Staying Safe on the Internet

Lesson 2: Internet Fraud

Teacher's Hints for Group Discussions

Sean's Story - Activities

Question 1:

"Think about things from Sean's point of view. Explore what mistakes Sean made and how he allowed himself to get into this situation."

Here are some hints for the group discussion:

- He let down his guard on the internet. Remember, it's much harder to tell who's genuine and who's false on the internet, because there's much less information to go on.
- He saw an email that said it came from the bank and had the bank's logo on it—is that proof that it came from the bank? Think of other ways he could have checked whether it was genuine or not: phone the bank; check its website; go into a branch?
- He allowed himself to be misled by the fraudster's fake website, because it looked like the bank's own website. It's easy to copy a website if you know how. Again, just because it looks real doesn't mean that it is!
- The email made him panic and think that he had to act immediately. These emails often do that, to get people to click on a link in the email without first determining whether the email is genuine or not.

Other tactics they try are:

- Sending potential victims emails that look like they've come from an online payment service, e.g. PayPal™, which make it appear that there has been an unauthorised payment made using their money.
- Sending potential victims emails which make it look as if there has been a problem with their seller account on an e-commerce website, e.g. on Amazon™ or eBay™.
- The victims feel that they must investigate immediately by clicking on the link in the email, which then takes them to a fake website set up by the fraudsters.
- Sending potential victims emails that look like they've come from a parcel delivery service, and making it seem as if the victim had a parcel delivered to them while they were out. The fraudsters want the victim to think they've got to pay for redelivery using their credit card, so that the victims click on a link in the email. This takes them to the fraudster's fake website which tricks them into entering their credit card security details.

Sean's Story - Activities

Question 2:

"Think about things from the Bank Manager's point of view. What guidance would you give to people like Sean so that they do not end up in this situation? How would you advise them to sort it out if they did end up in Sean's position?"

Here are some hints for the group discussion:

- Just because a link has the bank's website on it and it is underlined and in blue doesn't mean that it'll take you there when you click on it. That's how hyperlinks work—the link says one thing in its text and points somewhere else.
- Sometimes, fraudsters try and make the actual linked website address seem OK. They will put the name of the bank somewhere in a very long website address, but it will still point to the fraudster's website in the end.
- The email says it's come from "internetsecurity@hyperbank.com". It looks as if it comes from the right place!
- But it's quite easy to make an email appear to come from any email address at all, if you know how. Many responsible email providers now prevent people sending email that looks as though it has come from someone else, but there are still plenty that don't.
- Just because an email gets through to your email address doesn't mean that it's genuine. Online Fraudsters have many different ways of getting hold of email addresses.
- If you do get an email like this, don't ever click in on the link - the fraudster's website may try to infect your computer with a virus or a trojan.
- The bank always knows who its customers are. If they wanted to get in touch with its customers, they would send them a letter or contact them by phone. Banks always stress that they will never, ever send out an email asking customers to click on a link or enter their security details.
- If someone does get into that situation, they should contact their bank immediately. The bank will have to investigate and give the victim new security details and passwords.

Sean's Story - Activities

Question 3:

"Imagine you were an online fraudster. Explore how you would identify people like Sean and how you would obtain information from them by various means and methods."

Here are some hints for the group discussion:

Fraudsters need to get hold of people's email addresses:

- They can buy lists of email addresses from people who do spam email.
- There are programs that search the internet looking for email addresses.
- There are computer programs that try every possible combination of personal names and random numbers to see which ones work. Sean's username - Sean0880 - is quite easy to guess by this method.

The fraudster can trick the victim into believing that the email is genuine, by:

- Copying logos from the company they're trying to imitate.
- Changing the email address that the email appears to come from, so it looks like it has come from a bank—most people don't know that it's so easy to change.

The fraudster has to stay out of the way of law enforcement.

- For this reason, these phishing emails are usually sent out from countries where it's difficult to track down people.
- The websites are in countries where it's hard to get them shut down.

The fraudsters rely on getting the victim to panic or rush and click on the link in the email without thinking about whether it's genuine or not. They can do this by:

- Making it seem innocent—many of the early phishing emails said that their bank had updated their computer systems and needed people to log back in.
- Making the victim panic—for instance, by making them think that they've been robbed, or making them think that they will lose access to their money if they don't act immediately.
- Making them think that they will lose something valuable, for instance, making them think they've missed a parcel delivery, and that they will lose the parcel if they don't click on the link in the email.
- Making them think that they will miss out on a superb deal which is in fact too good to be true, for instance, promising computer software or consumer electronics at unbelievably low prices.