COSC 3050, Spring 2016
Security

Case 1:

You work for a Los Angeles area defense contractor on a secret project for the government and therefore have been investigated for and granted a Secret security clearance. At the end of each workday you lock all documents, files, and drawings in a safe in your office, according to the job requirements. One day, when you are almost home, you realize you may not have locked your safe. Returning to the office requires a 45-minute or more drive, each way through traffic. The rules of a Secret clearance require you to personally lock your own safe.

What should you do? You are thinking of calling one of your co-workers who is still working to have him check the safe for you.

COSC 3050, Spring 2016
Security

Case 2:

Lori Drew was a mother who was convicted of three misdemeanor counts of "accessing computers without authorization". She, with help from her 18-year-old temporary employee, created a fake MySpace account as a 16-year-old boy, "Josh Evans". They then used the account to gain the confidence of a former girl friend of her daughter. Testimony claims the reason for this was to find out what the girl, Megan Meier, 13, was saying about the daughter and others. Megan had a history of psychological problems, of which Lori Drew was aware. The upshot of the case was that "Josh" ended up dumping Megan. The last communication from him was on the order of "The world would be a better place without you." Megan promptly hanged herself in her bedroom.

If you managed MySpace or another social networking site, what kind of security would you (could you) put into place to ensure that this type of thing could not happen?

COSC 3050, Spring 2016
Security

Case 3:

You have just finished taking Jim Ward's course on Mobile Applications. You get this great idea about a new app. You spend the summer writing it and when it is perfected, you market it. Strangely enough, people buy it. You are not getting rich but you are making a few dollars a month, there have been about 10,000 downloads. Then one of your friends discovers that you have left a "back door" into the app so that if someone is using it, you can actually connect to their phone. You did this because you had some development problems early on and the app sometimes seemed to lock you out of the phone. Your friend thinks this is cool and **promises** not to tell anyone else.

What should you do now?

COSC 3050, Spring 2016
Security

Case 4:

You have finally gotten that old sheepskin. Now you can go out and make the big bucks. You have taken a job with a medium-sized company as a system administrator in their IT department. Your jobs include monitoring disk quotas, print quotas, email logs, and doing backups of user areas and the mail server. You work alone in the evenings part of the time and one evening you happened to notice a pattern in one of the administrative intern's emails. She was communicating, a lot, with one of the mid-level software engineers. Your curiosity was piqued and you did a little snooping. You find out that the emails are encrypted. You check around her home area and, sure enough, find her private key and her passphrase (my you ARE a snoop!). You decrypt a couple of the email messages she exchanged with the engineer. They seem to be having some kind of personal relationship.

This is not something you were supposed to even check into, but now you know. You know the intern personally, she is in the same university program you graduated from, just one year behind. Do you suggest, politely, to her that she gets her passphrase out of her home area? Make some remark that indicates that you know she is having this relationship and you think she should cool it? And what about **your** security violations, what will you do in the future?

COSC 3050, Spring 2016
Security

Case 5:

You have signed up for online training for *cold fusion* Web development software. Twenty minutes before the training, you attempt, as scheduled, to log onto the *cold fusion* Web site. You learn you cannot access their server because of your company's firewall. To request a change from your IT department will take about a day and a half. The *cold fusion* training will not be held again for six weeks, and you need it now to do a new project you have been assigned. Scotty, your co-worker, says not to worry, he can set up your computer to bypass the company firewall, but he asks that you not let IT know.

What should you do?

COSC 3050, Spring 2016
Security

Case 6:

You often telecommute in your job as a systems engineer. It is not unreasonable for you to remotely connect to the routers and switches, especially since they are not all in the same building, or even the same urban area. In the process of doing this, you need a large list of passwords because, of course, the passwords are different for each machine. You keep this all in a PDA, not your phone, because the PDA is more secure than a phone and is set to require a password for access.

Then one day at work, you find that there some files on your desktop that you did not put there, even though they are owned by you. You investigate and finally decide that your 10 year-old has somehow accessed your machine and is using it to play an MMORPG that you have forbidden her to play at home.

What do you do now? How did she gain access to your work machine, you are always so careful?