S. S. JAIN SUBODH P.G. (AUTONOMOUS) COLLEGE, JAIPUR

Introduction to Cyber Security

Programme- BBA III Sem.

Paper- Skill Enhancement Course (SEC)

1. Which of the following best defines cyberspace?

A) The physical world

B) The interconnected digital environment

C) The internet only

D) Computer hardware

2. What year is considered the birth of the modern internet?

A) 1969

B) 1982

C) 1990

D) 2000

3. Which is NOT a type of cybercrime?

A) Phishing

B) Robbery

C) Identity theft

D) Ransomware

4. Which of the following refers to practices that ensure data confidentiality, integrity, and availability?

A) Cyber Crime

B) Information Security

C) Internet History

D) Browser Management

5. What is the main purpose of computer ethics?

A) Increasing hardware speed

B) Ensuring responsible use of technology

C) Virus removal

D) Upgrading software

6. Email security aims to protect users from:

A) Spam

B) Malware

C) Unauthorized access

D) All of the above

7. Which security measure is MOST effective in securing web browsers?

A) Clearing cache

B) Using strong authentication

C) Bookmarking pages

D) Watching videos

8. Which software detects and removes malicious programs from computers?

A) Browser

B) Antivirus

C) PowerPoint

D) Excel

9. Which is a guideline for creating a secure password?

A) Use simple words only

B) Reuse old passwords

C) Mix letters, numbers, and symbols

D) Use only your name

10. Two step authentication increases security by:

A) Asking two security questions

B) Requiring two methods of verifying identity

C) Using passwords twice

D) Doubling the password length

11. Which tool helps users store passwords securely?

A) Antivirus

B) Password Manager

C) Firewall

D) Notepad

12. Wi Fi security measures typically include:

A) Strong passwords

B) Encryption

C) Limiting access

D) All of the above

13. What is phishing?

A) Fishing online

B) Fraudulently obtaining sensitive information

C) Encrypting data

D) Sending pictures

14. Spam emails are dangerous because they might:

A) Include jokes

B) Carry malware

C) Improve security

D) Provide food recipes

15. Which is MOST important for maintaining computer security?

A) Keeping the screen clean

B) Updating software regularly

C) Changing wallpaper

D) Increasing RAM

16. A strong password should be:

A) Easy to guess

B) Unique for each account

C) Your birthdate

D) Short and simple

17. Antivirus software primarily protects against:

A) Unauthorized printing

B) Malware and viruses

C) Forgot passwords

D) Editing documents

18. Which device is commonly attacked to gain unauthorized access?

A) Modem

B) Router

C) Speaker

D) Printer

19. Secure browser settings prevent:

A) Unauthorized access

B) System updates

C) Power saving

D) Automatic backups

20. Computer Ethics ensures:

A) Responsible behavior

B) Hacking

C) Virus creation

D) Only coding rules

21. Information Security focuses on:

A) Entertainment

B) Protecting data from threats

C) Hardware design

D) Web development

22. What is NOT an example of authentication?

A) Password

B) Fingerprint

C) Username

D) PIN

23. Setting up a secure password means:

A) Using admin as password

B) Using personal details

C) Using unpredictable combinations

D) Reusing passwords

24. Two factor authentication uses:

A) Password and phone code

B) Only password

C) IP address

D) Email signature

25. Cyber space consists of:

A) Only Facebook

B) All connected digital networks

C) Microsoft Word

D) Hard disk partitions

26. Which of the following is a basic Windows security guideline?

A) Avoid updates

B) Use strong passwords

C) Disabling firewall

D) Ignoring warnings

27. Social media security mainly involves:

A) Posting often

B) Protecting private information

C) Tagging friends

D) Liking posts

28. Which is a best practice for password management?

A) Write passwords everywhere

B) Use password manager

C) Use birthday as password

D) Share password with friends

29. Credit Card security involves:

A) Sharing CVV

B) Strong authentication and monitoring

C) Public sharing of number

D) Printing information

29. UPI security can be increased by:

A) Sharing PIN

B) Using official apps

C) Disabling notifications

D) Ignoring messages

30. Online Banking security guideline:

A) Use public Wi Fi

B) Monitor transactions

C) Share OTP

D) Use unsecured devices

31. Which of the following ensures secure mobile banking?

A) Download apps from unknown sources

B) Use official app stores

C) Ignore app updates

D) Log in from friend’s device

32. POS security includes:

A) Update POS systems

B) Ignore network issues

C) Use default settings

D) Print passwords

33. Smartphone security guideline:

A) Set up screen lock

B) Share phone with everyone

C) Disable security updates

D) Ignore suspicious apps

34. Debit card security tip:

A) Share card details freely

B) Enable transaction alerts

C) Ignore PIN safety

D) Use same PIN everywhere

35. E wallet security guideline:

A) Use weak passwords

B) Verify app authenticity

C) Ignore suspicious transactions

D) Disable phone security

36. What is essential for securing online transactions?

A) Unencrypted connections

B) SSL/TLS Encryption

C) Using old devices

D) No password at all

37. Social engineering is related to:

A) Mechanical engineering

B) Manipulating people into giving confidential information

C) Building infrastructure

D) Gardening online

38. Which is NOT a best practice for online banking?

A) Using public computers

B) Regular password changes

C) Monitoring account statements

D) Using secure connection

39. Mobile banking security includes:

A) Disabling two factor authentication

B) Keeping the app updated

C) Using random sources for downloads

D) Sharing phone PIN

40. Secure ATM usage tip:

A) Cover keypad while entering PIN

B) Ignore ATM alerts

C) Share ATM card details

D) Use random ATMs in isolated places

40. What helps prevent unauthorized debit card transactions?

A) Enable transaction alerts

B) Use easy PIN

C) Ignore security advice

D) Share card online

41. Which guideline is NOT related to POS security?

A) Strong passwords for POS terminals

B) Secure connections

C) No password needed

D) Monitor for malware

42. Smartphone security includes:

A) Installing antivirus apps

B) Ignoring updates

C) No screen lock

D) Sharing device widely

43. Which is a common social media threat?

A) Account hacking

B) Phone overheating

C) Battery drainage

D) Screen cracks

44. For e wallet safety:

A) Use official apps only

B) Share PIN openly

C) Set weak password

D) Ignore suspicious activity

45. Online banking can be secured by:

A) Keeping login info confidential

B) Sharing password

C) Logging in on public Wi Fi

D) Ignoring security alerts

46. UPI transactions should be done:

A) Through untrusted apps

B) Using official bank apps

C) Sharing PIN by message

D) Ignoring transaction details

47. Micro ATMs security involves:

A) Regular software updates

B) Ignoring alerts

C) Using default settings

D) No security check

48. Guidelines for password security include:

A) Changing periodically

B) Using easy combinations

C) Ignoring changes

D) Putting password in phone notes

49. What is the aim of social engineering attacks?

A) Physical damage

B) Manipulating people to reveal confidential info

C) Building computers

D) Fixing bugs

50. Which is NOT a type of social engineering?

A) Phishing

B) Baiting

C) Malware

D) Tailgating

51. Cyber criminals work by exploiting:

A) Software only

B) Human vulnerabilities

C) Hardware issues

D) Network cables

52. Prevention against being a victim of cyber crime includes:

A) Ignoring security reminders

B) Following best security practices

C) Disabling security apps

D) Sharing passwords

53. Which is part of a cyber threat landscape?

A) Malware

B) Ransomware

C) Phishing

D) All of the above

54. Which technique is used to hack people’s information through emails?

A) Phishing

B) Mining

C) Digging

D) Farming

55. What is a cyber security threat?

A) Security test

B) Potential for harm in digital systems

C) Hardware upgrade

D) Password reset

56. Which method helps prevent social engineering?

A) Awareness and training

B) Disabling employees' accounts

C) Sharing personal info

D) Using a single password

57. How do attackers often manipulate victims?

A) By intimidating

B) By impersonating trusted entities

C) By offering free gifts

D) By sending formal emails

58. What is NOT a type of social engineering attack?

A) Pretexting

B) Vishing

C) Updating software

D) Quizzes

59. The best defense against social engineering is:

A) User awareness

B) Ignoring emails

C) Disabling accounts

D) Installing games

60. A common characteristic of cyber criminals:

A) Acting alone always

B) Exploiting trust

C) Building systems

D) Fixing bugs

61. Ransomware is used to:

A) Encrypt user files for payment

B) Speed up computers

C) Print documents

D) Send emails

62. How can you protect yourself from phishing?

A) Clicking all links

B) Verifying sender identity

C) Ignoring all messages

D) Using weak passwords

63. Cyber threat techniques include:

A) Malware

B) Ransomware

C) Spyware

D) All of the above

64. What is a digital footprint?

A) Track of websites visited

B) Shoes online

C) Computer hardware

D) USB device

65. Preventing cyber crime involves:

A) Robust security policies

B) Weak authentication

C) Ignoring updates

D) Disabling security

66. What does malware do?

A) Entertains users

B) Damages or steal data

C) Refresh screen

D) Update hardware

67. Spyware is used to:

A) Spy on other networks legally

B) Secretly monitor user activities

C) Fix vulnerabilities

D) Secure system

68. Which best describes a cyber security threat?

A) A change of settings

B) Potential for digital attack or breach

C) Reboot system

D) Sign out

69. Which is an example of "pretexting" in cyber security?

A) Creating a fake scenario to obtain info

B) Playing games online

C) Learning programming

D) Updating browser

70. Cyber criminals often use:

A) Social tactics

B) Direct hardware access

C) Creative writing

D) Official notices

71. What is the most effective way to combat ransomware?

A) Ignoring it

B) Regular data backups

C) Paying immediately

D) Disabling firewall

72. Encryption helps:

A) Hide information from unauthorized access

B) Slow down computers

C) Reveal passwords

D) Remove viruses

73. Which is a key aspect of cyber security awareness?

A) Knowledge about threats and prevention

B) Ignoring risks

C) Sharing confidential info

D) Signing up for all online platfom

74. Which of the following is the primary function of a firewall?
a) Encrypting data
b) Blocking unauthorized access
c) Performing backups
d) Detecting viruses

75. A firewall operates mainly at which OSI layer?
a) Application Layer
b) Network Layer
c) Data Link Layer
d) Physical Layer

76. Which organization launched the Cyber Surakshit Bharat Initiative?
a) NITI Aayog
b) MeitY
c) RBI
d) CERT-In

77. The National Cyber Security Policy (NCSP) in India was first introduced in:
a) 2005
b) 2008
c) 2013
d) 2017

78. Which national agency is the nodal authority for cyber security incidents in India?
a) NIC
b) CBI

c) CERT-In
d) UIDAI

79. Which of the following is NOT a step in incident response?
a) Preparation
b) Identification
c) Eradication
d) Virtualization

80. The first step in handling a cyber security incident is:
a) Recovery
b) Identification
c) Containment
d) Eradication

81. Post-incident activity mainly focuses on:
a) System shutdown
b) Lessons learned
c) Data deletion
d) Backup removal

82. Cyber Security Assurance ensures:
a) Availability, Integrity, Confidentiality
b) Low-cost IT operations
c) Unlimited data storage
d) Automatic system recovery

83. Which of the following is an assurance method?
a) Penetration testing
b) Phishing
c) Social engineering
d) Malware infection

84. The process of validating security controls regularly is called:
a) Hardening
b) Assurance testing
c) Debugging
d) Patching

85. The Information Technology (IT) Act in India was enacted in:
a) 1999
b) 2000
c) 2005
d) 2010

86. Under the IT Act, unauthorized access to computer systems is punishable under:
a) Section 65
b) Section 66
c) Section 72
d) Section 79

87. The IT Act was amended in:
a) 2002
b) 2004
88. A hacker who finds vulnerabilities and reports them responsibly is called:
a) Black Hat
b) White Hat
c) Grey Hat
d) Script Kiddie

89. Which tool is commonly used by hackers for password cracking?
a) Wireshark
b) Nmap
c) John the Ripper
d) Burp Suite

90. The countermeasure to SQL Injection attack is:
a) Strong password
b) Input validation
c) Phishing awareness
d) Port scanning

91. The OWASP Top 10 project is related to:
a) Cyber law
b) Web application security risks
c) Cloud storage
d) Network hardware

92. Cross-Site Scripting (XSS) attacks occur when:
a) Malicious code is injected into a trusted website
b) Passwords are stolen through brute force
c) Network ports are blocked
d) Firewalls are bypassed

93. Which protocol ensures secure communication in web applications?
a) HTTP
b) HTTPS
c) FTP
d) Telnet

94. The National Critical Information Infrastructure Protection Centre (NCIIPC) in India was established in:
a) 2005
b) 2008
c) 2010
d) 2014

95. Defensive programming is mainly used to:
a) Increase execution speed
b) Handle unexpected inputs securely
c) Minimize memory usage
d) Avoid backup creation

96. Which of the following is a defensive programming practice?
a) Input sanitization
b) Code obfuscation
c) Malware injection
d) Phishing attacks

98. The process of permanently removing data from storage devices is called:
a) Encryption
b) Wiping
c) Backup
d) Restoration

99. Which tool is widely used for data recovery?
a) Recuva
b) Nmap
c) Wireshark
d) Snort

100. Which of the following is NOT a secure method of data destruction?
a) Physical shredding
b) Degaussing
c) Overwriting
d) File deletion using recycle bin

Answer Sheet

1 **B)** The interconnected digital environment
2 **A)** 1969
3 **B)** Robbery
4 **B)** Information Security
5 **B)** Ensuring responsible use of technology
6 **D)** All of the above
7 **B)** Using strong authentication
8 **B)** Antivirus
9 **C)** Mix letters, numbers, and symbols
10 **B)** Requiring two methods of verifying identity
11 **B)** Password Manager
12 **D)** All of the above
13 **B)** Fraudulently obtaining sensitive information
14 **B)** Carry malware
15 **B)** Updating software regularly
16 **B)** Unique for each account
17 **B)** Malware and viruses
18 **B)** Router
19 **A)** Unauthorized access
20 **A)** Responsible behavior
21 **B)** Protecting data from threats
22 **C)** Username
23 **C)** Using unpredictable combinations
24 **A)** Password and phone code
25 **B)** All connected digital networks
26 **B)** Use strong passwords
27 **B)** Protecting private information
28 **B)** Use password manager
29 **B)** Strong authentication and monitoring
29 (Duplicate question on UPI) **B)** Using official apps
30 **B)** Monitor transactions
31 **B)** Use official app stores
32 **A)** Update POS systems
33 **A)** Set up screen lock
34 **B)** Enable transaction alerts
35 **B)** Verify app authenticity
36 **B)** SSL/TLS Encryption
37 **B)** Manipulating people into giving confidential information
38 **A)** Using public computers
39 **B)** Keeping the app updated
40 **A)** Cover keypad while entering PIN
40 (duplicate) **A)** Enable transaction alerts
41 **C)** No password needed
42 **A)** Installing antivirus apps
43 **A)** Account hacking
44 **A)** Use official apps only
45 **A)** Keeping login info confidential
46 **B)** Using official bank apps
47 **A)** Regular software updates
48 **A)** Changing periodically
49 **B)** Manipulating people to reveal confidential info
50 **C)** Malware
51 **B)** Human vulnerabilities
52 **B)** Following best security practices
53 **D)** All of the above
54 **A)** Phishing
55 **B)** Potential for harm in digital systems
56 **A)** Awareness and training
57 **B)** By impersonating trusted entities
58 **C)** Updating software
59 **A)** User awareness
60 **B)** Exploiting trust
61 **A)** Encrypt user files for payment
62 **B)** Verifying sender identity
63 **D)** All of the above
64 **A)** Track of websites visited
65 **A)** Robust security policies
66 **B)** Damages or steal data
67 **B)** Secretly monitor user activities
68 **B)** Potential for digital attack or breach
69 **A)** Creating a fake scenario to obtain info
70 **A)** Social tactics
71 **B)** Regular data backups
72 **A)** Hide information from unauthorized access
73 **A)** Knowledge about threats and prevention
74 **B)** Blocking unauthorized access

75 **B)** Network Layer
76 **B)** MeitY
77 **C)** 2013
78 **C)** CERT-In
79 **D)** Virtualization
80 **B)** Identification
81 **B)** Lessons learned
82 **A)** Availability, Integrity, Confidentiality
83 **A)** Penetration testing
84 **B)** Assurance testing
85 **B)** 2000
86 **B)** Section 66
87 **b)** 2008
88 **B)** White Hat
89 **C)** John the Ripper
90 **B)** Input validation
91 **B)** Web application security risks
92 **A)** Malicious code is injected into a trusted website
93 **B)** HTTPS
94 **D)** 2014
95 **B)** Handle unexpected inputs securely
96 **A)** Input sanitization
98 **B)** Wiping
99 **A)** Recuva
100 **D)** File deletion using recycle bin

S. S. JAIN SUBODH P.G. (AUTONOMOUS) COLLEGE, JAIPUR

Programme- BBA III Sem.

Paper- Skill Enhancement Course (SEC)

Unit I

1. Introduction to Cyberspace

Cyberspace refers to the **virtual digital world** where computers, networks, and internet-connected devices interact.
It includes everything connected through the internet — websites, emails, social media, online banking, and cloud systems.

Key Features

- A global network of interconnected computers.
- Enables communication and data sharing.
- Not physical — it's a digital environment.

Example: Sending an email, browsing a website, or chatting online are all activities in cyberspace.

2. History of the Internet

The **Internet** evolved from early networking projects aimed at sharing information between computers.

Timeline:

- **1969:** ARPANET — the first network connecting four U.S. universities.
- **1971:** First email sent by Ray Tomlinson.
- **1983:** TCP/IP protocol adopted — the real birth of the modern Internet.
- **1990:** Tim Berners-Lee developed the World Wide Web (WWW).
- **2000 onwards:** Social media, e-commerce, and cloud computing made the internet a global necessity.

3. Cyber Crime

Cybercrime refers to **criminal activities** carried out using computers or networks.

Types of Cybercrime:

- **Phishing:** Tricking users into revealing sensitive data through fake emails.
- **Identity Theft:** Stealing someone's personal information.
- **Hacking:** Unauthorized access to computer systems.
- **Ransomware:** Encrypting files and demanding payment to unlock them.

Example: A hacker stealing your bank login credentials online.

4. Information Security

Information Security (InfoSec) means protecting data from **unauthorized access, modification, or destruction**.

Core Principles (CIA Triad):

- **Confidentiality:** Only authorized users can access data.
- **Integrity:** Data must remain accurate and unaltered.
- **Availability:** Data and systems should be available when needed.

Example: Encrypting sensitive files ensures confidentiality.

5. Computer Ethics and Security Policies

Computer Ethics

Refers to the **moral principles** that guide the use of computers and technology.

Examples:

- Do not access other people's data without permission.
- Respect intellectual property rights.
- Avoid spreading malware or misinformation.

Security Policies

Security policies are **rules and guidelines** designed by organizations to protect systems and information.

Examples:

- Strong password policy.
- Regular data backups.
- Restricted access to confidential files.

6. Email Security

Email is a common target for cyber threats like phishing or malware.

Email Security Practices:

- Do not click on suspicious links or attachments.
- Use spam filters.
- Verify sender identity before responding.
- Use **two-factor authentication** for your email accounts.

Example: Gmail's spam detection automatically filters suspicious messages.

7. Securing Web Browser

Browsers are gateways to the internet — securing them prevents online attacks.

Security Tips:

- Keep browser and plugins updated.
- Use **HTTPS** websites only.
- Avoid saving passwords in browsers.
- Enable pop-up blockers and disable unsafe extensions.

Example: Chrome's "Safe Browsing" warns users about malicious sites.

8. Antivirus

Antivirus software protects your computer from viruses, worms, trojans, and other malicious software.

Functions:

- Detects and removes malware.
- Scans files and emails.
- Provides real-time protection.

Examples: Windows Defender, McAfee, Quick Heal, Avast.

9. Guidelines for Secure Password and Wi-Fi Security

Secure Password Guidelines:

- Use a mix of **uppercase, lowercase, numbers, and symbols**.
- Avoid personal information like birthdates or names.
- Change passwords regularly.
- Use different passwords for different accounts.

Wi-Fi Security Guidelines:

- Use strong Wi-Fi passwords.
- Enable **WPA3/WPA2 encryption**.
- Hide your Wi-Fi network (SSID).
- Limit who can access your network.

10. Guidelines for Setting Up a Secure Password

A secure password should be:

- At least **8–12 characters** long.
- Contain letters, numbers, and special symbols.
- **Not** reused across multiple sites.
- Stored securely (preferably in a **Password Manager**).

Example:
✅ `T@jM@h@l2025!` (Strong)
❌ `shabanam123` (Weak)

11. Two-Step (Two-Factor) Authentication

Two-step authentication (2FA) adds an extra layer of protection to your account.

How It Works:

1. Enter your **password** (something you know).
2. Enter a **verification code** sent to your phone or email (something you have).

Example: Logging into Gmail and verifying using an OTP sent to your phone.

Benefits:

- Prevents access even if your password is stolen.
- Greatly improves account security.

12. Password Manager

A **Password Manager** is software that securely stores and manages passwords.

Functions:

- Stores all passwords in encrypted form.
- Creates strong random passwords automatically.
- Requires only one master password to access all others.

Examples:

- LastPass
- Dashlane
- Bitwarden
- 1Password

Benefits:

- No need to remember multiple passwords.
- Prevents reuse of weak or common passwords.

Summary Table

Topic	Key Idea
Cyberspace	Virtual world of digital communication
Internet History	Evolved from ARPANET (1969) to WWW
Cyber Crime	Illegal acts via computer/network
Information Security	Ensures Confidentiality, Integrity, Availability
Computer Ethics	Moral use of technology
Security Policies	Organizational protection rules
Email Security	Avoid phishing, verify sender
Browser Security	Update, use HTTPS, disable unsafe add-ons
Antivirus	Detects and removes malware
Secure Password	Mix of letters, numbers, symbols
Wi-Fi Security	Strong password + encryption
Two-Step Authentication	Extra login verification layer
Password Manager	Securely stores passwords

Unit II

1. Guidelines for Basic Windows Security

Windows is the most widely used operating system — and therefore, a frequent target for cyberattacks.

🔒 Best Practices

- **Use strong passwords** for all user accounts.
- **Install antivirus software** and keep it updated (e.g., Windows Defender).
- **Keep Windows updated** using "Windows Update" to patch security vulnerabilities.
- **Enable Firewall** to block unauthorized access.
- **Use limited (non-admin) user accounts** for daily use.
- **Turn on BitLocker** for disk encryption (Pro/Enterprise editions).
- **Avoid downloading unknown files or software.**

2. Guidelines for Social Media Security

Social media platforms (Facebook, Instagram, X, LinkedIn, etc.) are often exploited for scams, identity theft, and data leaks.

🔐 Safety Tips

- Do **not share personal information** (phone, address, etc.) publicly.
- **Adjust privacy settings** to limit who can see your posts.
- **Avoid clicking on suspicious links** or friend requests from unknown users.
- **Use unique passwords** for each platform.
- **Enable two-factor authentication (2FA)**.
- **Think before you post** — once online, always online.

3. Tips and Best Practices for Safer Social Networking

- **Be cautious** with what you share — avoid posting sensitive or location details.
- **Don't accept all friend requests** — verify people first.
- **Report and block suspicious accounts.**
- **Avoid sharing financial or login details via messages.**
- **Log out** when using public or shared computers.
- **Regularly review privacy settings** on social platforms.

Example: Never share OTPs or bank links received through DMs or comments.

4. User Account Password Guidelines

Passwords protect your user account from unauthorized access.

Best Practices

- Minimum **8–12 characters** long.
- Use **a mix of uppercase, lowercase, digits, and symbols.**
- **Avoid names, birth dates, or simple patterns.**
- **Change passwords periodically.**
- Do **not share passwords** with anyone.
- **Use a Password Manager** to securely store them.

Example of Strong Password: `MyS@feP@ss_2025!`

5. Smartphone Security Guidelines

Smartphones store sensitive data — banking apps, personal photos, and contacts — making them prime targets.

Tips

- **Set up screen lock** (PIN, pattern, fingerprint, or face ID).
- **Download apps only from official stores** (Google Play, Apple App Store).
- **Keep OS and apps updated.**
- **Install mobile antivirus** if possible.
- **Avoid public Wi-Fi for transactions.**

- **Enable remote tracking and data wipe** options.
- **Don’t root or jailbreak your phone.**

6. Online Banking Security

Online banking offers convenience but also requires strong security awareness.

Guidelines

- Access bank sites only through **official websites or apps.**
- **Do not share OTP, PIN, or password** with anyone.
- **Use private and secure networks**, never public Wi-Fi.
- **Monitor account statements** regularly for unauthorized transactions.
- **Logout** after every session.
- Enable **transaction alerts (SMS/Email).**

7. Credit Card and UPI Security

Credit Card Security

- Keep your **card number and CVV confidential.**
- Enable **transaction alerts** for every payment.
- Use **credit cards only on secure websites (HTTPS).**
- **Do not share OTPs or PINs.**
- Report **lost or stolen cards** immediately.

UPI Security

- Use **only official UPI apps** (BHIM, Google Pay, PhonePe, Paytm).
- **Never share UPI PIN** or approve unknown requests.
- Verify recipient’s name before sending money.
- **Enable app lock and device security.**

8. Online Banking Security (Expanded Focus)

- Use **strong, unique passwords** for banking logins.
- Enable **two-step authentication** (password + OTP).
- Avoid **clicking on links in emails/SMS claiming to be from banks.**
- Keep your **browser updated** and use secure (HTTPS) connections.
- **Don't save credentials** in browsers or public computers.

9. Mobile Banking Security

- **Download official bank apps only.**
- **Keep your mobile OS updated.**
- Use **biometric or PIN protection** to open the app.
- **Do not use rooted/jailbroken devices.**
- Enable **app notifications** for all transactions.
- Logout after each use.
- Report **any suspicious transactions immediately.**

10. Security of Debit and Credit Card

- **Do not share card details** (number, CVV, PIN).
- **Enable SMS/email alerts** for all transactions.
- **Cover keypad** while entering your PIN at ATMs.
- **Avoid using ATMs in isolated or poorly lit areas.**
- **Do not let merchants take your card out of sight.**
- Use **contactless transactions** only when necessary.

11. POS (Point of Sale) Security

POS systems process card transactions — they must be secured against malware and unauthorized access.

Security Measures

- **Use strong passwords** for POS devices.
- **Regularly update POS software.**
- **Encrypt data transmissions.**
- **Monitor systems for unusual activity.**
- Restrict **physical access** to POS terminals.
- Ensure **secure network connections** (not public Wi-Fi).

12. Security of Micro ATMs

Micro ATMs are used in rural and remote banking operations.

Security Guidelines

- **Regularly update system software.**
- **Use secure communication networks (VPNs).**
- **Authenticate users properly (biometric/PIN).**
- **Monitor logs** for unusual activities.
- **Train operators** on safe handling and reporting incidents.
- Ensure **device encryption and tamper resistance.**

13. E-Wallet Security Guidelines

E-wallets (e.g., Paytm, Google Pay, Amazon Pay, PhonePe) allow digital transactions conveniently — but must be protected.

Best Practices

- **Download only official e-wallet apps.**
- **Set strong login and app PINs.**
- **Do not share OTPs or passwords.**
- **Enable transaction notifications.**

- **Regularly review your transaction history.**
- **Avoid public Wi-Fi** for wallet transactions.
- **Log out** after each transaction on shared devices.

Summary Table

Area	Key Security Guideline
Windows Security	Use antivirus, updates, firewall
Social Media	Limit personal info, enable 2FA
Social Networking	Review privacy settings, report scams
User Password	Strong, unique, changed periodically
Smartphone	App from official store, screen lock
Online Banking	Use official apps, private network
Credit/UPI	No sharing PIN/OTP, monitor alerts
Mobile Banking	Use biometric login, update app
Debit/Credit Cards	Keep details secret, cover keypad
POS	Strong passwords, encrypted network
Micro ATMs	Secure network, software updates
E-Wallet	Official apps, enable alerts, avoid public Wi-Fi