsoever.
- Billy should have not engaged with the game of guess the number.
- Billy should have told mum and dad straight away – the moment the other user asked to try to guess the numbers.
- The Bank acted promptly, but were unable to recover all the money – as Billy breached the terms of use of the account, the Bank could have done nothing.