**Chris Fullerton Case Project 1-1**

I once had a friend get a new laptop for Christmas a few years ago, the friend then thought they could download a mobile game to the laptop. They were phished into thinking that they could do this by downloading on a fictitious site. They thought the website was legit and downloaded a virus on a brand new computer. The damage luckily was too severe due to the laptop being new. They luckily didn't damage the components but the virus was trying to steal data and made the laptop run incredibly slow. The virus was eating up all the ram and slugging the computer. Being a new computer it did not have any sensitive information except emails and log information. They didn't have anything tied to a bank account or other accounts logged in. They were lucky it was one of the first things they did. To fix the issue my friend contacted me and I was able to visit to assess the situation. I took a look at the computer and immediately realized it had a virus without running a detector. They didn't have the antivirus set up to check for viruses yet either. I tried to then run an anti virus program and that didn't take care of the virus. Next I decided to try and go into the files and see if I could find the corrupted file. I did manage to delete the virus but I still didn't feel safe about the situation. The last step I did was ask the friend if I could just reformat the computer and make it brand new again. I explained since it was new there wasn't anything to lose. They agreed and I reformatted the computer. After the format the computer was factory reset and the friend was back to square one. I then had to go into detail about what to look for in these fictitious sites and how mobile games won't be on a computer. The reason the attack was successful was mostly due to my friend not being educated to understand what phishing is and how it works. Also the antivirus has not been installed yet.