UTS

UNIVERSITY OF TECHNOLOGY SYDNEY

32557

ENABLING ENTERPRISE INFORMATION SYSTEMS

WEEK 4 SUBMISSION TEAM SUPER

Ethics Privacy and Information Security

by

Seoyoon Kim (25388442) [Group leader]
Jin Lee (25388733)
Ariel Manueke(25207919)
Nonthawat Praisompong (25233750)

March 15, 2024

Week 4 Submission Team Super

Team Member:
Seoyoon Kim (25388442) [Group Leader]
Jin Lee (25388733)
Ariel Manueke (25207919)
Nonthawat Praisompong (25233750)

Ethics Privacy and Information Security

32557 – Enabling Enterprise Information Systems
CB11.B3.101

Ethical Scenario Discussion

Question 1:

(A)

In our view, under the rights approach, monitoring internet browsing by supervisors is ethically contentious because it infringes on an individual's right to privacy. While employers may have legitimate interests in ensuring productive use of work time and protecting company assets, these interests must be balanced against employee's rights.

For example, if your company only monitors websites accessed using company equipment to ensure that employees do not visit harmful or inappropriate content that could threaten company security, and this is clearly communicated and agreed to by employees, the monitoring may be considered ethical under the rights approach. Furthermore, if the monitoring is explicitly stated in the employment contract, the employee was provided with information about the kind of monitoring, why it is necessary, and how the information collected will be used, and the employee agreed to work under these conditions, then it would be ethical. However, if a supervisor tracks an employee's personal email or social media activity without a policy or notice, it violates the employee's right to privacy and is clearly unethical because such monitoring violates an individual's rights without informed consent.

Therefore, from the perspective of rights approach, the ethics of monitoring internet browsing by managers should be based on the rights of employees, especially privacy and informed consent. The importance of respecting rights and ethical business practices, as emphasized in ”Business Ethics: A Stakeholder and Issues Management Approach,” requires a nuanced approach to managing stakeholder interests while respecting individual rights (Weiss, 2014). This monitoring must be respected and transparent, and employers must find the proper balance between legitimate business interests and protecting employees' fundamental rights.

Question B: Design requirements for an information system in an employment agency.
Utilitarianism emphasizes the maximization of overall happiness and satisfaction resulting from actions. The design of information systems should aim to exert a positive influence on as many individuals as possible, avoiding discrimination and offering equal opportunities to all candidates.

ACS Code of Professional Conduct Summary

ACS has three fundamental values in its professional ethics code: honesty, trustworthiness, and respect. These principles guide ICT professionals in creating a healthy work environment and maintaining the dignity and integrity of their profession.

YouTube Video Summary

Title: "How To Recognize and Avoid Phishing Scams — Explained - YouTube"
Length: 08:54
URL: https://www.youtube.com/watch?v=Yz0PnAkeRiI
This video explains phishing, a sophisticated cyberattack aimed at stealing user data through deceptive social engineering tactics. It emphasizes the importance of vigilance and awareness in guarding against these scams.

Discussion on Scams

According to the Australian Competition Consumer Commission, impersonation and product and service scams are prevalent, exploiting technology to deceive victims. Awareness and proper verification are key to protecting oneself from these scams.

1 Question 4

1.1 Protecting Yourself Against Website and Email Scams: Essential Tips

According to the Australian Competition & Consumer Commission (**?**), there are five principal scam types: social media, online messaging and app based scams; Website scams; Phone scams; Email scams and Text or SMS scams. From these scams I select website scams and emails scams due are the most recurrent kind of scams.

1.1.1 Website scams

- Verify correct website email: Make sure that the email associated with the website is legitimate and matches the official domain.
- Never authenticate from unknown links: Avoid logging in or providing personal information through links that you haven't verified as legitimate.

- Use well-known companies' websites for online purchases or transactions: Stick to reputable and established companies' websites when making online transactions to reduce the risk of scams.
- Google the company official website and authenticate there to check if the transaction or payment is recorded there too.

1.1.2 Email scams

- Always verify email address domains for authenticity: Check that the email address domain matches the legitimate domain of the organization or individual purportedly sending the email.
- In case of any money transfer, verify with the department or person requesting the transaction: Before proceeding with any money transfers requested via email, independently verify the request with the relevant department or person through a trusted communication channel.