UNIT 1

Cyber Crime – MCQ Questions

---

1. What is cyber crime?
a) Crime related to roads
b) Crime using weapons
c) Crime involving computers and internet
d) Crime committed by police
✓ **Answer:** c) Crime involving computers and internet

---

2. Which of the following is NOT a cyber crime?
a) Cyberbullying
b) Hacking
c) Robbing a bank physically
d) Identity theft
✓ **Answer:** c) Robbing a bank physically

---

3. Which term refers to sending fake emails to steal information?
a) Hacking
b) Malware
c) Phishing
d) Debugging
✓ **Answer:** c) Phishing

---

4. What is the full form of OTP?
a) One True Password
b) Online Time Pass
c) One-Time Password
d) Open Technical Program
✓ **Answer:** c) One-Time Password

---

5. Cyber crime can be committed:
a) Only in India
b) Only in large cities
c) From any part of the world
d) Only by software engineers
✅ **Answer:** c) From any part of the world

---

6. What is a Trojan Horse in cyber crime?
a) A military tool
b) A software that entertains
c) Malicious software disguised as useful software
d) A type of antivirus
✅ **Answer:** c) Malicious software disguised as useful software

---

7. Which of the following is used to prevent unauthorized access to a computer network?
a) Keyboard
b) Monitor
c) Firewall
d) Printer
✅ **Answer:** c) Firewall

---

8. Which one is a cyber security measure?
a) Leaving password on sticky note
b) Using strong passwords
c) Sharing passwords on social media
d) Ignoring software updates
✅ **Answer:** b) Using strong passwords

---

9. Identity theft means:
a) Using someone's identity for criminal activity
b) Printing ID cards
c) Saving contact details
d) Deleting files
✅ **Answer:** a) Using someone's identity for criminal activity

---

10. Cyberbullying is mainly done through:
a) Face-to-face meeting
b) Online platforms
c) Newspapers
d) Radio
✅ **Answer:** b) Online platforms

---

11. Which device is most commonly used in cyber crime?
a) Refrigerator
b) Air conditioner
c) Computer
d) Fan
✅ **Answer:** c) Computer

---

12. The act of illegally copying software is called:
a) Phishing
b) Piracy
c) Debugging
d) Networking
✅ **Answer:** b) Piracy

---

13. What is malware?
a) Helpful software
b) Security tool
c) Malicious software

d) Anti-virus
✅ **Answer:** c) Malicious software

---

14. What do cyber criminals usually want?
a) Friendship
b) Money, data, or control
c) To help others
d) To promote safety
✅ **Answer:** b) Money, data, or control

---

15. Which of these helps protect against cyber crime?
a) Ignoring suspicious emails
b) Clicking unknown links
c) Downloading from untrusted websites
d) Using simple passwords
✅ **Answer:** a) Ignoring suspicious emails

MCQs on History of the Internet (20 Questions)

1. Who is known as the "Father of the Internet"?

A. Bill Gates
B. Tim Berners-Lee
C. Vint Cerf
D. Steve Jobs
✓ **Answer: C. Vint Cerf**

---

2. What was the name of the first network that led to the development of the Internet?

A. WWW
B. ARPANET
C. Ethernet

D. Bitnet
✓ **Answer: B. ARPANET**

---

3. In which year was ARPANET launched?

A. 1965
B. 1969
C. 1975
D. 1983
✓ **Answer: B. 1969**

---

4. Who invented the World Wide Web (WWW)?

A. Vint Cerf
B. Steve Jobs
C. Tim Berners-Lee
D. Mark Zuckerberg
✓ **Answer: C. Tim Berners-Lee**

---

5. What does TCP/IP stand for?

A. Transfer Control Protocol / Internal Protocol
B. Transmission Control Protocol / Internet Protocol
C. Total Control Process / Internet Provider
D. Technical Communication Protocol / Inter Packet
✓ **Answer: B. Transmission Control Protocol / Internet Protocol**

---

6. When was the World Wide Web (WWW) introduced to the public?

A. 1989
B. 1990
C. 1991
D. 1995
✓ **Answer: C. 1991**

---

7. What was the first message ever sent over ARPANET?

A. Hello
B. Log in

C. Login
D. LO
✓ **Answer: D. LO**

---

8. What is the full form of ISP?

A. Internet Source Provider
B. Internet Service Provider
C. Internal Server Protocol
D. International System Provider
✓ **Answer: B. Internet Service Provider**

---

9. Which organization manages domain names on the Internet?

A. ICANN
B. W3C
C. IETF
D. UN
✓ **Answer: A. ICANN**

ICANN stands for **Internet Corporation for Assigned Names and Numbers**.

---

10. The first email was sent in which year?

A. 1971
B. 1980
C. 1969
D. 1990
✓ **Answer: A. 1971**

---

11. Who sent the first email?

A. Vint Cerf
B. Ray Tomlinson
C. Tim Berners-Lee
D. Larry Page
✓ **Answer: B. Ray Tomlinson**

---

12. What was the name of the first graphical web browser?

A. Internet Explorer
B. Netscape Navigator
C. Mosaic
D. Mozilla
✓ **Answer: C. Mosaic**

---

13. Which protocol is used to transfer web pages on the internet?

A. FTP
B. SMTP
C. HTTP
D. TCP
✓ **Answer: C. HTTP**

---

14. The Internet became widely available to the public in:

A. 1975
B. 1985
C. 1990
D. 1995
✓ **Answer: D. 1995**

---

15. Which of the following is *not* an internet protocol?

A. HTTP
B. TCP
C. FTP
D. PDF
✓ **Answer: D. PDF**

---

16. What does URL stand for?

A. Uniform Research Link
B. Unique Resource Locator
C. Uniform Resource Locator
D. Unified Reference Link
✓ **Answer: C. Uniform Resource Locator**

---

17. The term "Internet" is derived from:

A. Interconnect Technology
B. Internal Network
C. International Net
D. Interconnected Networks
✓ **Answer: D. Interconnected Networks**

---

18. The first website was published in:

A. 1989
B. 1991
C. 1993
D. 1995
✓ **Answer: B. 1991**

---

19. The World Wide Web was developed at:

A. NASA
B. CERN
C. Microsoft
D. MIT
✓ **Answer: B. CERN**

---

20. Which one of the following is responsible for setting standards for the World Wide Web?

A. IETF
B. ICANN
C. W3C
D. ISOC
✓ **Answer: C. W3C**

The **World Wide Web Consortium (W3C)** is the **main international standards organization** responsible for developing **web standards**.

🔐 Cyber Crime – MCQs with Explanations

1. What is cyber crime?

A. Crime related to space
B. Crime using computers and the internet ✅
C. Crime in real life
D. Crime using weapons
📝 **Explanation:** Cyber crime involves illegal activities carried out using computers or the internet — such as hacking, phishing, identity theft, etc.

---

2. Which of the following is a type of cyber crime?

A. Housebreaking
B. Cyber bullying ✅
C. Pickpocketing
D. Chain snatching
📝 **Explanation:** Cyber bullying is an online threat or harassment using digital platforms like social media, chat apps, etc.

---

3. Which Indian law deals with cyber crime?

A. Indian Penal Code
B. Information Technology Act, 2000 ✅
C. Cyber Crime Law, 1995
D. Digital Crime Act, 2005
📝 **Explanation:** The **IT Act 2000** is India's primary law dealing with cyber crimes and electronic commerce.

---

4. Phishing is:

A. Fishing in water
B. Sending fake emails to steal data ✅
C. Repairing software
D. None of the above
📝 **Explanation:** Phishing tricks users into providing personal or financial details by pretending to be a trusted entity via email.

---

5. Which is a financial cyber crime?

A. ATM fraud
B. Online banking fraud
C. Credit card fraud
D. All of the above ✅
📝 **Explanation:** All listed crimes involve unauthorized financial transactions or data theft, making them financial cyber crimes.

---

6. What is hacking?

A. Legal access to a website
B. Unauthorized access to a computer system ✅
C. Making software
D. Protecting data
📝 **Explanation:** Hacking means breaking into computer systems without permission, often to steal or damage data.

---

7. Cyber stalking involves:

A. Sending flowers
B. Following someone online continuously ✅
C. Playing games
D. Watching movies
📝 **Explanation:** Cyber stalking is online harassment involving following or threatening someone through digital means.

---

8. Spamming refers to:

A. Deleting files
B. Sending multiple unwanted emails ✅
C. Hacking websites
D. Sending viruses
📝 **Explanation:** Spamming floods users with irrelevant or unwanted emails, often containing ads or malware.

---

9. Cyber terrorism affects:

A. Personal accounts
B. Government & national security ✓
C. Online shopping
D. Entertainment
📝 **Explanation:** Cyber terrorism involves using the internet to attack government systems, military networks, or critical infrastructure.

---

10. The act of using another person's email or identity is known as:

A. Phishing
B. Spoofing ✓
C. Spamming
D. Cracking
📝 **Explanation:** Spoofing tricks the recipient into believing a message is from a trusted source by faking email headers or identities.

---

11. Which of the following is NOT a cyber crime?

A. Phishing
B. Hacking
C. Robbery ✓
D. Spamming
📝 **Explanation:** Robbery is a physical-world crime, not involving digital systems.

---

12. Who sent the first email?

A. Vint Cerf
B. Ray Tomlinson ✓
C. Tim Berners-Lee
D. Larry Page
📝 **Explanation:** Ray Tomlinson sent the first email in 1971 and introduced the use of “@” in email addresses.

---

13. Which government body investigates cyber crimes in India?

A. RBI
B. TRAI
C. CERT-In ✅
D. CBSE
📝 **Explanation: CERT-In (Indian Computer Emergency Response Team)** handles cybersecurity threats and incidents in India.

---

14. What is software piracy?

A. Legal use of software
B. Watching movies online
C. Illegal copying and distribution of software ✅
D. Using pirated CDs
📝 **Explanation:** Software piracy is using or distributing software without a legal license.

---

15. Cyber defamation is a crime against:

A. Government
B. Property
C. Person ✅
D. Nation
📝 **Explanation:** Cyber defamation harms a person's reputation by spreading false information online.

🔐 Information Security – MCQs with Answers & Explanation

Q1. **Which of the following is** not **a component of the CIA Triad?**

A. Confidentiality
B. Integrity
C. Authentication
D. Availability
✅ **Answer:** C. Authentication
📝 **Explanation:** The CIA triad includes **Confidentiality, Integrity, and Availability**. Authentication is a separate concept related to verifying identity.

Q2. **What is the main goal of confidentiality in information security?**

A. Ensuring data accuracy
B. Preventing unauthorized access
C. System availability
D. Detecting cyber threats

✅ **Answer:** B. Preventing unauthorized access

📝 **Explanation:** Confidentiality ensures that sensitive information is accessed **only by authorized individuals** and protected from others.

Q3. **A** brute-force attack **is related to:**

A. Flooding the server
B. Guessing passwords
C. Sending phishing emails
D. Injecting malware

✅ **Answer:** B. Guessing passwords

📝 **Explanation:** In brute-force attacks, attackers try **all possible combinations** of passwords until the correct one is found.

Q4. **Which of the following is a** passive attack**?**

A. Phishing
B. Eavesdropping
C. Ransomware
D. SQL Injection

✅ **Answer:** B. Eavesdropping

📝 **Explanation:** Passive attacks involve **monitoring** data transmission without altering it. Eavesdropping is a classic example.

Q5. **Which is** not **a type of malware?**

A. Worm
B. Trojan
C. Firewall
D. Ransomware

✅ **Answer:** C. Firewall

📝 **Explanation:** Firewall is a **security tool**, not malware. Worms, Trojans, and Ransomware are malicious programs.

Q6. **What is the purpose of** encryption**?**

A. To delete data
B. To store data
C. To protect data by converting it into unreadable form
D. To compress files

✅ **Answer:** C. To protect data by converting it into unreadable form

📝 **Explanation:** Encryption transforms readable data (plaintext) into unreadable form (ciphertext) to **prevent unauthorized access**.

Q7. **A firewall is used to:**

A. Speed up internet
B. Prevent data corruption
C. Filter incoming and outgoing traffic
D. Store data securely

✅ **Answer:** C. Filter incoming and outgoing traffic

📝 **Explanation:** A firewall monitors and controls network traffic to **block unauthorized access** and protect internal systems.

Q8. **Which of the following best describes** integrity**?**

A. Availability of system to users
B. Ensuring data is not altered
C. Hiding data from users
D. Encrypting the data

✅ **Answer:** B. Ensuring data is not altered

📝 **Explanation:** Data integrity means the information remains **accurate and unchanged** during transmission or storage.

Q9. **Which of the following is an example of** social engineering**?**

A. Denial-of-service attack
B. Phishing email
C. Keylogger
D. Man-in-the-middle attack

✅ **Answer:** B. Phishing email

📝 **Explanation:** Phishing is a **social engineering** tactic where attackers trick users into giving sensitive information like passwords.

Q10. **In cryptography,** plaintext **refers to:**

A. Encrypted message
B. Hidden message
C. Original message before encryption
D. Key used in encryption

✅ **Answer:** C. Original message before encryption

📝 **Explanation:** Plaintext is the **original readable message** before it is encrypted into ciphertext.

Q11. **What does** two-factor authentication (2FA) **require?**

A. Password only
B. Two different IP addresses
C. Password and one more verification method
D. Two passwords

✅ **Answer:** C. Password and one more verification method

📝 **Explanation:** 2FA adds an extra layer of security by requiring **something you know (password)** and **something you have (OTP, phone, etc.)**.

Q12. **Which Indian Act governs cybercrime and electronic commerce?**

A. Indian Penal Code
B. IT Act 2000
C. Data Protection Act
D. Copyright Act

✅ **Answer:** B. IT Act 2000

📝 **Explanation:** The **Information Technology (IT) Act 2000** is India's main law for **cybercrime, digital contracts**, and e-governance.

Q13. **What is** ransomware**?**

A. Antivirus software
B. Program that steals passwords
C. Malware that locks systems and demands payment
D. Data compression tool

✅ **Answer:** C. Malware that locks systems and demands payment

📝 **Explanation:** Ransomware **encrypts or blocks access** to a system and demands a **ransom** from the user to unlock it.

Q14. **Which of the following is the** strongest password**?**

A. password123
B. abcde
C. QwEr@321#
D. myname123

✅ **Answer:** C. QwEr@321#

📝 **Explanation:** Strong passwords include a mix of **uppercase, lowercase, symbols, and numbers**. Avoid dictionary words and patterns.

Q15. **Which of the following terms describes making sure only authorized users have access to data?**

A. Availability
B. Confidentiality
C. Encryption
D. Backup

✅ **Answer:** B. Confidentiality

📝 **Explanation:** Confidentiality is about **limiting access** to sensitive information only to people who are authorized.

Computer Ethics & Security Policies

Q1. What is computer ethics?

A. Rules for playing games
B. Rules for using computers correctly
C. Internet speed control
D. Fixing hardware

✅ **Answer:** B. Rules for using computers correctly

📝 **Explanation:** Computer ethics means following **right and fair rules** when using computers.

Q2. Is it okay to copy someone's code or file without permission?

A. Yes
B. No

✅ **Answer:** B. No

📝 **Explanation:** It is **unethical** to copy or use someone's work without asking or giving credit.

Q3. What is the purpose of a security policy?

A. To play games
B. To protect computers and data
C. To format the PC
D. To delete files

✅ **Answer:** B. To protect computers and data

📝 **Explanation:** A security policy helps in keeping **data safe and systems secure**.

Q4. Which one is an ethical action?

A. Sharing passwords
B. Using original (licensed) software
C. Sending viruses
D. Hacking into accounts

✅ **Answer:** B. Using original (licensed) software

📝 **Explanation:** Using **legal and genuine software** is a good ethical practice.

Q5. What does AUP (Acceptable Use Policy) mean?

A. Rules for using computers and internet properly
B. Rules for driving
C. Rules for cooking
D. Rules for mobile usage

✅ **Answer:** A. Rules for using computers and internet properly

📝 **Explanation:** AUP tells us **what we can or cannot do** on school/office computers.

Q6. What should you do if you see someone doing something wrong on a computer?

A. Ignore it
B. Help them do it
C. Report to teacher or boss
D. Take a screenshot and share

✅ **Answer:** C. Report to teacher or boss

📝 **Explanation:** If someone is doing something wrong, we should **inform the authority**.

Q7. What is plagiarism?

A. Making videos

B. Copying others' work and saying it's yours
C. Writing code
D. Creating a website

✅ **Answer:** B. Copying others' work and saying it's yours

📝 **Explanation:** Plagiarism means **stealing someone's idea or work** without giving credit.

Q8. Which is an example of unethical use of computers?

A. Sending good emails
B. Watching educational videos
C. Hacking someone's account
D. Making a presentation

✅ **Answer:** C. Hacking someone's account

📝 **Explanation:** Hacking is a **wrong and illegal use** of computers.

Q9. What is the best way to keep your password safe?

A. Share with friends
B. Write on desk
C. Keep it secret
D. Post it online

✅ **Answer:** C. Keep it secret

📝 **Explanation:** Passwords should be **kept private** to stay secure.

Q10. Who needs to follow computer ethics and security policies?

A. Only hackers
B. Only police
C. Everyone who uses a computer
D. Only teachers

✅ **Answer:** C. Everyone who uses a computer

📝 **Explanation:** Whether student, teacher or employee, **everyone** should follow ethics and policies.

Email Security & Web Browser Security

Email Security (1–8)

Q1. What is phishing?

A. Fishing in sea
B. Sending jokes
C. Sending fake emails to steal information
D. Sending music files

✅ **Answer:** C

📝 **Explanation:** Phishing means sending **fake-looking emails** to steal your data like passwords or bank details.

Q2. Which of the following is a sign of a phishing email?

A. Your name spelled correctly
B. Unknown sender and urgent message
C. Message from a friend
D. No spelling mistakes

✅ **Answer:** B

📝 **Explanation:** Phishing emails often have **urgent tone**, unknown senders, and suspicious links.

Q3. What is the best way to deal with a spam email?

A. Reply to it
B. Share it
C. Delete or report it
D. Save it

✅ **Answer:** C

📝 **Explanation: Never interact** with spam emails — just delete or report them.

Q4. Which password is safest for email?

A. 12345
B. yourname
C. M@ni$h#2025
D. abcabc

✅ **Answer:** C
📝 **Explanation:** A **strong password** has capital letters, numbers, and special characters.

Q5. What is the risk of clicking unknown email attachments?

A. It might not open
B. It may slow internet
C. It can contain viruses
D. It may delete emails
✅ **Answer:** C
📝 **Explanation:** Attachments from unknown senders may install **malware** on your computer.

Q6. What is a safe practice for email use?

A. Share password with friends
B. Open all links
C. Logout after using public computer
D. Keep inbox full
✅ **Answer:** C
📝 **Explanation:** Always **log out** from your account, especially on public devices.

Q7. Which of the following is an example of email spoofing?

A. Sending jokes
B. Receiving email from someone who didn't send it
C. Receiving OTP
D. Email from your college
✅ **Answer:** B
📝 **Explanation:** Email spoofing means an email **appears to be from a known sender**, but it's fake.

Q8. What does two-factor authentication (2FA) do for email?

A. Deletes inbox
B. Sends spam
C. Adds extra security using OTP
D. Slows the internet
✅ **Answer:** C
📝 **Explanation:** 2FA adds an extra step like **OTP or code**, making your account safer.

🌐 Web Browser Security (9–15)

Q9. What does the 🔒 padlock symbol in the browser mean?

A. Website is broken
B. Secure (HTTPS) connection
C. Download in progress
D. Unsafe site

✅ **Answer:** B

📝 **Explanation:** Padlock shows that the site is using **secure HTTPS connection**.

Q10. Why should you keep your web browser updated?

A. It looks better
B. For more games
C. To fix bugs and improve security
D. To delete data

✅ **Answer:** C

📝 **Explanation:** New versions of browsers **fix security issues** and protect from threats.

Q11. What does Incognito/Private mode do?

A. Speeds up browsing
B. Hides your history
C. Blocks the internet
D. Adds games

✅ **Answer:** B

📝 **Explanation:** Incognito mode **doesn't save** your browsing history or cookies.

Q12. What is a malicious extension in a browser?

A. Free antivirus
B. Extra tab
C. Harmful add-on that steals info
D. Internet booster

✅ **Answer:** C

📝 **Explanation:** Some browser extensions are **unsafe** and may track or steal your data.

Q13. What is the purpose of clearing cookies and cache?

A. Save battery
B. Play games
C. Remove saved data and improve privacy
D. Hide tabs

✅ **Answer:** C

📝 **Explanation:** Clearing cookies removes **saved site data** and improves privacy.

Q14. Which one is a secure web address?

A. http://shopping.com
B. ftp://mydata.net
C. https://bank.com
D. xyz@site

✅ **Answer:** C

📝 **Explanation:** HTTPS means **secure site**, useful for login or payment.

Q15. Which is a good practice to stay safe while browsing?

A. Click all pop-ups
B. Use same password everywhere
C. Avoid suspicious sites and ads
D. Share browser history

✅ **Answer:** C

📝 **Explanation:** Avoid clicking on **unknown or suspicious sites**, they may contain malware.

Antivirus, Password Security & Wi-Fi Security (MCQs)

1. What is the primary purpose of antivirus software?

A. Improve internet speed
B. Scan and remove malicious software
C. Update the operating system
D. Backup data

✅ **Answer: B**

---

2. Which of the following is NOT a type of malware?

A. Worm
B. Trojan
C. Firewall
D. Ransomware
✅ **Answer: C**

---

3. What does a strong password usually contain?

A. Only lowercase letters
B. Numbers only
C. Combination of uppercase, lowercase, numbers, and symbols
D. Only your name and birthdate
✅ **Answer: C**

---

4. Which one of these is a good password practice?

A. Use your pet's name
B. Use "12345678"
C. Change your password regularly
D. Use the same password everywhere
✅ **Answer: C**

---

5. Which of the following best protects your Wi-Fi network?

A. Keeping it open for guests
B. Using WPA3 encryption
C. Sharing password with everyone
D. Turning off the router every night
✅ **Answer: B**

---

6. What does WPA stand for in Wi-Fi security?

A. Wireless Protected Access
B. Wi-Fi Private Access
C. Wired Protected Access
D. Web Protected Access
✅ **Answer: A**

---

7. Which of the following passwords is the most secure?

A. Password123
B. Manish@2020
C. Welcome123
D. !G#rT7&bL
✅ **Answer: D**

---

8. What is the risk of using public Wi-Fi without a VPN?

A. Fast internet
B. No risk at all
C. High chance of data theft or eavesdropping
D. Improved signal strength
✅ **Answer: C**

---

9. Antivirus software should be updated regularly because...

A. It looks good
B. It cleans the disk
C. New viruses are created regularly
D. It increases battery life
✅ **Answer: C**

---

10. Which of the following is NOT a feature of antivirus software?

A. Real-time protection
B. Software development
C. Malware removal
D. Scheduled scanning
✅ **Answer: B**

---

11. What is brute force attack related to passwords?

A. Virus spreading attack
B. Guessing password using all combinations
C. Sending spam emails
D. Blocking Wi-Fi access
✅ **Answer: B**

---

12. Why should you avoid using the same password for multiple accounts?

A. It takes time to remember
B. It may confuse hackers
C. If one account is hacked, others are at risk too
D. It improves security
✅ **Answer: C**

---

13. Which one is a basic Wi-Fi security recommendation?

A. Use open network
B. Disable encryption
C. Change default router password
D. Share password with neighbors
✅ **Answer: C**

---

14. What is the function of a firewall in Wi-Fi networks?

A. Boost internet speed
B. Filter incoming and outgoing traffic
C. Increase download size
D. Disconnect users randomly
✅ **Answer: B**

---

15. What is two-factor authentication (2FA)?

A. Logging in twice
B. Using password and another verification step
C. Using only fingerprint
D. Using only password
✅ **Answer: B**

Topic: Two-Factor Authentication (2FA) & Password Manager – MCQs

1. What does 2FA stand for?

A. Two-Firewall Authentication
B. Two-Factor Authentication
C. Two-Form Access
D. Token-Free Access
✅ **Answer: B**

---

2. What is the purpose of Two-Factor Authentication?

A. To make login faster
B. To add an extra layer of security
C. To share password with friends
D. To connect to public Wi-Fi
✅ **Answer: B**

---

3. Which of the following is an example of 2FA?

A. Entering username only
B. Using password only

C. Entering password and receiving OTP on phone
D. Using browser cookies
✅ **Answer: C**

---

4. What are the common second factors in 2FA?

A. Date of birth
B. One-Time Password (OTP), fingerprint, security key
C. Email ID
D. Mother's maiden name
✅ **Answer: B**

---

5. Why is 2FA better than just using a password?

A. Passwords are usually strong
B. It avoids software updates
C. It reduces the risk of unauthorized access
D. It keeps the screen locked
✅ **Answer: C**

---

6. What is a password manager used for?

A. Sharing passwords
B. Generating and storing strong passwords
C. Reducing internet usage
D. Changing passwords daily
✅ **Answer: B**

---

7. Which of the following is a benefit of using a password manager?

A. Uses same password for all sites
B. Stores passwords in plain text
C. Remembers complex and unique passwords
D. Ignores weak passwords
✅ **Answer: C**

---

8. Which of these is a trusted password manager?

A. Chrome Notepad
B. LastPass
C. Notepad++
D. WordPad
✅ **Answer: B**

---

9. Where does a password manager usually store the passwords?

A. On a sticky note
B. On an unencrypted USB
C. In an encrypted vault/database
D. In email drafts
✅ **Answer: C**

---

10. What is the master password in a password manager?

A. Password for bank account
B. Password to access all stored passwords
C. Password for Wi-Fi
D. Any random password
✅ **Answer: B**