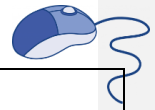
Formatted: Different first page header

SUBJECT and GRADE	**Computer Applications Technology - Grade 11**	
TERM 2	**Week 3**	
TOPIC	**SOCIAL IMPLICATIONS OF COMPUTER NETWORKS**	
AIMS OF LESSON	At the end of this lesson you should be able to know: • Define unauthorised access to networks • Describe the ethical use of networks • Explain what acceptable use policies (AUPs) in schools are • Define the social implications for network usage • Discuss network security and BYOD environments • Discuss privacy issues in relation to network security • Explain importance of database security and the concept of big data	
RESOURCES	***Paper based resources***	***Digital resources***
	Refer to your textbook (DBE Theory Book): • Chapter 8: Social Implications Computer Networks NB! You may also use your own textbook that refers to the sections above.	Links on the WCED ePortal: Theory Book: https://wcedeportal.co.za/eresource/88001
INTRODUCTION	In this unit, you will build on your knowledge of network security by exploring issues around authentication and by looking at what unauthorized network access is and its negative consequences, how networks must be used ethically and why AUPs (in schools and other environments) are drawn up. We will also discuss network safety and security issues, especially when it comes to BYOD	
CONCEPTS AND SKILLS	**UNAUTHORISED NETWORK ACCESS** • Unauthorised access on a network is when someone gains access to a network using someone else's credentials (such as username and password) or through other illegal methods (e.g. hacking) • Accessing a network, website, account or service that you do not have permission to access is illegal.	



HOW CAN UNAUTHORISED ACCESS BE PREVENTED?

Authentication

- The aim of authentication is to protect your personal information from unwanted access.
- Examples of authentication methods are:
    - Usernames and passwords
    - Biometric security such as (fingerprint-unlock or face-unlock)
    - PIN codes
    - Screen-lock patterns (commonly used on mobile devices such as smartphones and tablets)

Setting up a password

- Make sure to use a strong password: strong password is set in a way that will be difficult for machines or people to guess.
- A strong password is hard to guess, but it should be easy for you to remember. A strong password consists of the following:
    - At least 10 characters—the more characters, the better
    - A mixture of both uppercase and lowercase letters
    - A mixture of letters and numbers
    - Inclusion of at least one special character, e.g., ! @ # ?]

ETHICAL USE OF NETWORKS

- The word "Ethical" means being in agreement with the rules or standards of that particular environment.
- Since networks are used by a wide range of people, they must be used responsibly and ethically.

Why is it important that networks are used ethically?

Anything negative that any user does on a network can reflect negatively on the company, school or organisation whose network they are using.

What measures can schools, companies and other organisations put in place to ensure ethical use of networks?

- Schools, companies and other organisations have an ***Accessible Use Policy (AUP)*** that you have to read and then sign or acknowledge in some way.
- An AUP is a document stipulating restrictions, limitations and practices that a user must agree to, before they are allowed access to a network.

ACCEPTABLE USE POLICIES OF SCHOOLS

- In a school, an AUP is a contract between the users (learners, teachers and support staff) and the organisation (school) that outlines what users can and cannot do when using the school's network.

Guidelines that should be in school AUPs

- A list of basic netiquette rules, including not sending spam or hoax emails and how users should communicate using email or social media websites
- What may or may not be accessed online using the school's ICT facilities. This could include restricting access to social media websites
- How much information users may download from the internet (for example, no live streaming or downloads larger than a certain file size)
- Guidelines on respecting copyright, intellectual property laws and privacy, as well as how to avoid plagiarism
- When and how portable storage devices can be used
- Restrictions on what software can be installed on the school's computing devices
- What to do if users find that they have become the victims of identity theft, cyberstalking and cyber-bullying, and what to do if their devices become infected with viruses or malware
- Clear descriptions of what will happen to a user who breaks the rules outlined in the AUP

NETWORK SECURITY

- Network security is the process of taking hardware and software preventative measures to protect the network from unauthorised access

What measures can schools, companies and other organisations put in place to ensure network security?

- Using a Firewall
- Installing antivirus software
- Use passwords and usernames where necessary
- Understanding BYOD environments and applying all relevant safety requirements

Firewall

- A ***firewall*** is a program or hardware device that acts as a filter for data entering or leaving a network or computer. Firewalls are basically the security guards of a network. Everything that comes into your network from the internet should be going through a firewall.
- ***Hardware firewall***: is a physical device that connects to your network. This type of firewall provides protection for all the devices that are connected to the network.
- ***Software firewall***: is a program that you install on your computer to help protect it from unauthorised incoming and outgoing data. A software firewall will protect only the computer on which it has been installed. Additionally, many antivirus scanners include a software firewall.

Antivirus software

- An ***antivirus software*** is a utility program designed to protect your computer or network against computer viruses and other malware such Trojans, spyware and adware.
    - ***Adware*** is software that secretly installs itself; it displays unwanted advertisements on your computer. Adware programs will tend to serve you pop-up ads, can change your browser's homepage, add spyware and just bombard your device with advertisements.

- **_Spyware_** is unwanted software that installs itself to your computing device, stealing your internet usage data and sensitive information. Usually it aims to track and sell your internet usage data, capture your credit card or bank account information, or steal your personal identity.

- All the computers in a network should also have anti-virus software installed to protect them from being infected with malware, viruses and other harmful programs.

Passwords and usernames

- One of the most common policies is to give users a username that they can use to log into the network and have them choose a password.
- When you need to ***choose a password***, there are a few things you must keep in mind:
  - All passwords must be created using the guidelines for '*strong passwords'*
  - Do not use your name, a family member's name or the name of a pet.
  - Your password should not be something easy to guess, such as "password" or "12345".
  - Never give out your password to anyone and try not to share your account details
  - with anyone.
  - To make sure your passwords are safe, you should change them every two months or so.
  - You should never use the same password for different websites and networks.

Network Security and BYOD

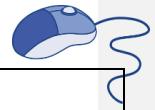
- ***Bring Your Own Device (BYOD)*** refers to a concept where network users are allowed to bring and use their own portable devices such as smartphones, laptops, tablets, etc. to work on and access the network instead of a device owned by the organisation (such as school or business).

Problems that may arise with the introduction of BYOD

- The main concern with personal devices that are used for work is how to keep the company's private data separate from a user's personal data and how to make sure that an employee does not accidentally share that private data.
- Another concern is that most mobile devices, such as smartphones and tablets, *might not have* anti-virus software installed, or, if there is anti-virus software, it is not up to date. This becomes a problem when users accidentally download applications that contain malware, adware or spyware.
- Mobile devices can also become infected with viruses. When these devices connect to the network, they can spread the infection, making the network unsecured.
- Employers cannot control what employees install on their devices. Employees may be able to install games or other media that can become a distraction at work.

Measures that can be put in place to prevent issues related to BYOD

- Organisations can set up a data loss prevention policy by using data loss prevention tools.
- Organisations can also use mobile device management software, such as Microsoft Intune, to manage the devices on their networks.
- Organisations must set up a clear AUP regarding what network users can and cannot do with their personal devices.



PRIVACY ISSUES

- Networks have become powerful tools to access, collect, store and share personal data.
- This data can be used to provide a company's customers with a better service, but this data can also be used by cyber-criminals to commit fraud or to steal.

What role can network users play to protect the network from external attacks?

- Make sure that your devices have up-to-date antivirus software installed.
- Never click on suspicious links or reply with personal information to suspicious emails.
- Respect others' privacy and products. Do not download or share content that has been obtained illegally (such as pirated movies or music) or content that violates someone else's copyright.
- Be careful what your share about yourself on the internet.
- Follow the AUPs of any network you are using.

DATABASES SECURITY

- Networks have databases, where personal information is stored. These databases are often the targets of cybercrimes, so database security is extremely important.
- Databases should be ***encrypted*** to make sure that the information stored in term is safe and secure.
- The data must only be accessed by people who have the correct permissions to view it. This can be done by making sure that access to the data is controlled.

BIG DATA

- Big data, is a term that describes the massive amounts of data that are generated every day by every single person.
- More and more companies are collecting this data and storing it on databases to use in marketing or product development.
- Companies also capture big data on consumer habits for targeted marketing. This has raised concerns about privacy because every time you click on a website, post on social media, use a mobile app and comment via email or to call centres, your data is collected for future use.
- As big data increases, it exposes more of our data to potential security breaches. For example, if you have approved a company to analyse your data, there is no guarantee that they will not fall prey to a cyber-attack or that they will not sell your data. This could result in your private data being in unsafe hands.

ACTIVITIES/ASSESSMENT

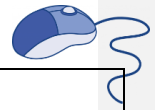
QUESTION 1: MULTIPLE CHOICE

1.1 Which of the following is NOT used to authenticate a user?

A. Username
B. Password
C. PIN
D. BYOD (1)

1.3 What does BYOD mean?

A. Bring your own device
B. Buy your online device
C. Bring your device
D. Bypass online detection (1)



1.2 Which of the following techniques cannot be used to authenticate user access to your smartphone?

A. Fingerprint scanner
B. Identity card
C. Screen-lock pattern
D. PIN (1)

1.4 What is the purpose of a firewall?

A. It removes malware from your computer.
B. It uninstalls programs from your computer.
C. It updates your computer's software.
D. It prevents outside devices or programs from accessing your network. (1)

QUESTION 2: TRUE OR FALSE

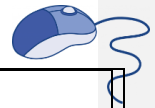
2. *Write True or False next to the question number. Correct the statement if it is FALSE. Change the underlined word(s) to make the statement TRUE. (You may not simply use the word NOT to change the statement.)*

a. **Authentication** is the process of working out whether something or someone is, in fact, what or who they claim to be. (1)
b. Using a network in an **unethical** manner can improve the reputation of an institution. (1)
c. On a network you must protect the **privacy** of others and yourself. (1)
d. **Unauthorised access** on a network is when someone legally gains access with another user's password. (1)

QUESTION 3: MATCHING ITEMS

Choose a term/concept from Column B that matches a description in Column A. Write only the letter next to the question number (e.g. 1J).

COLUMN A	COLUMN B
1. Encrypting people's personal information to ensure that it stays safe and secure.	A. Integrity B. Privacy issue C. Password protection D. Availability E. Big data F. Confidentiality
2. Controlling user access by making sure that data stored online can only be viewed by those who have the correct permissions to view it.	
3. Ensuring that users are able to have constant access to their online data	



	4. Matching the password that a person provides with the credentials stored on a database to prevent the unauthorised access of data and information. | G. Authentication H. Cryptocurrency

QUESTION 4: MEDIUM QUESTIONS

4.1 Why is it important that databases containing sensitive data be encrypted? (3)
4.2 List three AUP guidelines that should be used by schools. (3)
4.3 Discuss TWO advantages of big data for companies. (2)
4.4 Outline ONE concern that comes with BYOD. (1)

QUESTION 5: SCENARIO-BASED QUESTIONS

Stacy has recently had a friend of hers install a network in her house. Since she has a four-year-old daughter and a 14-year-old son who will eventually have access to this network, she needs to work out what safety precautions she must implement.

5.1 What type of network should Stacy install? Give a reason for your answer. (2)
5.2 What two things can Stacy do to control what her children can access on their home's network? (2)
5.3 Stacy's son has created a Facebook account. What three safety tips can Stacy give him about his use of this online platform. (3)
5.4 Which THREE measures can Stacy put in place in order to maximize the security of the network? (3)
5.5 Give three guidelines that Stacy can use when setting a strong password. (3)

CONSOLIDATION	• *Define unauthorised access to networks.* • *Describe the ethical use of networks.* • *Explain what acceptable use policies (AUPs) in schools are.* • *Discuss network security and BYOD environments.* • *Explain the privacy issues you can encounter on a network.* • *Discuss personal responsibility in relation to network security.* • *Define database security and big data.* • *Discuss advantages and disadvantages of big data*
VALUES	• Network owners have a responsibility to make sure that the data their network is accessed legally and that this data is only used for what they say its use will be. It is also their responsibility to make sure that this data is secure and safe. • Network users also have a responsibility to make sure that they do not expose a network they are using to external threats and attacks.