Cyber Security Tutorial 1

Instructions

In this tutorial you should work preferably in pairs or alone. Try to answer all the questions together and discuss the possible answers/solutions. You will be given 30 minutes to complete this task and, in the end, a general discussion will take place in class based on the content of this tutorial. Try to answer as many questions as you can!

Your answers might be slightly different in some questions are your perspective differs too. There are more discussion based questions than right/wrong in this tutorial.

Question 1

What is the difference when a website has an https:// instead of an http:// in a URL?

Sample answer: http is the protocol used for transferring data between a browser and the website that is connected to. The addition of "s" is the protocol's secure version which means that any exchange of data between the browser and the targeted website is encrypted.

Question 2

Discuss and come up with at least four criteria (either to do or not to do practices) that someone must follow when choosing a password.

Sample answer: To do or do not practices; 1) use of a combination of letters, numbers and symbols; 2) never use the same password for different services; 3) never use the same password for a long period of time; 4) never use words inside your password, birthdays and other information that is personal and can be obtained by outsiders.

Question 3

The human factor is claimed to be one of the most common factors responsible for an occurred cyber-attack to an organisation. Is this true? Explain why and how the human factor can play a role in a cyber-attack.

Sample answer: Human factor is one of the key aspects in every working environment. The knowledge of computing and especially cyber security is not common to be on a high level for all employees in a company. Therefore increasing cyber awareness through different types of training is necessary nowadays. Some of the things that can lead to a cyber-attack; leaving your work password on a post it note that anyone can access with a bit of effort is a bad practice that can still be encountered today; taking your work laptop home or leaving your work laptop with not any security mechanisms employed, while containing confidential work files; leaving important files unprotected or sharing them on possibly vulnerable cloud services; avoid the installation of any security updates of the manufacturer or installation of antivirus; not maintaining your security mechanisms in place; opening all emails and their content.

Question 4

Discuss the term Cyberwarfare and explain its importance by giving some well-known examples.

Sample answer: Cyberwarfare is the new type of battlefield. It describes any type of cyber attack against a nation state with political, military or other purposes. It is normally relevant to espionage and sabotage. Also, it describes both defensive and offensive activities. One well known example is

Stuxnet where the target was the Iranian nuclear facility, and no one has officially claimed their involvement, although there is a strong belief that other nations were involved in the role of the attacker.

Question 5

Pick a recent occurred cyber-attack and discuss this within your group, regarding the type, impact, and techniques used by the attackers. How this attack could be avoided?

Sample answer: The most important thing that you will notice is that when a cyber-attack is reported an investigation must originally take place. For this reason, the purpose of attack might not be obvious from the beginning alongside with the techniques used. This makes also the prevent mechanisms harder to be identified. Company X cyber-attack: Around 230000 clients' credit card details, billing information was stolen from the company. The type is not clear, but it is obvious that the attackers were passively gathering information as they remained undetected for more than 3 weeks. It is obvious that the company should have used encryption in their transaction system and had employed more secure ways of storing their customer data. For example, this valuable information should have been stored in a separate server and only accessed by authorized personnel which was necessary to do so.

Question 6

Kate is going to a café between classes, so she can work on her thesis; she has chosen the TEXT coffee shop as it has free WIFI connection. Is it safe for Kate to use the TEXT's WIFI? Can you suggest any techniques to Kate, in order to keep her online activities' secure?

Some ideas: Do not keep essential data on the laptop using with untrusted networks. Have antivirus employed and updated. Use of VPN, encryption. Do not log in to any accounts while on free Wi-Fi. If the free Wi-Fi asks you to register with an email and more details, does not mean that this connection is more secure because an authentication mechanism exists

Question 7

The board of Phoenix Corp is debating whether they should employ the use of Cloud Services for their data; What do you think can be the downfall and on the other hand the positive impact of this decision (on a cyber security aspect)?

Some ideas: Data stored on other countries? Be careful when choosing vendors. Same space shared with other companies. Do you know who is sharing the space with your company? Loss of data and leakage; unable to access data. Store only necessary data that will not cause data breach. Accessibility, outsourcing storage → decrement of necessary budget as the service is outsourced and most of the times it is cheaper than having your own infrastructure. One good solution is to build you own cloud service which gives more control but at the same time is more expensive. If the outsourcing solution is preferred, then attention to the contract is important so all the previously mentioned points will be taken into serious consideration and any necessary legalities will be put into place.