Staying Safe on the Internet

Lesson 3: Online Exploitation

Teacher's Hints for Group Discussions

Rukhsana's Story - Activities

Question 1:

"Think about things from Rukhsana's point of view. Explore how Rukhsana is leaving herself open to exploitation and what sort of exploitation – this could be identity theft, grooming, etc."

Here are some hints for the group discussion:

- Remember that on the Internet, anonymity can be a very useful protection. Information is power! Any information that you give out about yourself can be used by people with wrong intentions to hurt you or to abuse you.

Danger from Online Predators:

- Some Online Predators surf the Internet looking for profiles of people with certain characteristics, and then try to trap them. If Rukhsana had formed an online friendship with a Online Predator, or anyone else that wanted to hurt her, they could use the details of her full name and her town to find out her address, and from that, find her telephone number.
- Using details in the school photos on her social networking website, and knowing which town she lived in, Online Predators could easily work out which school she attends. If they were really determined, they could use this to track her down personally.
- They could also use these sorts of details to make her feel afraid, to make her feel that they knew where she lived and they could hurt her if they wanted to. They would do this in order to intimidate her and try to force her to do things she did not want to do.

Danger from identity theft:

- Using the details of her name and the town where she lived, an identity fraudster could find out her full address. She also gives out her birthday on her social networking profile; this is especially dangerous because the date of birth (with the year) is often used as a security question by banks and other organisations.
- Once they had details of her name, address and her date of birth, it would be easy for an identity fraudster to steal her identity, for example, making false loan applications in her name or getting credit cards in her name when she is old enough. They could even try to steal her vote when she becomes old enough.

Rukhsana’s Story - Activities

Question 2:

“Think about things from Amirah’s point of view. What advice would you give to people like Rukhsana about how they should be careful?”

Here are some hints for the group discussion:

Anonymity:

- Everyone that you need with online and that you don’t know from real life is a stranger, and remains a stranger, no matter how much you talk to them online.
- It’s very easy to pretend to be someone else on the Internet, and there are many people out there on the Internet who use this feature to try to hurt people. Any information which you make available to the whole world should be as anonymous as possible, so that nobody would be able to identify you personally, or find out your address, your age, or where you go to school, unless you allow them to.
- This also applies to online conversations with online friends you don’t know and trust from real life. You don’t really know who they are, and you’ve got no guarantee of what they’ll do with any personal information you give them.
- It’s actually not safe to go telling online friends all your personal problems if you don’t know and trust them from real life. There are Online Predators that sit in chat rooms and try to befriend young people who are going through a rough patch, who may be isolated or looking for some support—they build up trust with them, and then use this trust to put them in positions where they feel they can’t refuse, or are too frightened to refuse, and then attempt to abuse them.
- It’s OK to be anonymous, and it’s OK not to give away details to people that ask them from you, if you don’t feel comfortable about giving them out.

Photos:

- Be really careful about the photos that you put online or send to other people, even to friends. Some Online Predators do surf the web and pick up pictures of young people in revealing or suggestive poses to feed their appetite. Also, people who are friends now might not stay friends forever, and photos in electronic form can and do get misused when relationships go sour.

Levels of privacy:

- Some social networking sites (e.g. Facebook®) allow you to control who can see what on your profile. You can use this to restrict access to personally identifying information to only those that you know in real life.

Report:

- Remember, you can report any behaviour you feel to be suspicious to CEOP (the Child Exploitation and Online Protection Centre) through their website - www.ceop.gov.uk - and through the CEOP button in some Instant Messaging programs.

Rukhsana's Story - Activities

Question 3:

"Think about the risk from Online Predators. What methods would online predators use to identify people like Rukhsana, and what could they do to exploit her and her family as a result of her actions?"

Here are some hints for the group discussion:

Misusing information:

- Some Online Predators use information about age and sex to narrow down their search for victims.
- Some Online Predators collect revealing or suggestive pictures of young people just for their own collection, even if they don't actually try to pursue them in person. It does happen.
- There have been cases where Online Predators have sold private information on potential victims to other, more local Online Predators, so that they could target the victims in person.

Finding vulnerable people:

- Online Predators often prefer to find vulnerable people—they can try to build a trusting relationship with them and then try to abuse them. Vulnerable people may be feeling down or isolated, may not feel they have trusted adults in real life that they can turn to, or may just go online to find a listening ear and vent their troubles to online friends. Either way, it can give Online Predators a way in.

Using personal information to threaten or gain contact:

- Online Predators sometimes try to threaten potential victims by trying to make them think that they know who they are, where they are live and that they can hurt them if they want to. Others use location information to send their victims gifts as they develop a trusting relationship with them.

Using personal information to build a relationship with a victim:

- Some victims become online friends with Online Predators knowing who they are and how old they are. Think of the Laura Stainforth case. This is a greater danger on the internet because it's harder to tell where the boundaries are, and close friendships between young people and adults which would immediately set alarm bells ringing in "real life" can seem much more normal on the internet. Personal information can help Online Predators identify a potential victim and build up a relationship with a potential victim as they seek to befriend them.

Committing identity theft:

- Identity thieves can use information that people make publicly available online combined with information from other databases to steal a victim's identity.