



Province of the
EASTERN CAPE
 EDUCATION

DIRECTORATE SENIOR CURRICULUM MANAGEMENT (SEN-FET)
HOME SCHOOLING SELF-STUDY WORKSHEET SOFTWARE

SUBJECT	COMPUTER APPLICATIONS TECHNOLOGY	GRADE	10	DATE	Term 1 to 4
TOPIC	E-communication (Provided by DBE)	TERM 1 to 4 REVISION	✓ All software Gr 10		
TIME ALLOCATION	3 HOURS	<u>TIPS TO KEEP HEALTHY</u>			
INSTRUCTIONS	<ol style="list-style-type: none"> 1. This is a Theory Worksheet: 2. You will need a book to write your answers in and something to write with. 3. Answer the following questions in your workbook. 4. WHERE TO FIND THE ANSWERS: <ul style="list-style-type: none"> • USE THE POWER POINT PROVIDED ALSO AVAILABLE ON OUR WEBSITE – GR 10 https://drive.google.com/file/d/1DGV0hX57TMpFJyJFmNW_a_ijaJ5rpACR/view?usp=sharing • You may use your CAT textbook to find the answers or alternatively, you can use the free downloadable CAT textbook provided by the Department of Basic Education. • See the link below to download this FROM OUR provincial CAT and IT website. THEORY COMPUTER APPLICATIONS TECHNOLOGY: https://sites.google.com/view/itandcatinec/cat-grade-10?authuser=0 	<ol style="list-style-type: none"> 1. WASH YOUR HANDS thoroughly with soap and water for at least 20 seconds. Alternatively, use hand sanitizer with an alcohol content of at least 60%. 2. PRACTICE SOCIAL DISTANCING – keep a distance of 1m away from other people. 3. PRACTISE GOOD RESPIRATORY HYGIENE: cough or sneeze into your elbow or tissue and dispose of the tissue immediately after use. 4. TRY NOT TO TOUCH YOUR FACE. The virus can be transferred from your hands to your nose, mouth and eyes. It can then enter your body and make you sick. 5. STAY AT HOME. 			

Level 1 – Getting the basics → testing your knowledge


1. What is Internet communication? (4)
2. Define each of the following Internet communications (e-communication):
 - a. Instant messaging (4)
 - b. Social media (3)
 - c. E-mail (3)
 - d. Blog (3)
 - e. Voice over Internet protocol (VoIP) (2)
3. What is netiquette? (2)
4. What is a digital security risk? (3)
5. List some common digital security risks (6)
6. Define each of the following cybercrimes
 - a. Data/Information theft (1)
 - b. Identity theft (3)
 - c. Unauthorised access to computers or networks (2)
 - d. Unauthorised use of computers or networks (2)
 - e. Malware (5)
7. Define each of the following issues
 - a. Fake news (3)
 - b. Hoax (2)
 - c. Spam (3)
8. Define each of the following malware
 - a. Virus (4)
 - b. Trojan (2)
 - c. Worm (3)
 - d. Ransomware (3)
9. List three forms of fake news (3)
10. What is phishing? (3)
11. What is pharming? (4)
12. What is spoofing? (3)
13. What is email spoofing? (2)
14. What is IP spoofing? (2)
15. Provide one word/term/concept for each or the following descriptions
 - a. You log onto your bank's website but it redirects you to a bogus version of the website (1)
 - b. Digital content created and shared online using social websites (1)
 - c. You receive an email that informs you that there is a problem with your bank account and that you must provide your username and password to sort out problem else your account will be locked (1)
 - d. An email appearing to be from a legitimate source that requests you to provide sensitive personal/financial information (1)
 - e. A malicious program that infects a computer and then locks some part of it, preventing the user access to their computer or data. (1)
 - f. Cyber ethics that describe the unwritten rules of Internet courtesy (1)
 - g. Websites such as Facebook, twitter

- h. Small picture to show emotion on with electronic communication such as emails (1)
- 16. List three forms of fake news and give briefly describe each one (6)

Level 2 – Demonstrate your understanding and apply what you have learned

- 17. Compare a worm and a virus (6)
- 18. For each of the following, choose the item in the list that does not logically belong in the list and explain why it does not belong
 - a. Facebook, VoIP, YouTube, LinkedIn, Twitter (2)
 - b. Skype, WhatsApp, Viber, IRC, WebEx, WeChat ✓ (2)
- 19. In the context of email, explain the difference between cc and bcc and provide an example of how both are used appropriately (7)
- 20. Compare an email client (e.g. MS Outlook) to webmail (5)
- 21. Using an example, describe the relationship between email spoofing and phishing (5)
- 22. Describe five ways how you can spot phishing in an email (5)
- 23. Compare Phishing and Pharming (6)
- 24. Suggest two precautions/safeguards against each of the following:
 - a. Unauthorised use of computers or networks (6)
 - b. Internet and network attacks
 - c. Information theft
- 25. Describe how using the Bcc field when sending email could be an advantage over using the To or the CC fields (8)
- 26. Downloading illegal/pirated software is one of the most common ways a computer gets infected with viruses, malware. Explain how this could happen. (4)

Level 3 – Are you ready to analyse, evaluate, think critically and solve problems?

27. Mary created a backup copy of her data on a USB flash drive which she keeps next to her computer as she also uses it to save other files that she transfers between computers.
Critique Mary's practice and explain to why it is not regarded as best practice (9)
28. John wants to do some online shopping but is scared that it may not be safe. Use the web address below to explain to him what he should look out for and why. (5)
29.  <https://www.takealot.com/deals/app-only>
30. The following is listed as some of the Top computer mistakes beginners make. For each of the mistakes, critique the action(s) and suggest precaution(s) to avoid negative effects
- a. Clicking Next or OK without reading or making sure nothing extra is checked (2)
 - b. Opening e-mail attachments (2)
31. Someone gave you a USB flash drive with information to copy to your computer. What step(s) should you take to ensure that your computer does not get infected with malware? (2)
32. Downloading illegal/pirated software is one of the most common ways a computer gets infected with viruses, malware.
To stay safe, suggest and explain four actions to keep in mind when downloading anything (16)
33. You type the URL of an online shopping website you use often and log in with your password and order an item. The website requests that you enter your credit card information. The next day, you realise that your credit card has been used to for online shopping that you are not aware of. Explain what could have happened? (5)