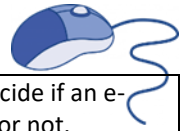
SUBJECT and GRADE	**CAT Grade 12**		
TERM 2	***Week 3***		
TOPIC	**Network technologies-Social implications**		
AIMS OF LESSON	Computer and cybercrimes, how to avoid security threats and safeguarding against criminals.		
RESOURCES	***Paper based resources***	***Digital resources***	
	DBE Gr 12 Theory online textbook (page numbers in this document refers to this book) Any other applicable and approved text book used in schools.	***YouTube video on phishing*** https://www.youtube.com/watch?v=PTE2oqMcfSw *Other scamming tactics* https://www.youtube.com/watch?v=KuBqn1f9uKc	
INTRODUCTION	• *Gr 11: LAN, WLAN, basic knowledge of some of the computer threats such as spyware, pharming, phishing and adware. Ways to protect hardware theft, definition of a firewall and its function.*		
CONCEPTS AND SKILLS	**Computer crime:** is the use of computer as an instrument for illegal online actions. It is also known as **cybercrime.** **Social engineering:** is any attempt to manipulate or con someone into revealing information such as passwords or account number **Hardware theft:** It means stealing computer equipment. Mobile devices are at high risk because of their size and weight that allows them to easily disappear into pockets and bags. **Protection against hardware theft:** • Use motion sensors • Lock computer rooms • Install CTV cameras • Use biometric security to access computer rooms **Bandwidth theft:** It means using bandwidth that you have no authorized access to.	**Identity theft:** The process in which a criminal/ someone uses the identity of another person dishonestly. **To prevent identity theft** • Use caution when giving personal information. • Do not respond to e-mails from unknown sender. • Do not give your personal details to anyone online. **Internet attacks:** attacks on the network, computers and data from anywhere on the internet. They include: (a) **DOS (denial of service):** In this attack a computer receives a huge amount of useless data in such a way that the computer/ network becomes too slow. (b) **Sniffer attacks**: A small program or device that can read data packets being sent to other users over a net-work. (c) **Bots:** computer (robot) that has been compromised (infected) and is being	**Prevention.** • Never click a link in an e-mail message. **Pharming:** Is a process whereby users are redirected to a fake website even though they enter correct URL. **E-mail spoofing:** It is the forgery of an e-mail header so that the e-mail appears to be from a different origin **Click jacking**: Users are tricked into clicking on an item on a webpage which acts as a concealed (hidden) link. **Protection against computer crime:** • **Use ABC:** ○ **Assume nothing**: don't assume you are safe and protected. ○ **Believe no one**: check up on people you are interacting with. ○ **Check everything**: bad spelling and grammar. • Check incorrect website URLs.



	Prevention of bandwidth theft-Use of username and passwords with ADSL hardware**.** **Malware:** Short for malicious software. Any type of software that can infect your computer without your permission. **Virus:** A malicious /damaging program that can copy itself, infecting the computer and altering the way it operates without permission or knowledge of the user, and spreading from one computer to another. **Worm:** A malicious program that replicates on a network using re-sources so that the network slows down or shut down completely. **Trojan**: A malicious program that is often disguised as legitimate software. **Spyware:** Malware that gathers information from your computer, without your knowledge or consent. **Keylogging:** A program that records every keystroke on a keyboard to gain fraudulent access to confidential information. **Software theft:** is the unauthorised or illegal copying, sharing or usage of copyright-protected software programs **For example:** • Someone steals software media • Software Piracy – unauthorised use of a program • Intentionally erase programs Software piracy has the following negative effects on the end-user: • No access to technical support • No upgrades • Incomplete or virus contaminated products	controlled remotely when switched on and connected to internet. (d) **Botnets:** large networks of bots that work together to bring down websites and corporate networks. (e) **Zombie**: A computer under the control of a bot. **(f) Cyber-attacks**: An attack on the infrastructure of the web itself. **Information theft:** Refers to the theft of personal or confidential information such as credit card numbers, etc. Information transmitted over network poses a high degree of risk because it can be intercepted during transmission. Use **encryption** or coding to protect sensitive information **Encryption** is the process of converting readable characters into unreadable characters to prevent unauthorized access. **Internet related fraud scams** **Scam**: is the process in which criminals get people to give them money by tricking them. **Phishing**: The fraudulent practice of sending emails pretending to be from reputable companies to convince individuals to reveal personal information. Indications that an email is a form of phishing • Sense of urgency, e.g. provide your details in 24hrs otherwise your account will be blocked • A link to take a user to another webpage • Unusual domain name • Spelling and grammatical mistakes	These things can help you decide if an e-mail or website is legitimate or not. **Safeguard against criminals, viruses and threats:** • Install antivirus and antispyware on your computer. • Update the antivirus regularly. • Delete chain letters and spam • Do not click on pop up messages and adverts. • Never give your login details to anyone else. *Nice to know:* **Grid/distributed computing:** The use of widely distributed computer resources to collectively solve a single problem. **Advantages** • More processing power and allows for sharing of resources and corresponding costs • Adding of computing devices as needed. Scalability. • If one computer is not available, another one can be used. **Disadvantages** • Requires faster connections and connectivity errors may occur. • Security issues are a challenge. • Requires skilled technicians and programmers **Theft of time and services**: this occurs when employees are paid for time and services that they did not provide. Theft of time occurs in the following cases: late arrival at work, early departure, taking long lunch hours or breaks.

ACTIVITIES/ASSESSMENT. Consolidation Activity

Match the statement in Column A to a response in Column B.

Column A:		**Column B**
1.1	The practice of rerouting users to bogus or unexpected websites when they enter a URL in their web browser	**A** .Cybercrime
1.2	A program that gathers information about a user without his or her knowledge	**B**. Hoax
1.3	A harmful program disguised to look like a trustworthy or useful application	**C**. Pharming
1.4	A technology to help avoid security threats on a network	**D** .Grid computing
1.5	An e-mail message warning one of a virus that does not exist	**E**. Spyware
1.6	Using the collective processing power of many computers to work on a single, common task	**F**. Trojan
1.7	A term used to describe illegal activities carried out on the Internet	**G**. Firewall

Short free response questions

2.1	Explain what phishing is AND why updating your antivirus program will not prevent you from becoming a victim of phishing.	**(2)**
2.2	State TWO ethical considerations to keep in mind when connecting to someone else's Internet connection.	**(2)**
2.3	Give TWO examples of how social engineering is done.	**(2)**
2.4	State THREE ways in which a user will know that his or her computer has a virus.	**(3)**
2.5	State TWO ways in which you can prevent a computer from getting a virus other than having updated antivirus software installed and not using the Internet at all.	**(2)**
2.6	Explain what identity theft is	**(2)**
2.7	Phishing is a world-wide problem. State TWO ways of identifying a possible phishing attack.	**(2)**
2.8	Give TWO reasons why it is difficult to fight cybercrime in south Africa.	**(2)**