Social and Legal Issues in Informatics

MSc Management – IS and Services Science

Computer Misuse

Giovanna Di Marzo Serugendo
Giovanna.Dimarzo@unige.ch, room B 235, 022 379 00 72
(Some slides from Roger Johnson, Birkbeck College)

Origins of the Problem

Prior to online systems, very few problems

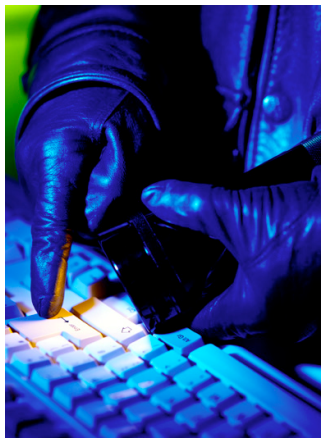
With remote access, unauthorised access to a computer started to become possible

With growing public access to computers via networks, problems started to increase

Computer Misuse Act 1990

The Act created three new offences:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material.



Unauthorised access to computer material

- Lowest level of offence
- Accessing materials without authorisation is illegal
- Offence committed even if no damage is done, and no files deleted or changed

- Offence carries a penalty of imprisonment up to six months and/or a fine

Unauthorised access with intent to commit or facilitate commission of further offences

- Builds on previous offence
- “Intent” means it has to be done deliberately, rather than by mistake
- Includes guessing or stealing a password, and using that to access, say another person’s on-line bank account and transferring their money to another account
- Penalty is up to five years’ imprisonment and/or a fine

Unauthorised modification of computer material

- Most serious offence
- Include deleting files, changing the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data
- Includes using a centre's computer to damage other computers outside the centre, even though the computer used to do this is itself not modified in any way
- Penalty of up to five years and/or a fine.

Challenges

Scenario One

A student on holiday from college comes into the centre, starts playing around with the desktop settings, and installs some unauthorised software which she has downloaded from the Internet. Before leaving after that session, she changes everything back and removes the software.

What do you do?

Answer

Before the student first used the machines, she should have been given the Acceptable Use Policy, and this should have been discussed with her. The fact that she has changed everything back to the way it was is irrelevant – an offence has been committed.

More practically, downloading software from the Internet is a risky thing to do, and could easily have introduced a virus to the centre's computers. A computer centre would consider the appropriate action here – this will probably be either a warning or temporary suspension.

Challenges

Scenario Two

Someone has been using a computer for e-commerce, to order some books. Rather carelessly, they had written down their credit card details on a piece of paper, and left it in the computer centre. Someone else finds it, and uses these details to make some orders of their own, changing only the delivery address.

What do you do?

Answer

This is quite clearly illegal, and falls under the second category of offences. It is no different from breaking into someone's house and stealing their property.

There is a clear argument for reporting this to the police.

Problems with CMA

Basically it was written for a pre-Internet world

Problem areas include:

- Phishing
- Denial of Service attacks
- Advance-Fee Fraud (e.g. Nigerian letter)
- Cookies
- Trojans

Strengthening the CMA

- Proposed increased punishment for breaching the act
- Proposed new offence “to obtain, distribute or write software that could be used by a hacker”
- What about penetration testing, sometimes called ethical hacking?
- How can you look for security weaknesses?

EU Convention on Cyber Crime

- Illegal Access
- Illegal Interception
- Data Interference
- System Interference
- Misuse of Devices
- Computer-related forgery
- Computer-related fraud
- Offences related to child pornography
- Infringement of copyright
- Signed 2001, entered into force 2004
- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

EU directive on

Other problems are:

- Virus writing
- Distributing malicious code
- Spamming – Spamhaus (http://www.spamhaus.org/)
  - Privacy and Electronic Regulations 2003 (EC Directive)
  - http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Cyber Crime and Intellectual Property section of the Criminal Division (US Dept of Justice)

- http://www.cybercrime.gov/