Course: Professional Issues in Information Technology

Week 13: Major Internet Security Issues

Lecturer: Martha Gichuki

Learning outcomes Lecture 13: Major Internet Security Issues

At the end of this lecture, the learner should be able to:

1. Describe the security issues around the Internet subject
2. Describe the various security technologies available
3. Describe various cyber attacks
4. Describe the public safety and welfare issues especially child protection

Course description

- The course begins with an introduction to terminologies like profession, data and Information Technology. This will be followed by a coverage of the data processing cycle, an introduction to Law, Ethics and the Concept of privacy. Cyber crimes will then be covered to see what the law says in relation to cyber crimes.
- A detailed coverage of Intellectual property rights will then follow with the learners being exposed to various property rights and the glaring issue of plagiarism.
- The four dimensions of ethical dilemmas will then follow to enable learners apply wisdom in matters related to ethical decision making.
- An evaluation of the effect of Information Technology in employment will culminate the course where learners will cover issues related to health and safety at work, Netiquette, Software contracts, major internet security issues and Computer misuse.

- **Some Internet Security Terminologies**
- **Authorization** -the process that ensures that a person has the right to access certain resources
- **Authentication**- the process by which one entity verifies that another entity is who they claim to be by checking credentials of some sort. E.g. Who sent this email?
- **Auditing**- the process of collecting information about attempts to access particular resources, use particular privileges, or perform other security actions

Some Internet Security Terminologies …

- **Privacy** - This is the right to be left alone and the right to be free of unreasonable personal intrusions. The idea is to keep information private[1]
- **Confidentiality - is a more formal and social concept** that deals with a set of rules that govern the use of **information held by institutions** about individuals and the conditions under which that information can be shared.

1 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 153

Some Internet Security Terminologies …

- **Integrity**- As applied to data, it is the ability to protect data from being altered or destroyed in an unauthorized or accidental manner. Data remains unchanged
- **Nonrepudiation**- The ability to limit parties from refuting that a legitimate transaction took place, usually by means of a signature

Perpetrators

- People who launch computer attacks and they have different objectives. Perpetrators include:
  - **Thrill seekers** wanting a challenge,
  - **Common criminals** looking for financial gain,
  - **Industrial spies** trying to gain a competitive advantage, and
  - **Terrorists** seeking to cause destruction to further their cause[2].
- Each perpetrator aims at accessing a particular resource, and can accept different levels of risk to accomplish his or her objective.
- Perpetrators make a decision to act in an unethical manner to achieve personal objectives.
- Knowing the profile of each set of likely attackers is the first step toward establishing effective countermeasures.

2 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 95

Types of Perpetrators[3]

Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

3 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 90, 95

Cyber Crime

This refers to computer generated offences.

Examples of cyber-crime include:

1. **Fraud**

Fraud refers to intentional deceit or trickery, often with the aim of financial gain.

2. **Cyber attacks**

These are electronic attacks, either criminal trespass over the Internet (cyber intrusion) or unauthorized access that results in damaged files, programs, or hardware (cyber vandalism). The individuals behind these attacks include hackers and crackers[4].

4 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 95

Hackers

- Hackers seek to exploit software and computer systems' weaknesses for personal gain
- Original hackers created the UNIX operating system and helped build the Internet, Usenet, and World Wide Web;
- Hackers use their skills to test the strength and integrity of computer systems.
- Over time, the term hacker refers to rogue programmers who illegally break into computers and networks.

Crackers

These are people who engage in unlawful or damaging hacking. They are also known as criminal hackers.

Other attackers

These include “script kiddies” who are ego-driven, unskilled crackers who use information and software (scripts) that they download from the Internet to inflict damage on targeted sites.

Types of Cyber Attacks

A. Technical attack

An attack perpetrated using software and systems knowledge or expertise e.g. Denial of Service attack (DoS)

B. Nontechnical attack

An attack in which a perpetrator uses persuasion to trick people into revealing sensitive information or performing actions that compromise the security of a network e.g. phishing

Common Vulnerabilities and Exposures

- These are publicly known computer security risks or problems.
- They include, DoS, Viruses, worms, keyloggers, phishing, malware, ransomware, trojan horses among others

✓Denial-of-Service (DoS) attack

- This is an attack on a Web site in which an attacker uses specialized software to **flood** target computers with data packets with the aim of **overloading the network resources.**

✓Distributed denial of service (DDoS) attack

- A DoS attack in which the attacker gains illegal administrative access to as many computers on the Internet as possible
- The attacker then uses these multiple computers to flood target computers with data packets[5].

5 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg.91

- ✓**Computer Viruses –** These are software codes that inserts themselves into a host, including the operating systems to circulate. They cannot run independently but require the host program to run for them to be activated[6]
- ✓**Ransomware** - software that locks computers via encryption and then offers the victim a decryption key at a fee
- ✓**Keyloggers**- They monitor user activity e.g. keys typed on the keyboard, mouse clicks, invoked menus, taking screen shots etc. Solution: Use anti-spyware for prevention, for detection use firewalls and for protection use automatic form fillers.

6 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 111

- ✓**Spam hoaxes** – Spam is the abuse of email systems to send unsolicited email to many people. Spam forces unwanted material into inboxes and this may make relevant emails to be hidden among unsolicited emails[7].
- ✓**Phishing** – creating fake profiles to steal information (identity theft). In a phishing scam, con artists send legitimate looking emails urging recipients to take action to avoid a negative consequence or to receive a reward. The action could be clicking a link to a web site or opening an email attachment. These emails lead consumers to counterfeit web sites designed to trick them into divulging personal data[8]

7 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 170
8 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 111

✓Worms

- These are software programs that run independently, consuming the resources of its host from within in order to maintain itself.
- A worm propagates a complete working version of itself onto another machine without user interventions.
- Worms reside in the active memory of the computer and duplicate themselves.

Negative effects of worms to an organization

i. Data and programs loss

ii. Low productivity - workers are unable to use their computers,

iii. Time wastage - workers attempting to recover data and programs,

iv. More effort for IT workers-cleaning up and restoring systems[9]

9 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 111

✓Trojan horse

- A program that appears to have a useful function (masquerades) but that contains a hidden function that presents a security risk
- They are designed to enable hackers destroy hard drives, corrupt files, control computer remotely or spy on users by recording keystrokes and transmitting them to a server operated by a third party[10]

✓ **Malware –** A generic term for **mal**icious soft**ware** which, users are normally prodded to download.

10 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 89

Security Risk Management Process

- ✓ A risk is a potential loss/danger occurrence to a firm
- ✓ **Risk assessment** involves checking security-related risks to the resources in an organization e.g. computers and networks both from internal and external threats. This helps identify areas where time and resources need to be invested to protect the organization from likely and serious threats.
- ✓ **Risk management** is a systematic process used to determine the likelihood of various security attacks occurring and to identify the actions needed to prevent or mitigate those attacks. More or less like ***Disaster Management planning***[11]

11 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 102

- **Types of risks**
  - Exposure and participation to fraudulent/scam activities
  - Privacy violations e.g. selling confidential data
  - Abuse of acceptable user policies – users posting sensitive information
  - Use of weak passwords and saving passwords on browsers and emails
  - Using unsecured untrusted devices to go online and using open WIFI hotspots
  - Not logging out of inactive online sessions and not closing inactive social media accounts
  - Inability to update devices with firmware patches and antivirus[12]

12 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 90, 93

Online Banking Threats and Risk Factors

a) Vulnerable Mobile Banking applications – e.g. use of weak authentication methods and password policies

b) Aggressive Banking Malware – Common trojans are used to steal login credentials for online accounts e.g. TrickBot, Dyre and Lurk. They use browser manipulation techniques to steal credentials and also install malware n user computers[13]

c) Identity Theft – criminals use phishing techniques to steal user information

13 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 173

Online Purchasing Risks

a) Fake E-Commerce sites – leading to identity theft. ***Solution:*** stick with trusted brands with a strong reputation

b) Credit card Fraud – Intercept online stores at payment portal. ***Solution:*** Stay alert and vigilant. Do not send credit card details via email or social media platforms

c) Adware – Illegitimate advertisements

d) Scam /Fraud – by sellers who never deliver

e) Sending sensitive information over un-encrypted sites. ***Solution:*** access sites over secure and encrypted connections (HTTPS)

f) Fake applications – steals personal information for sale or in ransomware attacks. ***Solution:*** Be wary of fake applications, do not download them[14]

14 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 173

Security Technologies

Internet and E-Commerce security is a thriving business and several companies have come up with technologies to enhance internet security such as:

1. **Firewalls**

- These are network nodes that create a protection barrier between the Internet (public networks) and local computers (private networks)
- They alert on unauthorized access and break in attempts and should permanently be turned on
- Firewalls are either hardware based (installed at the edge of a corporate network) or personal (software firewalls) installed on every computer connected to the Internet e.g. Windows firewall[15].

15 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 63, 106

2. Intrusion Detection Systems (IDS)

This is a special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees[16]

3. Anti-virus and Anti spyware
4. Secure, complex strong passwords
5. Regular back-ups
6. Regular updates and patches
7. Disabling guest accounts and permissions
8. Implementing physical security

NB: No single method is safe, it is good to apply several defense layers

16 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 63, 106

Educating Employees and contract workers

- This involves creating and enhancing user awareness of security policies
- Users must help protect an organization's information systems and data by doing the following:

i. Guarding their passwords to protect against unauthorized access to their accounts

ii. Prohibiting others from using their passwords

iii. Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction

iv. Reporting all unusual activity to the organization's IT security group

v. Taking care to ensure that portable computing and data storage devices are protected from theft[17]

17 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 105

Public Safety and Welfare

- Electronic media of all kinds have historically been regulated by governments
- Critical issues in E-commerce center around the protection of children.
- There are strong sentiments against pornography in public media, efforts to control gambling, and the protection of public health through restricting sales of drugs and cigarettes

Protecting Children

- ***Web filters*** - These prevent inappropriate content over the Internet through home computers and phones. They mostly restrict access to pornographic content and they enable you to set rules against certain search engines, words and phrases
- In many countries, it is a criminal offence to use any telecommunications device to transmit "any comment, request, suggestion, proposal, image or other communications which is obscene, filthy, or indecent" to minors (persons under the age of 18 years)

Protecting Children …

- Sometimes these communications are meant for “commercial purposes” but in the end they are harmful to ***minors***
- Private pressure from organized groups has also been successful in forcing some Web sites to eliminate the display of pornographic materials

Equity and the Digital Divide

- The Digital Divide refers to the large differences in Internet access and e-commerce access among income, ethnic, and age groups.
- Lack of such access affects the ability of children to improve their learning with educational software, of adults to acquire valuable technology skills, and of families to benefit from online connections to important health and civic information

Content Covered in Week 13: Major Internet Security Issues

We have been able to cover the following:

1. Describing the security issues around the Internet subject
2. Described the various security technologies available
3. Described various cyber attacks
4. Described the public safety and welfare issues especially child protection

Course Text Books

1. Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005)
2. Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011)
3. Computers in Society: Privacy, Ethics and the Internet. George, J.F. *Pearson Prentice Hall, New Jersey.* (2004)
4. Cyber-ethics: Morality and Law in Cyberspace, 5th ed., Spinello, R.A. *Jones & Bartlett, Burlington, Mass., USA.* (2013)
5. Contemporary Issues in Ethics and Information Technology. *Schultz, R.A. IRM Press, USA*. (2005)