

Social Implications ‘sub-scenario’

Information and Communication Technology (ICT) is not just about hardware and software issues. ICT also impacts on a wide range of issues such as social, legal, ethical, security and environmental issues.

1. Sibu received the following email, which was supposedly sent by an official at Empire Bank. Examine the email carefully and answer the questions below.

From: Empire Bank [mailto:john@empirebank.co.za]
Sent: 17 May 02:38 PM
To: Sibu_100@gmail.com
Subject: Empire Bank Verification - Sibu_100@gmail.com

Dear valued Empire Bank Member,

This email was sent by the Empire Bank server to verify your email address. You must complete this process by clicking on the link below and entering in the small window your Empire Bank and Password.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it. To verify your email address and access your bank account, click on the link below:

[Click here to update your data](#)

- 1.1 What general name is given to this kind of scam?
 - 1.1 [Phishing.](#)
- 1.2 There is a hyperlink at the bottom of the email.
 - 1.2.1 Briefly explain what a hyperlink is.
 - 1.2.1 [Hyperlinks can be found in electronic documents like emails and web pages. They are built-in connections, and if you click on them, they will take you to another place within the same document, or to another document – often another web page on the internet.](#)
 - 1.2.2 Should Sibu click on the link? Motivate your answer by explaining what would happen if she did.
 - 1.2.2 [No, Sibu should not click on the link, because she would probably be directed to a website that is a replica of the actual banking website, where she would be prompted to log on. She would thus be giving out personal, confidential details such as PIN numbers and passwords.](#)
- 1.3 What is the generic or general name given to techniques that rely on convincing people to give out information or to grant access by pretending to be someone who has the right to access this information?
 - 1.3 [Social engineering.](#)

- 1.4 What is the name given to the process where an email header is changed so that the email appears to be from a different origin (or person)?
- 1.4 Spoofing.
- 1.5 It is better to type the URL of a site, such as the URL of your e-banking site, into your browser, rather than clicking on a link. Would this help if your computer has been affected by a pharming 'attack'?
Motivate your answer by briefly explaining what pharming is.
- 1.5 No, pharming is a technique where a computer is compromised so that even if the user types the correct URL into the browser, the user will be directed to another website (often a replica of the 'real' one).
- 1.6 Mary has seen many warnings about ransomware. Explain what ransomware is.
- 1.6 Ransomware is malware that encrypts data (making it unavailable) until you pay the hacker a ransom fee (often using Bitcoin).
2. One of the trust members wants to make sure that Mary is taking all the necessary precautions when doing e-banking for the trust. He downloaded a document regarding safe online banking from their bank's website.
 - 2.1 Banks offer their online banking clients peace of mind by providing a number of security measures designed to make online banking as safe as possible.
Give two of these measures, besides the use of encryption (https).
 - 2.1 Any two of:
 - Logon passwords/PIN codes.
 - 'One time passwords', sent to a cellphone or via email for each e-banking 'session'.
 - Closing the e-banking 'session' after a period of inactivity.
 - Notifications sent to the user's cellphone that an e-banking 'session' has started, etc.
 - 2.2 One of the major things highlighted by the bank was the danger of doing one's e-banking in a public place like a cyber café, because of the dangers of *spyware* and *keyloggers* in particular.
 - 2.2.1 What is spyware? Explain your answer by referring to a keylogger and how it functions.
 - 2.2.1 Spyware is software that tries to monitor and track the way you use your computer. It then sends this information to third parties, without your consent or knowledge. A keylogger is software (type of spyware) that records your keystrokes as you type (and possibly even the movements of your mouse) and it could also takes screenshots of what is being displayed. It does so in an attempt to find your usernames, passwords, etc.
 - 2.2.2 Give two reasons why anti-spyware has to be regularly updated by briefly explaining how anti-spyware works.
 - 2.2.2 Anti-spyware software works by detecting spyware that has installed itself on a computer. Anti-spyware needs to be updated so that newer forms of spyware can be detected. In addition, anti-spyware programs also maintain a database of

websites known to spread spyware. The database is updated when the anti-spyware software is updated.

3. Vuyani uses a computer that is not connected to the internet. He is puzzled, as he seems to have a *virus* on the computer despite the fact that he has antivirus software installed and he is not connected to the internet. He is also sure that he did not accidentally install any malware such as a Trojan on the computer.
 - 3.1 Briefly explain what a computer virus is by referring to two of its general aims in your answer.
 - 3.1 A computer virus is a form of malicious software (malware) that is written to disrupt the normal functioning of a person's computer without their knowledge or consent. It can be used to turn a computer into a 'bot' (which can be controlled remotely via the internet), to spread malware or to create security loopholes for other programs. A collection of these bots are known as a *botnet*.
 - 3.2 What is a Trojan?
 - 3.2 A Trojan is a form of malware which is a destructive program disguised as a useful application. It can be used to install malware on a computer.
 - 3.3 Give three typical symptoms of a computer virus.
 - 3.3 Any two of:
 - A reduction in free disk space
 - A sudden (unexpected) reduction in performance
 - Reports from antivirus software
 - Software that has been uninstalled, changed or doesn't work any longer, etc.
 - 3.4 Give two possible reasons why Vuyani might still have a computer virus despite the precautions he seems to have taken.
 - 3.4 His anti-virus software (virus definitions) may be out of date and he may have used infected portable media, such as an infected flash disk.
4. One of the trust members suggested that an *acceptable usage policy* be drawn up for the use of the computers at the centre, and that a poster highlighting the key issues of *netiquette* be created.
 - 4.1 What does 'netiquette' refer to in broad terms?
 - 4.1 Netiquette refers to showing common courtesy to other users when you are online or communicating electronically.
 - 4.2 Give four netiquette 'rules' associated with email that could be included on the poster.
 - 4.2 Any three of:
 - Spell check messages before sending them.
 - Be courteous and concise.
 - Refrain from slander or gossip.
 - Avoid sending very large attachments.
 - Don't forward chain letters or hoaxes.
 - Do not type in capital letters, etc.

- 4.3 Give three items that ought to be included in an acceptable usage policy for the computers at the centre, besides any issues related to netiquette.
- 4.3 Any three of:
- Respect the privacy/data/intellectual property of others.
 - Do not access or store material that may be seen as offensive.
 - Do not tamper with the software settings or the hardware.
 - Report any problems you see to a staff member.
 - Do not install or uninstall software.
 - Details on when and where portable storage devices such as flash disks and portable media players may be used.
5. A number of the younger members of the local community make use of social networking sites such as Facebook and it appears that very few of them know how to set their privacy settings. Why is it so important to set your privacy settings when using a social networking site such as Facebook?
5. Privacy settings allow you to specify or limit who can view your information, including photos and posts. You can also set who can post to your wall.
6. A potential new donor has contacted the trust with the aim of sponsorship. They want to know that the trust is committed to green computing before they consider becoming a sponsor.
- 6.1 Briefly describe what *green computing* refers to in general.
- 6.1 Green computing refers to the use of (computer) technology in a way that is sensitive to the environment.
- 6.2 One of the ways the trust can save money and contribute to green computing is to reduce their amount of paper used for printing.
Give two ways in which this can be achieved.
- 6.2 Any two of:
- Encourage staff/users to proofread the electronic version of documents before printing.
 - Make greater use of e-communication (email, etc.) instead of printing to distribute documents.
 - Use duplex/'side-by-side' printing, etc.
- 6.3 Another way in which the trust can contribute to green computing is to reduce their power usage.
Give two practical ways in which they can achieve this goal.
- 6.3 Any two of:
- Use energy efficient equipment or hardware.
 - Use power-saving schemes on computers/hibernation mode.
 - Switch off equipment that is not being used, etc.
7. One of the key benefits to course members, after they have upgraded their ICT skills, is that they will be in a better position to pursue careers that involve *telecommuting*.
Briefly explain the concept of *telecommuting*.

7. Workers communicate with one another (their clients / employers / customers) electronically, instead of physically travelling to a traditional office to work.
8. One of the computers is equipped with a *braille* keyboard, and another with a *large trackball* instead of a 'normal' mouse.

What disabilities would a person be suffering from, if they made use of a *braille* keyboard or a *large trackball*, respectively?
8. Braille keyboard: visual impairment, blindness
Large trackball: poor motor control (paralysed, arthritic, etc.)
9. A UPS must be installed on the server.
 - 9.1 What is the function of a UPS?
9.1 To protect the computer / server against power problems (surges, spikes, outages)
 - 9.2 Why it is more important to install a UPS on a server, than on a client computer?
9.2 A server computer provides resources and services to (many) other computers on the network – so there are more far-reaching / negative / expensive consequences if a server were damaged through power problems, than if a client computer were damaged.
It also gives time to shut the server down properly when there is a power failure to prevent loss of data.
10. The Trust promotes Kickstarter – an online platform used by people to fund their creative business ideas.
 - 10.1 Give two advantages of using a platform such as Kickstarter to fund a business idea.
10.1 Any two of:
 - To determine whether there is demand or support for an idea or product, before you invest time, effort and money to create it.
 - The first batch of products is already 'sold' before they have been created.
 - Greater chance of funding by multiple donors (instead of relying on traditional loan institutions such as banks).
 - 10.2 Give one typical benefit that a person could expect to receive, by contributing (or 'pledging') to a business idea that turns out to be successful.
10.2 A reward of some sort (often commensurate with the amount of money pledged), such as:
 - Completed product at a lower price
 - Special features/customisations to the product that will be unavailable to people who did not pledge anything, etc.
11. Give one reason why it might not be a good idea to allow the computers to participate in a *grid computing* project – even though there is a fast Internet connection.
11. Any one of:
 - Computers might be slowed down
 - Possibility of malware infections
 - Risk of computer damage through overheating