

COMP1205 Presentation Programme 2013-14

Monday 12th May Building 34 Room 3001, 12.00-13.45

Su & Rikki

Presenting: Groups: E, F, G, H

Marking Groups: I, J, K, L

Schedule and Topics

12.00-12.05: Introduction and protocol for the session

12.05-12.25 Group E: Creative commons, open source, open movements

12.25-12.45 Group F: Trolling, Banter, Cyber Hate, Online Bullying

12.45-13.05 Group G: Personal Privacy and Security

13.05-13.25 Group H: Crime online; cyber security

13.25-13.45: Wash-up: feedback session for presentation groups

Abstracts

12.05 Group E: Creative commons, open source, open movements

Abstract

Intellectual property is work that you have created that is unique and you have legal rights to those works. Copyright licenses can be used to restrict modification and distribution of such works, it is given to the author upon publication of the work but can be sold or licensed. Owning a copyright gives you the exclusive rights to the work which means it is illegal for anyone without it to copy, lend/rent, display/perform, or adapt the work in any way. In software, sale of software is a form of licensing the copyright as it gives the user the right to store the program on a personal machine (considered a form of copying).

Creative Commons is an organisation which provides multiple types of licenses to people who want to share work with limited restrictions on its use, these are much less strict than copyright and are highly flexible, and can be combined to suit the work and desires of the author. For software, there is the

Open Source Initiative which is another organisation dedicated to reviewing and approving licenses that follow an Open Source Definition. It has a set of criteria that must be met in order to apply an open source license.

12.25 Group F: Trolling, Banter, Cyber Hate, Online Bullying

Abstract

Our team goal was to create a presentation which showed the audience the causes of Trolling, Banter, Cyber Hate, Online Bullying and ways to encounter situations.

We gathered research throughout the Easter vacation and came back with plenty of research to implement into the presentation. Each person had a role and some were partnered for more difficult subjects

There were several meetings that included working on the presentation and gathering ideas that would help us explain the subject more clearly.

We assigned each other different parts of the presentation to give out equal amounts of workload.

Throughout the presentation showed various key points of the sub topic points and give a general explanation of each topic. It was also necessary to show the audience ways to address the situation and factual information that would stop them from performing such actions.

12.45 Group G: Personal Privacy and Security

Abstract

This presentation discusses the ever growing use of the Internet to fulfil everyday needs and the increasing threat that has arisen by supplying online services with detailed information about people lives. More specifically the presentation talks about digital tattoos, UK legislation and also users who inadvertently compromise their integrity by accepting conditions with blind faith.

When conducting resource for this topic, we discovered that organisations are conducting detailed analysis of users to produce a “digital Tattoo” or online profile in order to better target them. UK legislation, such as the Data Protection Act, tries to protect users, however it has not been able to keep up with the rapidly changing technology industry and is now not enough for today's society. However, more interestingly user's adoption and increasing use of services placed online has fuelled this extensive collection of data. This is partly due to users not understanding how their information is being used by organisations.

The aim of the presentation is to link these sections together so that users are more informed of why their personal privacy and security online is important and how time for reversing these effects is running out.

13.05 Group H: Crime online; cyber security

Abstract

With the great number of transactions that take place over the internet, it is important to understand the legislation that is in place that protects a business or an individual, as well as the possible repercussions that can be taken in response to the failure to comply with such rules. To address this, this presentation concerns itself with legislation regarding several key areas in cyber security: fraud and theft, cyber terrorism, computer misuse and sexual offences. A real life example of cybercrime, namely the anonymous marketplace Silk Road, is then explored. We finish by analysing the financial costs that cybercrime has cost the government in financing cyber security that tries to uphold against attacks, as well as the encounters with cyber crime that members of the public encounter.