Unit 2 Evidence C

E-consumer awareness

Online identity theft has long been an epidemic, but slowly and steadily it is on the decrease

An official definition of online identity theft is the practice of pretending to be someone else on the internet. The purpose can be quite harmless (like chatting with someone under someone else's account), but when referred to in the media, it's often about the criminal activity of stealing someone's personal information for his or her own financial gain. More often than not, it involves phishing (online fraud) for a person's banking information and using that to order goods or transfer money to another bank account.

A very recent study by the better business bureau shows that only 11.6% of identity fraud happens online. This is because of the high security and encryption offered by top transactional websites, this makes it virtually impossible for an identity theft to steal personal information.

Most identity fraud happens offline, e.g. stolen wallet, or even friends or family who have access to personal information.

The following is a recent real life story of a victim of identity theft:

"On June 11th, I received a call at my home from a collection agency in Missouri. They stated that they were calling on behalf of (a phone company) and wanted to collect an outstanding bill due for services rendered. Upon questioning the caller, I soon realized I had been a victim of identity theft. I never lived at the address in question, nor had I ever known anyone who lived at the address. The next day, I contacted the New York State Troopers and Albany, New York, Police Department in an effort to file criminal charges. After filing formal charges, I was advised to contact (the phone company) in an effort to begin clearing my name of this outstanding balance. I left 5 messages with the Fraud Dept, all of which went unanswered. My husband then contacted the President's Hotline for (the phone company), a number provided by a customer service representative. We were then contacted by an 'Escalations Manager' from (the company). We were advised by this person that identity theft is becoming common. When we asked what the process was for establishing a phone line, we were told that a person could establish a phone line using someone else's social security number." (This story posted online on 06/06/05)

This is a report of a person who has been a victim of identity fraud, this person is from the USA where identity theft is at its highest.

A similar case happened, where a person was issued e-mails and letters saying that they have multiple late payments, whereas this person didn't even apply for a credit card from this company.

Companies/organizations responsible for maintaining data protection.

The Information Commissioners Office regulate and enforce the data protection act and the freedom of information act, they are the UK's independent public body, and if there is a problem then the victim can

download a form from the website and fill it in and send it to them via post, or the victim can telephone them, but the best way to contact them is probably by email.
Another organization responsible for the data protection act and the freedom of information act is superhighway safety, they clearly give out the rules and regulations and how to contact them if the rule is breached.

What is meant by the term "Phishing?"
The most precise term for phishing is the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do. For example: sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing comes from the analogy that internet scammers are using email bait to fish for passwords and financial data from the sea of internet users. Since hackers have a tendency of replacing "f" with "ph", the term phishing was derived. The term has evolved over the years to include not only obtaining user account details but access to all personal and financial data.
The following is a preview of a newspaper article from the guardian about "phishing" and how it haunts all bank customers. This newspaper article was published on 04/02/06

"Identity fraud is costing Britain £1.7bn a year, Home Office ministers revealed this week, underlining the case for ID cards. But are the banks doing enough to protect us? Critics accuse high street banks of skimping on security despite record profits, expected to exceed £30bn this year. One study claims that sloppy call centre security at the banks leaves current (...) "

To see the whole of this article visit this link,
http://money.guardian.co.uk/scamsandfraud/story/0,,1701731,00.html

Clearly "phishing" is a big problem that major banks and even transactional websites should fix, even though profits and popularity of online banking is soaring, unfortunately with this identity crime is also soaring, which is a major issue, which the banks must overcome to gain full trust from the users and customers.

What is the 'sale of goods act'? What do the advertising standard authorities do and finally what are 'distance selling regulations?'

Under the ‘sale of goods act’ the traders must sell goods that are as described and of satisfactory quality.