# UP RAJYA VIDYUT UTPADAN NIGAM LIMITED

राष्ट्रीय साइबर सुरक्षा जागरूकता माह | NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER 2026

# CYBER HYGIENE HANDBOOK

## साइबर स्वच्छता पुस्तिका




## #CyberHygieneOurCulture

**PAUSE • CHECK • VERIFY • REPORT**

**Safe people • Safe systems • A stronger UPRVUNL**

**सुरक्षित कर्मचारी • सुरक्षित प्रणालियाँ • सशक्त UPRVUNL**

# 1. Cyber Hygiene in 60 seconds | 60 सेकंड में साइबर स्वच्छता




Cybersecurity is a daily work habit, not only an IT job. Everyone at UPRVUNL who uses email, SAP/ERP, a desktop PC, official files or plant systems is part of the security boundary.

साइबर सुरक्षा केवल IT का कार्य नहीं, रोज़मर्रा की कार्य-आदत है। ई-मेल, SAP/ERP, डेस्कटॉप पीसी, कार्यालयी फाइल या प्लांट सिस्टम उपयोग करने वाला हर कर्मचारी सुरक्षा व्यवस्था का हिस्सा है।

**The golden rule: PAUSE • CHECK • VERIFY • REPORT**

**सुनहरा नियम: रुकें • जाँचें • सत्यापित करें • रिपोर्ट करें**

| Habit | What it means at work | आदत |
|---|---|---|
| 1. Pause | Urgent, scary or too-good-to-be-true? Wait before you click, pay or reply. | रुकें: जल्दबाज़ी अक्सर जाल होती है। |
| 2. Check | Look at the sender address, link, number and attachment. | जाँचें: प्रेषक, लिंक, नंबर और अटैचमेंट देखें। |
| 3. Verify | Confirm through a saved number or the official portal, never the message itself. | सत्यापित करें: सेव किए गए नंबर या आधिकारिक पोर्टल से पुष्टि करें। |
| 4. Protect | Use MFA, lock your screen, share only what is needed. | सुरक्षित रखें: MFA, स्क्रीन लॉक और आवश्यक जानकारी ही साझा करें। |
| 5. Report | Tell IT/security at once. Reporting early is never a mistake. | रिपोर्ट करें: तुरंत IT/सुरक्षा टीम को बताएँ। |

## Why this matters here | यहाँ यह क्यों मायने रखता है

A generation unit runs on digital systems: SAP/ERP for finance, HR and procurement, email for approvals, and plant systems for operations. One careless click can disrupt work, expose payroll or tender files, cause financial loss or damage trust.

विद्युत उत्पादन, वित्त, HR, खरीद और संचार डिजिटल सिस्टम पर निर्भर हैं। एक लापरवाह क्लिक काम में बाधा, वेतन/टेंडर डेटा का खुलासा, वित्तीय नुकसान और भरोसे को चोट पहुँचा सकता है।

# 2. Spot the trap: phishing, scams and deepfakes | जाल पहचानें




A polished message can still be fraud. Attackers now use AI to write flawless emails in English and Hindi, so good language is no longer proof of a genuine sender.

अच्छी भाषा वाला संदेश भी धोखाधड़ी हो सकता है। AI की मदद से अब बिना गलती वाले हिंदी/अंग्रेज़ी संदेश बनाना आसान है।

## Who they pretend to be

| Pretending to be | Typical request | What to do |
|---|---|---|
| Senior officer or CMD office | "Urgent, buy gift cards / pay this vendor today, keep it confidential." | Call the officer on a saved number. Follow normal approval. |
| HR or Payroll | "Update your bank details or log in to see your salary slip." | Open the official portal yourself. |
| Vendor or contractor | "Our bank account has changed; pay to the new one." | Verify with a known contact before any change. |
| IT support or bank | "Share the OTP / install this remote-support app." | Hang up. Real support never asks for OTPs. |
| Government or courier | "Pay a small fee, scan this QR code." | Do not scan. Check on the official website. |

## Try it: spot the 6 red flags

From: it-support@uprvunl-helpdesk.com Subject: URGENT: Your SAP password expires in 1 hour Dear user, click here to keep your account active: bit.ly/xxxx. Reply with your OTP to confirm. Do not tell anyone. Regards, CMD Office

Answers: (1) look-alike domain, not the official one; (2) artificial urgency; (3) shortened link; (4) asks for an OTP; (5) "do not tell anyone"; (6) vague sender with no name or extension.

## Red flags at a glance | खतरे के संकेत

- Unexpected urgency, threats or secrecy. / अचानक जल्दबाज़ी, धमकी या गोपनीयता का दबाव।
- Extra letters or look-alike spelling in the sender address or domain. / प्रेषक के ई-मेल/डोमेन में अतिरिक्त अक्षर।
- Unknown links, QR codes, attachments or shortened URLs. / अज्ञात लिंक, QR कोड, अटैचमेंट या छोटा URL।
- Requests for passwords, OTPs, PINs or confidential files. / पासवर्ड, OTP, PIN या गोपनीय फाइल की माँग।
- A payment or bank-detail change nobody independently verified. / बिना पुष्टि भुगतान या बैंक विवरण में बदलाव।

## Deepfakes: voice and video fraud | डीपफेक

- AI can copy a familiar voice or build a convincing video call. A familiar face or voice is not proof of identity when money, credentials, sensitive information or urgent approval is involved. / AI परिचित आवाज़ की नकल कर सकता है या विश्वसनीय दिखने वाला वीडियो बना सकता है। धन, लॉगिन, संवेदनशील जानकारी या तत्काल अनुमोदन में परिचित चेहरा/आवाज़ पहचान का प्रमाण नहीं है।
- Pause: urgency is a pressure tactic. / रुकें: जल्दबाजी एक दबाव डालने की रणनीति है ।
- Call back on a saved, known number, never the one in the message. / सेव किए गए ज्ञात नंबर पर कॉल करें।
- Ask a question only the real person can answer, or use a private family passphrase. / ऐसा प्रश्न पूछें जिसका उत्तर केवल असली व्यक्ति दे सके।
- Follow the official payment and approval workflow. Never bypass it. / अनुमोदन की आधिकारिक प्रक्रिया न छोड़ें।
- No payment or confidential disclosure based on a call or video alone. / केवल कॉल/वीडियो के आधार पर भुगतान या गोपनीय जानकारी साझा न करें।

# 3. Lock your accounts and your desk | खाते और डेस्क सुरक्षित रखें







## Passwords and MFA | पासवर्ड और MFA

Length beats complexity. A long passphrase of several unrelated words is stronger and easier to remember than a short string of symbols.

लंबा पासफ़्रेज़ (कई असंबंधित शब्द) छोटे जटिल पासवर्ड से ज़्यादा सुरक्षित और याद रखने में आसान होता है।

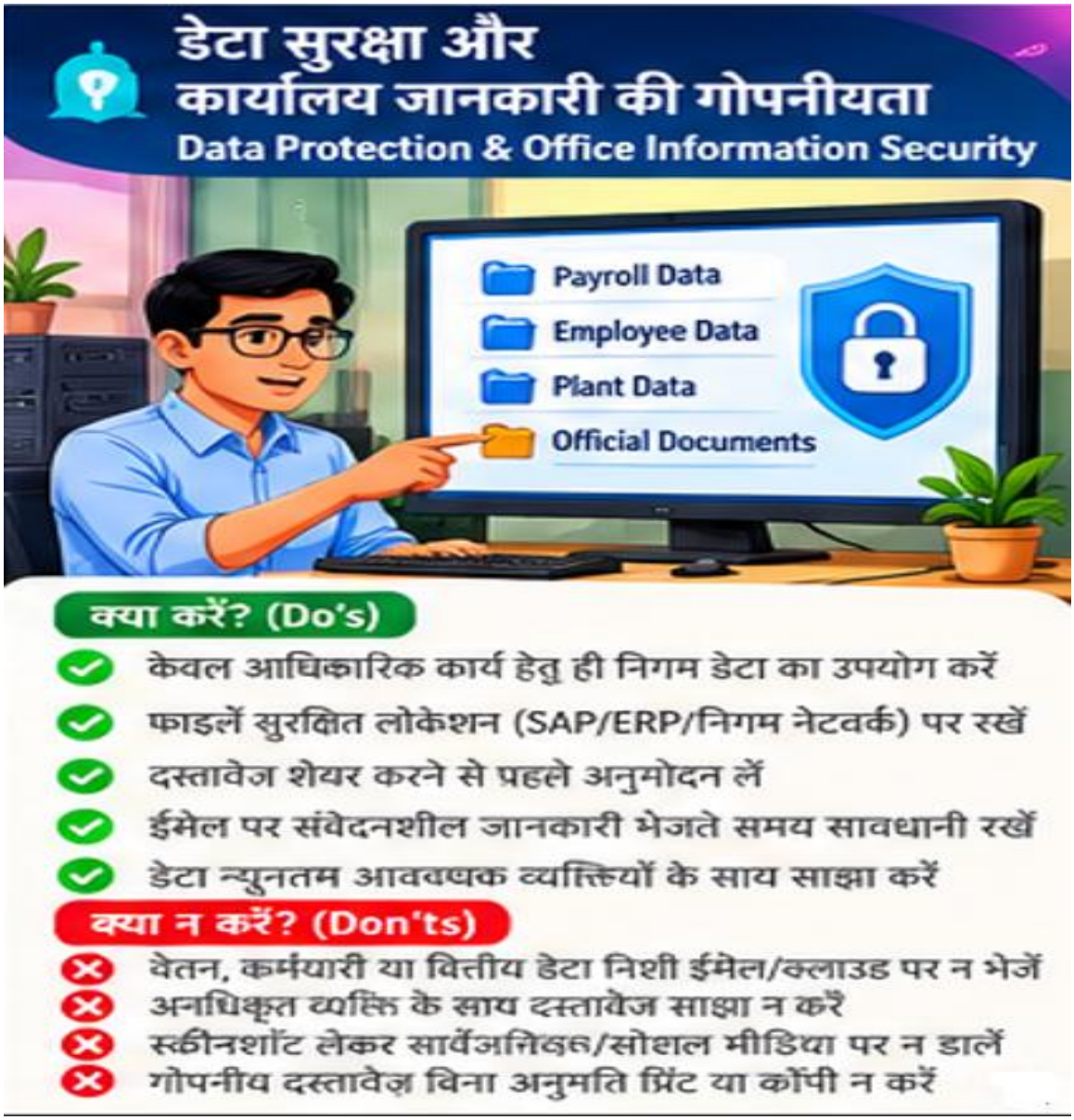
| Do | Don't |
|---|---|
| Use long, unique passphrases for each account. | Reuse official passwords on personal apps or sites. |
| Turn on Multi-Factor Authentication (MFA) wherever available. | Share passwords, OTPs, recovery codes or access tokens. |
| Prefer an authenticator app or hardware key over SMS. | Write passwords on sticky notes or in unapproved apps. |
| Change default passwords once authorised. | Approve a login prompt you did not start. |

- MFA fatigue is a real attack. Criminals who already have your password send prompt after prompt hoping you tap "Approve" to make them stop. If you did not start it, reject it and report it. / MFA थकान एक वास्तविक हमला है। आपने शुरू नहीं किया, तो अनुरोध अस्वीकार करें और रिपोर्ट करें।
- An OTP is a key, not a formality. If you did not start the action, do not approve it. / OTP चाबी की तरह है, औपचारिकता नहीं। कार्रवाई आपने शुरू नहीं की, तो स्वीकार न करें।

## Desktop and PC security | डेस्कटॉप / पीसी सुरक्षा

- Lock the screen whenever you step away (Windows + L). / डेस्क छोड़ते समय स्क्रीन लॉक करें।
- Clear papers, notes and passwords from view. / गोपनीय कागज़ात और स्क्रीन सार्वजनिक नज़र से बचाएँ।
- Secure devices: install only authorised software and keep OS, browser, office apps and endpoint protection updated. / केवल अधिकृत सॉफ्टवेयर उपयोग करें और अपडेट रखें।
- Never plug in unknown USB drives, and never switch off antivirus to get past a warning. / अज्ञात USB न जोड़ें; चेतावनी से बचने के लिए एंटीवायरस बंद न करें।
- Before leaving your desk: LOCK • CLEAR • SECURE / डेस्क छोड़ने से पहले: लॉक करें • साफ़ रखें • सुरक्षित करें

# 4. Protect official information | आधिकारिक जानकारी की सुरक्षा




Employee records, payroll, SAP/ERP credentials, procurement and tender files, network diagrams, audit reports, plant information and internal correspondence are for authorised work only.

कर्मचारी रिकॉर्ड, वेतन डेटा, SAP/ERP लॉगिन, खरीद/टेंडर फाइलें, नेटवर्क डायग्राम, ऑडिट रिपोर्ट, प्लांट जानकारी और आंतरिक पत्राचार केवल अधिकृत कार्य हेतु उपयोग करें।

| Rule | नियम |
|---|---|
| Access only what your duties need. | केवल कार्य हेतु आवश्यक जानकारी तक पहुँचें। |
| Never forward official files to personal email, WhatsApp or personal cloud storage. | कार्यालयी फाइल निजी ई-मेल, WhatsApp या क्लाउड पर न भेजें। |
| Use only authorised USB/removable media and approved collaboration channels. | केवल अधिकृत USB/मीडिया और स्वीकृत माध्यम उपयोग करें। |

| Rule | नियम |
|---|---|
| Do not connect unauthorised devices (phones, laptops, hotspots) to office, IT or OT networks. | कार्यालय, IT या OT नेटवर्क से अनधिकृत डिवाइस न जोड़ें। |
| Follow plant-specific IT/OT procedures. Convenience never overrides security controls. | प्लांट-विशिष्ट IT/OT प्रक्रिया अपनाएँ; सुविधा के लिए सुरक्षा न छोड़ें। |
| Do not post plant photos, layouts or screens on social media. | प्लांट की तस्वीरें, लेआउट या स्क्रीन सोशल मीडिया पर न डालें। |

Share only what is needed, with the right person, through the approved channel.

केवल आवश्यक जानकारी, सही व्यक्ति को, स्वीकृत माध्यम से साझा करें।

## 5. AI at work: Think before you prompt | AI का सुरक्षित एवं जिम्मेदार उपयोग



- AI can help draft, translate and summarise, but treat every AI tool as an outside party. Unless the organisation has approved it, anything you type or upload may be stored, reviewed, used for training or exposed. AI output is a starting point, not an official source or an approval. / AI मसौदा, अनुवाद और सारांश में मदद करता है, पर अनुमोदित न होने पर आपके डाले गए डेटा को संग्रहीत, समीक्षित या लीक किया जा सकता है। AI का उत्तर शुरुआती सामग्री है, आधिकारिक स्रोत या अनुमोदन नहीं।
- The rule: if you would not put it on a public noticeboard, do not paste it into an unapproved AI tool. / जिसे सार्वजनिक सूचना-पट्ट पर नहीं लगाएंगे, उसे अनधिकृत AI टूल में भी न डालें।

## The data traffic light | डेटा ट्रैफ़िक लाइट

| Level | Examples at UPRVUNL | Rule |
|---|---|---|
| **RED:** never in any AI tool without written authorisation | Passwords, OTPs, API keys, tokens. Employee or payroll data. SAP/ERP exports. Tender and procurement files. Network diagrams, IP addresses, OT/plant configurations. Audit and vigilance reports. Source code. Legal files. | Do not upload or type. **लाल:** बिना लिखित अनुमति कभी नहीं। |
| **AMBER:** approved tools only, after removing identifiers | Draft circulars, meeting notes, internal reports, general queries about plant or process topics. | Remove names, employee IDs, vendor names, amounts and locations first. **पीला:** केवल स्वीकृत टूल, पहचान हटाकर। |
| **GREEN:** safe to use | Published press releases, public regulations, general technical concepts, generic letter formats. | Use freely, then verify the result. **हरा:** उपयोग करें, फिर जाँचें। |

## How AI creates new risks | AI से नए जोखिम

| Risk | What can happen | Your defence |
|---|---|---|
| Data leakage | Pasted text or uploaded files are stored, reviewed or reused by the provider. Public share links expose whole chats. | Follow the traffic light. Never create public share links. |
| Fake or unapproved AI apps | Cloned chatbots, free "AI summariser" sites and browser extensions that steal data or carry malware. | Use only organisation-approved platforms from official stores. |
| Prompt injection | Hidden instructions in a web page, email, PDF or document trick an AI assistant into leaking data or taking actions. | Do not let an AI tool with file or email access read untrusted content. Check before acting on its output. |
| Over-powered AI agents and connectors | An AI tool linked to your mail, drive or calendar can read, send or delete on your behalf. | Grant the least access possible. Review integrations and permissions. Never link official accounts to personal AI tools. |
| Hallucination | Invented facts, rules, clause numbers, dates or references that sound convincing. | Verify against the original source. Add human review for anything sensitive. |

| Risk | What can happen | Your defence |
|---|---|---|
| AI-powered fraud | AI-written phishing, cloned voices, deepfake video calls. | Verify through a saved number or official channel (see Section 2). |
| Unsafe AI-generated code or scripts | Code may contain flaws, outdated or malicious packages. | Review and test in a safe environment. Never run unreviewed scripts on official or plant systems. |
| Account takeover | A weak or reused password on an AI account exposes your chat history. | Use a unique password and MFA. Do not sign up for personal AI tools with your official email. |

AI के नए जोखिम: डेटा लीक, नकली AI ऐप/एक्सटेंशन, प्रॉम्प्ट इंजेक्शन, अत्यधिक अनुमतियाँ, गलत तथ्य (hallucination), AI-आधारित धोखाधड़ी, असुरक्षित कोड और खाता हैक। बचाव: स्वीकृत टूल, कम अनुमतियाँ, सत्यापन और मानव समीक्षा।

## Do and don't | क्या करें और क्या न करें

| Do | Don't |
|---|---|
| Use only GoI-approved AI platforms for work. | Use personal or free AI accounts for official files. |
| Remove names, IDs, amounts and locations before prompting. | Upload employee lists, payroll, tenders, audit reports or source code. |
| Check the tool's data, browser, integration and sharing settings. | Enter passwords, OTPs, API keys or any secret. |
| Verify facts, dates, figures and references against original sources. | Copy AI output into official notes, tenders or approvals unchecked. |
| Keep a human accountable for every decision. | Let AI approve, sign off or decide on finance, HR, safety or legal matters. |
| Get engineering review before using AI advice for plant or OT work. | Ask AI to change or advise on live plant control settings without review. |

- Before you press Enter: the 5-second check | भेजने से पहले
- Is this tool approved by GoI? / क्या यह टूल स्वीकृत है?
- Would I be comfortable putting this on a public noticeboard? / क्या मैं इसे सूचना-पट्ट पर लगा सकता/सकती हूँ?
- Have I removed names, IDs, numbers and locations? / क्या पहचान योग्य विवरण हटा दिए?
- Will I verify the answer before using it? / क्या उत्तर को उपयोग से पहले जाँचूँगा/जाँचूँगी?
- Am I, not the AI, responsible for the outcome? / क्या अंतिम जिम्मेदारी मेरी है?
- If you shared something by mistake | गलती से डेटा साझा हो गया
- Report it to IT/security straight away. Note the tool, the time and what was shared. Follow IT's instructions on removal and password changes. Do not wait to see whether anything happens. / तुरंत IT/सुरक्षा टीम को बताएँ। टूल का नाम, समय और साझा की गई जानकारी नोट करें। हटाने और पासवर्ड बदलने के लिए IT के निर्देश मानें।
- Open item for IT: insert the list of UPRVUNL-approved AI tools and the contact for requesting approval of a new one.
- AI helps. You decide. Verify everything. / AI सहायता करता है। निर्णय आपका है। हर बात की पुष्टि करें।

# 6. Safe on the move and ready to recover | मोबाइल, नेटवर्क, बैकअप




## Mobile, Wi-Fi and internet | मोबाइल, नेटवर्क और इंटरनेट

- Install apps only from official stores. Avoid unknown APK files. / ऐप केवल आधिकारिक स्टोर से; अज्ञात APK से बचें।
- Deny unnecessary camera, microphone, contacts, location and background permissions. / अनावश्यक अनुमतियाँ रोकें।
- Use a strong screen lock, biometrics and a short auto-lock time. / मजबूत स्क्रीन लॉक और कम ऑटो-लॉक समय रखें।
- Hide OTP and message previews on the lock screen. / लॉक स्क्रीन पर OTP की झलक छिपाएँ।
- Avoid sensitive transactions on open public Wi-Fi and turn off auto-join. / खुले सार्वजनिक Wi-Fi पर संवेदनशील लेन-देन न करें।
- Use the organisation-approved VPN when required. / आवश्यकता पर संगठन का स्वीकृत VPN उपयोग करें।
- Scan a QR code only when you trust where it was printed. / QR कोड तभी स्कैन करें जब स्रोत पर भरोसा हो।
- Personal phone, official desktop and home Wi-Fi all need safe habits. / निजी मोबाइल, कार्यालयी डेस्कटॉप और घर का Wi-Fi: सभी पर सुरक्षित आदतें जरूरी हैं।
- Updates, backups and ransomware | अपडेट, बैकअप और रैनसमवेयर
- A backup matters only if it can be restored. Follow approved backup and retention rules, check that backups finish, and keep access to them protected. / बैकअप तभी उपयोगी है जब उससे डेटा वापस मिल सके। स्वीकृत बैकअप नियम अपनाएँ, सफलता की जाँच करें और पहुँच सुरक्षित रखें।

| Habit | आदत |
|---|---|
| Install approved security updates and restart promptly. | स्वीकृत सुरक्षा अपडेट करें और समय से रीस्टार्ट करें। |
| Keep browsers, office apps, PDF readers and endpoint protection current. | ब्राउज़र, ऑफिस ऐप, PDF रीडर और एंडपॉइंट सुरक्षा अपडेट रखें। |
| Keep protected backups and test recovery through approved procedures. | सुरक्षित बैकअप रखें; स्वीकृत प्रक्रिया से रिकवरी जाँचें। |
| Report repeated backup failures and security warnings. | बार-बार बैकअप विफल होने या चेतावनी आने पर रिपोर्ट करें। |
| On a suspected infection, do not delete evidence or try your own recovery. | संदिग्ध संक्रमण पर साक्ष्य न मिटाएँ और स्वयं रिकवरी न करें। |

Never pay, delete or investigate alone. Report and follow the incident-response process.

स्वयं भुगतान, डिलीट या जाँच न करें। रिपोर्ट करें और घटना-प्रतिक्रिया प्रक्रिया अपनाएँ।

# 7. Something went wrong? Report, don't hide | रिपोर्ट करें, छिपाएँ नहीं




- Report suspicious emails, unexpected MFA prompts, accidental data sharing (including into AI tools), suspected malware, unusual account activity or lost devices straight away. Early reports limit damage.
- संदिग्ध ई-मेल, अनपेक्षित MFA अनुरोध, गलती से डेटा साझा होना (AI टूल सहित), मैलवेयर का संदेह, असामान्य गतिविधि या डिवाइस खोने की सूचना तुरंत दें।
- Stop. Do not reply, click again or talk further to the caller. / रुकें, आगे कार्रवाई न करें।
- Keep the evidence. Do not delete emails, files, chats or logs. Take a screenshot if safe. / साक्ष्य सुरक्षित रखें।
- Report. Contact UPRVUNL's designated IT/security channel and follow plant procedures. / निर्धारित IT/सुरक्षा माध्यम पर रिपोर्ट करें।
- Follow instructions. Change credentials only through approved steps. / पासवर्ड स्वीकृत प्रक्रिया से ही बदलें।
- If money is involved, call your bank at once and use the official cybercrime reporting channels. / धन प्रभावित हो तो बैंक को तुरंत बताएँ।

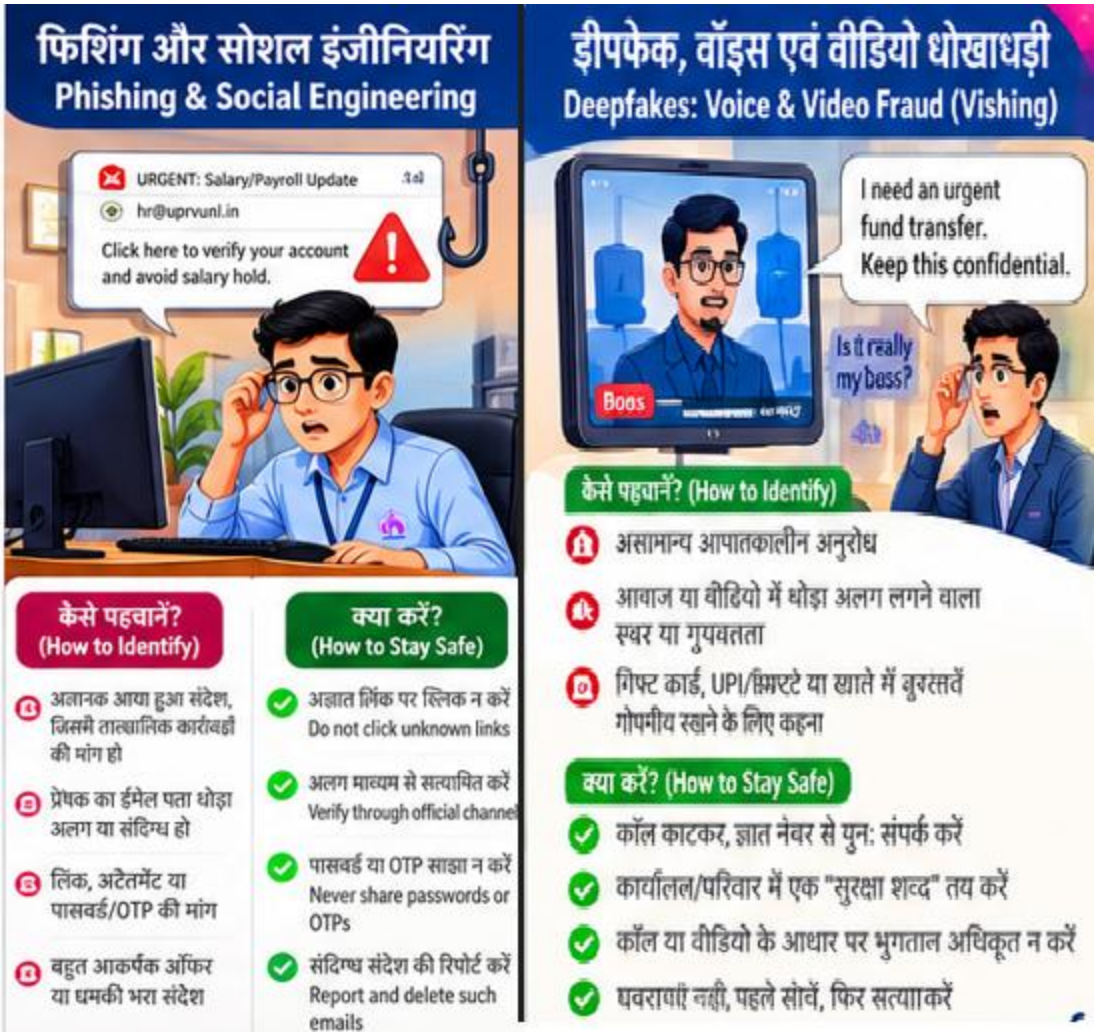
## Who to contact | संपर्क

| Contact | Details |
|---|---|
| UPRVUNL IT/security helpdesk | Pragati Unit at HQ Lucknow |
| Plant IT/OT or control-room security officer | IT Division of the Project |
| CERT-In incident desk | incident@cert-in.org.in, helpline 1800-11-4949 (toll-free), cert-in.org.in |
| Cyber Swachhta Kendra | csk.gov.in |
| Financial cyber fraud (personal) | National Cyber Crime Reporting Portal, cybercrime.gov.in, helpline 1930 |

Internal notification comes first. External contacts do not replace UPRVUNL's reporting and escalation procedures. Under CERT-In's 2022 directions, organisations must report certain cyber incidents to CERT-In within six hours of noticing them, so a quick internal report matters. The IT/security team makes that external report, not individual employees.

अंदरूनी सूचना पहले। बाहरी संपर्क UPRVUNL की रिपोर्टिंग प्रक्रिया का विकल्प नहीं हैं। CERT-In के 2022 निर्देशों के अनुसार संगठनों को कुछ साइबर घटनाओं की सूचना छह घंटे के भीतर देनी होती है, इसलिए तुरंत रिपोर्ट करना ज़रूरी है।

# 8. At home and online | घर पर और ऑनलाइन




- Cyber hygiene is a family habit. The same scams that target the office reach your phone at home. / साइबर स्वच्छता परिवार की आदत है। साइबर घोटाले जो दफ्तर को निशाना बनाते हैं, आपके घर पर आपके फोन तक भी पहुँच जाते हैं।
- Use unique passwords for banking, email, shopping and social accounts, and turn on MFA. / हर खाते के लिए अलग पासवर्ड और MFA।.
- Never share OTPs, PINs, card details or screen-sharing access with anyone claiming to be support staff. / सहायता कर्मी बताने वाले को OTP, PIN, कार्ड या स्क्रीन-शेयरिंग न दें।
- Check investment, job, refund and prize offers independently, especially those asking for upfront payment. / निवेश, नौकरी, रिफंड और इनाम के ऑफर की स्वतंत्र पुष्टि करें।
- Avoid oversharing location, travel plans, family details or workplace photos online. / लोकेशन, यात्रा और कार्यालयी तस्वीरें अधिक साझा न करें।
- Talk to family about voice-cloning scams and agree a safe verification word. / परिवार के साथ सत्यापन का तरीका तय करें।
- Teach children and elders to use only approved apps and AI tools carefully, and never to share photos, voice or ID documents with unknown chatbots. / बच्चों और बुज़ुर्गों को AI टूल सावधानी से उपयोग करना सिखाएँ।
- Block and report impersonation and suspicious accounts, and keep evidence when safe. / प्रतिरूपण वाले खाते ब्लॉक/रिपोर्ट करें।

**Myth or fact? | मिथक या तथ्य?**

| Myth | Fact |
|---|---|
| "Hackers only go after big companies." | Attackers target people. Anyone with email access is useful to them. |
| "If the email has no spelling mistakes, it is safe." | AI now writes clean, convincing messages. Check the sender, link and request instead. |
| "My phone call is from my officer, I know his voice." | Voices can be cloned. Verify through a saved number. |
| "Deleting the suspicious email fixes it." | Deleting destroys evidence. Report first. |
| "Cybersecurity is the IT department's job." | IT builds the walls. Employees decide who walks through the door. |
| "Free AI tools are harmless." | If the product is free, your data may be the price. Use approved tools only. |
| "An AI answer is always correct." | AI can invent facts and references. Verify before use. |

# 9. Quiz, challenge and pledge | प्रश्नोत्तरी, चुनौती और संकल्प

## Quick quiz: answers are at the end | त्वरित प्रश्नोत्तरी

1) An urgent ERP password-reset link arrives from an unfamiliar email. What do you do? / अपरिचित ई-मेल से ERP पासवर्ड रीसेट लिंक आता है। क्या करेंगे?
2) A familiar voice asks you to send confidential files to a personal email. What is safest? / परिचित आवाज़ निजी ई-मेल पर गोपनीय फाइल माँगती है। सुरक्षित कदम?
3) You get an MFA prompt you did not start. What now? / अपने शुरू न किया MFA अनुरोध आए तो?
4) You suspect a malicious attachment opened on your PC. Do you delete the email? / संदिग्ध अटैचमेंट खुल गया, क्या ई-मेल मिटाएँगे?
5) An AI tool offers to "summarise" a spreadsheet of employee salaries. What do you check? / AI टूल वेतन सूची का सारांश बनाने को कहता है। क्या जाँचेंगे?
6) You find a free browser extension that promises to "write all your emails with AI". Should you install it? / क्या मुफ़्त AI एक्सटेंशन इंस्टॉल करेंगे?
7) An AI assistant gives you a clause number from a government rule. Is it enough to quote it in a note? / क्या AI द्वारा दिया गया नियम संख्या सीधे नोट में लिख सकते हैं?
8) You pasted a draft tender into a public AI chatbot by mistake. What next? / गलती से टेंडर ड्राफ्ट AI चैटबॉट में डाल दिया। आगे क्या?

## Challenge | चुनौती

| Week | Challenge | चुनौती |
|---|---|---|
| 1 | Turn on MFA on your email and one personal account. | ई-मेल और एक निजी खाते पर MFA चालू करें। |
| 2 | Spot and report one suspicious message to IT. | एक संदिग्ध संदेश की रिपोर्ट करें। |
| 3 | Review your AI tool permissions and delete any unapproved extensions. | AI टूल अनुमतियाँ जाँचें और अनधिकृत एक्सटेंशन हटाएँ। |
| 4 | Teach one colleague or family member the golden rule and agree a verification word. | एक सहकर्मी या परिवार को सुनहरा नियम सिखाएँ। |

## The UPRVUNL cyber hygiene pledge | संकल्प

☐ I will protect official information.

☐ I will use only authorised systems and approved AI tools.

☐ I will verify unexpected requests before acting.

☐ I will report incidents promptly.

☐ I will practise safe digital habits at work and at home.

मैं आधिकारिक जानकारी की सुरक्षा करूँगा/करूँगी, अधिकृत सिस्टम और स्वीकृत AI टूल उपयोग करूँगा/करूँगी, अनपेक्षित अनुरोधों की पुष्टि करूँगा/करूँगी, घटनाओं की समय पर रिपोर्ट करूँगा/करूँगी और कार्यालय तथा घर दोनों जगह सुरक्षित डिजिटल आदतें अपनाऊँगा/अपनाऊँगी।

**PAUSE • CHECK • VERIFY • REPORT | #CyberHygieneOurCulture**

रुकें • जाँचें • सत्यापित करें • रिपोर्ट करें

## Answer key | उत्तर

1) Do not click. Open the official portal yourself. / क्लिक न करें; पोर्टल स्वयं खोलें।
2) Verify through a known contact channel and follow approved sharing rules. / ज्ञात संपर्क माध्यम से पुष्टि करें।
3) Reject it and report promptly. / अस्वीकार करें और रिपोर्ट करें।
4) No. Report immediately and preserve evidence. / नहीं; रिपोर्ट करें, साक्ष्य रखें।
5) Is the tool approved, and is this data authorised for upload? Salary data is RED: do not upload. / वेतन डेटा लाल श्रेणी है; अपलोड न करें।
6) No. Use only approved tools and extensions from official sources. / नहीं; केवल स्वीकृत टूल।
7) No. AI can invent references. Check the original source first. / नहीं; मूल स्रोत से जाँचें।
8) Report to IT/security immediately with the tool name, time and what was shared, and follow their instructions. / तुरंत IT/सुरक्षा को रिपोर्ट करें।

# YOUR HABITS PROTECT OUR POWER.

## आपकी डिजिटल आदतें हमारी ऊर्जा-सुरक्षा की रक्षा करती हैं।

## #CyberHygieneOurCulture

**PAUSE • CHECK • VERIFY • REPORT**
**रुकें • जाँचें • सत्यापित करें • रिपोर्ट करें**