Course unit: SCS 3101 - Introduction to Computer Systems

Module name/Topic: Ethics in computer networks

Contributors: Reagan Onditi, Elisha Abade, Paul Rabala, Charles Katua, Selina Ochukut

Duration: 1 hr

Reviewed by: Reagan Onditi

Module Description

Welcome to this lesson in which you will learn more about ethical issues with regards to computer communication network systems consisting of hardware, software, and humanware. The hardware and software allow the humanware,the users,to create, exchange, and use information. The hardware consists of a collection of nodes that include the end systems, commonly called hosts, and intermediate switching elements that include hubs, bridges, routers and gateways. We will collectively call all of these network or computing elements, or sometimes without loss of generality, just network elements. The software, all application programs and network protocols, synchronize and coordinate the sharing and exchange of data among the network elements and the sharing of expensive resources in the network.

Module learning outcomes:

By the end of the module the learner should be able to:

1) Define the nexus between ethics and computer networks
2) Explain why is Ethics significant in use of computer networks

3) Describe ethical issues in computer networks
4) Apply responsible approaches to tackle ethical challenges faced by computer network professionals

Topic/Module content:

Introduction

Computer ethics address issues related to the misuse of computers and how they can be prevented. It primarily imposes the ethical use of computing resources. It includes methods to avoid violating the unauthorized distribution of digital content. The core issues surrounding computer ethics are based on the use of the network, network privacy and related services, and user interaction with websites. The inter networks (Internet) has changed our lifestyle. It has become a part of our life. It allows us to communicate with a person from another part of the world. collecting information on any topic, social meets, and many other activities. But at the same time, some people are always trying to cheat or harm others.

Ethics Significant to Network Security

In network attacks, the targeted data is usually very sensitive and personal. It can be potentially devastating for your institution if you lose that sensitive data and it is crucial that you have the full trust of the individuals you've hired to protect it. It is necessary that the employees working in the field of network security have a strong sense of ethics and respect for the privacy of your members as cyber security professionals have access to the sensitive personal data they were hired to protect.

A strong ethical core is necessary to navigate as the field of network security expands and shifts. It is very necessary that your employee can determine what is in the best interest of your customers and the company as a whole. Specific scenarios that your employees might confront can sometimes be impossible to foresee, so a strong ethical core can be the foundation that lets employees act in those best interests even in difficult, unpredictable circumstances.

Network Security Ethical Issues

Here ethical issues refer to the consequences, whether damages or benefits, that can come from the choices of cyber security professionals. For instance, it is easy to know how ethical issues in fields like engineering and aeronautics can have severe impacts on both individuals and companies. In the same way, ethical issues take place in network security too, and below are some of the key issues:

a) Harm to privacy

When it comes to network security, individuals and institutions have sensitive data that increases the chances of threats like identity thefts as hackers seek to steal and use these data for financial transactions or other forms of crime. As cyber security experts are the initial defense against attacks so they are trusted to guarantee privacy but poor cyber security practices increase the risks of a data breach. These practices can cause significant privacy harm.

b) Harm to property

Network attacks destruct organizations both digital and physical property. The network can be manipulated when professionals fail to carry out their responsibilities ethically and the exploitation of loopholes by profit-seeking criminal enterprises, politically motivated groups, and more. It is expected that professionals have to protect their organization's network at all times.

c) Network security interests

It is true that hacking has a negative reaction, but ethical hacking is now a thing today, even though there are many concerns about it. In the hacking community, it has always been the topic of debate about the need for teaching students hacking skills. Opponents say that it encourages illegal activities, while proponents say that it empowers students to identify and protect themselves from black hats. There is a possibility that these skills could be wrongly used in the absence of education and emphasis on cyber security ethics.

Common Ethical Challenges For Network Security Professionals

A wide range of challenges is faced by cyber security professionals on a daily basis. It is necessary to know these challenges and take a stand on them to ensure ethical and effective cyber security practice.

a) Ethical challenges in confidentiality

Confidentiality is a most important element in network security. It is the duty of the network security professionals to keep the data confidential and he will be exposed to both private and proprietary data. There might be pressure from time to time to know the sensitive information about a user or the company, but professionals must practice what is known as the 'butler's credo.' The butler never tells.

b) Ethical challenges in threats

It is the responsibility of the cyber security professionals to respond to threats and data breaches. How they respond to cyber threats matters. Many people can afford to leave their computer unattended to or ignore notifications, but for a cyber security expert, this should be done.

c) Ethical challenges in network monitoring and user privacy

With regards to network monitoring and user privacy, many network security professionals often find themselves in the dilemma of carrying out their responsibilities without making unjustifiable intrusions on users and their privacy. This seems to be quite difficult, but it helps professionals to inform users of the network of active monitoring and also to what extent it will be done.

Knowledge of Users and System Administrators

The limited knowledge computer users and system administrators have about computer network infrastructure and the working of its protocols does not help advance network ethics,In fact, it increases the dangers.

This lack of knowledge leads to other problems that further complicate ethics in the network. Among such factors are the following:

- Network administrators do not use effective encryption schemes and do not use or enforce a sound security policy.

- Less knowledgeable administrators and users quite often use blank or useless passwords, and they rarely care to change even the good ones.

- Users carelessly give away information to criminals without being aware of the security implications.

- Network administrators fail to use system security filters. According to security experts, network servers without filters "are the rule rather than the exception."

Case Studies: Have a case to apply facts

Assignments:

Discuss the risks of networking technology

Quizzes:

1) Leaking your Institutional data to the outside network without prior permission of senior authority is a crime.

a) True

b) False

Answer: a

Explanation: Without prior permission of the senior authority or any senior member, if you're leaking or taking our company's data outside (and which is confidential), then it's against the code of corporate ethics.

2) The legal risks of ethical hacking include lawsuits due to __________ of personal data.

a) stealing

b) disclosure

c) deleting

d) hacking

Answer: b

Explanation: The legal risks of ethical hacking contain lawsuits due to disclosure of personal data during the penetration testing phase. Such disclosure of confidential data may lead to a legal fight between the ethical hacker and the organization.

3) ___________ is the branch of network security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.

a) Social ethics

b) Ethics in cyber-security

c) Corporate ethics

d) Ethics in black hat hacking

Answer: d

Explanation: Ethics in cyber-security is the branch of network security that deals with morality and provides different theories and principles' regarding the view-points about what is right and what need not to be done.

4) Which of the following is not a proper aspect of user integration?

a) Employee's authentication

b) Physical authorization

c) Access control

d) Representing users in the database

Answer: b

Explanation: There are 3 main aspects that need to be kept in mind when putting together new employees or users into an application. These are: Representing users in the database, Access control, and Employee's authentication.

5) One who disclose information to public of a company, organization, firm, government and private agency and he/she is the member or employee of that organization; such individuals are termed as ___________

a) Sponsored hackers

b) Crackers

c) Hactivist

d) Whistleblowers

Answer: d

Explanation: Whistleblowers are those individuals who is a member or an employee of any specific organization and is responsible for disclosing private information of those organizations, firms, either government or private.

References

Kizza, J. M. (2003). *Social and Ethical Issues in the Information Age* (2nd ed.). Springer.