कोयला मंत्रालय
Ministry of Coal

सत्यमेव जयते

National Cyber Security Awareness Month

October – 2025

Cyber Jagrit Bharat

Cyber Hygiene Handbook

ICT DIVISION
GONDWANA PALACE
CMPDI HQ, RANCHI – 834008
www.cmpdi.co.in

कोयला मंत्रालय
Ministry of Coal

सत्यमेव जयते

सीएमपीडीआई
मिनी रत्न
cmpdi
Mini Ratna

Cyber Security Pledge

I, solemnly pledge to contribute to building a **Cyber Jagrit Bharat** — a digitally secure and resilient India.

I commit to:

- **Stay vigilant** and practice safe cyber habits at work and beyond.
- **Protect** sensitive information by following all organisational security policies and guidelines.
- **Report** any suspicious activities or potential cyber threats immediately to the concerned authorities.
- **Use strong, unique passwords** and regularly update them to safeguard my accounts and devices.
- **Be cautious** while clicking links, opening emails, and downloading attachments to avoid phishing and malware attacks.
- **Keep my software and devices updated** with the latest security patches and antivirus protections.
- **Respect** privacy and confidentiality of data entrusted to me and ensure its secure handling.
- **Promote awareness** among my colleagues, friends, and family to foster a culture of cybersecurity in my community.

Together, through responsible actions and awareness, I will help make India a **Cyber Jagrit Bharat** — a nation where every citizen is alert, empowered, and secure in the digital world.

I pledge to uphold these principles today and always.

Source: https://www.staysafeonline.in/pledge
(An Online Cyber Awareness Campaign by ISEA under MeitY)

Password Security

A password is the lock on your digital door. If it's long, unique, and secret, it keeps intruders out. If you reuse the same password across many sites, one stolen key can open all your doors. Use a passphrase (a short sentence or a few unrelated words) rather than a short, complex jumble—longer is stronger and easier to remember.

Why longer and unique?

- Length resists guessing and brute force. Aim for 14+ characters (more is better).
- Uniqueness stops credential stuffing (Scammers try your leaked password from one site on other sites).
- Memorable patterns like "Name@123" are predictable; attackers try those first.

Possible Threats

- Credential stuffing: Scammers buy or download leaked username/password lists and try them on email, banking, or e-office portals. Reused passwords fall first.
- Brute force / guessing: Short/common passwords ("Welcome@123", "Password@123") are cracked quickly.
- Phishing: Fake pages, emails, or calls trick you to type or tell your password/OTP.
- Shoulder surfing & keylogging: Someone watches you type, or malware records your keystrokes.
- Password reset abuse: Attackers trigger "Forgot Password," intercept OTPs, or answer weak security questions.

How to build a strong passphrase?

- Pick 4–5 unrelated words + a number/symbol you can remember. Example pattern: Word1-Word2-Word3#Year → River-Lotus-Frame#1998
- Avoid personal info (name, birthday, department, vehicle number).
- For high-value accounts, consider longer or add one more word.

✓ **Do's**

- Different passwords for work email, e-office, bank, UPI, and personal accounts—never overlap.
- Turn on login alerts (email/SMS/app) and review account activity monthly.
- Change your password immediately after:
  - a suspicious email/link click,
  - repeated unexpected MFA prompts,
  - device loss/theft, or
  - news of a breach affecting a service you use.
- Harden password reset options:
  - Use strong security answers (treat them like passwords—non-obvious).
  - Keep recovery email/phone current and secure.
- Lock your screen when away (2–5 min auto-lock).
- Use MFA (e.g., Kavach for email) wherever available.

× **Don'ts**

- Don't reuse passwords across sites—ever.
- Don't share passwords on calls, chats, or with colleagues (even "IT" or "bank" staff).
- Don't store passwords in plain text (notes, spreadsheets, sticky notes, screenshots).
- Don't use predictable patterns like Name@123, Dept@Year, or sequential numbers.
- Don't save work passwords in personal browsers or unapproved apps.
- Don't enter passwords after clicking a link in an email/SMS—type the official address or use a bookmark.
- Don't approve MFA prompts you didn't start.

Best Practices

- ✓ One account → one unique passphrase (14+ characters).
- ✓ Password manager + MFA stops most takeovers.
- ✓ If anything feels off, change password + review sessions (sign out of all devices) and report in the Golden Hour.
- ✓ Keep browser and OS updated—it helps block malicious password stealers.
- ✓ Traveling or using shared systems? Avoid typing critical passwords; use mobile hotspot + VPN for sensitive work.

Practical examples

- Bad: Ravi@123, Welcome@123, Password@2024 (short/predictable).
- Better passphrase: Paper-Horizon-Carpet#27 (long, unrelated words).

What to do if you suspect compromise?

- Change the password for the affected account(s) immediately (from a clean device).
- Revoke active sessions / "Sign out of all devices"; review recent activity.
- Turn on/confirm MFA; regenerate backup codes and store them offline.
- Scan your device with updated antivirus/EDR; update OS and browser.
- Monitor bank/UPI/email for alerts or unfamiliar activity for the next few days.
- Report to your IT Helpdesk for office PC.

Quick myths vs facts

- Myth: "Complex = secure."
  Fact: Length + uniqueness matters more than symbols alone. A 4-word passphrase beats an 8-char jumble.
- Myth: "I can share my password with my team—it's official work."
  Fact: Shared passwords remove accountability and increase risk. Use proper access controls, not shared secrets.
- Myth: "I changed it last year; I'm safe."
  Fact: Change after incidents and when reuse/weakness is discovered; otherwise focus on long, unique, MFA-protected credentials.

Regular Software Updates (Patch Management)

What it means

- Updates (patches) are repairs for your computer, phone, and apps. They fix security holes that Scammers use to sneak in, and they also improve stability. If you skip updates, you are leaving the door open.

Why it matters

- Most real-world attacks succeed because a known hole wasn't patched.
- A single unpatched browser plugin or router can let attackers in, spread to shared drives, and steal or lock data (ransomware).
- Possible Threats (how attackers exploit unpatched systems)
- Known vulnerabilities: Scammers scan the internet for devices running old Windows, browsers, plugins, or apps and then use public exploits to break in.
- Drive-by downloads: Just visiting a hacked or malicious website with an outdated browser can silently install malware.
- Exploit kits: Toolkits chain multiple bugs (browser + plugin + OS) to gain control.
- Unpatched routers/IoT: Old home/office routers, cameras, or printers get hijacked and used as stepping stones into your network.

How updates work

- Security patches fix the exact hole an attacker is trying to use.
- Feature updates add functions; quality updates improve reliability.
- Some updates require a restart to finish—until you restart, you are not fully protected.

✓ **Do's**

- Turn on auto-updates for:
  - Operating systems (Windows/macOS/iOS/Android),
  - Browsers (Chrome/Edge/Firefox),
  - Office suite and core apps,
  - Security tools (EDR/antivirus),
  - Drivers/firmware when prompted by IT.
- Restart weekly so updates complete installation.
- Update router firmware (office/home): change default admin password, use WPA2/WPA3 security.
- Remove or replace apps that are no longer supported (end-of-life).
- Keep only what you use: fewer apps/extensions mean fewer holes to patch.

× **Don'ts**

- Don't postpone critical updates with "Remind me later."
- Don't use end-of-life OS/apps (e.g., very old Windows releases, outdated Java/Flash/Plugins).
- Don't install drivers/firmware from untrusted links—use official vendor or IT-approved tools.
- Don't ignore repeated prompts to restart—security fixes may not be active yet.

Best Practices

- ✓ Patch early, patch often.
- ✓ Fewer apps = fewer problems (uninstall what you don't need).
- ✓ Browser first: keep your browser and its extensions fully updated.
- ✓ When in doubt, update it—or ask IT helpdesk if it's safe to remove.

Practical examples

- Drive-by case: You visit a news site. A hidden ad targets an old browser and installs a password-stealer. If your browser was current, it would have blocked the exploit.
- Router case: An outdated home router with default password gets hijacked. All traffic (including email logins) passing through can be snooped or altered.
- Office plugin case: An old PDF/Office plugin lets ransomware in via a Weaponized document.

Myths vs Facts

- Myth: "Updates slow my device, so I'll skip them."
  Fact: Security patches are essential. If performance dips, remove bloatware—don't skip protection.
- Myth: "Antivirus is enough."
  Fact: AV helps, but unpatched holes can bypass it. You need both updates and AV.
- Myth: "I'll update later."
  Fact: Attackers exploit known bugs quickly. Delays increase risk dramatically.

Email Security

What it means

- Email is the most common path Scammers use to reach you. They pretend to be someone you trust—a senior official, bank, vendor, or IT desk—to make you click a bad link, open an attachment, share credentials/OTP, or send money. Good email habits stop most attacks.

Why it matters

- One click can reveal passwords, install malware, or redirect payments.
- Scammers use Business Email Compromise (BEC): they hijack/spoof a real work email and then quietly change payment details or ask for urgent transfers.

Possible Threats

- Look-alike domains & display-name spoofing: name@g0v.in vs name@gov.in; the display name looks right, the address is wrong.
- Urgency & fear tactics: "Account blocked," "Final warning," "Immediate approval needed."
- Malicious links/attachments: Fake login pages; attachments with macros or scripts (e.g., .html, .iso, .zip, .xlsm, .exe).
- BEC (Business Email Compromise): Real (or convincingly spoofed) internal or vendor email asks to change bank details or pay urgently.
- Thread hijacking: Attackers reply within a real ongoing thread after compromising an account, so it feels legitimate.
- Invoice/PO fraud: New "updated invoice" with changed beneficiary, or fake tax/filing notices.

- From address doesn't match the display name or known domain.
- Spelling/grammar slightly off; odd greetings or signatures.
- Urgent tone + unusual request (gift cards, bank detail change, new payee).
- Links go to misspelled or unfamiliar domains (hover to preview).
- Attachments you didn't expect, or requests to enable macros.
- Requests to move the conversation to personal email/WhatsApp.
- Payment or bank detail changes communicated only by email.

✓ **Do's**

- Verify the sender: Expand/inspect the full email address and domain (not just the name).
- Hover before you click: Place your mouse over links to view the real URL; if unsure, don't click.
- Type the address yourself: For portals/banking/e-office, type the official URL or use bookmarks.
- Call back on a known number: For approvals, payment changes, or sensitive requests, verify on a second channel (directory number, vendor master) — not the number in the email.
- Use MFA (Kavach) on email/e-office; keep your OS/browser updated.

× Don'ts

- Don't open unexpected attachments or enable macros from Office files.
- Don't enter credentials on any page reached via an email link—go directly to the site.
- Don't call phone numbers listed in the suspicious email—look up the number yourself.
- Don't approve vendor/bank detail changes based on email alone—use second-channel verification and two-person approval.
- Don't forward suspicious emails inside the org without labeling them as suspicious; report them instead.

Best Practices

- ✓ Pause → Verify → Proceed. When unsure, escalate—not click.
- ✓ Use official channels only (typed URLs, known phone numbers).
- ✓ Keep filters updated: allow IT-approved anti-phish, attachment sandboxing, and safe-link protections.
- ✓ Train & test: participate in cyber awareness trainings and aware about latest threats.

Practical Examples

- Look-alike domain: finance@g0v.in asks for "urgent portal re-login." The "0" (zero) instead of "o" (letter) is easy to miss.
- Thread hijack (BEC): A real vendor thread continues with a new "updated account details" PDF. It's the attacker controlling that vendor's mailbox.
- Fake support: "Security Team" sends an .html attachment "for password reset." Opening it shows a perfect copy of your login page—hosted on an unknown site.

Myths vs Facts

- Myth: "It came from a colleague's address, so it's safe."
  Fact: Accounts get compromised; verify unusual requests out-of-band.
- Myth: "The attachment is a PDF; PDFs are safe."
  Fact: PDFs can contain links or exploits; open only if you expect it and verify the sender.
- Myth: "The logo and signature look perfect."
  Fact: Logos are easy to copy. Check the domain and link preview.

Device Security

What it means

- Your PC/laptop and phone are like a wallet full of official documents. If someone steals or even briefly handles them, they can copy files, read email, reset passwords, plant spying tools, or misuse your identity. Good physical habits protect your data—even if the device is lost.

Why it matters

- A minute of unattended time is enough to copy data or insert malware via USB.
- Stolen devices can expose email, chats, documents, and saved passwords.
- With full-disk encryption and remote-wipe, a lost device is far less damaging.

Possible Threats

- Unattended devices: Left in meeting rooms, taxis, cafeterias, hotel lobbies; a quick USB copy or grab-and-go theft.
- "Evil-maid" access: Someone gets brief physical access (hotel room/office) to install a backdoor or hardware keylogger.
- Shoulder surfing: People watch you type passwords or read sensitive content in public spaces.
- Juice-jacking: Malicious public charging ports/cables that try to access data.
- Rogue accessories: USB sticks or dongles that act like keyboards/network cards (BadUSB) to run commands.
- Supply-chain tampering: Untrusted repair shops or modified chargers/cables.

✓ Do's

- Lock automatically: Set auto-lock to 2–5 minutes. Use a strong passcode/biometric (Windows Hello/Touch ID/Face ID).
- Encrypt the disk: Ensure full-disk encryption is on (BitLocker/FileVault/Android & iOS encryption).
- Enable recovery: Turn on Find My Device/Find My iPhone/Find My and remote-wipe capability. Keep IMEI/serial numbers recorded.

- Physically secure at work: Use cable locks, locked drawers, or lockers. Keep devices within sight in meeting rooms.
- Protect your screen: Use privacy filters on laptops/phones when traveling or working in open areas.
- Use your own charger: Prefer your own adapter and cable; if using public USB power, use a data-blocker or a wall adapter (AC).
- Carry minimal data: Keep sensitive files in approved cloud/official drives; download only what you need and delete offline copies after use.
- Update & AV: Keep OS, apps, and security tools updated; run endpoint protection (AV/EDR).

× **Don't**

- Don't leave devices unattended—even "just for a minute." Lock the screen or take them with you.
- Don't plug in unknown USBs/accessories (freebies, found drives, unknown dongles).
- Don't share devices casually.
- Don't use public/shared PCs for official work or to log in to email/portals.
- Don't hand devices to unapproved repair shops—use authorized service only.
- Don't store passwords in browsers on shared or unmanaged devices.

Best Practices

- ✓ Tap & Lock every time you step away.
- ✓ If it's unknown, don't connect (USBs, chargers, adapters).
- ✓ Encrypt by default; assume a device can be lost and plan for minimal impact.
- ✓ Carry-out discipline: Before leaving rooms/cafés/cabs, do a device check (laptop, phone, external drives, ID card).
- ✓ Report quickly: If the device is missing or tampered, act in the Golden Hour—call 1930 and file at cybercrime.gov.in

Practical examples

- Conference room lapse: You leave your unlocked laptop to get printouts. A visitor inserts a USB, copies your "Confidential.xlsx," and leaves in 45 seconds.
- Airport charging kiosk: You plug into a free USB port; a hidden device attempts to read your phone. Your data-blocker blocks the connection.

Quick settings

- Windows 10/11: BitLocker On; auto-lock via Settings → Accounts → Sign-in options; Windows Hello; screen timeout 2–5 min.
- macOS: FileVault On; Lock Screen hot corner or Control+Cmd+Q; screen timeout 2–5 min.
- Android: Strong PIN; Find My Device; encryption (default); screen lock 30 sec–2 min; disable "Install unknown apps."
- iOS/iPadOS: Face ID/Touch ID + strong passcode; Find My; Auto-Lock 1–2 min; USB Restricted Mode On.

Myths vs Facts

- Myth: "My office is secure; I can leave the laptop unlocked."
  Fact: Shared spaces, visitors, and brief absences create risk. Tap & Lock every time.
- Myth: "A phone PIN is enough."
  Fact: Use biometrics + strong PIN and encryption; enable remote-wipe.
- Myth: "Public charging is safe."
  Fact: Use a data-blocker or wall adapter; avoid direct USB data ports.

Wi-Fi Security (Office/Home/Public)

What it means

- Wi-Fi is how your device talks to the internet. On a trusted, secured network, your traffic is harder to spy on. On public or poorly configured Wi-Fi, anyone nearby (or the hotspot owner) could try to read, redirect, or tamper with your data. Think of public Wi-Fi like discussing secrets in a crowded room—assume others can hear.

Why it matters

- Logins, emails, and files can be intercepted on open or fake networks.
- Attackers can create look-alike hotspots ("GovGuest", "Airport_Free_WiFi") to trick you.
- A weak home/office router can be hijacked, letting Scammers snoop or inject malware.

Possible Threats

- Rogue/evil-twin hotspots: A fake network using a familiar name lures you to connect; the operator watches or alters your traffic.
- Open networks (no password): Traffic is unencrypted; others can capture what you send.
- Weak router setup: Default admin passwords, old firmware, or weak Wi-Fi encryption (WEP/WPA) let attackers break in.
- Session hijacking: If apps don't enforce HTTPS properly, attackers can steal your session cookies and impersonate you.
- Man-in-the-middle (MitM): Traffic is intercepted and modified (e.g., redirect to fake logins).
- Bluetooth/Hotspot leaks: Unused radios left on expose your device to drive-by probes and pairing tricks.

✓ **Do's**

- Prefer trusted networks:
  - Office Wi-Fi for official work; at home, use a personal router you control.
  - On public Wi-Fi, connect only if necessary and use VPN before any sensitive task.
- Secure your home/office router:
  - Change default admin password, set WPA2/WPA3 (never WEP), hide/rename SSID if policy allows.
  - Update router firmware periodically; disable WPS and remote admin unless required.
  - Create a guest network for visitors/IoT; keep official devices on a separate SSID.
- Harden your device:
  - Disable auto-connect; forget old networks.
  - Turn Wi-Fi and Bluetooth off when not in use.
  - Ensure firewall and OS/browser updates are on; use EDR/AV as mandated.
- Use encryption end-to-end:
  - Check HTTPS padlock for websites; use official apps instead of web links where possible.
  - Use VPN for office systems or any sensitive work outside the office.

× **Don'ts**

- Don't perform sensitive tasks (e-office, banking, GOV email, uploads of confidential files) on public Wi-Fi without VPN.
- Don't share office Wi-Fi passwords with visitors—give them the guest SSID.
- Don't connect to look-alike networks just because the name seems right—verify with the venue.
- Don't keep auto-connect enabled for cafés/airports/hotels you once used.
- Don't leave personal hotspots open or unsecured.

Best Practices

✓ Known network + VPN = safer session.
✓ No VPN? No sensitive access.
✓ Update routers and devices regularly; strong admin/Wi-Fi passwords only.
✓ Separate networks: Staff vs. Guest vs. IoT wherever possible.

Practical Examples

- Evil-twin café: You join "Cafe_Free_WiFi_2". It's a rogue hotspot. Your login to a site without strict HTTPS is captured; the attacker reuses your session.
- Home router risk: The router still has admin/admin and old firmware. A botnet compromises it and silently watches traffic.
- Hotel Wi-Fi: You open e-office without VPN. A MitM tool injects a fake login page; your credentials are stolen.

Myths vs Facts

- Myth: "HTTPS makes public Wi-Fi totally safe."
  Fact: HTTPS helps a lot, but attackers can still do evil-twin tricks, force captive portals, or target apps that don't enforce HTTPS correctly. Use VPN for sensitive work.
- Myth: "If the Wi-Fi has a password, it's secure."
  Fact: The router may still be weak/outdated. You need WPA2/WPA3, updated firmware, and a strong admin password.
- Myth: "My phone's hotspot is always safe."
  Fact: Weak hotspot passwords or exposed SSIDs can be brute-forced. Use strong passphrases and turn it off when not needed.

If you suspect a Wi-Fi-related compromise?

- Disconnect immediately (turn off Wi-Fi/Bluetooth).
- Connect via mobile hotspot + VPN (or trusted office/home network).
- Change passwords to any accounts used on the suspicious network; revoke sessions and confirm MFA.
- Capture details: SSID name, location, time, screenshots.
- Inform IT helpdesk in case of office PC; request a device health check (AV/EDR scan, logs).

Safe URL Browsing

What it means

- A URL is a website's address. Attackers create look-alike addresses (e.g., c0alindia.in) or use pop-ups and ads to trick you into visiting fake pages that steal passwords or install malware. Before you type a password, make sure you're on the real site.

Why it matters

- One wrong click can lead to a fake login page or a silent download that infects your device.
- Even a familiar logo and design can be copied. Your best defense is to verify the URL and use built-in browser protections.

Possible Threats

- Look-alike domains: mygov.in vs myg0v.in (zero instead of "o").
- Drive-by downloads: Visiting a compromised site triggers a hidden download that exploits an outdated browser or plugin.
- Malvertising/pop-ups: Ads or fake alerts ("Your PC is infected—download now!") push you to install rogue "cleaners" or remote-control tools.
- Search-engine poisoning: Fake support or banking sites appear in results above the real one.
- HTTP downgrade: Sites that don't enforce HTTPS can be tampered with on unsafe networks.

How to verify a site (5 quick checks)?

- Look at the domain name carefully (before the first single /). Spot typos, extra words, or strange endings.
- Check HTTPS padlock in the address bar. No padlock? Do not enter credentials or payment info.
- Click the padlock (or site info) to see certificate details if unsure.
- Use bookmarks for official portals (e-office, bank, HRMS) or type the URL yourself.
- Ignore page design (logos/colors can be copied); trust only a verified domain.

✓ **Do's**

- Use bookmarks/typed URLs for any site where you log in or pay.
- Enable your browser's Safe Browsing / SmartScreen and popup blocking.
- Keep the browser up to date (and remove unused extensions).
- Preview links (hover to see the real URL) before clicking in emails/SMS/chats.
- Prefer official apps for banks and government services, installed from official stores.
- Use VPN when accessing office portals from outside the office.

× Don'ts

- Don't ignore certificate warnings ("Connection not private", "Invalid certificate"). Stop and verify the URL.
- Don't download software from pop-ups, banner ads, or "scan now" sites.
- Don't enter credentials on a site opened from a shortened link or a QR code unless you verify the destination.
- Don't install browser extensions from unknown publishers or links in messages.

Best Practices

- ✓ Padlock + proper domain before entering credentials.
- ✓ When in doubt, don't click—type the official address or use a bookmark.
- ✓ Fewer extensions = fewer risks. Remove anything you don't use.
- ✓ Public Wi-Fi? Use VPN before logging in anywhere.

Practical examples

- Fake banking site: An SMS says "KYC expired—update now." The link opens bank-verify-kyc.info. It looks perfect, but the domain is wrong.
- Tech-support pop-up: A page shows a loud alert: "Virus detected! Call this number / install this tool." Real vendors don't do this.
- Search-result trap: You search "e-office login" and click the first ad result—it's a fake page collecting passwords. Always check the domain.

Myths vs Facts

- Myth: "The padlock means the site is genuine."
  Fact: The padlock means the connection is encrypted, not that the site is trustworthy. You must check the domain.
- Myth: "If it's first on search results, it's safe."
  Fact: Ads and poisoned results can place fake sites on top. Verify the exact URL.
- Myth: "Antivirus will stop bad sites."
  Fact: AV helps, but good browsing habits (verify URL, avoid downloads from ads) are essential.

If you clicked by mistake

- Close the tab immediately (don't interact with pop-ups).
- Clear downloads you didn't intend; don't run anything you just downloaded.
- Change passwords for any accounts you might have exposed—do it from a known-good device.
- Run a security scan (EDR/AV) and ensure OS/browser are updated.
- Capture evidence (screenshots, URL) for the security team.
- Report to IT Helpdesk in case of office machine.

Quick tips for day-to-day browsing

- Prefer bookmarks for critical sites.
- For links in emails/SMS/QRs, verify first (domain check) before visiting.
- If a page asks to install something, stop and check with report to IT helpdesk.
- If anything looks odd (spelling errors, off-brand domain, aggressive pop-ups), leave immediately and report.

Identity Theft Security

What it means

- Identity theft happens when Scammers collect pieces of your personal information—like Aadhaar, PAN, phone number, date of birth, selfies, bank details, or OTPs—and use them to impersonate you, open accounts/loans, take over your SIM or email, or steal money. They rarely need "everything"; a few accurate details plus urgency tricks are often enough.

Why it matters

- Fraud done in your name can damage credit history, drain bank/UPI balances, and expose official data.
- Recovery takes time; early detection and quick action reduce loss.

Possible Threats

- Data leaks & breaches: Details from old sign-ups or public documents get sold and reused.
- Social media scraping: Public posts reveal phone, birthday, school, family, or office info used for convincing pretexts.
- SIM swap / SIM hijack: Attackers persuade the mobile operator to issue a duplicate SIM, then intercept OTPs to reset bank/email/UPI.
- Fake KYC / verification links: Phishing sites or chat messages ask you to upload ID photos, PAN, or record a video KYC.
- Deepfake & vishing: Realistic voice/video used to demand details or "urgent verification".
- Shoulder-surfing & lost documents: Photos of IDs shared casually in chats, or documents left on desks/photocopiers.
- Malicious apps: Unofficial APKs request excessive permissions and exfiltrate contacts, SMS, and device IDs.

✓ Do's

- Share the minimum: Provide only required fields; redact (black out) unneeded parts (e.g., mask Aadhaar).
- Use official channels: Do KYC only on official apps/sites you open yourself (typed URL or bookmarked) or visit to local bank branch.

- Enable alerts: Turn on SMS/app/email alerts for bank, UPI, email logins, credit reports (if available).
- Review monthly: Check bank/UPI statements, credit card bills, and email security logs.
- Secure resets: Use strong, non-obvious recovery answers; keep recovery email/phone current and protected with MFA.
- Lock what you can: Use profile locks (where supported), disable SIM port-out/SIM-swap via carrier security PIN if available.
- Device hygiene: Keep OS/apps updated; install apps only from official stores; run approved security/EDR.

× Don'ts

- Don't share ID images, CVV, OTP, or passwords on calls/chats—no bank/IT/police will ask.
- Don't click KYC/verification links from SMS/WhatsApp—open the official app/portal yourself.
- Don't post photos of IDs, badges, boarding passes, or live locations on social media.
- Don't email scans of IDs to personal addresses/cloud drives for official work.
- Don't keep ID photos and sensitive PDFs in open, shared folders or chats.

Best Practices

- ✓ Verify only through official channels (typed URL/bookmark/official app).
- ✓ Strong passphrases + MFA on email, bank, e-office; keep recovery info secure.
- ✓ Suspect a SIM swap? Block the SIM immediately, alert your bank, change passwords, and report.
- ✓ Least data, least risk: Share the minimum required; redact the rest.

Practical Examples

- SIM-swap chain: Your phone loses network suddenly. An attacker got a duplicate SIM, then resets your email/bank with intercepted OTPs.
- Fake KYC link: "Your account will be frozen—update KYC now." The link collects PAN, Aadhaar, and a selfie. Days later, a loan appears in your name.
- Document overshare: You send an unredacted ID scan on a chat group. It's forwarded beyond the group and later used to open an account.

Early Warning Signs

- Sudden no network on your phone (while others have signal).
- Bank/UPI/email OTP or login alerts you didn't request.
- New loans/cards on your credit report; collection calls for unknown accounts.
- Password reset emails or "new device logged in" notifications you didn't trigger.

Myths vs Facts

- Myth: "They need my full Aadhaar/PAN + everything to harm me."
  Fact: Partial data + OTP or email access often suffices. Protect each piece.
- Myth: "If I don't shop online, I'm safe."
  Fact: Breaches of other services (old portals, forums) still expose data used for impersonation.
- Myth: "Losing network is a telecom issue."
  Fact: It can indicate SIM-swap. Act fast: contact carrier, secure accounts, and report.

MFA for Email Accounts

What it means

- Multi-Factor Authentication (MFA) adds a second lock to your account. Even if someone steals your password, they still need your one-time code, approval prompt, or a hardware/token to get in. For official email and e-office, use Kavach or other department-approved MFA solutions.

Why it matters

- Most account takeovers start with a stolen or reused password.
- MFA blocks the attacker even when the password is known.
- Email is the "master key" used to reset other accounts—protect it first.

Possible Threats

- MFA fatigue (push-prompt bombing): Attackers keep sending approval prompts at odd hours hoping you'll tap "Approve" by mistake just to stop the noise.

- Phishing proxies / reverse proxies: A fake login page relays your username/password to the real site in real time and then presents the real MFA prompt. If you approve, the attacker hijacks the session cookie.
- Prompt spoofing via call/SMS: Fraudsters pose as "IT/Bank/Police" and ask you to read out an OTP or approve a "safety verification."
- SIM swap: If MFA codes arrive by SMS, a duplicate SIM lets attackers receive your codes.
- Malware/stealers: If your device is infected, screen-overlay apps or stealers can capture codes or session tokens.

✓ **Do's**

- Enable MFA (Kavach) on official email and e-office immediately; use department-approved methods (app prompt, hardware token).
- Use app-based or hardware MFA where possible (e.g., authenticator app, security key). Prefer these over SMS.
- Keep backup codes offline (printed and locked, or stored in an authorized password manager's secure notes).
- Approve prompts only when you initiated login and the location/device looks right.
- Label devices in your account security settings; remove old or unknown devices.
- Turn on sign-in alerts for your email account; review security activity monthly.
- Harden recovery options: Use strong, non-obvious security answers; secure the recovery email/phone with its own MFA.

× Don'ts

- Don't share OTPs, approval codes, or push-prompt approvals—no IT/bank/police will ask.
- Don't approve a prompt you did not start yourself (especially at odd hours).
- Don't store OTPs, backup codes, or QR seeds in chat apps, email drafts, or plain-text notes.
- Don't rely on SMS-only MFA if stronger options (app/hardware) are available.
- Don't ignore repeated unexpected prompts—this is a sign someone has your password.

Best Practices

- Two locks are better than one: Password + MFA on email and e-office.
- Unexpected MFA prompt = Deny + Change Password + Report.
- Prefer app/hardware MFA over SMS; secure backup codes offline.
- Review devices/sessions monthly and remove anything unfamiliar.

Practical Examples

- Push-bombing at midnight: You receive multiple "Approve sign-in?" prompts while asleep. You didn't try to log in—deny, change your password, and report.
- Phishing proxy: An email sends you to a perfect-looking login page. You enter credentials and then see an MFA prompt. Approving it hands over a valid session to the attacker. The fix is to type the official URL yourself and only approve prompts you triggered.
- SIM-swap risk: Your phone loses network without reason. If your MFA uses SMS, attackers might be receiving your codes. Call the carrier, block SIM, and secure accounts.

Myths vs Facts

- Myth: "MFA is annoying; I'll disable it once things are calm."
  Fact: Attackers strike when it's "calm." MFA stops most takeovers.
- Myth: "MFA means I'm 100% safe."
  Fact: Phishing proxies can still steal sessions if you approve blindly. Approve only what you start and use typed/bookmarked URLs.
- Myth: "SMS is enough."
  Fact: SIM-swap defeats SMS. Prefer app-based or hardware MFA.

QR Code Security

What it means

- A QR code is just a shortcut—one scan can open a website, start an app action, or initiate a payment. Scammers exploit this by placing fake stickers, sending QRs in messages, or redirecting you to look-alike sites. If you scan without checking, you might pay the wrong person, share credentials, or install malicious apps.

Why it matters

- A tampered QR on a shop's stand can silently divert your money to a fraudster.

- Message/Poster QRs can open fake KYC sites or prompt APK installs (malware).
- Some QRs request "collect" (pull) payments you never intended to make.

Possible Threats

- Tampered merchant boards: A fake sticker over the real QR sends payment to a scammer.
- Collect request traps: After scanning or contacting "support," you get a collect request—entering your UPI PIN pays the attacker.
- Quishing (QR + phishing): Posters or messages lead to fake bank/KYC pages that steal passwords/IDs.
- QR login phishing: Fake "login via QR" pages for services (email/message apps) capture your session.
- Malicious app installs: QR opens a link to install an unofficial APK or a rogue browser extension.
- Dynamic-QR manipulation: Printed QR replaced with one tied to the attacker's account; amount/remarks pre-filled to confuse you.

✓ **Do's**

- Verify on screen: After scanning, check payee name and UPI ID in your app before approving.
- Use the official app's scanner: Open your bank/UPI app first; scan inside it (don't rely on random camera apps).
- Confirm with the merchant: If in doubt, ask the shop to confirm their name/UPI ID.
- Enter amount yourself: If an amount auto-appears, double-check it.
- Prefer saved/verified beneficiaries: For frequent payments, save the correct UPI ID in your app.
- Inspect physical stickers: Look for overlays, peeling, or mismatched branding; if suspicious, ask for an alternate method.

× **Don'ts**

- Don't scan random posters/stickers in public places (parking, fines, donations) without verification.
- Don't accept or approve unknown "collect" requests. To receive money, you never need your UPI PIN.
- Don't follow QR links to install apps—install only from official stores.
- Don't open bank/KYC pages from QR codes on messages—type the official URL or use the official app.
- Don't rush approvals: If the name/UPI ID or amount looks off—even slightly—cancel and verify.

Best Practices

- Scan → Verify → Pay (never Scan → Pay).
- Receiving money never needs your UPI PIN.
- Type official addresses or use bookmarks for banking/KYC; avoid QR-led logins for critical accounts.
- Set low per-transaction and daily limits; keep payment alerts on.
- When in doubt—stop, verify via a second channel, then proceed.

Practical Examples

- Overlaid sticker: A scammer places a sticker on a kirana shop's stand. You scan and see a different payee name—you almost miss it. You cancel and ask the cashier; it was tampered.
- Refund support scam: After a failed payment, "support" sends a QR and later a collect request— "Enter PIN to receive refund." You refuse; genuine refunds never need your PIN.
- Poster trap: A parking poster says "Pay here via QR." It opens a fake site that requests card/UPI credentials. You exit and pay at the official counter/app instead.

Red Flags

- Payee name/UPI ID doesn't match the merchant/shop.
- QR is peeling, over-stuck, or looks freshly pasted.
- You receive a collect request you didn't initiate.
- The QR opens a KYC or app-install page instead of your UPI app.
- Urgent/discount messages pushing you to scan quickly.

Myths vs Facts

- Myth: "If the QR is inside a shop, it's safe."
  Fact: Stickers get swapped. Always check the name/UPI ID on your screen.
- Myth: "To get a refund, I must enter my UPI PIN."
  Fact: Never. PIN is only for sending money.
- Myth: "Camera app scan is fine."
  Fact: Use your bank/UPI app's built-in scanner; it shows payee details clearly.

Backup of Important Files

What it means

- A backup is a separate safety copy of your important files. If your laptop is lost, your phone breaks, or ransomware locks your data, a good backup lets you get your work back quickly. A backup is only useful if you can restore it—so testing matters.

Why it matters

- Ransomware can encrypt your laptop and shared folders.
- Devices get lost, stolen, dropped, or corrupted.
- Accidental deletions and overwrites happen.
- A planned, tested backup prevents small mistakes from becoming big disasters.

Possible Threats

- Ransomware & malware: Encrypt or delete files, including network shares.
- Hardware faults: Disk/SSD failures, power issues, phone memory errors.
- Human error: Deleting or overwriting the wrong folder.
- Theft/loss: Laptops/phones lost in transit; offices compromised.
- Sync mistakes: Cloud sync (not backup) can propagate deletions to the cloud.

✓ **Do's**

- Use approved backup solutions: IT-managed endpoint backup, enterprise cloud backup, or server snapshots as per policy.
- Schedule automatic backups: Daily (or more often) for critical files; weekly for less critical.
- Keep one copy immutable/offline: Maintain an offline/air-gapped or object-locked copy for ransomware resilience.
- Test restores quarterly: Pick a few files and restore them—confirm they open and are up to date.
- Versioning on: Enable file version history so you can roll back to last week's clean copy.
- Encrypt backups: Use password-protected/managed encryption (BitLocker To Go, encrypted cloud) to protect data at rest.
- Document the plan: Know what is backed up, where, how often, and who to contact for recovery.
- Back up after big changes: Major project milestones, device changes, or before travel.

× **Don'ts**

- Don't rely on a single copy—especially a USB always plugged in (ransomware will encrypt it).
- Don't assume sync = backup: If you delete it locally, many sync tools delete it in the cloud too.
- Don't postpone backups after major edits or before travel.
- Don't store backups unencrypted on personal media or unapproved cloud.
- Don't forget mobile data—move official photos/docs from phones to approved storage.

Best Practices

- ✓ Back up before you need it.
- ✓ 3-2-1: Three copies, two media, one offsite/immutable.
- ✓ A backup you can't restore is no backup—test restores regularly.
- ✓ Keep backup scopes small and clear: Back up what matters, not everything on the desktop.
- ✓ Label and log: Maintain a simple record of critical folders and last successful backup date.

Practical Examples

- Ransomware day: A malicious attachment encrypts your laptop and shared drive. IT helpdesk team restores yesterday's immutable backup; you're back in business the same day.
- Accidental overwrite: You replace "Q3_Summary.xlsx" with the wrong version. Version history lets you restore the copy from two days ago.

Myths vs Facts

- Myth: "We use cloud, so we don't need backups."
  Fact: Cloud sync is not backup. Accidental deletions, ransomware, or account issues can still remove files; you need versioned backups.
- Myth: "I'll plug in a USB drive and keep it attached."
  Fact: Ransomware encrypts attached drives. Keep at least one copy offline/immutable.

UPI Security

What it means

- Unified Payments Interface (UPI) moves money instantly. That's convenient—but it also means mistakes and frauds happen instantly. Always verify the payee name, UPI ID, and amount on your screen before you approve a payment. Remember: to receive money, you never need your UPI PIN.

Why it matters

- A single rushed approval can send money to a fraudulent ID.
- Fake "support" or "refund" messages trick users into entering PINs or clicking malicious links.
- Early action (within the Golden Hour) helps banks attempt transaction recall/hold.

Possible Threats

- Fake collect requests (pull payments): You get a request to "approve" a debit; entering your UPI PIN sends money out.
- Spoofed IDs / display names: Attackers use look-alike UPI IDs or similar names to fool quick approvals.
- Refund/support scams: After a failed/slow transaction, "support" contacts you via SMS/WhatsApp with a QR/link to "process refund"—then sends a collect request.
- Impersonation (KYC/lottery/loan): Links lead to fake portals asking for card/UPI credentials or remote-control app installs.
- QR tampering: A replaced merchant QR diverts your payment to the attacker.
- Screen-sharing/remote apps: Fraudsters persuade you to install remote tools; they watch you type your PIN and approve payments.

✓ **Do's**

- Verify on-screen every time: Check payee name, UPI ID, and amount before entering your PIN. If anything looks off, cancel.
- Use the official app only: Open your bank/UPI app yourself; avoid links in SMS/chats.
- Set low limits & alerts: Keep per-transaction and daily limits modest; turn on SMS/app/email alerts for each debit.
- Save trusted beneficiaries: For recurring payments, save verified payees to reduce mistakes.
- Reconcile monthly: Review bank/UPI statements and flag anomalies immediately.
- Secure your phone: Lock screen (PIN/biometric), keep OS/apps updated, and disable app installs from unknown sources.
- Contact the bank via official channels: Use the app's built-in support or the official helpline—not numbers from messages.

× **Don'ts**

- Don't enter UPI PIN to receive money. Receiving does not need your PIN.
- Don't click payment/KYC links received via SMS/WhatsApp—use the official app or type the URL.
- Don't approve unknown collect requests or those with unexpected amounts.
- Don't rely on display name alone; verify the UPI ID carefully (watch for typos).
- Don't install remote-access or screen-sharing apps at anyone's request.
- Don't store screenshots of cards/UPI IDs with sensitive details in chat apps.

Best Practices

- ✓ Type → Check → Pay. When unsure, don't transact—verify first.
- ✓ Receiving money never needs your UPI PIN.
- ✓ Keep limits low + alerts on to catch mistakes quickly.
- ✓ Use saved, verified beneficiaries for frequent transfers.
- ✓ Report in the Golden Hour if anything goes wrong.

Practical Examples

- Refund trap: "Support" sends a link: "Refund in 5 minutes—approve the request." You receive a collect request for ₹9,999. You decline; real refunds never need your PIN.
- Look-alike ID: You mean to pay shop@bank, but the screen shows shop1@bank and a different payee name. You cancel and ask the cashier to confirm their exact UPI ID.
- QR diversion: A pasted sticker on a counter routes to the attacker. You inspect the sticker, scan with your app, and verify the name on-screen before paying.

Red Flags

- Collect requests you didn't initiate.
- Urgent messages to "update KYC" or "avoid account freeze" with a payment link.
- Payee name doesn't match the merchant/recipient you expect.
- Requests to install remote apps or share OTP/PIN.
- Amounts that are rounded/odd or changed at the last step.

Myths vs Facts

- Myth: "To get a refund, I must enter my UPI PIN."
  Fact: Never. PIN is only for sending money.
- Myth: "If the display name looks right, it's the correct account."
  Fact: Names can be similar; verify the exact UPI ID and amount on screen.
- Myth: "Links from the bank on WhatsApp are fine."
  Fact: Attackers spoof messages. Use the official app or type the URL yourself.

Data Encryption

What it means

- Encryption scrambles your data so only authorized people (with the right key/password) can read it. It protects lost or stolen devices, files sent over the internet, and data stored on servers or drives. Ransomware is Scammers using encryption against you—malware locks your files and demands money.

Why it matters

- If your laptop or phone is stolen, full-disk encryption keeps stored data unreadable.
- When you send files or log in, encrypted connections (HTTPS/TLS/VPN) prevent snooping.
- If ransomware hits, having backups + segmentation limits damage and speeds recovery.

Possible Threats

- Phishing → malware: An attachment/script installs ransomware or a stealer.
- Unpatched software: Known vulnerabilities let attackers in, then they move laterally to file shares.
- Privilege abuse: Excess admin rights let malware encrypt more systems faster.
- Data exfiltration + extortion: Attackers steal copies first, then encrypt and threaten to leak.

✓ **Do's**

- Turn on full-disk encryption on laptops/phones (BitLocker/FileVault; Android/iOS encryption).
- Use encrypted channels: Prefer HTTPS/TLS, S/MIME/PGP (if mandated), and VPN for internal systems.
- Limit privileges: Give users only the access they need; separate critical servers from general user networks.
- Keep EDR/AV active and updated; enable real-time protection.
- Maintain offline/immutable backups (3-2-1 rule) and test restores regularly.
- Apply patches promptly for OS, apps, and firmware.

× **Don'ts**

- Don't enable macros from unknown documents or disable security prompts "just this once."
- Don't work as local admin for everyday tasks; use a standard account.
- Don't store encryption keys/passphrases in emails or plain-text notes.
- Don't pay ransom—follow organisational SOPs and legal guidance.

Best Practices

- ✓ Encrypt by default: device, at rest, and in transit.
- ✓ Prepare beats repair: Backups + patching + EDR prevent long outages.
- ✓ Detect early, isolate fast, report immediately.

Practical Examples

- Encrypted share drive: Ransomware starts encrypting a user folder, but least-privilege stops it spreading to finance and HR shares.
- Unpatched server: A known flaw gets exploited; timely patches would have blocked it.

Data Protection (Handling & Sharing)

What it means

- Data protection means giving the right information to the right person via approved channels—and nothing more. Share the minimum necessary, keep sensitive data classified, and control who can view, edit, or forward it.

Why it matters

- Oversharing (wrong email address, public links, over-broad permissions) causes leaks.
- Unapproved apps/cloud weaken control and auditing.
- Misuse or accidental exposure can lead to legal, financial, and reputational damage.

Possible Threats

- Excessive permissions on shared drives (Everyone = Edit).
- Personal cloud or messaging apps used for official files.
- Screenshots/photos of internal dashboards posted to social media.
- Lost USBs or unencrypted removable media.

✓ **Do's**

- Classify and label documents (e.g., Public/Internal/Confidential/Restricted) and follow handling rules.
- Least-privilege access: Share with named individuals or groups; set view vs edit as needed; time-limit access for vendors.
- Use approved channels: Official email, enterprise cloud, secure portals; encrypt when required by policy.
- Use watermarking/DLP where mandated; apply download/reshare restrictions for sensitive files.
- Verify recipients: Double-check addresses; avoid "reply-all" traps.
- Review access regularly: Remove stale users; revoke links after projects end.
- Sanitise documents: Redact personal identifiers (Aadhaar/PAN) not required; remove hidden metadata if policy requires.

× **Don'ts**

- Don't move official data to personal email/cloud or consumer messengers.
- Don't create "Anyone with the link can view/edit" for sensitive material.
- Don't post internal screenshots to social media or public forums.
- Don't share passwords to "give access." Provision proper access instead.
- Don't store sensitive files on unencrypted USBs or unattended laptops.

Best Practices

✓ Right data → right person → right channel.
✓ Share the minimum necessary; remove access when no longer needed.
✓ Encrypt when required and prefer managed platforms with audit trails.
✓ Document retention: Keep what policy requires; dispose securely when done.

Practical Examples

- Public link leak: A spreadsheet with personal data shared as "anyone with link—edit." It gets copied outside the org. Fix: named recipients only, no public links.
- Misaddressed email: Auto-complete picks the wrong consultant. Fix: verify recipients; use secure portals for sensitive files.
- Vendor access sprawl: Temporary vendor retains access after project. Fix: time-bound access and quarterly reviews.

Myths vs Facts

- Myth: "If it's in the cloud, it's automatically safe."
  Fact: Safety depends on permissions and how you share. Public links leak data.
- Myth: "Sending to my personal email is fine for quick work."
  Fact: Personal accounts lack mandated controls and auditing—don't do it.
- Myth: "Screenshots are harmless."
  Fact: Screenshots can expose names, IDs, and internal systems; treat them like documents.

Internet Ethics

What it means

- Everything you post, like, forward, or comment on reflects on you and your organisation. The internet keeps records. Be accurate, respectful, and cautious—especially with official information, personal data, photos, and locations.

Why it matters

- Scammers and scammers collect public details (ID photos, office locations, daily routines) to craft targeted attacks (phishing, impersonation, stalking, social engineering).
- A single careless post can cause legal, reputational, or security harm to you and the organisation.

Possible Threats

- Doxxing & oversharing: Publicly exposing your ID number, badge, family details, or travel plans helps attackers impersonate you or time their scams.
- Impersonation & deepfakes: Fake accounts copy your name/photo; audio/video deepfakes can spread false statements in your name.
- Targeted phishing (spear-phishing): Details from your posts (projects, tools, vendors) are used to create convincing scams.
- Harassment & trolling: Provocations that try to pull you into public arguments; screenshots can be used out of context.
- Policy breaches: Posting internal screenshots, draft documents, or confidential updates violates organisational rules and law.

✓ Do's

- Think before you post: Ask "Would I be comfortable seeing this on a public notice board?"
- Verify before resharing: Share only confirmed information; avoid rumours and unverified "alerts."
- Separate personal views from official roles: Use clear disclaimers when appropriate and follow departmental social-media policy.
- Use platform safety tools: Enable privacy settings, 2FA/MFA on accounts, and report/flag impersonation or abuse promptly.
- Mind the metadata: Remove or blur sensitive details in photos (ID badges, desks, monitors, addresses, vehicle numbers).
- Ask before posting group photos: Especially from office premises, meetings, or site visits—respect consent and policy.
- Keep contact info minimal: Share the least identifying data publicly; use official channels for official contact.

× Don'ts

- Don't post photos of ID cards, passes, official badges, or live locations and travel itineraries.
- Don't share internal memos, dashboards, or screenshots of official systems.
- Don't engage with trolls or respond emotionally—preserve evidence and report.
- Don't discuss ongoing internal matters (investigations, tenders, security, unreleased reports) online.
- Don't click sensational links shared in comments/DMs—verify first.

Best Practices

- ✓ Post with purpose; protect your org and yourself.
- ✓ When unsure—don't share. Ask a supervisor/PRO if it relates to official matters.
- ✓ Lock down accounts: Strong passphrases + MFA; review privacy settings quarterly.
- ✓ Minimal public footprint: Share only what's necessary; keep personal details private.

Practical Examples

- Badge in selfie: A staff selfie shows the ID barcode and building access area. A scammer reprints the badge and attempts tailgating.
- Trip announcement: "On official tour to City X, back Monday." A fraudster uses the absence to email your team (impersonating you) with an urgent payment request.
- Dashboard screenshot: A post revealing internal project names and vendor details helps a spear-phisher craft convincing fake invoices.

Red Flags

- New accounts pretending to be you or your department.
- DMs asking for OTP, PIN, passwords, or "urgent verification."
- Comments urging you to open short links or install "viewer" apps.
- Requests to discuss official matters on personal messaging apps.

Myths vs Facts

- Myth: "My account is private, so I can post anything."
  Fact: Screenshots and re-sharing bypass "private." Assume anything online can spread.
- Myth: "If it's already public, it's fine to repost."
  Fact: Context matters; reposting sensitive info can still violate policy or law.
- Myth: "It's just a selfie."
  Fact: Backgrounds reveal locations, monitors, documents, and access points.

Social Engineering

What it means

- Social engineering is when Scammers trick people—not computers—to give up information, money, or access. They impersonate trusted sources (bank/IT/senior officials), create urgency or fear, and push you to click, pay, or approve without proper checks. It includes:
- Phishing (email), Smishing (SMS/chats), Vishing (voice calls)
- Quishing (QR-code led phishing)
- Business Email Compromise (BEC)
- MFA fatigue (push-prompt bombing)
- Tech-support scams & remote-tool abuse
- Deepfakes (voice/video), Pretexting (fake roles), Baiting (infected USB/freebies)
- Tailgating (following into secure areas), Shoulder-surfing (watching screens/keystrokes)

Why it matters

- A single convinced click, approval, or disclosure can defeat many technical protections. Process discipline (verification, dual control) is your strongest defence.

How the tricks work

- Phishing/Smishing/Vishing: "Your account will be blocked—verify now", fake KYC links, OTP requests, "urgent escalation from HQ".
- Quishing (QR): Tampered merchant stickers or message QRs leading to fake sites or collect requests.
- BEC: A spoofed/compromised senior or vendor asks for bank-detail change or urgent payment.
- MFA fatigue: Repeated push prompts at odd hours so you click Approve just to stop them.
- Tech-support scam: Pop-ups or callers claiming to be "IT/Bank/Police" asking you to install remote tools or share OTPs.
- Deepfakes & pretexting: Realistic voice/video or convincing "inspector/auditor" personas to demand data or entry.
- Baiting/Tailgating/Shoulder-surfing: Infected USB giveaways; someone slips in behind you; someone reads your screen or keypad.

Red Flags

- Urgent requests that bypass normal approval routes ("just this once").
- Requests for OTP/PIN/password/CVV (no legitimate entity asks).
- Payment/bank detail changes by email/DM without secondary confirmation.
- Unfamiliar links/QRs/attachments; requests to install remote control apps.
- Unexpected MFA prompts or login alerts you didn't initiate.
- Visitors without badges, or people tailgating into secure areas.

✓ **Do's**

- Use PVR: Pause – Verify (second trusted channel) – Report.
- Dual control for risk: Two-person approval for payments, bank-detail changes, or sensitive data releases.
- Verify independently: Call back using numbers you look up yourself (directory/vendor master), not the number in the message.
- Type it yourself: For portals/banking/e-office, type the official URL or use bookmarks; avoid link-led logins.

- Harden your environment: Lock screens, use privacy filters, keep devices with you; challenge tailgaters politely.
- Turn on MFA (Kavach) and security alerts; keep OS/apps updated and AV/EDR active.
- Report suspicious contact to Security/IT with screenshots, headers, phone numbers, and timestamps.

× Don'ts

- Don't share OTP/PIN/password/CVV—no bank/IT/police will ask.
- Don't approve MFA prompts you didn't start.
- Don't scan random QR codes or accept unknown collect requests.
- Don't install remote-access or screen-sharing tools at a caller's request.
- Don't bypass normal approvals "just to be helpful" or because "it's urgent".

Best Practices

- ✓ Trust is verified, not assumed.
- ✓ Two-person rule for risky approvals (payments, bank-detail changes, sensitive data).
- ✓ Use official channels only (typed URLs, known helplines, directory numbers).
- ✓ Document and escalate anything unusual; never act alone under pressure.

Practical Examples

- BEC invoice switch: "Vendor" emails new bank details from a thread you recognise. You call the vendor using the number on file—they never changed accounts.
- MFA push bombing at 2 AM: You get multiple prompts. You deny, change your password, and report.
- QR on poster: You scan and see a collect request. You cancel—receiving money never needs your UPI PIN.
- "IT" on the phone: Caller asks you to install a remote app to "fix email." You refuse, hang up, and report to IT helpdesk.
- Simple Office Routine (habit-forming)
- For money or access: PVR and dual approval.
- Type/bookmark official URLs; no link-led logins.
- Lock screens when away; challenge tailgaters.
- Verify caller/sender identity on a second channel.
- Report anything suspicious immediately.

Myths vs Facts

- Myth: "If the email is in an existing thread, it's safe."
  Fact: Attackers hijack real threads. Verify out-of-band for changes and payments.
- Myth: "He sounded exactly like my boss."
  Fact: Deepfakes and cloned voices exist. Always verify via a second channel.
- Myth: "It's rude to challenge tailgaters."
  Fact: It's professional. Challenge politely and protect secure areas.

Removable Device Security (USBs & External Media)

What it means

- USB drives and external hard disks are convenient, but they can also carry malware, leak sensitive files, or be used to take data out of the organisation. Treat them like sealed envelopes—open only trusted ones, and handle contents securely.

Why it matters

- A single infected USB can install malware or ransomware within seconds.
- Lost or unencrypted media can expose confidential documents outside the organisation.
- BadUSB devices can impersonate a keyboard or network card, silently running harmful commands.

How attacks happen

- Baiting: "Found" USBs left in cafeterias/parking lots tempt users to plug them in.
- BadUSB/malicious firmware: A device appears as a keyboard/network adapter and runs commands automatically.
- Autorun/infected files: Opening a document triggers macros or scripts that install malware.
- Data exfiltration: Sensitive files copied to personal or unencrypted drives leave the organisation.

- Supply-chain tampering: Counterfeit or modified media are compromised before you receive them.

✓ Do's

- Use only approved, encrypted media (e.g., hardware-encrypted drives or BitLocker To Go as per policy).
- Scan every device with up-to-date antivirus/EDR before opening files.
- Label and inventory official drives; log checkout/return and keep chain of custody for sensitive data.
- Enable read-only/write-protect switches when available; use write blockers for forensic or one-way transfers.
- Follow data classification: Copy only the minimum required; encrypt sensitive files/folders.
- Eject safely and store media in locked drawers or cabinets when not in use.
- Report immediately if media is lost, stolen, or suspected infected; follow sanitisation procedures.

× Don'ts

- Don't plug in unknown, found, or gift USB sticks/dongles.
- Don't use personal USBs for official data; don't share office media with outsiders.
- Don't bypass USB-port controls, MDM/DLP policies, or admin approvals.
- Don't copy classified/sensitive data to unapproved or unencrypted media.
- Don't leave drives lying on desks, in meeting rooms, or in vehicles.

Best Practices

- ✓ If it's not sanctioned, don't connect. If it's not encrypted, don't use.
- ✓ Assume unknown media is hostile; hand it to IT/Security for safe handling.
- ✓ Encrypt data at rest and in transit; verify recipients before handing over media.
- ✓ Keep DLP/EDR active; remove unused USB permissions from systems where possible.

Practical examples

- Lobby lure: A "32GB Free" USB is found near reception. A user plugs it in; it acts like a keyboard and runs commands to install a backdoor.
- Meeting room lapse: A visitor borrows a USB "to share slides"—their device auto-runs a macro that spreads ransomware to a shared drive.
- Lost drive: An unencrypted external disk with monthly

Myths vs Facts

- Myth: "If a file opens, it's safe."
  Fact: Documents can contain macros that install malware. Always scan and avoid enabling macros.
- Myth: "Company laptops are protected; any USB is fine."
  Fact: BadUSB can bypass normal checks. Only approved devices should be used.
- Myth: "Encrypting the drive is complicated."
  Fact: IT-approved tools (e.g., BitLocker To Go) make encryption straightforward.

Digital Arrest

What it means

- A "digital arrest" scam is when fraudsters pose as police/CBI/ED/court officials (often on WhatsApp/phone/video call) and threaten that you are under virtual detention until you "cooperate." They may show fake IDs, case numbers, or screenshots, demand KYC details, make you stay on a video call for hours, or force you to transfer money to "verify" funds or avoid "immediate arrest."

Why it matters

- The goal is control and fear. Once you are isolated on a call, they extract money and data

using threats: "Your parcel has drugs," "Your SIM is used in crime," "Your account will be frozen," or "Your face appeared in illegal activity."

How the scam works

- Authority impersonation: Fake badges, case IDs, background banners, or spoofed caller IDs of police/courts/CBI/ED.
- Isolation tactic: "Stay on video call; don't hang up; don't talk to anyone—national security case."
- Fake evidence: Forged FIRs, warrants, or videos shared on chat.
- Financial coercion: "Transfer funds to a safe/escrow account for verification" or "pay fines immediately to avoid arrest."
- KYC/remote control: Ask to install screen-sharing apps, submit Aadhaar/PAN/selfies, or record statements.
- Gag order: "Don't tell anyone; you'll obstruct investigation."

Red Flags

- Demands to remain on a continuous call or not contact anyone.
- Requests for immediate payment, "security deposits," or fund verification.
- Pressure to install remote apps, share screens, or provide OTP/PIN.
- Threats of instant arrest, account freeze, or media defamation.
- Use of WhatsApp/Telegram for official "investigation."

✓ **Do's**

- PVR: Pause – Verify – Report.
- Verify on a second channel: End the call. Dial the official number of the local police station/court/agency from their website; never call back the number that contacted you.
- Consult your Security Cell/Nodal Officer/Legal immediately if any official reference is claimed.
- Keep records: Screenshots of caller ID, chat, shared "documents," and timestamps.
- Educate family (parents/wards): tell them about this scam so they don't panic-pay.

× **Don'ts**

- Do not stay on the call under pressure. End the call and verify independently.
- Do not pay or transfer funds to "verification/escrow/safe" accounts.
- Do not share OTP/PIN/passwords or upload IDs/selfies to links they provide.
- Do not install remote-access or screen-sharing apps at their request.
- Do not keep it secret—report such incidents to local police asap.

Best Practices

✓ Lawful process is verifiable. Real agencies won't demand money over chat/call or forbid you from contacting others.
✓ Independent verification via known official numbers only.
✓ No remote tools, no OTP/PIN, no "escrow."
✓ If threatened, hang up, verify, and report.

Practical Examples

- Parcel ruse: Caller says a parcel in your name contains contraband. They show a fake warrant and keep you on video while demanding a "security deposit." You hang up, dial the official station number—no such case exists.
- Bank freeze threat: "Your account is used for money laundering—transfer to a secure wallet now." You refuse, call your bank's official helpline, and inform the Security Cell.
- CBI impersonation: WhatsApp DP/ID looks official. They ask for a video confession. You end the call, verify with the CBI office via the number on their website, and report.

Deepfakes & Synthetic Media

What it means

- Deepfakes are realistic-looking fake audio or video created by AI. Attackers clone a senior's voice or face to issue "urgent" instructions (payments, sharing data, changing bank details) or to defame and coerce victims. Even trained people can be fooled for a few seconds—process, not instinct, is your defence.

Why it matters

- A convincing 20-second clip can trigger high-risk actions (fund transfers, data release). Treat unexpected voice/video instructions like any other high-risk request: verify on a second channel and apply two-person approval.

How attacks happen

- Voice cloning: Short public audio samples produce a fake voice call asking for urgent approvals.
- Video deepfakes: A CEO/official "appears" on a brief call/recording requesting secrecy and speed.
- Context piggybacking: Attackers reference real projects or meetings (from emails/LinkedIn) to sound credible.
- Extortion & harassment: Manipulated images/videos used to demand money or silence.

Red Flags

- Urgent, secret instructions that bypass normal approvals.
- Slight lip-sync mismatches, odd intonation/latency, background that doesn't change naturally.
- Requests to move to private channels (personal chat) and act immediately.
- Payment/bank detail changes communicated only by call/clip.

✓ **Do's**

- Verify via a second trusted channel (your saved official number, directory listing, or scheduled in-person/video confirmation).
- Apply two-person approval for payments, bank changes, or data releases—no exceptions.
- Use code words/callback protocols for sensitive approvals if your department supports them.
- Preserve evidence: Save the audio/video, call logs, and metadata; note time and context.
- Inform Security/IT helpdesk/Legal/PRO for coordinated response if the org's image is involved.

× **Don'ts**

- Don't act on voice/video alone—no approvals without verification.
- Don't forward the clip widely; contain and escalate through official channels.
- Don't share OTP/PIN/passwords or open links sent along with the clip.
- Don't use personal messengers for official approvals.

Best Practices

- ✓ Process over persuasion: If it's urgent and sensitive, verify + dual control.
- ✓ Official channels only; avoid ad-hoc approvals via unfamiliar calls/DMs.
- ✓ Awareness first: Train teams about deep fakes; practice callbacks and code-phrase checks.
- ✓ Protect your own media: Be cautious about posting long, clean voice/video samples publicly.

Practical Examples

- Voice-cloned boss: You get a call that "sounds like" your GM urging a confidential vendor payment. You call back on the official directory number and discover it was fake.
- Video drop-in: A brief video message from a senior asks for an immediate bank-detail change for a project. You follow SOP: dual approval + second-channel verification → scam averted.
- Defamation clip: A fake video circulates online. You preserve the file, notify

Security/Legal/PRO, and avoid public commentary until the official response.

Myths vs Facts

- Myth: "I'd always spot a fake."
  Fact: Short, urgent clips can fool anyone. Process (verification + dual control) is your safety net.
- Myth: "If the number matches the name, it's real."
  Fact: Numbers can be spoofed. Call back via a saved/official contact.
- Myth: "Only top executives are targeted."
  Fact: Any approver or data custodian can be targeted—train everyone.

Social Media Security

What it means

- Social media accounts (Facebook, X/Twitter, Instagram, LinkedIn, YouTube, WhatsApp, Telegram, etc.) represent you and can reflect on your organisation. If an attacker takes over—or if you overshare—your identity can be misused to spread scams, steal data, or damage reputations. Secure the accounts, share thoughtfully, and separate personal from official use.

Why it matters

- Compromised accounts are used to phish colleagues, post malicious links, or impersonate officials.
- Photos, captions, and comments can reveal locations, IDs, routines, systems, and contacts for targeted attacks.
- Public posts can travel fast—deleting later rarely fixes the impact.

Possible Threats

- Account takeovers: Reused/weak passwords, no MFA, phishing logins via DMs or fake login pages.
- Impersonation & clone accounts: Attackers copy your name/photo and message your contacts.
- Malicious links & attachments: Short links/QRs in comments or DMs that steal credentials or install apps.
- Metadata leakage: Photos reveal badges, documents on screens, addresses, vehicle numbers, or children's schools.
- Social engineering: Attackers befriend staff over time ("relationship-building") to request data or favours.
- Malvertising: Compromised ad accounts push harmful links; billing fraud drains funds.
- Doxxing/harassment: Personal data posted to intimidate or coerce.

Red Flags

- Login alerts from unknown locations/devices.
- Messages/DMs asking for OTP, PIN, passwords, or urgent verification.
- Posts/comments pushing short links, QR codes, or app installs.
- Look-alike accounts using your name/logo contacting your network.
- Unexplained ad spend or billing changes on managed pages.

✓ **Do's**

- Secure accounts first:
  - Use long, unique passphrases (14+ chars) stored in an approved password manager.
  - Enable MFA on every platform; prefer app-based or hardware keys.
  - Review connected apps and remove anything you don't recognize.
- Harden privacy & visibility:
  - Set profiles to private where suitable; limit who can tag, mention, or DM you.
  - Review audience for past posts; restrict sensitive ones.

- Post thoughtfully:
  - Blur or crop badges, desks, whiteboards, or computer screens.
  - Delay sharing location until after you've left; avoid daily routines/timetables.
  - Separate personal views from official matters; use disclaimers as per policy.

- Verify before re-sharing:
  - Share only confirmed information; avoid rumours and "urgent alerts."
  - For official pages/groups:
  - Use role-based accounts (not personal) with least-privilege roles and two-person approval for high-risk actions (ads, password resets).
  - Keep backup admins and updated contact lists; document handover when staff change roles.

× **Don'ts**

- Don't reuse passwords across platforms; don't store them in chats or notes.
- Don't click login links from DMs/emails—type the platform URL or use the official app.
- Don't post photos of IDs, access badges, live locations, internal dashboards, or meeting rooms with sensitive info.
- Don't install "profile booster/analytics" extensions from unknown vendors.
- Don't manage official pages from personal or shared devices; use managed, up-to-date systems.

Best Practices

✓ Lock it down: Long, unique passphrases + MFA everywhere.
✓ Think before you post: If it's not okay on a public noticeboard, don't post it online.
✓ Official channels only: For announcements, use approved organisational handles and processes.
✓ Least privilege: Minimal roles on pages; remove ex-staff promptly.
✓ Report & preserve: If something looks off, don't delete evidence—capture and escalate.

Practical Examples

- Phish login via DM: "Verify your account or it will be suspended—click here." The link is a fake login page. You ignore the link, open the app directly, and see no alerts.
- Photo overshare: A project selfie includes a whiteboard with server names and phone numbers. You remove the post, inform Security, and re-share a sanitised image after approval.

Myths vs Facts

- Myth: "My profile is private, so I'm safe."
  Fact: Screenshots and reshares ignore "private." Post as if it could go public.
- Myth: "Blue check = always genuine."
  Fact: Verified accounts can be compromised; always verify requests through a second channel.

Universal Cyber Security Golden Rules

PVR—Pause · Verify · Report

❖ Pause when a request is urgent, secret, or emotional.
❖ Verify on a second trusted channel (typed official number/URL, directory contact—not the one that reached out).
❖ Report suspicious activity to Security/IT helpdesk, and if crime is suspected, 1930 / cybercrime.gov.in.

No Secrets to Strangers

❖ Never share OTP, PIN, passwords, CVV, login links, or backup codes.
❖ No bank/IT/police will ask for them—ever.

Type, Don't Tap

❖ For banking, e-office, HRMS, and portals: type the URL or use a bookmark.
❖ Avoid logging in via links in emails/SMS, ads, or QR codes.

MFA Everywhere That Matters

- Enable Kavach/approved MFA on email and e-office.
- Unexpected MFA prompt = Deny + Change Password + Report.

Long, Unique Passphrases

- Use a password manager; one account → one 14+ character passphrase.
- Change immediately after any suspicious activity.

Update to Stay Safe

Auto-update OS, browsers, apps, and routers; restart weekly to finish patching.

Known Network + VPN

- Use office/home Wi-Fi you control; on public Wi-Fi use VPN or avoid sensitive work.

UPI/QR—Scan → Verify → Pay

- On screen, check payee name + UPI ID + amount before entering PIN.
- Receiving money never needs your UPI PIN.

Email Skepticism

- Check sender/domain, hover to preview links, distrust urgent money or credential requests.
- Report suspicious emails with full headers.

Lock & Encrypt Devices

- Auto-lock (2–5 min), full-disk encryption, Find My Device, remote-wipe readiness.

Approved Channels Only

- Use sanctioned email/cloud/VPN; no official files on personal email/cloud/messengers.

Minimum Necessary Sharing

- Right data → right person → right channel, with least-privilege permissions and time-bound access.

Backups You Can Restore

- Follow 3-2-1 (3 copies, 2 media, 1 offsite/immutable); test restores quarterly.

Removable Media Are High Risk

- Use approved, encrypted USBs only; scan first; maintain chain of custody.

No Remote Tools on Request

- Never install screen-sharing/remote access because someone told you to on a call/chat.

Spot Social Engineering

- Urgency, secrecy, authority pressure, or look-alike domains/QRs = verify elsewhere.
- Assume numbers and voices can be spoofed/deep faked.

Mind Your Digital Footprint (Internet Ethics)

- Don’t post IDs, badges, live locations, internal screenshots.
- Keep social accounts private and MFA-protected.

Prepare Beats Repair

Good hygiene (patching, MFA, backups, least privilege, EDR) prevents most damage.

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY

ALWAYS REPORT CYBER FRAUD IN GOLDEN HOUR

1. Always Think Before You Click
2. Verify Before You Share
3. Report Before It's Too Late

Call 1930 to register any complaint about cybercrime

Contact the nearest Cyber Police Station to file your complaint

File your complaint online with supporting documents through **www.cybercrime.gov.in**

Image & content sources: ISEA, CERT-in, MeitY, Generative AI
Prepared by: Anil Kumar, Sr. Manager (Systems), ICT Division, CMPDI