SUPERNOVA SCHOOL (SNS) One thing that you have learned from this worksheet.

CAMBRIDGE COMPUTING — GRADE 6

UNIT 3: NETWORKS & DIGITAL COMMUNICATION

Worksheet: Topics 3.1 and 3.2

Student's Name: _____

Class: _____ **Date:** _____

SECTION A: STORING AND TRANSFERRING DATA ON A NETWORK

Question 1: Complete the Sentences

Complete each sentence using the correct computing term. No word bank is provided.

1. The electronic exchange of information between devices is called _____.
2. Digital content can include text, images, audio, video, graphics, and _____.
3. A special computer that stores and manages data for users is called a _____.
4. A private network that is available only within an organisation is called an _____.
5. Sending audio or video content in small parts so that it can be played before the entire file arrives is called _____.
6. A network that connects devices using physical cables is known as a _____ network.
7. Wireless networks transmit data using _____ waves.
8. The maximum amount of data that can be transmitted over a network connection in a given amount of time is called _____.
9. A device that directs data between networks and allows devices to share an internet connection is called a _____.
10. A network that uses mobile communication towers to transfer data wirelessly is called a _____ network.
11. The system that uses satellites to help determine a device's location is called _____.
12. When too many devices attempt to use a network's available capacity, _____ may occur.

Question 2: Answer the Following Questions

a. What is digital communication? Give two examples of digital communication.

b. What is digital content? Name four types of digital content.

c. Explain the role of a server in a computer network.

d. What is an intranet? Give one example of how an intranet could be used in a school.

e. Explain the difference between downloading a file and streaming a video.

f. Describe two advantages of streaming content instead of downloading an entire file before playing it.

1. _____
2. _____

g. State two differences between wired and wireless networks.

Wired Network	**Wireless Network**
1. _____	1. _____
2. _____	2. _____

h. Explain how Wi-Fi allows a device to connect to a network.

i. Describe the purpose of a router in a home or school network.

---

j. Explain how a cellular network allows people to access the internet while travelling.

Question 3: Identify the Correct Networking Term

Read each description and write the correct term on the line.

1. A computer stores school documents so that authorised users can access them.
   Term: _____
2. A student watches a video online while the remaining parts of the video are still being transmitted.
   Term: _____
3. Computers in a school laboratory are connected using Ethernet cables.
   Term: _____
4. A student connects a tablet to the internet without using a physical cable.
   Term: _____
5. A school uses a private network to share information among its staff.
   Term: _____
6. A student uses a phone's mobile data connection while travelling in a car.
   Term: _____
7. A phone receives location information from satellites to help its user find directions.
   Term: _____
8. Many devices are using the internet simultaneously, causing videos and websites to load slowly.
   Term: _____

Question 4: True or False?

Write **True** or **False** beside each statement. Rewrite the false statements correctly.

1. A server can store documents, images, videos, and other digital content.

Answer: _____

Correction, if false: _____

2. An intranet is a private network used within an organisation.

Answer: _____

Correction, if false: _____

3. Streaming requires the entire video file to be downloaded before playback can begin.

Answer: _____

Correction, if false: _____

4. A wired network uses physical cables to connect devices.

Answer: _____

Correction, if false: _____

5. Wireless networks use radio waves to transmit data.

Answer: _____

Correction, if false: _____

6. GPS and cellular networks perform exactly the same function.

Answer: _____

Correction, if false: _____

7. A router can allow several devices to share an internet connection.

Answer: _____

Correction, if false: _____

8. High bandwidth generally allows more data to be transmitted in a given amount of time.

Answer: _____

Correction, if false: _____

9. Network overload can cause delays when loading websites and videos.

Answer: _____

Correction, if false: _____

10. Connecting more devices to a network will always make the internet faster.

Answer: _____

Correction, if false: _____

SECTION B: BANDWIDTH AND NETWORK OVERLOAD

Question 5: Understanding Bandwidth

a. Define bandwidth.

b. Explain the relationship between bandwidth and the amount of data that can be transmitted over a network.

c. A student is watching an online video. The video repeatedly pauses while loading.

Give two possible network-related reasons for this problem.

1.
2.

d. Explain why a network with higher available bandwidth may provide a better experience when several people are streaming videos.

e. Bandwidth is sometimes compared to the width of a road.

Explain how this comparison helps us understand network performance.

Question 6: Scenario — The Busy School Network

A school has 30 computers connected to its network. During a Computing lesson, students begin downloading large files while several teachers stream educational videos. Other students are trying to access websites for research.

Soon, the network becomes very slow.

Answer the following questions.

a. Identify the network problem described in the scenario.

b. Explain why the network has become slow.

c. Describe two symptoms that students might notice when using an overloaded network.

1.
2.

d. Suggest three ways the school could reduce network congestion.

1.
2.
3.

e. Explain why increasing the available bandwidth could improve the situation.

f. Would increasing bandwidth guarantee that the network could never become overloaded? Explain your answer.

Question 7: Apply Your Knowledge

Read each situation and select the most suitable answer.

1. A student needs a reliable connection for an online examination in a computer laboratory. Which connection would generally be the best choice?

□ A. Wired Ethernet connection
□ B. Cellular connection only
□ C. GPS connection
□ D. No network connection

2. A student wants to use a tablet while moving around the school building. Which connection is most suitable if the school provides wireless network coverage?

□ A. Ethernet cable only
□ B. Wi-Fi
□ C. GPS only
□ D. A printer connection

3. Several family members are streaming high-quality videos while other devices are downloading large files. What is the most likely result?

□ A. The available bandwidth may become insufficient for all activities.
□ B. The router will automatically create unlimited bandwidth.
□ C. All files will become smaller.
□ D. The network will stop using data.

4. Which action is most likely to reduce unnecessary network traffic?

□ A. Starting more large downloads
□ B. Streaming several videos at once
□ C. Pausing downloads that are not currently needed
□ D. Connecting every available device

5. A student wants to find directions to a museum using a navigation app. Which technology helps determine the phone's location using satellites?

□ A. Bandwidth
□ B. GPS
□ C. Ethernet
□ D. Intranet

SECTION C: NETWORK CONNECTIONS IN REAL-LIFE SITUATIONS

Question 8: Wired or Wireless?

For each scenario:

- Identify the most suitable connection: **Wired** or **Wireless**.
- Give a reason for your choice.

Scenario 1

A school computer laboratory requires stable connections for students completing programming tasks.

Connection: _____

Reason: _____

Scenario 2

A student wants to use a tablet in the school library without carrying a network cable.

Connection: _____

Reason: _____

Scenario 3

An office needs reliable connections between desktop computers that frequently transfer large files.

Connection: _____

Reason: _____

Scenario 4

A visitor wants to access the internet using a smartphone at a café that provides Wi-Fi.

Connection: _____

Reason: _____

Scenario 5

A hospital needs reliable network connections for desktop computers used to access patient records.

Connection: _____

Reason: _____

Scenario 6

A person is travelling on a bus and wants to browse the internet using mobile data.

Connection: _____

Reason: _____

SECTION D: SECURING DATA

Question 9: Complete the Sentences

Complete each sentence using the correct computing term. No word bank is provided.

1. Protecting digital information from unauthorised access, use, or theft is called _____.

2. Checking a user's identity before allowing access to a device or account is known as user _____.
3. A secret combination of characters used to protect an account is called a _____.
4. A security method that identifies a user by scanning the unique patterns on a finger is called _____ recognition.
5. A security method that uses a person's facial features to verify their identity is called _____ recognition.
6. A fraudulent attempt to trick someone into revealing personal information is called _____.
7. When someone uses another person's personal information to pretend to be that person, it is known as identity _____.
8. Changing readable data into an unreadable form to protect it is called _____.
9. A fraudulent message that appears to come from a trusted organisation may be an example of a _____ attack.
10. A secret combination of characters that is difficult to guess is an example of a _____ password.

Question 10: Why Must Data Be Kept Secure?

a. Explain why personal data needs to be protected when it is shared online.

---

b. Give three examples of sensitive information that should be kept secure.

1. ---
2. ---
3. ---

c. Explain what is meant by unauthorised access.

---

d. Describe two problems that could occur if someone's personal information were stolen.

1. ---

2. _____

e. Explain the difference between fraud and identity theft.

_____

_____

_____

f. Why is it important to keep your account login details private?

_____

_____

_____

Question 11: User Authentication

a. What is user authentication?

_____

_____

b. State three methods that can be used to authenticate a user.

1. _____
2. _____
3. _____

c. Explain how fingerprint recognition can be used to authenticate a user.

_____

_____

_____

d. Describe one advantage and one limitation of facial recognition.

Advantage: _____

_____

Limitation: _____

_____

e. Explain why a password should be difficult to guess.

_____

_____

f. A student uses the same password for their email, gaming account, and school account.

Explain why this is a security risk.

g. Is using a username and password alone an example of two-factor authentication? Explain your answer.

Question 12: Evaluate Password Strength

Examine the passwords below.

Password	Strength rating (1–5)	Reason for your rating
Arun123	_____	_____
qwerty123	_____	_____
Purple123	_____	_____
CatLoverP@ncake!492	_____	_____
Pomegranate23	_____	_____

a. Which password in the table is the strongest? Explain your choice.

b. Which password is the weakest? Give two reasons for your answer.

c. State three characteristics of a strong password.

1.
2.
3.

d. Explain why a long password made entirely from predictable words may still be vulnerable.

e. A student wants to improve a weak password. Describe three changes that could make it harder to guess.

1.
2.
3.

f. Explain why passwords should not contain easily guessed personal information, such as a name or date of birth.

g. Create an example of a strong password. Do not use your real name, birthday, or any password that you currently use.

Example password: _____

Explain two features that make your example difficult to guess.

1.
2.

SECTION E: RECOGNISING ONLINE SECURITY RISKS

Question 13: Safe or At Risk?

Read each scenario. Write **Safe** or **At Risk** and explain your answer.

Scenario 1

Ali receives an email claiming to be from his bank. It asks him to click a link and enter his account password.

Decision: _____

Reason: _____

Scenario 2

Sara posts her home address, phone number, and date of birth on a public social media account.

Decision: _____

Reason: _____

Scenario 3

Hassan uses a different, strong password for each of his important online accounts.

Decision: _____

Reason: _____

Scenario 4

Ayesha receives a message claiming she has won a free laptop. She is asked to provide her bank details to receive the prize.

Decision: _____

Reason: _____

Scenario 5

Usman receives an unexpected attachment from an unknown sender. He opens it without checking whether it is safe.

Decision: _____

Reason: _____

Scenario 6

Mariam checks the website address carefully and independently visits her bank's official website instead of clicking a suspicious link.

Decision: _____

Reason: _____

Question 14: Understanding Phishing

a. What is phishing?

b. Describe three different ways in which a phishing attack might occur.

1.

2.

3.

c. Explain why a phishing message may appear to come from a trusted person or organisation.

d. Give three warning signs that an email or message might be a phishing attempt.

1.

2.

3.

e. What should you do if you receive a suspicious message asking for your password?

f. Explain why you should not enter personal information on a website simply because it displays a padlock symbol.

SECTION F: EXTENDED SCENARIO-BASED QUESTIONS

Question 15: The School Network

SuperNova School has installed a network to help students and teachers share resources.

The network includes:

- Desktop computers in the computer laboratory.

- Laptops and tablets used by teachers.
- A central server containing learning materials.
- A printer shared by several computers.
- A wireless access point that allows mobile devices to connect.

Answer the following questions.

a. Identify the device that stores the school's shared learning materials.

b. Explain one benefit of storing learning materials on a central server rather than keeping a separate copy on every computer.

c. Which type of connection would generally be most suitable for the laboratory desktop computers: wired or wireless? Give a reason.

d. Explain how wireless connectivity benefits teachers using laptops and tablets.

e. During a busy lesson, students report that videos are buffering and websites are loading slowly.

Explain how bandwidth and network overload might contribute to this problem.

f. Suggest two actions the school could take to improve network performance.

1.
2.

g. Explain why the school should protect access to its server and shared files.

h. Recommend two security measures the school could use to protect its network and data.

1. _____

2. _____

Question 16: Protecting an Online Account

Zara uses an online learning platform to access her schoolwork. She receives an email asking her to confirm her account details through a link. The email looks official, but Zara does not recognise the sender. She also uses the same password for several websites.

Answer the following questions.

a. Identify the possible security threat in the email.

---

b. Describe two warning signs that Zara should check before trusting the email.

1. _____

2. _____

c. Explain what Zara should do instead of clicking the link.

---

d. Explain why reusing the same password on several websites is risky.

---

e. Recommend two ways Zara could improve the security of her online accounts.

1. _____

2. _____

f. Explain how user authentication helps protect Zara's schoolwork.

---

g. Zara enables fingerprint authentication on her phone. Explain how this could help protect access to her device.

SECTION G: CHALLENGE QUESTIONS

These questions require you to apply your knowledge to unfamiliar situations.

Question 17: Choose and Justify

A family has four smartphones, two laptops, a smart television, and several smart home devices connected to the same Wi-Fi network.

In the evening, everyone starts streaming videos, while one laptop downloads a large file.

a. Explain why the internet connection might become slow.

b. Identify one device or activity that could be temporarily disconnected or paused to reduce network congestion.

c. Explain why increasing the available bandwidth may improve the family's internet experience.

d. Suggest one additional action the family could take to improve network performance.

Question 18: Explain the Differences

Explain the difference between each pair of terms.

a. Server and router

b. Wired network and wireless network

c. Streaming and downloading

d. Bandwidth and network overload

e. Authentication and encryption

f. Phishing and identity theft

Question 19: A Complete Network and Security Plan

A school plans to provide students with online access to digital textbooks, videos, assignments, and research materials. Students will use desktop computers, laptops, and tablets.

The school wants the network to perform efficiently while keeping student information secure.

Write a short report explaining how the school should set up and protect its network.

Your report should include:

- The purpose of a server.
- The use of wired and wireless connections.
- The importance of bandwidth.
- The problem of network overload.
- Two ways to protect student data.
- The role of user authentication.
- One example of a possible online security threat and how to avoid it.

Your report:

One thing that you have learned from this worksheet.

SUPERNOVA SCHOOL (SNS)

CAMBRIDGE COMPUTING — GRADE 6

UNIT 3: NETWORKS & DIGITAL COMMUNICATION

Worksheet Answer Key: Topics 3.1 and 3.2

SECTION A: STORING AND TRANSFERRING DATA ON A NETWORK

Question 1: Complete the Sentences

1. Digital communication
2. Animations
3. Server
4. Intranet
5. Streaming
6. Wired
7. Radio
8. Bandwidth
9. Router
10. Cellular
11. GPS (Global Positioning System)
12. Network overload

Note: Other suitable answers may be accepted where appropriate.

Question 2: Answer the Following Questions

a. What is digital communication? Give two examples.

Digital communication is the electronic exchange of information between devices.

Examples:

- Sending an email.
- Making a video call.

b. What is digital content? Name four types.

Digital content is information that can be stored or transmitted digitally.

Examples include text, images, audio, and video.

c. Explain the role of a server in a computer network.

A server is a computer that stores and manages data and provides resources or services to other devices on a network.

d. What is an intranet? Give one school example.

An intranet is a private network used within an organisation. A school might use an intranet to share lesson plans, announcements, and learning resources with staff.

e. Explain the difference between downloading a file and streaming a video.

Downloading transfers a file to a device so that it can be stored and accessed later. Streaming sends data continuously or in small parts, allowing a video or audio file to play before the entire file has arrived.

f. Give two advantages of streaming.

1. Users can start watching or listening without waiting for the entire file to download.
2. Streaming can reduce the need to store large media files permanently on a device.

g. State two differences between wired and wireless networks.

Wired Network	Wireless Network
Uses physical cables to connect devices.	Uses radio waves to connect devices.
Usually provides a stable connection with low interference.	Allows greater mobility but may experience wireless interference.

h. Explain how Wi-Fi allows a device to connect to a network.

Wi-Fi uses radio waves to connect a device wirelessly to a local network, usually through a wireless access point or router.

i. Describe the purpose of a router.

A router directs data between networks and can share an internet connection among multiple devices.

j. Explain how a cellular network allows people to access the internet while travelling.

A cellular network uses mobile communication towers to connect a phone to the network. As the person travels, the phone can connect to different towers, allowing mobile data services to continue where coverage is available.

Question 3: Identify the Correct Networking Term

1. Server
2. Streaming
3. Wired network
4. Wireless network
5. Intranet
6. Cellular network
7. GPS
8. Network overload

Question 4: True or False?

1. **True**
2. **True**
3. **False** — Streaming allows playback to begin before the entire video has been received.
4. **True**
5. **True**
6. **False** — GPS helps determine location using satellites, while cellular networks provide mobile communication and data services.
7. **True**
8. **True**
9. **True**
10. **False** — More connected devices can increase network demand and may slow the connection.

SECTION B: BANDWIDTH AND NETWORK OVERLOAD

Question 5: Understanding Bandwidth

a. Define bandwidth.

Bandwidth is the maximum amount of data that can be transmitted over a network connection in a given amount of time.

b. Explain the relationship between bandwidth and data transmission.

Higher bandwidth allows more data to be transmitted in the same amount of time. Lower bandwidth limits the amount of data that can be transmitted.

c. Give two possible reasons for a video repeatedly pausing.

1. The available bandwidth may be too low.
2. Too many devices may be using the network at the same time.

d. Why may higher bandwidth improve streaming?

Higher bandwidth allows more data to be transmitted at a time, helping videos load more smoothly when sufficient capacity is available.

e. Explain the road comparison.

A road with more lanes can carry more traffic at once. Similarly, a network with higher bandwidth can carry more data in a given amount of time.

Question 6: Scenario — The Busy School Network

a. Identify the network problem.

Network overload or network congestion.

b. Explain why the network has become slow.

Many students and teachers are downloading large files and streaming videos simultaneously. Their combined demand may exceed the available network bandwidth.

c. Give two symptoms of network overload.

1. Videos pause or buffer repeatedly.
2. Websites and files take longer to load or download.

d. Suggest three ways to reduce network congestion.

1. Pause downloads that are not currently needed.
2. Schedule large downloads outside busy school hours.
3. Limit unnecessary high-bandwidth activities during lessons.

e. Why could increasing bandwidth help?

It would increase the amount of data the network can transmit in a given amount of time, helping it handle more simultaneous activities.

f. Would increasing bandwidth guarantee that overload could never occur?

No. Network overload could still occur if demand becomes greater than the available capacity. Other network limitations can also affect performance.

Question 7: Apply Your Knowledge

1. **A — Wired Ethernet connection**

2. **B — Wi-Fi**
3. **A — The available bandwidth may become insufficient for all activities.**
4. **C — Pausing downloads that are not currently needed**
5. **B — GPS**

SECTION C: NETWORK CONNECTIONS IN REAL-LIFE SITUATIONS

Question 8: Wired or Wireless?

Scenario 1: School computer laboratory

Connection: Wired

Reason: A wired connection generally provides a stable and reliable connection for programming tasks.

Scenario 2: Tablet in the school library

Connection: Wireless

Reason: Wi-Fi allows the student to connect without using a physical network cable.

Scenario 3: Office computers transferring large files

Connection: Wired

Reason: Ethernet connections generally provide stable, reliable data transfer and are less affected by radio interference.

Scenario 4: Smartphone at a café

Connection: Wireless

Reason: Wi-Fi allows the visitor to access the internet without connecting the phone to a cable.

Scenario 5: Hospital desktop computers

Connection: Wired

Reason: A wired network can provide a stable and reliable connection for accessing important patient records. Appropriate security measures are also required.

Scenario 6: Internet access on a bus

Connection: Wireless

Reason: A cellular network allows the person to access mobile data while travelling, provided mobile coverage is available.

Accept other suitable answers if students provide a reasonable explanation.

SECTION D: SECURING DATA

Question 9: Complete the Sentences

1. Data security
2. Authentication
3. Password
4. Fingerprint
5. Facial
6. Phishing
7. Theft
8. Encryption
9. Phishing
10. Strong

For Question 1, accept "securing data" or "data security." For Question 6, "phishing" is the expected answer.

Question 10: Why Must Data Be Kept Secure?

a. Why does personal data need protection?

Personal data needs protection because unauthorised people could steal, misuse, or share it without permission. This could lead to fraud, identity theft, or loss of privacy.

b. Give three examples of sensitive information.

1. Home address and date of birth.
2. Bank account details.
3. Medical records.

c. What is unauthorised access?

Unauthorised access occurs when someone accesses a device, account, or data without permission.

d. Give two problems caused by stolen personal information.

1. Someone could use the information to pretend to be another person.
2. Someone could use it to commit fraud or access private accounts.

e. Explain the difference between fraud and identity theft.

Fraud involves deceiving someone to gain an unfair or illegal benefit, often money. Identity theft occurs when someone uses another person's personal information to pretend to be that person.

f. Why should login details remain private?

Keeping login details private reduces the risk of unauthorised people accessing accounts, viewing personal information, or changing or deleting data.

Question 11: User Authentication

a. What is user authentication?

User authentication is the process of checking that a user is who they claim to be before allowing access to a device, system, or account.

b. State three authentication methods.

1. Password
2. Fingerprint recognition
3. Facial recognition

A PIN or security key is also acceptable.

c. How does fingerprint recognition work?

A fingerprint sensor scans the user's fingerprint and compares it with the stored reference data. If the system finds a sufficient match, it allows access.

d. Give one advantage and one limitation of facial recognition.

Advantage: It allows a user to unlock a device without typing a password.

Limitation: It may fail to recognise the user under certain conditions, or its reliability may depend on the device and system being used.

e. Why should a password be difficult to guess?

A difficult-to-guess password makes it harder for unauthorised people to access an account.

f. Why is reusing the same password risky?

If one account is compromised, someone may try the same password on the user's other accounts, putting them at risk.

g. Is a username and password alone two-factor authentication?

No. A password is one authentication factor. A username identifies the account but is not a second authentication factor. Two-factor authentication requires two different types of evidence, such as a password and a fingerprint.

Question 12: Evaluate Password Strength

Suggested ratings are provided below. Ratings may vary slightly if students justify their choices appropriately.

Password	Suggested rating (1–5)	Reason
Arun123	1	Short and predictable; contains a name and a common number sequence.
qwerty123	1	Uses a common keyboard pattern and predictable numbers.
Purple123	1	Contains a common word followed by predictable numbers.
CatLoverP@ncake!492	4	Long and contains uppercase and lowercase letters, symbols, and numbers, although its words may be predictable.
Pomegranate23	2	Longer than some examples but uses a dictionary word followed by predictable numbers.

a. Which password is strongest?

CatLoverP@ncake!492 is the strongest option in this list because it is relatively long and includes different character types. However, it is not guaranteed to be secure, particularly if its words or pattern are predictable.

b. Which password is weakest? Give two reasons.

qwerty123 is one of the weakest because:

1. It uses a common keyboard pattern.
2. It ends with a predictable number sequence.

c. State three characteristics of a strong password.

1. It is long, preferably at least 12 characters.
2. It is difficult to guess and does not contain easily guessed personal information.
3. It avoids common patterns and reused passwords.

d. Why might a long password made from predictable words be vulnerable?

Attackers can use tools that test common words and predictable combinations. Length helps, but predictability can make a password easier to guess.

e. Suggest three ways to improve a weak password.

1. Replace predictable patterns with a less predictable combination.
2. Make the password longer.
3. Use a randomly generated password or a long, unique passphrase.

f. Why should passwords avoid personal information?

Names, birthdays, and other personal details may be easy to discover or guess, making passwords based on them less secure.

g. Create a strong password and explain two features.

Example: River!Cloud7Maple#42

Features:

1. It is long and contains uppercase and lowercase letters, numbers, and symbols.
2. It does not directly use a person's name or birthday.

This is an illustrative example. Students should not adopt a password displayed in a shared worksheet as their actual password.

SECTION E: RECOGNISING ONLINE SECURITY RISKS

Question 13: Safe or At Risk?

Scenario 1: Email claiming to be from a bank

Decision: At Risk

Reason: The email may be a phishing attempt. Ali should not click the link or enter his password. He should contact the bank through an official channel if verification is needed.

Scenario 2: Sharing personal details publicly

Decision: At Risk

Reason: Strangers could misuse Sara's address, phone number, or date of birth.

Scenario 3: Using different strong passwords

Decision: Safe

Reason: Different strong passwords reduce the risk that one compromised password will put multiple accounts at risk.

Scenario 4: Message offering a free laptop

Decision: At Risk

Reason: The message may be a scam designed to steal Ayesha's bank details. She should not provide the information.

Scenario 5: Opening an unknown attachment

Decision: At Risk

Reason: The attachment could contain malware or lead to a harmful website. Usman should verify the sender and check the attachment before opening it.

Scenario 6: Visiting the official bank website independently

Decision: Safe

Reason: Mariam avoids the suspicious link and independently accesses the bank's official website. She should still verify the address carefully.

Question 14: Understanding Phishing

a. What is phishing?

Phishing is a type of online scam in which an attacker pretends to be a trusted person or organisation to trick someone into revealing information or performing an unsafe action.

b. Describe three ways phishing can occur.

1. **Email phishing:** A fake email asks the user to click a link or provide login details.
2. **Text-message phishing:** A fraudulent text contains a harmful link or requests personal information.
3. **Phone-call phishing:** A caller pretends to represent a trusted organisation to obtain private information.

Other acceptable answers include phishing through social media messages or fake websites.

c. Why might a phishing message appear trustworthy?

The sender may imitate a real organisation's name, logo, writing style, or email address to make the message appear genuine.

d. Give three warning signs of phishing.

1. Unexpected requests for passwords or financial information.

2. Suspicious links or website addresses.
3. Messages that create urgency or promise unexpected prizes.

e. What should you do if a suspicious message asks for your password?

Do not click its links or share the password. Report the message, delete it if appropriate, and verify the request through an official channel.

f. Why is a padlock symbol not enough to prove a website is trustworthy?

The padlock indicates that the connection is encrypted, but it does not guarantee that the website itself is genuine. A fraudulent website can also use an encrypted connection. Users should check the website address and confirm that the site is legitimate.

SECTION F: EXTENDED SCENARIO-BASED QUESTIONS

Question 15: The School Network

a. Identify the device that stores the school's shared learning materials.

The server.

b. Give one benefit of a central server.

It allows authorised users to access shared learning materials from different computers without keeping separate copies on every device.

c. Which connection is most suitable for laboratory desktop computers?

A wired Ethernet connection is generally suitable because it provides a stable and reliable connection.

d. How does wireless connectivity benefit teachers?

It allows teachers to connect laptops and tablets to the school network without being physically connected by network cables, making movement easier.

e. Explain how bandwidth and network overload may cause slow performance.

Bandwidth determines how much data can be transmitted in a given amount of time. If many students stream videos or download files simultaneously, their combined demand may exceed the available capacity. This can cause buffering and slow website loading.

f. Suggest two ways to improve performance.

1. Increase the available network bandwidth if the existing connection is insufficient.

2. Schedule large downloads outside busy periods or reduce unnecessary high-bandwidth activities.

g. Why should access to the server and shared files be protected?

The school needs to prevent unauthorised people from viewing, stealing, changing, or deleting important information.

h. Recommend two security measures.

1. Use strong, unique passwords and appropriate user authentication.
2. Apply suitable access permissions so users can only access the files they are authorised to use.

Other suitable measures include encryption, security updates, and reliable backups.

Question 16: Protecting an Online Account

a. Identify the possible security threat.

Phishing.

b. Give two warning signs.

1. Zara does not recognise the sender.
2. The email unexpectedly asks her to confirm account details through a link.

c. What should Zara do instead of clicking the link?

She should avoid clicking the link and access the learning platform through its official website or app. If necessary, she should contact the school or platform administrator through a trusted channel.

d. Why is reusing passwords risky?

If one account is compromised, an attacker may try the same password on Zara's other accounts.

e. Recommend two ways to improve account security.

1. Use a different, strong password for each account.
2. Enable multi-factor authentication where available.

f. How does authentication protect Zara's schoolwork?

Authentication checks a user's identity before allowing access, helping prevent unauthorised people from viewing or changing her schoolwork.

g. How can fingerprint authentication help?

The device compares Zara's fingerprint with stored reference data. If it matches sufficiently, the device allows access, reducing reliance on a password alone.

SECTION G: CHALLENGE QUESTIONS

Question 17: Choose and Justify

a. Why might the internet connection become slow?

Many devices are streaming videos and downloading a large file at the same time. The combined demand may exceed the available bandwidth.

b. Identify one activity that could be paused.

The large file download could be paused until the network is less busy.

c. Why could increasing bandwidth help?

It would increase the amount of data that can be transmitted in a given amount of time, allowing the network to handle more simultaneous activities.

d. Suggest one additional way to improve performance.

Schedule large downloads for quieter periods or stop unnecessary streaming activities.

Question 18: Explain the Differences

a. Server and router

A server stores and manages data or provides services to other devices. A router directs data between networks and can share an internet connection.

b. Wired and wireless networks

A wired network connects devices using physical cables. A wireless network uses radio waves to connect devices without physical network cables.

c. Streaming and downloading

Streaming allows content to play while data is being received. Downloading transfers a file to a device for storage and later access.

d. Bandwidth and network overload

Bandwidth is the maximum amount of data that can be transmitted over a connection in a given amount of time. Network overload occurs when demand on the network exceeds its available capacity.

e. Authentication and encryption

Authentication checks whether a user is who they claim to be. Encryption changes readable data into a protected form so that unauthorised people cannot easily understand it.

f. Phishing and identity theft

Phishing is an attempt to trick someone into revealing information or performing an unsafe action. Identity theft occurs when someone uses another person's personal information to pretend to be them.

Question 19: A Complete Network and Security Plan

Sample Answer

A school can use a server to store digital textbooks, videos, assignments, and research materials. This allows authorised students and teachers to access shared resources.

Wired Ethernet connections can be used for desktop computers because they generally provide stable and reliable connections. Wi-Fi can be provided for laptops and tablets so that students and teachers can connect without network cables.

The school should ensure that sufficient bandwidth is available to support its users. If too many students stream videos or download large files at the same time, network overload may occur. The school can reduce congestion by scheduling large downloads outside busy hours and upgrading the network connection if necessary.

Student data must be protected from unauthorised access. The school should use strong passwords, appropriate user authentication, and access permissions. Encryption can also help protect sensitive information.

Phishing is one possible online security threat. Students should avoid suspicious links, never share passwords through unexpected messages, and access learning platforms through official websites or apps.

These measures can help the school maintain an efficient network while protecting student information.

TEACHER'S MARKING NOTES

- Accept alternative answers when they demonstrate correct computing knowledge.
- Award credit for appropriate examples and clear explanations.
- In scenario-based questions, accept different connection choices when the student provides a technically sound justification.

- In password questions, treat the numerical ratings as suggested judgements rather than absolute security measurements.
- In Question 19, assess whether students explain the key concepts and apply them appropriately to the school scenario.
- For security questions, distinguish between **authentication** (verifying identity), **encryption** (protecting the meaning of data), and **phishing** (tricking users into disclosing information or taking unsafe actions).

End of Answer Key