NIELIT

cccguru.in
Visit Website for Online Test Series

CCC

Course on Computer Concepts

हिंदी & English

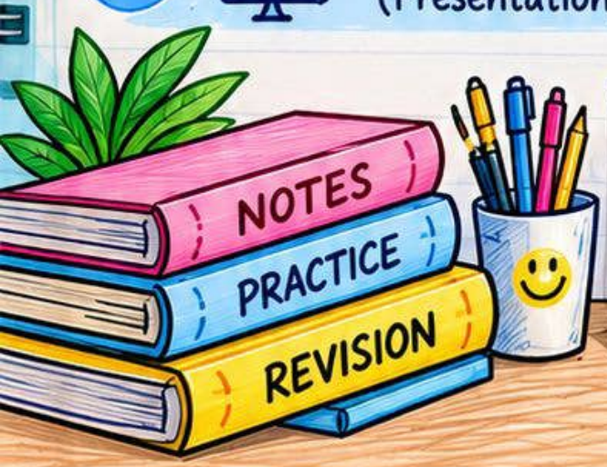
NIELIT CCC EXAM 2026

Quick Revision Notes

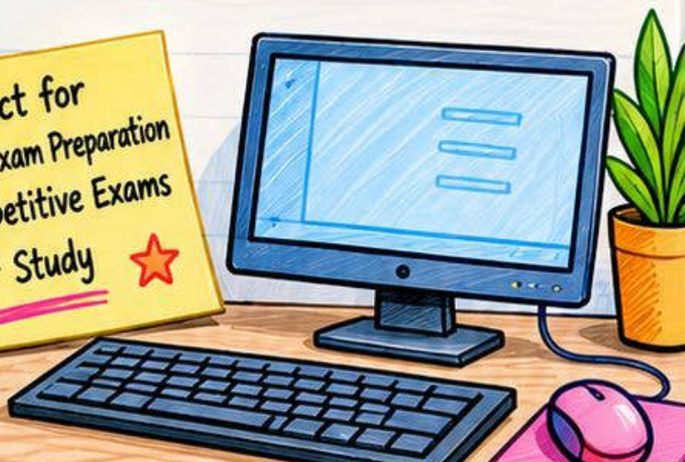
- Short Notes
- Important Points
- Key Definitions
- Diagrams & Tables
- Exam Oriented

Chapter-wise Complete Study Notes

1. Introduction to Computer & Hardware
2. Operating Systems (GUI)
3. LibreOffice Writer (Word Processing)
4. LibreOffice Calc (Spreadsheet)
5. LibreOffice Impress (Presentation)
6. Internet & Web Browsing
7. E-mail, Social Media & E-Governance
8. Digital Financial Tools & Banking
9. Cyber Security & Future Skills



- Perfect for
- CCC Exam Preparation
- Competitive Exams
- Self Study



Chapter - 9

साइबर सुरक्षा का परिचय

(Overview of Cyber Security)



1 Cyber Security - Introduction

Cyber Security क्या है ?

- Computer, Mobile, Network और Data को Online खतरों, चोरी और बिना Permission Access से सुरक्षित रखना Cyber Security कहलाता हैं।

Example: Gmail Account कों Strong Password और 2FA से सुरक्षित रखना।

2 Important Terms

- **Cyber Attack:** Computer या Data पर हमला करने की कोशिश।
- **Cyber Crime:** Internet या Computer से किया जाने वाला अपराध।
- **Hacker:** Computer Security की जाँच करने या उसमें प्रवेश करने वाला व्यक्ति। यह काम अनुमति के साथ या बिना अनुमति भी हो सकता हैं।
- **Unauthorized Access:** बिना Permission किसी Account या Data को खोलना।

3 Cyber Threats

- **Malware:** नुकसान पहुँचाने वाला Software।
- **Virus:** Files या Programs को Infect करने वाला Malware।
- **Worm:** अपने आप फैलने वाला Malware।
- **Trojan Horse:** असली Software जैसा दिखने वाला खतरनाक Program।
- **Ransomware:** Files Lock करके पैसे माँगने वाला Malware।
- **Spyware:** चोरी-छिपे जानकारी इकट्ठा करने वाला Software।

4 Exam Facts

- **Malware** = Malicious Software.
- **Ransomware** = Files Lock + Ransom Demand.
- **Worm** = Self-Replicating Malware.

cocguru.in

2 Need and Goal of Cyber Security

Cyber Security की जरूरत

1. Personal Data सुरक्षित रखने के लिए।
2. Online Banking Fraud से बचने के लिए।
3. Computer और Mobile को Malware से बचाने के लिए।
4. Email और Social Media Accounts सुरक्षित रखने के लिए।
5. Password और जरूरी Files की चोरी रोकने के लिए।
6. Online Services सुरक्षित रखने के लिए।

Cyber Security के 3 Goals

CIA Triad

- **Confidentiality** (Privacy)
- **Integrity** (Data सही रखना)
- **Availability** (Data उपलब्ध होना)

1 Confidentiality (Privacy)

- Data केवल Authorized व्यक्ति ही देख सके।

Example: Password से Personal Files सुरक्षित रखना।

2 Integrity (Data सही रखना)

- बिना Permission कोई Data बदल न सके।

Example: Student के Marks में गलत बदलाव रोकना।

3 Availability (Data उपलब्ध होना)

- जरूरत पड़ने पर Data और Services उपलब्ध रहें।

Example: Banking Website का काम करना।

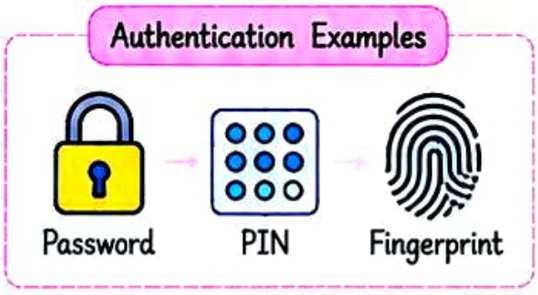
Exam Point: CIA = Confidentiality, Integrity, Availability।

3. Basic Security Concepts

1 Authentication (पहचान सत्यापन)

- User की पहचान Verify करना
- यह सुनिश्चित करता हैं कि आप वही हैं, जैसा आप दावा करते हैं।

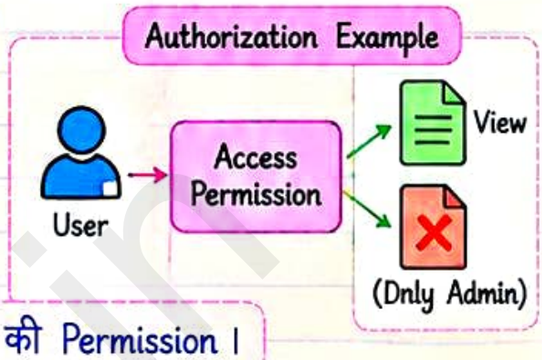
उदाहरण: Password, PIN या Fingerprint।



2 Authorization (अनुमति प्रदान करना)

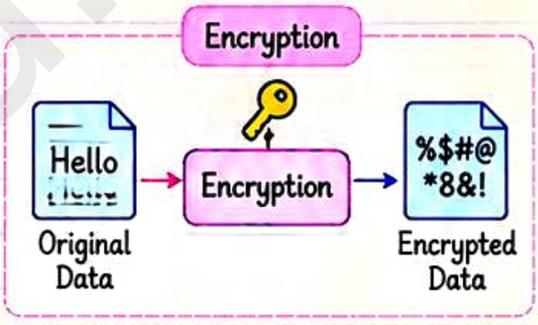
- User को यह Permission देना कि वह क्या Access कर सकता हैं।
- हर User को सभी काम करने की अनुमति नहीं होती हैं।

उदाहरण: केवल Admin को File Delete करने की Permission।



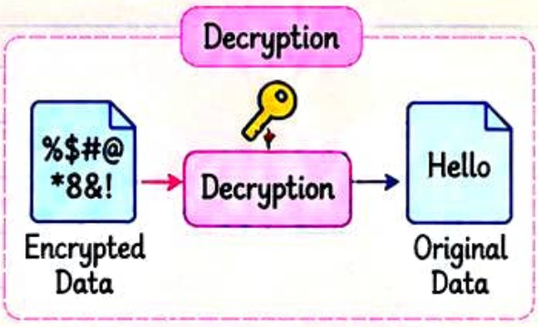
3 Encryption (एनक्रिप्शन)

- Data को ऐसे सुरक्षित रूप में बदलना जिसे सही Key के बिना पढ़ना मुश्किल हो।
- यह Data को चोरी या बिना अनुमति Access से सुरक्षित रखता हैं।



4 Decryption (डीक्रिप्शन)

- Encrypted Data को वापस पढ़ने योग्य रूप में बदलना।
- इसके लिए सही Key की आवश्यकता होती हैं।



5 Strong Password (मजबूत पासबर्ड)

- लंबा और Unique Password रखें।
- अलग-अलग Accounts में अलग Password रखें।
- Password किसी को न बताएँ।



Quick Difference (त्वरित अंतर)

Term	Meaning
Authentication	पहचान Check करना
Authorization	Permission देना
Encryption	Data को सुरक्षित Code में बदलना
Decryption	Data को पढ़ने योग्य बनाना

Exam Point: Password और Fingerprint, Authentication के उदाहरण हैं।

ccguru.in

4. Securing PC


PC Security

PC Security :

Computer को Malware, Data Theft और Unauthorized Access से सुरक्षित रखना।

PC Security के मुख्य तरीके

1 Antivirus

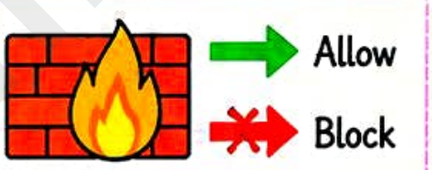
- Malware को Detect, Block और Remove करने में मदद करता हैं।

उदाहरण : Microsoft Defender Antivirus ।


Antivirus

2 Firewall

- Network Traffic को Security Rules के अनुसार Allow या Block करता हैं।



Firewall

3 Software Update

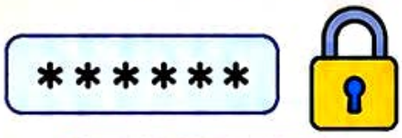
- Operating System और Applications Updated रखें।



Software Update

4 Strong Password

- Computer Login के लिए Unique Password रखें।



Strong Password

5 Screen Lock

- Computer इस्तेमाल न करते समय Lock करें।

Windows Shortcut : Win + L



Screen Lock

Antivirus और Firewall

Antivirus	Firewall
• Malware Detect करता हैं।	• Network Traffic Control करता हैं।
• Files Scan करता हैं।	• Connections Allow/Block करता हैं।

Exam Point : Antivirus और Firewall दोनों Security Tools हैं, लेकिन इनके काम अलग हैं।

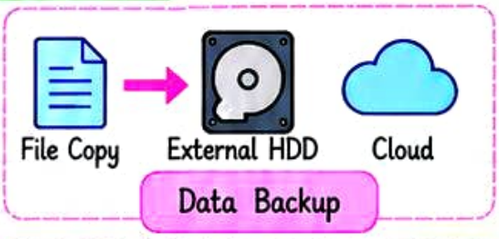
ccguru.in

4. Securing PC

Other Security Methods (अन्य सुरक्षा तरीके)

6 Data Backup

- Important Files की Extra Copy रखना।



7 Trusted Software

- Official या Trusted Source से Software Install करना।



8 USB Security

- Unknown Pen Drive से सावधान रहना।



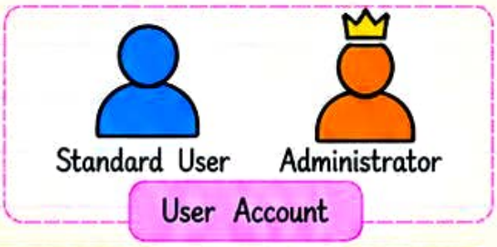
9 Suspicious Links

- Unknown Links या Attachments न खोलना।



10 User Account

- ज़रूरत के अनुसार Standard User Account इस्तेमाल करना।



Backup के प्रकार

1. **Local Backup :** Pen Drive या External Hard Disk।
2. **Cloud Backup :** Online Cloud Storage।
3. **Restore :** Backup से Data वापस प्राप्त करना।

Important Security Features

1. **Automatic Update :** Software Security Fixes Install करने में मदद करता हैं।
2. **Screen Lock :** Unauthorized Access का जोखिम कम करता है।
3. **Backup :** Data Loss होने पर Recovery में मदद करता है।

Quick Revision (त्वरित पुनरावृत्ति)

Antivirus	Malware Protection
Firewall	Network Protection
Backup	Data Recovery
Win + L	Lock Windows PC
Update	Security Fixes



cscguru.in

5. Securing Browser

Web Browser :

Internet पर Websites खोलने वाला Software है।

Web Browser Examples

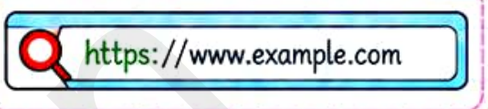


Browser Security Tips (ब्राउज़र सुरक्षा सुझाव)

1. **Browser Updated रखें।**
   हमेशा Browser का नवीनतम Version इस्तेमाल करें।



2. **Website URL ध्यान से Check करें।**
   URL सही है या नहीं, ध्यान से देखें।



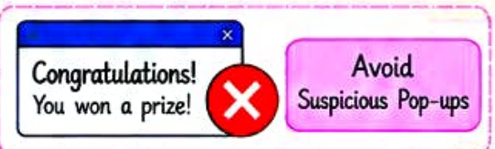
3. **HTTPS वाली Websites को प्राथमिकता दें।**
   Secure (HTTPS) Websites का उपयोग करें।



4. **Unknown Links पर Click न करें।**
   अज्ञात या संदिग्ध Links पर Click करने से बचें।



5. **Suspicious Pop-ups से बचें।**
   संदिग्ध Pop-ups पर Click न करें।



6. **Unknown Extensions Install न करें।**
   केवल Trusted Extensions ही Install करें।



7. **Shared Computer पर Logout करें।**
   सार्वजनिक या Shared Computer पर काम करने के बाद Logout करना न भूलें।



8. **Camera और Location Permission सोच-समझकर दें।**
   केवल जरूरत होने पर ही Camera और Location की Permission दें।



HTTP और HTTPS

HTTP :

Hypertext Transfer Protocol.

- HTTP में Encryption जरूरी नहीं होता।
- यह Data को बिना Encrypt किए भेज सकता है।

HTTPS :

Hypertext Transfer Protocol Secure.

- HTTPS में Data Transfer TLS से Encrypt होता है।
- यह अधिक सुरक्षित होता है।



Exam Facts :

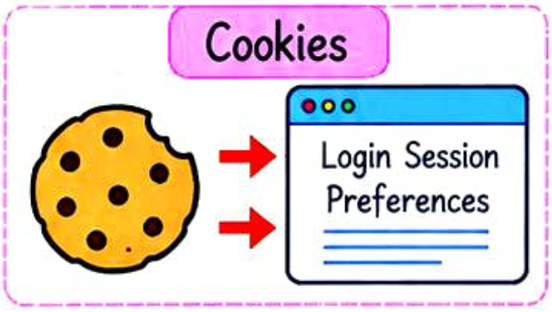
1. HTTPS, HTTP का Secure Version है।
2. HTTPS, Data Transfer को सुरक्षित बनाता है, लेकिन Website असली होने की गारंटी नहीं देता।
3. URL = Uniform Resource Locator.

ccourse.in

5. Securing Browser

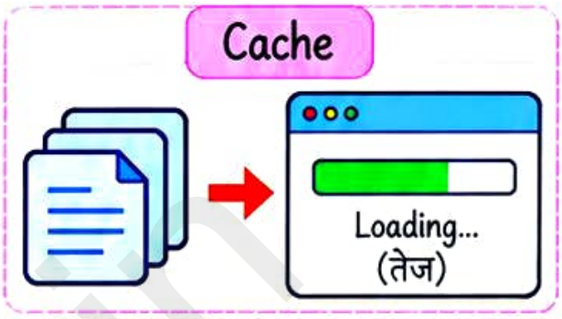
1 Cookies

→ छोटी Data Files जिनसे Website Login Session और Preferences जैसी जानकारी याद रख सकती है।



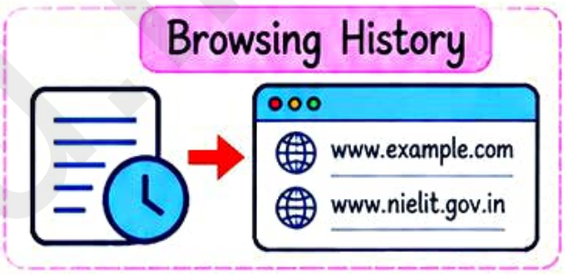
2 Cache

→ Website की कुछ Files Temporary Save करता है, जिससे Website जल्दी Load हो सकती है।



3 Browsing History

→ पहले खोली गई Websites का Record।



4 Incognito / Private Mode

→ इस Mode में Browser सामान्यत: Session बंद होने के बाद Local Browsing History Save नहीं करता।



Browser Security Facts

- Cookies = Session और Preferences।
- Cache = Temporary Website Files।
- History = Visited Websites का Record।
- Incognito = Private Browsing Mode।
- Incognito Mode पूरी तरह Anonymous नहीं बनाता।

Quick Difference

Term	Main Work
Cookies	Website Preferences/Session
Cache	Loading तेज करना
History	Visited Websites का Record
Incognito	Local Browsing Privacy

6. Securing Email Accounts

Email Security के तरीके

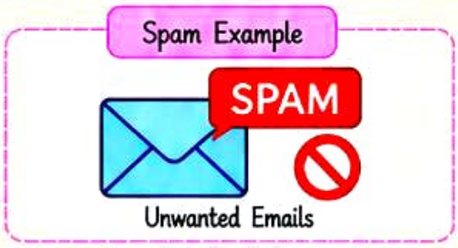
1. Strong और Unique Password रखें।
2. Two-Factor Authentication Enable करें।
3. Unknown Email Links पर Click न करें।
4. Suspicious Attachments Download न करें।
5. OTP और Password Share न करें।
6. Shared Computer पर Logout करें।
7. Recovery Email और Phone Number Updated रखें।
8. Unknown Login Activity Check करें।





Important Terms

1. **Spam :**
   - बिना माँगे आने वाले Emails।
   - Unwanted या Junk Emails भी कहते हैं।



2. **Phishing :**
   - Fake Email, Link या Website से जानकारी चुराने की कोशिश।
   - यह आपके Password, OTP या Personal Information चुरा सकता है।



3. **Email Attachment :**
   - Email के साथ भेजी गई File।
   - इसमें Document, Image, PDF आदि हो सकते हैं।



Two-Factor Authentication (2FA)

- Login के लिए दो अलग तरह के Authentication Factors का इस्तेमाल।
- यह आपके Account को अधिक सुरक्षित बनाता है।

Exampte : Password + Authenticator App Code।



OTP (One Time Password)

- Full Form : One Time Password.
- आमतौर पर एक बार इस्तेमाल होने वाला Verification Code।

Important : OTP, Password और Recovery Code किसी को न बताएं।



coguru.in

7. Phishing and Online Fraud

1 Phishing

- Fake Email या Website से Personal Information चुराने की कोशिश।

Example : Fake Bank Login Page।

Phishing Example



2 Smishing

- SMS के जरिए होने वाला Phishing Attack।

Example : Fake KYC Update SMS।

Smishing Example



3 Vishing

- Phone Call के जरिए होने वाला Phishing Attack।

Example : Fake Bank Officer बनकर OTP माँगना।

Vishing Example



4 Social Engineering

- किसी व्यक्ति को धोखा देकर Password या Private Information लेना।

Social Engineering Example



Important Differences (मुख्य अंतर)

Term	Main Means
Phishing	Fake Email/Website/Message
Smishing	SMS
Vishing	Voice Call

Examples



Safety Rules (सुरक्षा नियम)

1. Unknown Links न खोलें।
2. OTP और PIN Share न करें।
3. Fake Customer Care Calls से सावधान रहें।
4. Login करने से पहले सही Website Address Check करें।

Safety Icons



Exam Point :

- Smishing = SMS Phishing और Vishing = Voice Phishing।
- Phishing Email/Website/Message के जरिए होता है।

8. Secure Social Media Accounts

1 Facebook Security

1. Strong Password रखें।
2. Two-Factor Authentication ON करें।
3. Privacy Settings Check करें।
4. Unknown Friend Requests से सावधान रहें।
5. Unknown Devices से Logout करें।

Facebook Security Icons



2 Instagram Security

1. Two-Factor Authentication Enable करें।
2. Fake Giveaway और Suspicious Links से बचें।
3. Login Activity Check करें।
4. Unknown Accounts को Block या Report करें।
5. Personal Information Public न करें।

Instagram Security Icons



3 WhatsApp Security

1. Two-step Verification Enable करें।
2. 6-Digit Verification PIN सेट करें।
3. Registration OTP किसी को न बताएँ।
4. Linked Devices Check करें।
5. Unknown Linked Devices से Logout करें।
6. App Lock या Biometric Lock लगाएँ।
7. जरूरत के अनुसार End-to-End Encrypted Backup Enable करें।

WhatsApp Security Icons



End-to-End Encryption (E2EE)

- End-to-End Encryption का मतलब है कि Message का Content केवल भेजने वाला और जिसे Message भेजा गया है, वही पढ़ सकते हैं।
- उदाहरण: WhatsApp के Personal Messages और Calls।

End-to-End Encryption Example



Phishing के प्रमुख प्रकार

Type	अर्थ
Phishing	Fake Email या Website से जानकारी चुराना
Smishing	SMS के जरिए Phishing
Vishing	Phone Call के जरिए Phishing

Exam Point :

- OTP, Password और Recovery Code कभी Share न करें।

ccguru.in

9. Securing Smart Phone

Smartphone Security :

Mobile के Data, Apps और Accounts को Digital खतरों से सुरक्षित रखना।

Smartphone Security



Keep Your Mobile Safe

Smartphone Security Tips (मुख्य सुझाव)

1. **Screen Lock :** PIN, Password या Biometric Lock लगाएं।
2. **Software Update :** Android/iOS और Apps Updated रखें।
3. **Trusted Apps :** Official App Store या Trusted Source से Apps Install करें।
4. **App Permissions :** Camera, Location, Contacts और Microphone Permissions Check करें।
5. **Public Wi-Fi :** Unknown Wi-Fi पर Sensitive Transactions से बचें।
6. **Bluetooth :** जरूरत न होने पर Bluetooth बंद रखें।

Phone Security Icons



Biometric Authentication

Physical Features से पहचान Verify करना।



Biometric Example



Examples :

- Fingerprint Recognition
- Face Recognition
- Iris Recognition

Other Mobile Security Tips

7. **Data Backup :** Important Files और Photos की Extra Copy रखें।
8. **Device Tracking :** Find My Device या Find My जैसी Service Enable करें।
9. **Unknown APK :** Suspicious APK Files Install न करें।
10. **Remote Lock :** Phone खोने पर उपलब्ध Service से Lock करें।

Data Backup & Tracking Icons



VPN (Virtual Private Network)



VPN Device और VPN Server के बीच Encrypted Connection बनाता है।

Phone खो जाने पर (Steps)

1. Device Track करने की कोशिश करें।
2. जरूरत हो तो Remote Lock करें।
3. Important Passwords बदलें।
4. SIM Block करवाएं।
5. जरूरत पड़ने पर Remote Erase करें।

Lost Phone Actions



App Permission → App Access Control

App Permissions यह तय करते हैं कि App आपके Phone के किन Features को Access कर सकता है।

Exam Point : Fingerprint, Biometric Authentication का Example है।

10. Summary - Exam Quick Revision

Cyber Security One-Liners (एक पंक्ति में महत्वपूर्ण बातें)

1. Cyber Security, Computer और Data को सुरक्षित रखती है।
2. CIA के 3 Goals: Confidentiality, Integrity, Availability।
3. Malware का अर्थ Malicious Software है।
4. Virus, Malware का एक प्रकार है।
5. Worm अपने आप फैल सकता है।
6. Trojan असली Software जैसा दिख सकता है।
7. Ransomware Files Lock/Encrypt कर सकता है।
8. Spyware चोरी-छिपे जानकारी इकट्ठा करता है।
9. Antivirus Malware Detect और Remove करता है।
10. Firewall Network Traffic Control करता है।
11. Authentication User की पहचान Check करता है।
12. Authorization Access की Permission देता है।
13. Encryption Data को सुरक्षित रूप में बदलता है।
14. Backup से Data Restore होता है।
15. HTTPS Data Transfer को Encrypt करता है।
16. Cookies Website Preferences याद रख सकती है।
17. Cache Website Loading तेज कर सकता है।
18. Incognito Mode पूरी Online Anonymity नहीं देता।
19. 2FA Account Login Security बढ़ाता है।
20. OTP किसी को Share नहीं करना चाहिए।
21. Smishing, SMS के जरिए Phishing है।
22. Vishing, Voice Call के जरिए Phishing है।
23. WhatsApp में Two-step Verification उपलब्ध है।
24. E2EE Messages का Content सुरक्षित रखता है।
25. Fingerprint, Biometric Authentication है।
26. VPN, Device और VPN Server के बीच Encrypted Connection बनाता है।
27. App Permissions, Mobile Security के लिए जरूरी हैं।
28. Software Updates Security Fixes देते हैं।

CIA Goals



Types of Malware



Security Tools



Important Concepts



Web Browser



Account & Fraud Security



WhatsApp Security



Mobile Security



VPN



11. Important Full Forms

S. No.	Short Form	Full Form
1	CIA	Confidentiality, Integrity, Availability
2	IT	Information Technology
3	PC	Personal Computer
4	OS	Operating System
5	HTTP	Hypertext Transfer Protocol
6	HTTPS	Hypertext Transfer Protocol Secure
7	URL	Uniform Resource Locator
8	TLS	Transport Layer Security
9	SSL	Secure Sockets Layer
10	OTP	One Time Password
11	2FA	Two-Factor Authentication
12	MFA	Multi-Factor Authentication
13	VPN	Virtual Private Network
14	E2EE	End-to-End Encryption
15	PIN	Personal Identification Number
16	USB	Universal Serial Bus
17	SMS	Short Message Service
18	APK	Android Package Kit
19	KYC	Know Your Customer

Quick Revision (याद रखने के लिए)

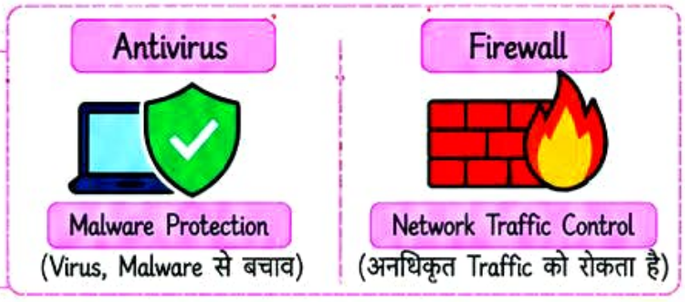
- HTTP → Hypertext Transfer Protocol
- HTTPS → Hypertext Transfer Protocol Secure
- URL → Uniform Resource Locator
- OTP → One Time Password
- VPN → Virtual Private Network
- 2FA → Two-Factor Authentication
- E2EE → End-to-End Encryption
- PIN → Personal Identification Number
- USB → Universal Serial Bus
- SMS → Short Message Service
- APK → Android Package Kit
- KYC → Know Your Customer

ccguru.in

12. Most Important Facts

1 Antivirus vs Firewall

- Antivirus → Malware Protection
  (Malware से बचाता है)
- Firewall → Network Traffic Control
  (Network Traffic को Control करता है)



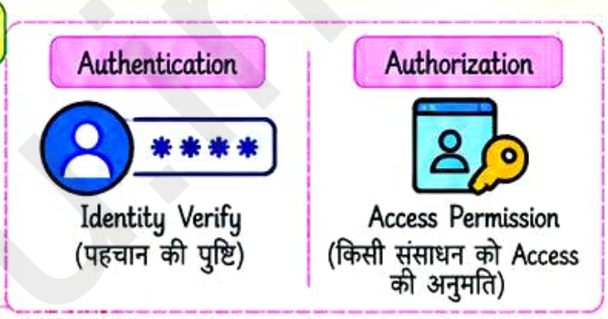
2 HTTP vs HTTPS

- HTTP → Encryption जरूरी नहीं
- HTTPS → Encrypted Connection
  (Data Transfer TLS से Encrypt होता है)



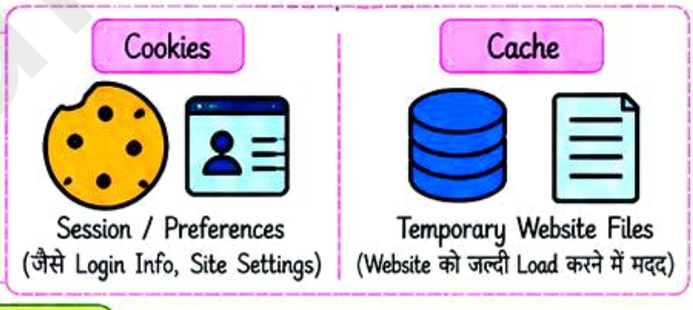
3 Authentication vs Authorization

- Authentication → Identity Verify
  (User की पहचान Check करना)
- Authorization → Access Permission
  (किसी संसाधन को Access की अनुमति देना)



4 Cookies vs Cache

- Cookies → Session/Preferences
  (Login Session और Preferences)
- Cache → Temporary Website Files
  (Website को जल्दी Load करने में मदद)



5 Phishing vs Smishing vs Vishing

- Phishing → Fake Online Messages/Websites
  (Fake Email या Website)
- Smishing → SMS
  (SMS के जरिए Phishing)
- Vishing → Voice Call
  (Phone Call के जरिए Phishing)



Important True/False Facts (सही / गलत)

S. No.	Statement (कथन)	True / False
1	Antivirus Malware से बचाता है।	True
2	Firewall केवल Virus हटाता है।	False
3	HTTPS हर Website को Fraud-free बनाता है।	False
4	Incognito Mode पूरी Anonymity देता है।	False
5	OTP किसी को Share करना सुरक्षित है।	False
6	Fingerprint, Biometric Authentication है।	True
7	Backup से Data Restore किया जा सकता है।	True
8	VPN सभी Cyber Attacks रोकता है।	False
9	Strong Password Account Security बढ़ाता है।	True
10	Software Updates Security के लिए जरूरी हैं।	True

coduri.in

13. Model Questions and Answers

1 **Q1. Cyber Security क्या है?**

Ans : Digital Devices और Data को Online खतरों से सुरक्षित रखना।



2 **Q2. CIA के तीन Goals क्या हैं?**

Ans : Confidentiality, Integrity, Availability।



3 **Q3. Malware का Full Form क्या है?**

Ans : Malicious Software।



4 **Q4. कौन-सा Malware अपने आप फैल सकता है?**

Ans : Worm।



5 **Q5. कौन-सा Malware Files Lock करके पैसे माँगता है?**

Ans : Ransomware।



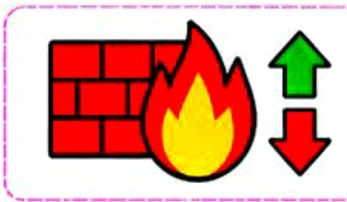
6 **Q6. Antivirus का काम क्या है?**

Ans : Malware Detect, Block या Remove करना।



7 **Q7. Firewall का मुख्य काम क्या है?**

Ans : Network Traffic Control करना।



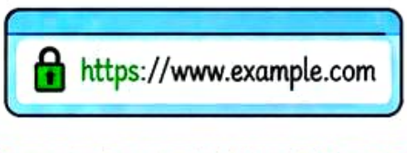
8 **Q8. Authentication क्या है?**

Ans : User की पहचान Verify करना।



9 **Q9. HTTPS का Full Form क्या है?**

Ans : Hypertext Transfer Protocol Secure।



10 **Q10. Windows Lock Shortcut क्या है?**

Ans : Win + L।



ccguru.in

13. Model Questions and Answers

Q11. Phishing क्या है ?

Ans : Fake Email, Link या Website से जानकारी चुराने की कोशिश।



Q12. Smishing क्या है ?

Ans : SMS के जरिए Phishing ।



Q13. Vishing क्या है ?

Ans : Voice Call के जरिए Phishing ।



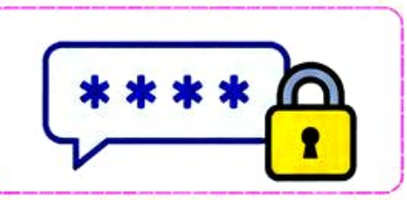
Q14. 2FA का Full Form क्या है ?

Ans : Two-Factor Authentication ।



Q15. OTP का Full Form क्या है ?

Ans : One Time Password ।



Q16. WhatsApp में कौन-सा Account Security Feature है ?

Ans : Two-step Verification ।



Q17. E2EE का Full Form क्या है ?

Ans : End-to-End Encryption ।



Q18. Biometric Authentication का Example क्या है ?

Ans : Fingerprint Recognition ।



Q19. VPN का Full Form क्या है ?

Ans : Virtual Private Network ।



Q20. Backup का उपयोग क्यों किया जाता है ?

Ans : Data Loss होने पर Data Restore करने के लिए।



CCC GURU

Your Partner in CCC Preparation

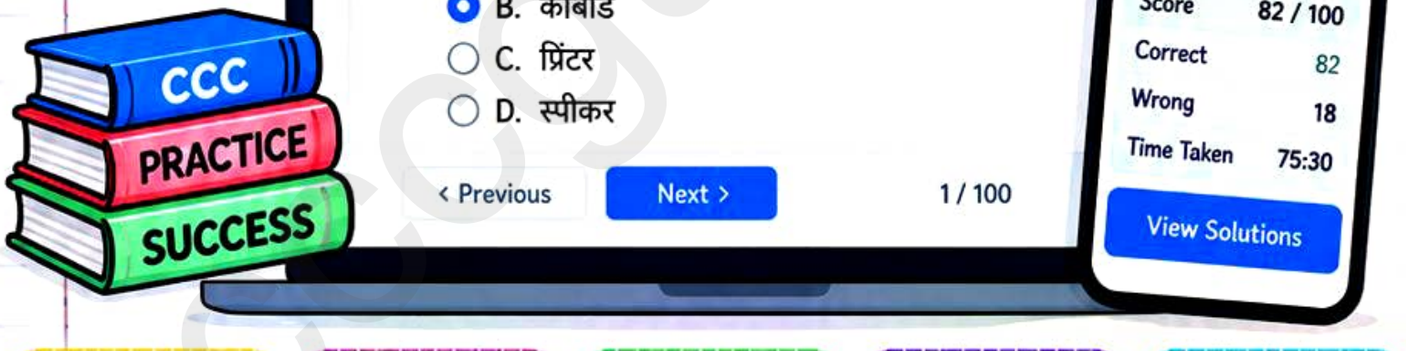
Notes पढ़ लिए?

अब Test देकर तैयारी जाँचें!

FREE CCC ONLINE TEST 2026

NIELIT CCC की तैयारी अब और आसान

- ✓ Practice
- ✓ Improve
- ✓ Get Ready for Exam



- 100 Questions • 90 Minutes
- Hindi + English Tests
- Chapter-wise Practice
- Instant Result & Solutions
- Full Mock Tests

आज ही अपना FREE Mock Test शुरू करें!

www.cccguru.in

Mobile और Computer दोनों पर Practice करें

Independent preparation platform • Not affiliated with NIELIT