



Province of the
EASTERN CAPE
EDUCATION

DIRECTORATE SENIOR CURRICULUM MANAGEMENT (SEN-FET)

HOME SCHOOLING SELF-STUDY WORKSHEET ANSWER SHEET

SUBJECT	COMPUTER APPLICATIONS TECHNOLOGY	GRADE	10	DATE	Term 1 to 4
TOPIC	E- communication Provided by DBE	TERM 1 TO 4 REVISION		All software covered	

Level 1

1. What is Internet communication? (4)
Refers to the different ways✓ people can communicate✓ over the World Wide Web (WWW) ✓ using devices such as a computer/ mobile phone✓
2. Define each of the following Internet communications (e-communication):
 - a. Instant messaging (4)
Real-time✓, typed conversation (voice notes included) ✓ with another online/connected ✓ user where one can also exchange photos, videos and other content✓?
 - b. Social media (3)
Content (photos, videos, music, tweets, podcasts blogs, etc.)✓ that users create and share✓ online using social websites✓
 - c. E-mail (3)
Transmission✓ of messages and files✓ via a computer network✓
 - d. Blog (3)
An informal website✓ consisting of time-stamped✓ articles or posts in a diary or journal format, usually listed in reversed chronological✓ order
 - e. Voice over Internet protocol (VoIP) (2)
A technology that allows you to make voice calls✓ using a broadband Internet connection✓
3. What is netiquette? (2)
Considerate behaviour✓ when you are communicating online✓
4. What is a digital security risk? (3)
Any event or action ✓ that could cause a loss of or damage to✓ computer devices, hardware, software, data, information or processing capability✓.
5. List some common digital security risks (6)
Internet and network attacks✓, unauthorised access and use✓, hardware theft✓, software theft, ✓ information theft, ✓ system failure✓
6. Define each of the following cybercrimes

- a. Data/Information theft (1)
When someone steals personal or confidential data/information✓
 - b. Identity theft (3)
Using another person's data illegally✓ (like ID numbers and banking details – usually stolen) to pretend to be that person✓ to make transactions, purchases and loans✓
 - c. Unauthorised access to computers or networks (2)
The use✓ of a computer or network without permission✓
 - d. Unauthorised use of computers or networks (2)
The use of a computer/network or its data✓ for unapproved or possible illegal activities✓
 - e. Malware (5)
Any computer software✓ with a malicious intent ✓ → designed to cause damage to a computer, server, client, computer network ✓ or to exploit a computer ✓ user or facilitate any computer crime✓
7. Define each of the following issues
- a. Fake news (3)
News or stories✓ created to deliberately✓ misinform/disinform or mislead✓ readers.
 - b. Hoax (2)
Usually an email✓ with the intend to deceive or trick✓/cause false fears/hope/sympathy, etc.
 - c. Spam (3)
Unwanted✓ digital communication ✓ that is sent in bulk to many recipients✓
8. Define each of the following malware
- a. Virus (4)
Potentially damaging software,✓ designed to spread ✓ that affects or infects a computer negatively by altering the way the computer works ✓ without a user's knowledge or permission✓
 - b. Trojan (2)
Potentially malicious software ✓ that hides within or looks like legitimate software✓
 - c. Worm (3)
Potentially malicious software✓ that copies itself repeatedly✓ in a computer's memory or on a network, using up resources and potentially shutting the computer down✓
 - d. Ransomware (3)
Malicious software✓ that blocks or limits access to a computer or files or encrypts data✓ until the user pays a specified amount of money✓
9. List three forms of fake news (3)
Disinformation✓, misinformation✓, propaganda✓
10. What is phishing? (3)
A scam✓ in which a perpetrator sends an official looking message (email or SMS) from a legitimate institution✓ to lure/trick a person into providing personal and/or financial information✓
11. What is pharming? (4)
A scam✓ of directing Internet users to a bogus website✓ that mimics the appearance of a legitimate one✓, in order to obtain personal/financial information✓
12. What is spoofing? (3)
A technique ✓ that a perpetrator uses to disguise the origin of an electronic message/internet transmission✓ to appear to come from a trusted source ✓

13. What is email spoofing? (2)
Happens when a sender's email address or components of the email header are altered ✓ so that it appears as if the email originated from a different sender ✓ such as a legitimate institution.
14. What is IP spoofing? (2)
When an intruder computer ✓ fools a network into believing its IP address is associated with a trusted source ✓
15. Provide one word/term/concept for each or the following descriptions
- You log onto your bank's website but it redirects you to a bogus version of the website (1)
Pharming ✓
 - Digital content created and shared online using social websites (1)
Social Media ✓
 - 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)
Phishing ✓
 - An email appearing to be from a legitimate source that requests you to provide sensitive personal/financial information (1)
Email spoofing /Spoofing ✓ Also accept Phishing
 - A malicious program that infects a computer and then locks some part of it, preventing the user access to their computer or data. (1)
Ransomware ✓
 - Cyber ethics that describe the unwritten rules of Internet courtesy (1)
Netiquette
 - Websites such as Facebook, twitter (1)
Social networks ✓
 - Small picture to show emotion on with electronic communication such as emails (1)
Smiley/Emoji ✓
16. List three forms of fake news and give briefly describe each one (6)
Disinformation ✓ Spreading deliberately false information ✓
Misinformation ✓ Erroneous or incorrect information ✓. Not always be deliberate; it's just wrong or mistaken
Propaganda ✓ - Information, ideas, or rumors deliberately spread widely to help or harm a person, group, movement, institution, nation etc ✓

Level 2

17. Compare a worm and a virus (6)
A virus spreads by inserting a copy of itself into and becoming part of another program/file (it needs a host file) ✓ and requires human action to replicate, such as sending them through emails ✓ and clicking/opening the infected file to activate ✓ whilst a worm is standalone software ✓ that does not need human help but can replicate itself ✓ and spread itself exploiting a vulnerability on the network/ system ✓
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)
VoIP ✓ – others are social websites ✓
- b. Skype, WhatsApp, Viber, IRC, WebEx, WeChat ✓ (2)
IRC ✓ is text based ✓
19. In the context of email, explain the difference between cc and bcc and provide an example of how both are used appropriately (7)
CC is short for carbon copy or courtesy copy ✓ and is a copy of an e-mail to be shared but requires no reply or action ✓. Generally speaking, one should not reply to an e-mail if your e-mail address is in the CC field ✓. For example, an employee sending an important message to other employees may also CC their manager or boss to help keep them up-to-date ✓
Bcc is short for blind carbon copy ✓ and BCC sends copies of e-mail without displaying any of the names or e-mails in the e-mail ✓. For example, when you send an e-mail to many recipients and you want to avoid that everyone see all recipients email addresses to protect privacy ✓
20. Compare an email client (e.g. MS Outlook) to webmail (5)
Both perform the same function: they allow the user to send and receive e-mail ✓.
However, an e-mail client requires the user to install software directly onto their computer, while webmail is completely cloud-based ✓;
Also, many e-mail clients cost money while webmail is free ✓
Email clients are generally more secure ✓
A user can access webmail e-mail from any device that is connected to the Internet, and from any location ✓
21. Using an example, describe the relationship between email spoofing and phishing (5)
A perpetrator uses spoofing ✓ to create a fake email pretending to be from a legitimate institution ✓, in an attempt to steal your personal/financial information ✓ either through luring/tricking you to send them the information ✓ or clicking a link that will take you to a fake website, imitating the website of the legitimate institution, where you would log in providing your personal/financial information ✓
22. Describe five ways how you can spot phishing in an email (5)
The email appears to be from a legitimate institution such as a bank, but it uses a non-standard format email address ✓
The sender's email address appears to be legitimate, but the reply address is different from the sender's address (Gmail or similar) ✓
The message contains a mismatched URL ✓
URLs contain a misleading domain name ✓
The email uses poor grammar use or contains several spelling mistakes ✓

The email is poorly formatted ✓

The email contains commands and/or threads ✓

The email does not contain any contact information ✓

The email asks you to provide sensitive personal information that you would not normally share with anyone ✓ Any five valid explanations

23. Compare Phishing and Pharming (6)

Both are scams that attempts to steal personal/financial information ✓

With Phishing, some user response is required ✓, e.g. replying to a spoofed email to provide personal/financial information requested in the email ✓ or clicking on a link in an email (uses email spoofing))that takes you to a bogus website that seems legitimate where you enter personal/financial information ✓

With Pharming, no user response is required ✓ the user simply type/clicks a trusted URL ✓ on his computer, e.g. your Bank's URL but the IP address that corresponds to the Bank's URL is changed ✓ (by malicious code (uses IP spoofing)) and take you to a bogus website that looks like your Banks website where you enter personal/financial information

24. Suggest two precautions/safeguards against each of the following:

a. Unauthorised use of computers or networks (6)

Use usernames and passwords ✓

Turn off your computer when not using it ✓

b. Internet and network attacks

Use antivirus software ✓

Be suspicious of unsolicited email and attachments ✓

Scan removable media for malware before using it ✓

Use a firewall ✓

Update software regularly ✓

Backup regularly ✓ (any 2)

c. Information theft

Do not respond to spoofing ✓

Check if a website is secure/using encryption by checking if the URL starts with https before you provide personal/financial information ✓

25. Describe how using the Bcc field when sending email could be an advantage over using the To or the CC fields (8)

▪ The privacy of email addresses is protected in the original message ✓. Recipients will receive the message, but won't be able to see the addresses listed in the BCC field ✓.

▪ When an email is forwarded, the addresses of everyone in the To and CC fields are also forwarded along with the message ✓. Addresses that have been placed in the BCC field are not forwarded ✓.

▪ If you have placed a large list of recipients in the To or CC field, all of them will receive the reply ✓. By placing recipients in the BCC field, you can help protect them against receiving unnecessary replies from anyone using the Reply All feature ✓.


▪ Many viruses and spam programs are able to sift through mail files and address books for email addresses ✓. Using the BCC field acts as an anti-spam precaution as it reduces the likelihood that recipients will receive spam messages ✓ or a virus from another recipient's infected computer.

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)

Many developers include other bundled programs or toolbars to subsidize costs ✓, and if you are not careful, you may install them during the download install ✓
Also, sites offering free things like cursors, fonts, wallpaper, smileys/emojis, and other small downloads ✓ may be bundled with other bad software ✓.

Level 3

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)
The USB flash drive can become infected with malware ✓ when transferring files and that could also damage backed up files ✓
The USB flash drive could be lost ✓ and your backup will be gone with it ✓
The USB flash drive could be misplaced/taken ✓ and someone could get hold of all your information/data ✓
Backup should be kept save in an alternative location ✓ such as the cloud or external drive that is locked away in a safe ✓
USB stick can easily become corrupt ✓
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)

 <https://www.takealot.com/deals/app-only>

To ensure that sending confidential information over the Internet, such as usernames, passwords, or credit card numbers, are secure ✓, look out for a lock icon ✓ or URL starting with https ✓
While the lock is in the locked position, data is encrypted ✓, which helps prevent anyone from understanding the data if it's intercepted. When no lock is visible or in the unlocked position, all information is plain text ✓ and could be read if intercepted.

29. 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 (2)
- a. Clicking Next or OK without reading or making sure nothing extra is checked (2)
Make sure you read every prompt before agreeing ✓, or you may be agreeing to install new browser toolbars, a program you didn't intend to install ✓.
- b. Opening e-mail attachments (2)
A common method of getting infected with a computer virus or malware is from opening e-mail attachments ✓. Be extremely cautious and doubtful on all e-mail attachments you receive especially if it comes from someone you do not know ✓. One of the most common tactics malicious users use to send viruses is from people you know to gain a false sense of trust.
30. 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)
Make sure the antivirus is updated before inserting it ✓
Use sandbox mode ✓
31. Downloading illegal/pirated software is one of the most common ways a computer gets infected with viruses, malware. (16)
- a. To stay safe, suggest and explain four actions to keep in mind when downloading anything (16)
- Read the screen ✓ – check for boxes ticked (that should be unticked) or warning that other software will be downloaded as well ✓

- Where are you getting the download? ✓
There are malicious people who download valid copies of a popular download, modify the file with malicious software, and then upload the file with the same name ✓. Make sure you are downloading from the developer's web page or a reputable company ✓
- Do not simply just install a download manager ✓
Many sites suggest or require you to install an installer or a download manager before allowing you to download a program you may be interested in downloading ✓. These tools can cause your computer more problems, and may even have malware or spyware ✓. Avoid any site claiming anything must be installed first before you can continue with your download ✓.
- Avoid advertisements on download pages ✓
To help make money and pay for the bandwidth costs of supplying free the software, the final download page may have ads ✓. Watch out for anything that looks like advertisements on the download page ✓. Many advertisers try to trick viewers into clicking an ad with phrases like Download Now, Start Download, or Continue and that ad may open a separate download ✓.
- Cancel or deny any automatic download ✓
Some sites may give the appearance that something needs to be installed or updated before being able to see the site or video ✓. Never accept or install anything from any site unless you know what is downloading ✓

32. 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)

You made a small, common typo when you entered the URL ✓. Fraudsters created a website identical to the online shopping one because they realised that people sometimes make this mistake when typing the URL ✓ and the incorrect URL directed you to their fraudulent website where they harvested your credit card information to use for online shopping ✓ OR
You fell victim to pharming ✓ through URL spoofing redirecting you to a fake website where they harvested your credit card information to use for online shopping
In both instances you did not check the URL or the security of the website before entering your information ✓