



Gurukul Technicals Institute

Computer education · Robotics · Science projects · Delhi

FREE EBOOK

PROGRAMMING AND WEB

Cyber Security Basics Study Book

The complete study notes, practice questions and glossary for Cyber Security Basics

INSIDE THIS BOOK

- Strong Passwords and Password Managers
- Two-Factor Authentication
- Phishing, Smishing and Vishing
- UPI and OTP Fraud
- Malware: Types and How It Spreads
- ...and 2 more chapters, practice questions and a glossary

Beginner

Students and computer users who want to stay safe online

engineergurukul.com

+91 97116 99511

Cyber Security Basics Study Book

Protect your accounts, money and data: strong passwords, two-factor authentication, spotting phishing and UPI fraud, malware, safe browsing, backups and social media privacy.

WHO IT IS FOR	Students and computer users who want to stay safe online
LEVEL	Beginner
SUBJECT AREA	Programming and web
WHAT IS INSIDE	7 chapters, practice questions with answers, and a glossary

CONTENTS

1	Strong Passwords and Password Managers	3
2	Two-Factor Authentication	5
3	Phishing, Smishing and Vishing	7
4	UPI and OTP Fraud	9
5	Malware: Types and How It Spreads	12
6	Updates, Antivirus and Safe Browsing	14
7	Backups and Privacy on Social Media	16
	Practice questions	18
	Answers	23
	Glossary	25

Free ebook: you may read, print and share it for learning; it may not be sold or changed. © 2026 Gurukul Technicals Institute. First edition, October 2026. Contact details are on the back cover.

Strong Passwords and Password Managers

Why passwords still matter

Your email, UPI apps, bank account, social media and college portal all sit behind a password. If someone learns that password, they can read your messages, reset your other accounts and pretend to be you. Many account break-ins need no clever hacking: attackers simply guess weak passwords or reuse passwords leaked from another website.

What makes a password weak

- It is short, so a computer can try every combination quickly.
- It uses personal details such as your name, date of birth, mobile number or pet's name, which are easy to find on social media.
- It is a common choice such as 123456, password or qwerty.
- It is reused on many websites. If one site is breached, criminals try the same email and password everywhere else. This is called **credential stuffing**.

What makes a password strong

Length matters more than anything else. A long **passphrase** made of several unrelated words, such as mango-river-pencil-cloud, is easier to remember and far harder to guess than a short jumble like Ri@9.

- Use at least 12 characters; longer is better.
- Make every password **unique**: one account, one password.
- Avoid anything connected to you personally.
- Change a password straight away if a website reports a breach or you suspect someone knows it.

Never share your password with anyone, including friends, "customer care" callers or someone claiming to be from your bank. A genuine organisation will never ask for it.

Password managers

Nobody can remember fifty long, unique passwords. A **password manager** solves this. It is an app or browser feature that stores all your passwords in an encrypted vault. You remember one strong **master password**, ideally protected with two-factor authentication, and the manager remembers the rest.

Most password managers can:

1. Generate long random passwords for you.
2. Fill them in automatically on the correct website. Because autofill matches the saved website address, the manager will not offer your password on a fake look-alike site, which is a useful warning sign.
3. Sync your vault between your phone and computer.
4. Warn you about reused or leaked passwords.

Browsers such as Chrome, Edge and Firefox have built-in password managers, and separate password manager apps are also available. Whichever you choose, the master password must be strong and must never be written on a sticky note beside the computer.

Passkeys

Many large services, including Google, Microsoft and Apple, now also support **passkeys**. A passkey lets you sign in with your phone's or computer's fingerprint, face unlock or screen lock (PIN or pattern) instead of typing a password. The website never receives a secret you could be tricked into typing, and a passkey works only on the genuine website it was created for, so it resists phishing far better than a password.

Example

Priya used the same password for her email and a small shopping website. When the shopping site was breached, criminals logged in to her email and reset her social media password too. With a unique password for each site, the breach would have exposed only that one shopping account.

KEY POINTS

- Length matters most: use a passphrase of at least 12 characters.
- Use a different password for every account.
- A password manager keeps passwords in an encrypted vault behind one master password.
- Never share a password, even with someone claiming to be from your bank.
- Passkeys sign you in with your device screen lock and resist phishing.

TRY THESE EXERCISES

1. Write three practice passphrases (not ones you will really use) of at least four unrelated words each, count the characters in each one, and check that none of them contains your name, date of birth, mobile number or any other personal detail.
2. Open the password manager built into your browser, such as Google Password Manager in Chrome or the Passwords page in Edge, count how many passwords are saved, and run its password check to list any that are reused, weak or leaked.
3. List your five most important accounts, such as email, banking app and social media; change any password that is short or reused to a unique passphrase, and set up a passkey on any of those accounts that offers one.

CHAPTER 2

Two-Factor Authentication

What is two-factor authentication?

Two-factor authentication (2FA), also called two-step verification, asks for a second proof of identity in addition to your password. It is the most common form of multi-factor authentication (MFA), which means using two or more proofs. Even if a criminal steals your password, they still cannot sign in without the second factor.

The three kinds of factors

Factor	Meaning	Examples
Something you know	A secret in your memory	Password, PIN
Something you have	A device you own	Phone receiving an OTP, authenticator app, security key
Something you are	A feature of your body	Fingerprint, face recognition

True 2FA combines two **different** kinds. A password plus a security question is still "something you know" twice, so it is much weaker.

Common types of second factor

SMS or email OTP

A one-time password (OTP) is sent to your registered mobile number or email. It is easy to use and far better than no 2FA. However, criminals can trick you into reading the OTP out to them, and if someone gets a duplicate SIM issued in your name (a **SIM swap**), they receive your OTPs too.

Authenticator apps

Apps such as Google Authenticator and Microsoft Authenticator show a new six-digit code every 30 seconds or so. The code is generated on your phone itself and does not travel over SMS. You set it up once by scanning a QR code shown by the website.

Push approval

Some services send a notification asking "Is this you trying to sign in?" Tap **Approve** only if you are signing in at that very moment. Attackers sometimes send many requests, hoping you tap Approve just to stop the alerts. If you get a prompt you did not start, deny it and change your password.

Security keys and passkeys

A physical security key (a small USB or NFC device) or a passkey gives the strongest protection, because it works only with the genuine website and cannot be read out over the phone.

Backup codes

When you turn on 2FA, most services offer a set of **backup codes**. Each code works once. Print them or store them somewhere safe and offline. If you lose your phone, these codes let you back into your account.

Where to turn on 2FA first

1. Your main email account, because it can reset every other password.
2. Banking and payment apps (most already use an OTP or PIN).
3. Social media and messaging, such as Instagram, Facebook and WhatsApp (WhatsApp calls it two-step verification and uses a six-digit PIN).
4. Cloud storage such as Google Drive or OneDrive.

An OTP is like the key to your house. Never tell an OTP to anyone, even if they say they are from your bank, a courier company or the police.

Example

Rahul's email password leaked in a data breach. Because he had set up an authenticator app, the attacker got stuck at the second step. Rahul saw a security alert, changed his password and lost nothing.

KEY POINTS

- 2FA adds a second proof of identity, so a stolen password alone is not enough.
- The factors are something you know, something you have and something you are.
- Authenticator apps are safer than SMS OTPs; security keys and passkeys are strongest.
- Deny any sign-in approval request you did not start.
- Keep backup codes offline in case you lose your phone.

TRY THESE EXERCISES

1. Open the security settings of your main email account, turn on two-step verification, and write down every kind of second factor it offers, such as SMS code, authenticator app, sign-in prompt on your phone or passkey.
2. Install an authenticator app such as Google Authenticator or Microsoft Authenticator, link it to one of your accounts by scanning the QR code shown by the website, then sign out and sign in again to confirm the six-digit code works.
3. Generate the backup codes for that account, print them or copy them onto paper and keep them somewhere safe away from your phone; then turn on two-step verification with a six-digit PIN in WhatsApp under Settings > Account.

CHAPTER 3

Phishing, Smishing and Vishing

What is phishing?

Phishing is a trick in which a criminal pretends to be someone you trust, such as your bank, a delivery company, an employer or a government department, to make you click a link, open an attachment, or reveal passwords, card details or OTPs. The name comes from "fishing": the attacker throws out bait and waits for someone to bite.

Types of phishing

Name	Channel	Typical example
Phishing	Email	"Your account will be suspended. Verify now."
Smishing	SMS or chat apps	"Your parcel is on hold. Pay ! 25 to release it."

Name	Channel	Typical example
Vishing	Voice call	A caller claims to be from your bank's "KYC department".
Spear phishing	Targeted message	An email that uses your name, college and teacher's name.

Warning signs

- **Urgency or fear:** "Your electricity will be cut tonight", "Your account will be blocked in 2 hours".
- **Too good to be true:** lottery wins, surprise cashback, or a part-time job paying a lot for "liking videos".
- **Requests for secrets:** passwords, OTPs, UPI PINs or card CVV numbers. Genuine organisations do not ask for these.
- **Odd sender details:** a free email address claiming to be a bank, or a look-alike website address such as `yourbank-kyc-update.com` instead of the bank's real address.
- **Unexpected attachments**, especially files that ask you to "enable content", or app files (.apk) sent on WhatsApp.
- **Spelling and grammar mistakes**, although well-made phishing can look perfect, so never rely on this sign alone.

Vishing in detail

Phone scams work because a confident voice creates pressure. The caller may already know your name and the last digits of your card, which makes them sound genuine. Common stories include KYC updates, a "blocked" SIM card, a refund that needs your PIN, or a fake police officer saying a parcel in your name contains illegal items. Some fraudsters keep victims on a video call and claim they are under "digital arrest". Real police and investigating agencies do not arrest people over video calls or demand money to close a case.

When in doubt, hang up and call the organisation back on the number printed on your card, passbook or official website. Never use a number given by the caller or written in the suspicious message.

What to do with a suspicious message

1. Do not click links or download attachments.
2. Do not reply or call the number in the message.
3. Check directly through the official app or website you already use.
4. Report it: most email services have a **Report phishing** option, and banks have official ways to report fraud.
5. Delete the message.

If you already clicked

Change the password of the affected account from a safe device, turn on 2FA, inform your bank at once if you shared any financial details, and run an antivirus scan. Acting quickly limits the damage.

Example

Anjali received an SMS: "Dear customer, your PAN is not updated and your account will be blocked today. Click here." Instead of clicking, she opened her bank's official app. Everything was normal, so she reported the message and deleted it.

KEY POINTS

- Phishing impersonates a trusted source to steal secrets or install malware.
- Smishing uses SMS or chat apps; vishing uses voice calls.
- Urgency, prizes and requests for OTPs or PINs are red flags.
- Verify by calling the official number on your card or the official website.
- If you clicked, change passwords, enable 2FA and tell your bank quickly.

TRY THESE EXERCISES

1. Collect five suspicious SMS, email or WhatsApp messages from your own phone, or a family member's phone with their permission, without clicking any link or replying, and for each one write down the warning signs it shows: urgency, a prize, a request for an OTP or PIN, an odd sender or a look-alike address.
2. Write ten short example messages of your own, five genuine and five phishing, mix them up, and ask a classmate to sort them into the two groups and name the warning sign in each phishing message.
3. Write a short script of what you would say to a vishing caller who claims to be from your bank's KYC department, ending with hanging up and calling the number printed on your card, and role-play it with a friend taking the caller's part.

CHAPTER 4

UPI and OTP Fraud

The one rule that stops most UPI fraud

UPI (Unified Payments Interface) lets you send money instantly from apps such as BHIM, Google Pay, PhonePe, Paytm or your bank's own app. Payments are approved with your secret **UPI PIN**.

You never need to enter your UPI PIN or scan a QR code to **receive** money. The PIN is for paying money out of your account, never for receiving it.

Common UPI and OTP frauds

Fake payment requests and links

A fraudster sends a link, a QR code or a payment request dressed up as a "refund", "cashback" or "prize". If you approve it with your UPI PIN, money leaves your account. Read every screen carefully: if it asks for your PIN, you are paying.

QR code tricks

A "buyer" on an online marketplace, perhaps for your old sofa, sends a QR code and says, "Scan this to receive the payment." Scanning a QR code and entering your PIN always **sends** money from you.

OTP sharing

Criminals call pretending to be from a bank, a mobile network or a shopping site and ask you to "confirm" the OTP you just received. That OTP was generated for a transaction or account change they started. Read the whole OTP message: it usually says what the OTP is for and warns you not to share it.

Screen-sharing and remote-access apps

A fake "customer care" agent asks you to install a screen-sharing or remote-access app to "solve your problem". Once it is installed, they can watch you type PINs and OTPs. Never install such apps at a stranger's request.

Fake customer care numbers

An internet search for a company's helpline can show numbers posted by fraudsters. Take helpline numbers only from the official app, the official website or the back of your card.

Fake payment screenshots

A shopkeeper may be shown a fake screenshot of a "successful" payment. Merchants should confirm every payment in their own app, bank SMS or payment sound box before handing over goods.

Safe habits

- Keep your UPI PIN secret; never write it on your phone cover or save it in notes.
- Use a screen lock and an app lock on payment apps.
- Check the receiver's name on the confirmation screen before paying.
- Set a sensible transaction limit in your banking app if it offers one.

- Turn on SMS and email alerts for every transaction.

If you are a victim

Speed matters: the sooner fraud is reported, the better the chance of stopping the money.

1. Call your bank immediately on its official number and ask it to block your card, UPI or net banking.
2. Report the fraud on the national cyber crime helpline **1930**, or on the National Cyber Crime Reporting Portal at cybercrime.gov.in.
3. Keep evidence: screenshots, transaction IDs, the fraudster's number and the messages.
4. Change the passwords and PINs of the affected accounts.

Example

Suresh listed his old cooler for sale online. A "buyer" sent a QR code to "pay" ! 4,000. Suresh remembered that receiving money never needs a PIN, refused to scan it, and gave the buyer his UPI ID instead. No money ever arrived, which showed it was a scam.

KEY POINTS

- You never need a UPI PIN or a QR scan to receive money.
- Never share an OTP; read what the OTP message says it is for.
- Do not install screen-sharing apps at a stranger's request.
- Take helpline numbers only from official apps, websites or your card.
- Report fraud at once to your bank and on 1930 or cybercrime.gov.in.

TRY THESE EXERCISES

1. Open your UPI app, or a family member's with their permission, and find where it shows the receiver's name before a payment (stop at that screen without entering your UPI PIN, so no money is sent), where the transaction history is kept and whether you can set a transaction limit; write down the menu path to each.
2. Read five OTP messages already on your phone and copy down, for each one, what the OTP was sent for and the warning the message gives about not sharing it.
3. Make a one-page poster for a shop counter or your home titled "PIN only to pay, never to receive", listing the six frauds described in this lesson and the national cyber crime helpline number 1930 for reporting fraud.

Malware: Types and How It Spreads

What is malware?

Malware means malicious software: any program written to harm a device, steal data or take control of it. Malware usually arrives through infected downloads, pirated software, email attachments, fake apps, malicious advertisements or infected pen drives.

Main types of malware

Type	What it does
Virus	Attaches itself to a file or program and spreads when that file is run or shared.
Worm	Spreads by itself across networks without anyone opening a file.
Trojan	Pretends to be useful software, such as a free game or a "crack", but hides harmful code.
Ransomware	Encrypts your files and demands payment, often in cryptocurrency, to unlock them.
Spyware	Secretly watches your activity and sends information to the attacker.
Keylogger	Records the keys you press, capturing passwords and card numbers.
Adware	Floods you with unwanted advertisements and pop-ups.
Rootkit	Hides deep in the system to keep an attacker's access secret, even from security tools.

A computer controlled remotely by an attacker is called a **bot**, and a large group of them is a **botnet**. Botnets are used to send spam or flood websites with traffic until they stop working.

Virus, worm and trojan: the key difference

Students often confuse these three. Remember it like this:

- A **virus** needs a host file and a person to run it.
- A **worm** needs no host file and copies itself across a network automatically.
- A **trojan** does not copy itself; it tricks you into installing it.

Ransomware in more detail

Ransomware is especially damaging for businesses. A shop's billing computer holding years of GST invoices can become unusable overnight. Paying the ransom does not guarantee you will get your files back, and it funds more attacks. The best defence is a recent backup kept disconnected from the computer, together with updates and careful behaviour.

Signs a device may be infected

- It suddenly becomes very slow, or the fan runs loudly while you are doing nothing.
- Pop-ups appear even when no browser is open.
- The browser's home page or search engine changes by itself.
- Friends receive messages you never sent.
- Files are renamed with strange extensions and a ransom note appears.
- On a phone: the battery drains quickly, data usage jumps, or unknown apps appear.

How malware gets in, and how to keep it out

1. **Pirated software and cracks** are a very common source of trojans. Use genuine software or legitimate free alternatives.
2. **Unknown apps**: on Android, install apps from the Google Play Store and avoid app files sent over WhatsApp or SMS.
3. **Attachments**: do not open unexpected files, even from friends, until you have checked with the sender.
4. **Pen drives**: scan USB drives before opening files, especially after using shared computers in a cyber cafe or office.
5. **Scary pop-ups**: do not click website pop-ups that say "Your PC is infected!"; they are often scams themselves.

If you think a computer is infected, first disconnect it from the internet and the office network, then run a full antivirus scan.

KEY POINTS

- Malware is any software designed to harm, spy on or control a device.
- A virus needs a host file, a worm spreads by itself, a trojan disguises itself.
- Ransomware encrypts files and demands payment; an offline backup is the best defence.
- Pirated software, unknown apps, attachments and pen drives are common routes in.

TRY THESE EXERCISES

1. Make a table of the eight malware types in this lesson with three columns: what it does, how it usually gets onto a device, and one sign that a device may have it.
2. Open the Windows Security app on a computer, go to Virus & threat protection, run a Quick scan, and note how many files were scanned and when the protection updates were last installed.
3. Plug a pen drive into a Windows computer, right-click it in File Explorer (choose Show more options first on Windows 11 if needed), select Scan with Microsoft Defender before opening any file, and record the result.

CHAPTER 6

Updates, Antivirus and Safe Browsing

Why updates matter

All software contains mistakes, and some of them, called **vulnerabilities**, let attackers break in. When a company fixes one, it releases a **patch** in an update. Criminals study these patches and then attack devices that have not installed them, so delaying updates for months is risky.

- On Windows 11, updates are under **Settings > Windows Update** (on Windows 10, **Settings > Update & Security > Windows Update**).
- Windows 10 reached its end of support in October 2025. After that, a Windows 10 PC receives security updates only if it is enrolled in Microsoft's time-limited Extended Security Updates (ESU) programme, so moving to Windows 11 on supported hardware is the long-term answer.
- On Android and iPhone, check Settings for system updates, and keep apps updated through the Play Store or App Store.
- Browsers such as Chrome, Edge and Firefox usually update themselves but need a restart to finish.

Antivirus software

Antivirus software scans files and watches running programs to detect and block malware. Windows 10 and 11 include **Microsoft Defender Antivirus** in the Windows Security app, and it stays on unless another antivirus product takes over. Good habits:

- Keep real-time protection switched on.
- Let the antivirus update its definitions automatically.
- Run only **one** real-time antivirus at a time; two can conflict and slow the computer down.

- Avoid "free PC cleaner" or "speed booster" tools from unknown websites; some are malware themselves.

Windows also includes a **firewall**, which controls which network connections are allowed in and out. Leave it switched on. Remember that antivirus and firewalls are safety nets, not guarantees; careful behaviour is still the strongest defence.

Safe browsing and HTTPS

When a website address starts with `https://`, the connection between your browser and the website is **encrypted**, so others on the same network cannot read what you send, such as passwords. Browsers show this with a padlock or a similar icon beside the address.

HTTPS means the connection is private. It does **not** mean the website is honest. Many phishing sites use HTTPS too.

So always check the **domain name** itself. In `https://www.examplebank.in/login` the domain is `examplebank.in`. In `https://examplebank.in.secure-login.xyz/login` the real domain is `secure-login.xyz`, and the bank's name at the start is only decoration. Find the website name, which ends just before the first single slash, and read it from right to left: the real domain is at the right-hand end.

Other safe-browsing habits

1. Type important addresses yourself or use bookmarks instead of clicking links in messages.
2. Download software only from the official website or app store.
3. Do not allow notifications from random websites; scammers use them to show fake alerts.
4. On public Wi-Fi at railway stations, cafes or malls, avoid banking; use mobile data for sensitive tasks.
5. On shared computers, such as those in a cyber cafe, use a private window, never let the browser save your password, and sign out when you finish.
6. Take browser warnings such as "Your connection is not private" seriously and do not enter anything sensitive on that site.

KEY POINTS

- Updates patch vulnerabilities, so install them promptly.
- Windows 10 and 11 include Microsoft Defender Antivirus; run only one real-time antivirus.
- HTTPS encrypts the connection but does not prove a site is genuine.
- Check the real domain name before entering a password.
- Avoid banking on public Wi-Fi and sign out on shared computers.

TRY THESE EXERCISES

1. Open Windows Update in Settings on a computer, check for updates, and note the date of the most recent update in the update history and whether a restart is pending; then check your phone for a system update and update all its apps from the Play Store or App Store.
2. In the Windows Security app, confirm that Real-time protection is on under Virus & threat protection > Virus & threat protection settings > Manage settings, and that the firewall is on for every network type under Firewall & network protection, and write down anything that shows a warning.
3. Write ten made-up website addresses that use the name of a bank or shop, some genuine-looking and some tricks with the name at the start, then for each one underline the real domain by finding the first single slash and reading leftwards from it.

CHAPTER 7

Backups and Privacy on Social Media

Why back up?

A backup is an extra copy of your data kept somewhere else. Hard disks fail, phones get lost or stolen, ransomware locks files and people delete things by mistake. With a backup, each of these becomes an inconvenience instead of a disaster.

The 3-2-1 rule

A simple, widely used guideline:

- **3** copies of important data (the original plus two backups),
- on **2** different types of storage, such as your laptop and an external hard disk,
- with **1** copy kept off-site, such as in cloud storage or at another location.

Backup options

Option	Good for	Watch out for
External hard disk or SSD	Large amounts of data, fast restore	Unplug it after backing up so ransomware cannot reach it
Pen drive	Small, quick copies	Easy to lose; not ideal as the only backup
Cloud storage (Google Drive, OneDrive, iCloud)	Automatic, off-site copies	Protect the account with a strong password and 2FA

Windows includes **File History** for backing up personal folders to an external drive, phones can back up photos and contacts to the cloud automatically, and WhatsApp chats are backed up separately from WhatsApp's own settings.

Syncing is not the same as a backup. If a synced file is deleted or encrypted on your PC, that change can sync to the cloud as well. Use version history or keep a separate backup copy.

Every few months, try restoring one file from your backup. A backup you have never tested is only a hope.

Privacy on social media

Anything you post can be copied, screenshotted and shared, even after you delete it. Criminals collect details from public profiles to guess passwords, answer security questions and make phishing messages convincing.

What not to share publicly

- Your phone number, home address or daily routine.
- Photos of your Aadhaar card, PAN card, tickets, boarding passes or bank documents. When you must share an Aadhaar copy for verification, many services accept a **masked Aadhaar**, which shows only the last four digits of the number.
- Your live location while you are away, for example "Off to Goa for a week!" while the house stands empty.
- Answers to common security questions, such as your first school or your mother's maiden name.

Privacy settings to review

1. Make your profile private, or limit who can see your posts, friends list and tagged photos.
2. Control who can find you by phone number or email.
3. Remove third-party apps and quizzes you no longer use from your account.
4. Turn off location tagging on photos if you do not need it.

Fake profiles and impersonation

Scammers copy a person's photos and name to create a duplicate account, then message that person's friends asking for urgent money. If a friend suddenly asks for money online, call them on the number you already have to confirm. Report fake profiles using the platform's report option.

Before posting, ask yourself: would I be comfortable if a stranger, a future employer or a fraudster saw this?

KEY POINTS

- Follow 3-2-1: three copies, two kinds of storage, one copy off-site.
- Keep an unplugged backup to survive ransomware, and test restoring files.
- Syncing alone is not a backup.
- Never post Aadhaar, PAN, tickets or your live location publicly.
- Confirm unexpected money requests from friends by phone.

TRY THESE EXERCISES

1. Plan a 3-2-1 backup for your own phone and computer in a table that lists your important data, the two kinds of storage you will use and where the off-site copy will be kept, then make one backup copy to a pen drive or external disk.
2. Copy a practice file into your backup, delete the original from the computer, and then restore it from the backup, noting how long the restore took and whether the file opens correctly.
3. Open the privacy settings of one social media account you use, make the profile private or limit who can see your posts, turn off finding you by phone number, and remove any connected third-party apps you no longer use.

CHECK YOURSELF

Practice questions

Choose the best answer for each question. The answers, with a short explanation, are in the next chapter.

1. Which of these passwords is the strongest?

- a) Password@12345
- b) mango-river-pencil-cloud-42
- c) Ravi@Delhi1998
- d) 9876543210

2. What is credential stuffing?

- a) Saving many passwords in one browser profile
- b) Watching someone type their PIN over their shoulder
- c) Trying passwords leaked from one site on other sites
- d) Guessing a password by trying every possible combination

3. What does a password manager mainly do?

- a) Stores passwords in an encrypted vault behind one master password
- b) Scans the computer and removes viruses and other malware
- c) Speeds up your internet connection by caching pages
- d) Sends a copy of every password you use to your bank for safekeeping

4. How do you usually sign in with a passkey?

- a) By typing a long password from memory each time
- b) By entering a code that arrives by post
- c) By answering a security question about your first school
- d) With your device's fingerprint, face or screen lock

5. Which combination is true two-factor authentication?

- a) A password and a code from an authenticator app
- b) A password and the answer to a security question
- c) Two different passwords typed one after the other
- d) A username and a password typed on a trusted PC

6. A fingerprint belongs to which type of authentication factor?

- a) Something you know
- b) Something you are
- c) Something you have
- d) Something you share

7. Why is an authenticator app generally safer than an SMS OTP?

- a) It lets you sign in without using any password at all
- b) It sends the code to your email as well as your phone
- c) The code is made on your phone and does not travel by SMS
- d) It still works even when you do not have your phone with you

8. Your phone shows a sign-in approval request that you did not start. What should you do?

- a) Deny it and change your password
- b) Approve it to stop the alerts
- c) Ignore it and approve the next one
- d) Turn off two-factor authentication

9. What are 2FA backup codes for?

- a) Backing up your photos and files to the cloud
- b) Getting back into your account if you lose your phone
- c) Making your existing password longer and stronger
- d) Skipping the password every time you sign in

10. Smishing is phishing carried out through which channel?

- a) Voice phone calls
- b) Infected pen drives
- c) SMS or chat messages
- d) Printed letters sent by post

11. Vishing is phishing carried out through which channel?

- a) Video files
- b) Email attachments
- c) Fake mobile apps
- d) Voice phone calls

12. A caller says he is from your bank and asks for your card details to "update KYC". What is the safest response?

- a) Hang up and call the bank on the number printed on your card
- b) Give the details because he already knows your name
- c) Ask him for his direct number and call him back on that number
- d) Share only the CVV but never the full card number

13. Which is a common warning sign of a phishing message?

- a) It is written in clear and simple language
- b) It creates urgency, such as "act within 2 hours"
- c) It arrives during normal office hours
- d) It contains no links and no attachments at all

14. What is spear phishing?

- a) Phishing emails sent to millions of random addresses
- b) A virus that spreads from phone to phone over Bluetooth
- c) A deep antivirus scan that searches for hidden phishing files
- d) A phishing message aimed at one person, using their details

15. On a video call, a person in uniform says you are under "digital arrest" and must pay to clear your name. What is true?

- a) You must pay within one hour to avoid being sent to jail
- b) It is a scam: police never arrest or collect money on video calls
- c) You should share your screen so they can check your account
- d) You should send them your OTP so they can prove that you are innocent

16. A buyer says, "Scan this QR code and enter your UPI PIN to receive ! 5,000." What will actually happen?

- a) ! 5,000 will be credited to your account
- b) Your UPI ID will only be verified
- c) Nothing will happen until the buyer approves
- d) Money will be sent from your account

17. Which statement about the UPI PIN is correct?

- a) It is needed only to pay money, never to receive it
- b) It must be entered every time you receive money
- c) Bank staff may ask for it on a call to verify your account
- d) It is the same as the OTP that arrives by SMS

18. A "customer care" agent asks you to install a screen-sharing app to fix a payment problem. Why is this dangerous?

- a) It makes your phone battery charge much more slowly
- b) It permanently changes your registered mobile number with the bank
- c) They can watch your screen while you type PINs and OTPs
- d) It switches off your phone's camera and microphone

19. Where should you find a bank's helpline number?

- a) In the first result of any internet search for the bank
- b) The bank's official app or website, or the back of your card
- c) In an SMS saying that your account has been blocked
- d) From a helpful stranger in a social media comment

- 20. Which number is the national cyber crime helpline in India for reporting online financial fraud?**
- a) 1930
 - b) 108
 - c) 1098
 - d) 139
- 21. Which type of malware spreads across a network by itself without anyone opening a file?**
- a) Trojan
 - b) Adware
 - c) Worm
 - d) Keylogger
- 22. A free "cracked" game that secretly installs harmful code is an example of which malware?**
- a) Worm
 - b) Firewall
 - c) Software patch
 - d) Trojan
- 23. What does ransomware do?**
- a) Shows unwanted advertisements and pop-ups only
 - b) Speeds up an old computer by deleting junk files
 - c) Encrypts your files and demands payment to unlock them
 - d) Copies your files to the cloud as a backup
- 24. What does a keylogger capture?**
- a) Your screen brightness settings
 - b) Your Wi-Fi speed
 - c) The keys you press, including passwords
 - d) The pages you print and the printer settings
- 25. You suspect an office computer is infected. What should you do first?**
- a) Copy its files to colleagues' computers for safety
 - b) Install a second antivirus alongside the first one
 - c) Click the website pop-up that offers to clean the computer
 - d) Disconnect it from the network, then run a full scan
- 26. What is a botnet?**
- a) A network of chat robots that answer website visitors
 - b) A group of infected computers controlled by an attacker
 - c) A strong password made of several random words
 - d) A backup copy of your files stored in the cloud
- 27. Why should software updates be installed promptly?**
- a) They fix security holes that attackers could use
 - b) They always make the device run much faster than before
 - c) They remove the need for passwords and PINs
 - d) They free up space by deleting old photos
- 28. Which antivirus is built into Windows 10 and Windows 11?**
- a) Microsoft Defender Antivirus
 - b) Windows Media Player
 - c) File Explorer
 - d) Microsoft Paint

29. A website address begins with https:// and shows a padlock. What does this tell you?

- a) The website is definitely genuine
- b) The website is run by the government
- c) The website contains no malware or fake content
- d) The connection to the site is encrypted

30. In the address https://examplebank.in.secure-login.xyz/login, what is the real domain?

- a) examplebank.in
- b) secure-login.xyz
- c) login
- d) https

31. What is the safest choice for online banking when you are on free public Wi-Fi at a railway station?

- a) Bank on the Wi-Fi because the station runs it
- b) Turn off your phone's screen lock to save time
- c) Use your own mobile data instead of the free Wi-Fi
- d) Continue even if the browser shows a security warning

32. What does the 3-2-1 backup rule recommend?

- a) Three passwords, two email accounts and one registered phone number
- b) Back up three times a day on two days of each week
- c) Three copies, on two types of storage, with one kept off-site
- d) Three backups, all kept together on one pen drive

33. Why should an external backup drive be unplugged when it is not in use?

- a) So that the drive never needs to be replaced
- b) Because Windows cannot read a drive that is left connected all the time
- c) To make the computer start up a little faster
- d) So ransomware on the computer cannot encrypt the backup too

34. In a masked Aadhaar, how much of the 12-digit Aadhaar number can be seen?

- a) Only the first four digits
- b) Only the last four digits
- c) Only the first eight digits
- d) All twelve digits

35. A friend messages you on social media asking for urgent money. What is the best first step?

- a) Call the friend on the number you already have to confirm
- b) Send the money quickly before it is too late
- c) Reply with your UPI PIN so that they can collect the money faster
- d) Share the message publicly

Answers

1. **(b) mango-river-pencil-cloud-42.** A long passphrase of unrelated words is much harder to guess than a short password or one built from a name, birth year or phone number.
2. **(c) Trying passwords leaked from one site on other sites.** Attackers reuse leaked email and password pairs on other sites, which is why every account needs a unique password.
3. **(a) Stores passwords in an encrypted vault behind one master password.** A password manager remembers and fills in long, unique passwords so you only need to remember the master password.
4. **(d) With your device's fingerprint, face or screen lock.** A passkey uses your device and its screen lock, so there is no password to type or be tricked into revealing.
5. **(a) A password and a code from an authenticator app.** True 2FA uses two different kinds of factor; a password (something you know) plus an app code (something you have) qualifies.
6. **(b) Something you are.** Body features such as fingerprints and faces are "something you are".
7. **(c) The code is made on your phone and does not travel by SMS.** An authenticator app creates the code on the device itself, so it cannot be intercepted in transit or redirected by a SIM swap.
8. **(a) Deny it and change your password.** An unexpected request means someone may have your password; denying it blocks them and changing the password removes their access.
9. **(b) Getting back into your account if you lose your phone.** Each backup code works once and lets you sign in when your usual second factor is unavailable.
10. **(c) SMS or chat messages.** Smishing combines SMS and phishing: fake messages that try to make you click a link or reveal details.
11. **(d) Voice phone calls.** Vishing means voice phishing, where a caller pretends to be from a bank, company or authority.
12. **(a) Hang up and call the bank on the number printed on your card.** Calling the official number yourself confirms whether the request is genuine; a number given by the caller could belong to the fraudster.
13. **(b) It creates urgency, such as "act within 2 hours".** Fraudsters create urgency or fear so you act before you think.
14. **(d) A phishing message aimed at one person, using their details.** Spear phishing is targeted: it uses details such as your name, workplace or college to look convincing.
15. **(b) It is a scam: police never arrest or collect money on video calls.** Police and investigating agencies do not conduct arrests over video calls or demand payment; this is a well-known fraud.

- 16. (d) Money will be sent from your account.** Scanning a QR code and entering your PIN always pays money out; receiving money never needs a PIN.
- 17. (a) It is needed only to pay money, never to receive it.** The UPI PIN authorises payments out of your account and must be kept secret from everyone.
- 18. (c) They can watch your screen while you type PINs and OTPs.** Remote-access and screen-sharing apps let a fraudster see or control your phone, including your banking apps.
- 19. (b) The bank's official app or website, or the back of your card.** Fraudsters post fake helpline numbers online and in messages, so take the number only from official sources.
- 20. (a) 1930.** 1930 is the national cyber crime helpline; reporting quickly improves the chance of stopping the money.
- 21. (c) Worm.** A worm copies itself across networks automatically and does not need a host file or a user action.
- 22. (d) Trojan.** A trojan disguises itself as something useful so that you install it yourself.
- 23. (c) Encrypts your files and demands payment to unlock them.** Ransomware locks files with encryption and demands a ransom; an offline backup is the best protection.
- 24. (c) The keys you press, including passwords.** A keylogger records keystrokes so the attacker can read passwords and card numbers.
- 25. (d) Disconnect it from the network, then run a full scan.** Disconnecting stops the malware spreading or sending data out while you scan and clean the computer.
- 26. (b) A group of infected computers controlled by an attacker.** Infected computers (bots) are linked into botnets and used to send spam or flood websites.
- 27. (a) They fix security holes that attackers could use.** Attackers target known vulnerabilities on devices that have not installed the patch.
- 28. (a) Microsoft Defender Antivirus.** Microsoft Defender Antivirus is part of the Windows Security app in Windows 10 and 11.
- 29. (d) The connection to the site is encrypted.** HTTPS protects data in transit, but phishing sites can use HTTPS too, so the domain still needs checking.
- 30. (b) secure-login.xyz.** Read the website name (everything before the first single slash) from the right: the registered domain is secure-login.xyz, and "examplebank.in" is only a subdomain prefix chosen to fool you.
- 31. (c) Use your own mobile data instead of the free Wi-Fi.** Public Wi-Fi is shared with strangers, so sensitive tasks are safer on your own mobile data.
- 32. (c) Three copies, on two types of storage, with one kept off-site.** Multiple copies on different media, with one away from the original, protect against failure, theft and disasters.
- 33. (d) So ransomware on the computer cannot encrypt the backup too.** Ransomware can encrypt any drive it can reach, so a disconnected backup stays safe.
- 34. (b) Only the last four digits.** A masked Aadhaar hides all but the last four digits of the number, which reduces the risk of misuse when you share a copy.

- 35. (a) Call the friend on the number you already have to confirm.** Scammers often impersonate friends with copied profiles; a call to their known number confirms whether the request is real.

WORD LIST

Glossary

Authenticator app

A phone app, such as Google Authenticator or Microsoft Authenticator, that generates a new short sign-in code every 30 seconds or so as a second factor.

Backup

An extra copy of your data kept on a separate device or in the cloud, so it can be restored if the original is lost, damaged or locked.

Credential stuffing

An attack in which criminals try email and password pairs leaked from one website on many other websites, hoping people have reused them.

Encryption

Scrambling data with a key so that only someone who has the correct key can read it.

Firewall

A security feature that controls which network connections are allowed into and out of a device or network.

HTTPS

HyperText Transfer Protocol Secure, the secure form of the web protocol HTTP, which encrypts the connection between your browser and a website; it keeps data private but does not prove the website is honest.

Malware

Any software written to harm a device, steal data or take control of it, including viruses, worms, trojans, ransomware and spyware.

OTP

A one-time password: a short code sent by SMS or email, or generated by an app, that works only once and expires after a short time.

Passkey

A sign-in method that uses your device's fingerprint, face unlock or screen lock instead of a password and works only on the genuine website it was created for.

Passphrase

A long password made of several unrelated words, which is easier to remember and much harder to guess than a short jumble of characters.

Password manager

An app or browser feature that stores your passwords in an encrypted vault behind one master password and fills them in for you on the correct websites.

Patch

A software fix, delivered in an update, that corrects a bug or closes a security vulnerability.

Phishing

A trick in which a criminal pretends to be a trusted person or organisation to make you click a link, open an attachment or reveal secrets such as passwords or OTPs.

Ransomware

Malware that encrypts the files on a device and demands payment to unlock them.

SIM swap

A fraud in which a criminal gets a duplicate SIM card issued in your name, so your calls and OTP messages reach them instead of you.

Smishing

Phishing carried out through SMS or chat-app messages, such as a fake parcel or electricity bill alert.

Spear phishing

A phishing message aimed at one particular person or group that uses details such as their name, college or workplace to look genuine.

Spyware

Malware that secretly watches what you do on a device and sends the information to an attacker.

Trojan

Malware disguised as useful software, such as a free game or a crack, that tricks you into installing it and does not copy itself.

Two-factor authentication (2FA)

Signing in with a second, different kind of proof of identity, such as a code from your phone, in addition to your password; it is the most common form of multi-factor authentication.

UPI PIN

The secret number that approves payments out of your bank account in a UPI app; it is never needed to receive money.

Virus

Malware that attaches itself to a file or program and spreads when that file is run or shared.

Vishing

Phishing carried out over a voice call, where the caller pretends to be from a bank, company, government office or the police.

Vulnerability

A mistake in software that an attacker can use to break into a device or gain access it should not have.

Worm

Malware that copies itself across networks automatically, without needing a host file or anyone to open it.



Gurukul Technicals Institute

Computer education institute in Delhi, with authorised member centres, robotics classes and science projects, working models and DIY kits.

COURSES

Computer & Office Skills · Accounting & Business Software · Programming & Web Development · Design & Digital Skills · Hardware & Networking · Robotics & Coding · Other Programmes

PROJECTS AND KITS

Ready-made school projects · DIY and STEM kits · Robotics and coding · Components and spares · Engineering projects

CONTACT

Head office: A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007

Phone: 011 2721 1512 · **Mobile and WhatsApp:** +91 97116 99511

Email: engineergurukul@yahoo.co.in

Website: engineergurukul.com · **Instagram:** [@science_projects_club](https://www.instagram.com/science_projects_club)

More free ebooks for computer courses, robotics and science projects: engineergurukul.com/resources/ebooks/

Free to read, print and share. Not for sale.