PROMPT LIBRARY | DEFENSIVE SECURITY | PRINT EDITION

# CyberPrompts

AI prompt sheet for cybersecurity: 43 ready-to-use prompts for OSINT, VAPT, SOC, incident response, cloud, awareness content, victim help, careers and Indian cyber law explainers.

**[PLACEHOLDER]** replace every green chip with your own details before you run a prompt

CyberWithMadhav | Madhav Pandya

CATEGORIES


| | | |
|---|---|---|
| 01 | Recon and OSINT | 3 |
| 02 | VAPT and AppSec | 5 |
| 03 | SOC and Detection | 4 |
| 04 | Incident Response | 2 |
| 05 | Cloud and Hardening | 2 |
| 06 | Malware and Reporting | 2 |
| 07 | Content Creation | 5 |
| 08 | Cyber Law Explainers | 3 |
| 09 | Compliance | 3 |
| 10 | Victim Help | 4 |
| 11 | Career | 4 |
| 12 | Training | 3 |
| 13 | SOC Basics | 3 |


// DISCLAIMER

**Disclaimer:** These prompts are for education, authorised testing and defensive security only. Use them only on systems, accounts and data you own or have written permission to test. Unauthorised access is a civil wrong under IT Act s.43 and, if done dishonestly or fraudulently, an offence under s.66. AI outputs can be wrong, so verify every result, and never paste passwords, OTPs, client data or personal information into an AI tool. CyberWithMadhav and Madhav Pandya accept no liability for misuse.

PREPARED BY

**Madhav Pandya**

CyberWithMadhav | iammadhavpandya-oss.github.io/cyberwithmadhav

00 // READ FIRST

# Scope, ethics and how to use these prompts

**AUTHORISED AND DEFENSIVE USE ONLY**

- Use offensive-security prompts only on systems you own or have **written permission** to test, inside the agreed scope and time window.
- Unauthorised access is a civil wrong under IT Act s.43 and, with dishonest or fraudulent intent, an offence under s.66.
- These prompts are written to help you understand, detect, report and fix. They deliberately avoid working exploit code and step-by-step attack instructions.

**PROTECT DATA AND CHECK THE OUTPUT**

- **Never paste** passwords, API keys, private keys, session tokens or client personal data. Mask IPs, hostnames, usernames and IDs first.
- Check your employer's or client's AI policy and the tool's data retention settings. Personal data is covered by the DPDP Act 2023.
- AI output can be wrong or invented. Verify CVE IDs, Event IDs, section numbers and commands against primary sources before use.

## Prompt anatomy

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Role** | **Context** | **Task** | **Format** | **Guardrails** |
| "Act as a senior SOC analyst..." | Scope, assets, audience, `[PASTE DATA]` | One clear job, with limits | Table, checklist, word cap | "If missing, write `[NEEDS INFO]`" |

Card layout: category and number, title, when to use it, the prompt (green chips are placeholders), and a pro tip. Groups 01 to 06 were written for this sheet; groups 07 to 13 come from the CyberWithMadhav prompt library.

CyberWithMadhav | Madhav Pandya

## 01 Recon and OSINT

### 01 Passive OSINT plan for an authorised engagement

Plan passive reconnaissance on an organisation you have written permission to assess.

> Act as an OSINT analyst on an authorised assessment. Client: `[ORGANISATION]`. Scope and rules of engagement: `[PASTE SCOPE]`. Authorisation reference: `[RoE / CONTRACT ID]`. Build a passive-only recon plan (no scanning, no login attempts, no social engineering). Cover: domains and subdomains from public sources, certificate transparency, public code repos, leaked-credential exposure checks via legitimate breach-notification services, employee role exposure at the job-title level only, and technology fingerprints from public pages. For each step give: source, what to record, and the privacy risk. Output a table plus a list of items that are out of scope and must not be collected.

PRO TIP Paste the actual scope text. If the AI suggests anything active, it is outside passive recon: strike it.

### 02 Image geolocation reasoning (verification work)

Verify where a public photo or video frame was taken, for fact-checking or a victim's own case.

> Help me geolocate a public image for verification. Context: `[WHY YOU ARE VERIFYING, e.g. viral claim check]`. Visible clues I can see: `[DESCRIBE SIGNAGE, SCRIPT, VEHICLES, PLATES FORMAT, VEGETATION, SHADOWS, ARCHITECTURE]`. Claimed location: `[CLAIMED PLACE]`. Walk through the clues one by one, say what each suggests and how confident you are, list two or three candidate areas, and tell me which free tools (map street view, sun-angle calculators, reverse image search) I should use to confirm each. Do not identify private individuals in the image.

PRO TIP Describe the clues in text rather than uploading faces. Treat any final answer as a lead to confirm, not a fact.

### 03 Personal digital footprint review

Audit your own (or a consenting client's) online exposure and reduce it.

> I want to review my own digital footprint. Name and handles: `[YOUR NAME / USERNAMES]`. Platforms I use: `[LIST]`. Build a checklist to find what is publicly visible about me (search operators, people-search sites common in India, old accounts, data broker listings, public documents such as Aadhaar or PAN photos posted by mistake). For each finding type, give the fix: privacy setting, takedown request, or account deletion route, and the Indian complaint channel if misuse is involved (1930, cybercrime.gov.in, platform grievance officer).

PRO TIP Run this only on yourself or someone who has given you written consent.

## 02 VAPT and AppSec

### 04 Nmap output triage

Turn raw scan output from an in-scope host into a prioritised list.

> You are a senior penetration tester reviewing scan output from an authorised test. Scope: `[IN-SCOPE RANGE]`. Authorisation reference: `[RoE / CONTRACT ID]`. Scanning without permission is a contravention under IT Act s.43(a) and may be an offence under s.66. Paste: `[NMAP -sV OUTPUT, SANITISED]`. For each open port and service: likely software and version, why it matters, known weakness classes to check (with CVE IDs only if you are confident, else say 'check NVD'), and the next safe verification step. Rank findings High / Medium / Low with one-line reasoning. Flag anything that looks out of scope or fragile (e.g. OT, printers, production DB) so I can confirm with the client before touching it.

PRO TIP Replace real IPs and hostnames with `[HOST-A]`, `[HOST-B]` before pasting.

### 05 Scan plan within scope

Draft a low-risk scanning plan before the test window opens.

> Draft a network test plan for `[CLIENT]` within this scope: `[CIDRs / URLs]`. Authorisation reference: `[RoE / CONTRACT ID]`. Scanning without permission is a contravention under IT Act s.43(a) and may be an offence under s.66. Exclusions: `[EXCLUDED HOSTS]`. Test window: `[DATES AND TIMES IST]`. Constraints: `[e.g. production, no DoS, rate limits]`. Give phases (discovery, service detection, vulnerability verification), the tool and safe flags for each, expected traffic level, stop conditions, and who to call if something breaks. End with a pre-test checklist: signed authorisation, emergency contact, backups confirmed, monitoring team informed.

PRO TIP Have the client sign off the plan itself, not just the scope.

### 06 CVE brief for a mixed audience

Explain a published vulnerability to engineers and management in one page.

> Write a one-page brief on `[CVE-ID]` for `[AUDIENCE]`. Our affected assets: `[PRODUCT, VERSION, WHERE USED]`. Use only these sources I paste: `[VENDOR ADVISORY TEXT / NVD ENTRY / CERT-In ADVISORY]`. Sections: What it is (2 lines, plain English), Who is affected, Severity and exploitability (CVSS and whether exploitation is reported, citing the source), What we should do (patch, workaround, detection), Deadline recommendation. Do not include exploit code or step-by-step exploitation.

PRO TIP If the AI states 'actively exploited', check the source says so (for example a CISA KEV or vendor note).

### 07 OWASP WSTG test checklist

Build a web app test checklist mapped to OWASP WSTG for an authorised test.

> Create a test checklist for `[APP NAME]`, a `[TECH STACK]` app with these features: `[LOGIN, PAYMENTS, FILE UPLOAD, API, etc.]`. Authorisation reference: `[RoE / CONTRACT ID]`. Scanning without permission is a contravention under IT Act s.43(a) and may be an offence under s.66. Map each test to its OWASP WSTG ID and category. For each: what to test, safe test idea, evidence to capture, and pass/fail criteria. Prioritise by the features listed. Add a short section for API-specific checks (OWASP API Top 10) if an API is present. Mark tests that need extra client approval (e.g. account lockout, payment flows).

PRO TIP Ask the AI to output CSV so you can track status per test.

### 08 Pentest finding write-up

Turn your raw notes into a client-ready finding.

> Write a pentest finding from my notes. Notes: `[PASTE NOTES, SANITISED]`. Affected asset: `[ASSET]`. Format: Title; Severity with CVSS v3.1 vector and a one-line justification; Description; Impact in business terms; Steps to reproduce at a level the client's developers can follow; Evidence references `[SCREENSHOT IDs]`; Remediation (short-term and long-term); References (OWASP, CWE). Keep it factual. If my notes do not support a claim, write `[NEEDS EVIDENCE]`.

PRO TIP Severity is your call, not the AI's. Recheck the CVSS vector yourself.

## 03 SOC and Detection

### 09 L1 alert triage

Decide quickly whether an alert is benign, suspicious or an incident.

> Act as an L2 SOC analyst coaching an L1. Alert: `[ALERT NAME AND RULE]`. Raw event fields: `[PASTE, WITH USERNAMES AND IPs MASKED]`. Asset context: `[ROLE OF HOST / USER]`. Walk me through: what the rule detects, three benign explanations, three malicious explanations, the exact pivots to check next (which logs, which fields), and a decision: close as benign, escalate, or open an incident. Give the ticket note I should write in 4 lines.

PRO TIP Keep a library of your best triage notes and paste one as an example to get consistent output.

### 10 Phishing email analysis

Analyse a reported email safely and decide on response.

> Analyse this reported email for phishing. Headers: `[PASTE FULL HEADERS]`. Body text (links defanged as hxxp): `[PASTE]`. Attachment names and hashes only: `[LIST]`. Check SPF/DKIM/DMARC results, sender and reply-to mismatch, lookalike domains, urgency cues, and link destinations. Give a verdict with confidence, IOCs in a table (type, value, action), and user-facing advice in 3 lines. Do not open or fetch any link.

PRO TIP Never paste the live attachment. Use hashes and sandbox reports from your approved tool.

### 11 SIEM query writer (SPL / KQL / Sigma)

Turn a detection idea into a query you can test.

> Write a detection for: `[BEHAVIOUR, e.g. 10+ failed logins then a success from a new country within 30 minutes]`. Log source and field names: `[PASTE A SAMPLE EVENT]` (mask usernames, hostnames, IPs and email addresses). Give the query in `[SPL / KQL / Sigma]`, explain each line, list expected false positives, and suggest a threshold to start tuning. Also give a test case: a sample event set that should trigger and one that should not.

PRO TIP Paste a real field list. Most broken AI queries come from guessed field names.

CyberWithMadhav | Madhav Pandya

### 12 Windows event log hunting

Plan a hunt across Windows logs for a suspected technique.

> Help me hunt for `[TECHNIQUE, e.g. suspicious PowerShell, new service creation, lateral movement]` on Windows endpoints. Available logs: `[SECURITY, SYSMON, POWERSHELL OPERATIONAL, DEFENDER]`. List the relevant Event IDs and fields, the MITRE ATT&CK technique IDs, a query for `[SIEM]`, what normal looks like in a typical Indian SME environment, and what would make me escalate.

PRO TIP Check the Event IDs against Microsoft documentation before you build a rule on them.

## 04 Incident Response

### 13 IR first hour (CERT-In 6-hour clock)

Structure the first hour of a suspected incident in an Indian organisation.

> We may have an incident. What we know: `[SUMMARY]`. Time first noticed: `[DATE, TIME IST]`. Systems: `[AFFECTED ASSETS]`. Our sector: `[SECTOR]`. Give me a first-hour checklist: contain without destroying evidence, preserve logs (note CERT-In Directions 2022: reportable incidents within 6 hours of noticing the incident or being told of it, logs kept 180 days), who to inform internally, what to capture for the CERT-In report, and whether personal data may be involved (DPDP Rules 2025, Rule 7, once in force (about 13 May 2027): notify affected people and the Board without delay, detailed report to the Board within 72 hours; until then IT Act s.43A and the SPDI Rules 2011 apply). End with a decision list for the incident lead.

PRO TIP This is a starting checklist, not legal advice. Confirm reporting duties with counsel and your sector regulator.

### 14 Incident timeline builder

Merge messy notes and log extracts into one clean timeline.

> Build an incident timeline from these inputs: `[PASTE NOTES, LOG EXTRACTS, EMAILS, ALL IN IST OR WITH TIMEZONE]` (redact names, emails, phone numbers and client identifiers first). Normalise every time to IST, sort chronologically, and output a table: time, source, event, actor/asset, confidence, evidence reference. Flag gaps longer than `[X]` minutes and contradictions between sources. Do not invent events to fill gaps.

PRO TIP Keep the original evidence untouched. Work only from copies.

## 05 Cloud and Hardening

### 15 Cloud IAM review

Spot risky permissions in an AWS, Azure or GCP policy.

> Review this IAM policy / role assignment export for least privilege: `[PASTE JSON, ACCOUNT IDs MASKED]`. Context: this identity is used for `[PURPOSE]`. List risky permissions (wildcards, admin, privilege escalation paths, cross-account trust), explain the risk of each, and propose a tightened policy. Add a checklist for MFA, key rotation and unused identities.

PRO TIP Test the tightened policy in a non-production account first.

### 16 Linux server hardening plan

Produce a hardening checklist for a server you administer.

> Create a hardening plan for `[DISTRO AND VERSION]` running `[SERVICES]`. Exposure: `[INTERNET-FACING / INTERNAL]`. Map items to CIS Benchmark sections where possible: SSH config, users and sudo, patching, firewall, logging and time sync (NTP, needed for CERT-In log rules), file permissions, services to disable. For each item give the check command, the fix, and the rollback.

PRO TIP Apply changes in a maintenance window and keep console access in case SSH breaks.

## 06 Malware and Reporting

### 17 Static script triage (safe)

Understand what a suspicious script does without running it.

> Explain what this script does, statically, without executing anything. Script (defanged, URLs as hxxp): `[PASTE]`. Tell me: purpose in one line, step by step behaviour, persistence or network activity, IOCs (domains, IPs, file paths, registry keys), MITRE ATT&CK mapping, and a detection idea. If parts are obfuscated, describe the technique; do not produce a working deobfuscated payload that could be reused.

PRO TIP Handle samples only in an isolated analysis environment approved by your organisation.

### 18 Executive summary for leadership

Turn a technical report into a one-page summary a CEO will read.

> Write an executive summary of this security report for `[AUDIENCE, e.g. CEO and board]`. Report: `[PASTE KEY FINDINGS]`. Business context: `[WHAT THE COMPANY DOES]`. Structure: overall risk in one sentence, top 3 risks with business impact in rupees or downtime terms where I gave figures, what is already fixed, decisions needed from leadership with owners and dates. Plain English, no jargon, max 300 words.

PRO TIP Give the AI your real numbers. If you do not, it must say `[FIGURE NEEDED]`, not estimate.

## 07 Content Creation

### 19 Scam News Story to Hinglish Reel Script

Turn a verified Indian scam news report into a 30 to 45 second awareness Reel in Hinglish.

> You are a cyber awareness scriptwriter for an Indian Instagram and YouTube Shorts page called `[PAGE NAME]`, aimed at `[AUDIENCE, e.g. working adults in Mumbai and Palghar]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. News facts: `[PASTE NEWS SUMMARY]`. Source: `[SOURCE NAME AND DATE]`. Case status: `[UNDER INVESTIGATION / CHARGESHEETED / CONVICTED]`. Write a `[30/45/60]` second Reel script in natural Hinglish (Roman script). Constraints: explain how the scam works only at a level that helps a victim recognise it, never step by step instructions a criminal could reuse; do not name accused persons or companies if the case is ongoing, use 'police ke mutabik' or 'allegedly'; no fear mongering, keep it calm and practical; mention helpline 1930 and cybercrime.gov.in at the end. Output format: 1) On-screen text hook for 0 to 2 seconds (max 6 words). 2) Spoken hook line. 3)

CyberWithMadhav | Madhav Pandya

Three beats labelled Kya hua, Kaise pehchane, Kya kare, each with spoken line and on-screen text. 4) CTA line. 5) Caption in English (max 60 words) with 5 relevant hashtags. 6) A one-line source credit.

PRO TIP Paste the actual article text instead of a headline so the AI does not invent details, and always re-read the final script against the source before recording.

### 20 Marathi Cyber Awareness Reel

Create a short awareness Reel in simple spoken Marathi for Maharashtra audiences, including seniors.

You are a Marathi-speaking cyber safety educator creating content for `[PAGE NAME]` for viewers in `[REGION, e.g. Vasai, Palghar, Thane]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Topic or scam type: `[TOPIC]`. Key facts: `[FACTS]`. Target viewer: `[e.g. senior citizens, homemakers, students]`. Write a `[30/45]` second Reel script in simple, conversational Marathi written in Devanagari, with an optional Roman transliteration below each line. Avoid heavy Sanskritised words; use everyday words people in `[REGION]` actually use, and keep common English tech words like OTP, UPI, link, app as they are. Rules: protective guidance only, no instructions that teach the scam; no names of accused in ongoing cases; end with 1930 and cybercrime.gov.in. Output: hook text (max 5 words), spoken script in 3 short beats, a 'he kara / he karu naka' (do / do not) list of 3 items each, and an English caption under 50 words.

PRO TIP Ask a native Marathi speaker from your target area to read the script aloud once; if they stumble on a word, replace it.

### 21 Instagram Carousel Outline

Plan a 7 slide educational carousel on a scam or safety topic that people save and share.

You are a social media content strategist specialising in Indian cyber awareness carousels for `[PAGE NAME]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Topic: `[TOPIC]`. Facts and examples: `[FACTS]`. Language: `[HINGLISH / ENGLISH / MARATHI]`. Brand style: `[e.g. navy background, cyan and red accents]`. Create a 7 slide carousel outline. Slide 1: cover with an alert tag and a question hook (max 7 words). Slides 2 to 5: one idea per slide, max 25 words each, with a suggested visual (e.g. phone mockup showing a blurred fake SMS). Slide 6: 'Kya kare / Kya na kare' with 3 ticks and 3 crosses. Slide 7: CTA with 'Report: 1930 | cybercrime.gov.in', Save and Share prompt, and handle `[HANDLE]`. Constraints: blur or replace any real phone numbers, names, UPI IDs or links in example visuals; do not explain how to execute the scam; do not name accused parties in ongoing cases. Output as a table with columns: Slide, Headline, Body text, Visual notes. Then give a caption (max 80 words) and 5 hashtags.

PRO TIP Write slide 1 last. Once the inner slides are clear, the strongest hook is usually the most surprising fact from slide 2 or 3 turned into a question.

### 22 YouTube Long-Form Explainer Script

Draft an 8 to 12 minute YouTube explainer on a cyber fraud trend in India for monetisable long-form content.

You are a YouTube scriptwriter for an Indian cyber awareness channel, `[CHANNEL NAME]`, presented by `[PRESENTER NAME]` in `[HINGLISH / HINDI / ENGLISH]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Topic: `[TOPIC]`. Verified facts, stats and sources: `[FACTS WITH SOURCES]`. Target length: `[MINUTES]`. Viewer: `[AUDIENCE]`. Structure: 1) Cold open (first 30 seconds) with a relatable situation, no clickbait claims. 2) What the scam is. 3) Why people fall for it (psychology: urgency, authority, fear, greed). 4) Red flags checklist. 5) What to do in the first hour if it happens: call 1930, report on cybercrime.gov.in, contact the bank, preserve evidence. 6) Common myths. 7) Recap and CTA. Rules: awareness only, never a how-to for committing fraud; attribute every statistic to the source I gave; for ongoing cases say 'allegedly' and avoid naming accused; where law is discussed, add a line that viewers should consult a lawyer for their specific case. Output: full script with section headings, timestamps estimate, B-roll suggestions in `[brackets]`, 3 title options under 60 characters, and a description with chapter markers.

PRO TIP Ask the AI for the script first, then in a second message ask it to cut 15 percent. Tighter scripts hold retention much better.

### 23 Thumbnail Headline and Concept Ideas

Generate honest, high click-through thumbnail text and concepts for a cyber awareness video.

You are a YouTube thumbnail strategist for Indian tech and cyber awareness channels. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Video topic: `[TOPIC]`. Key takeaway: `[ONE LINE]`. Language: `[HINGLISH / HINDI / MARATHI / ENGLISH]`. Presenter will appear: `[YES / NO]`. Brand colours: `[COLOURS]`. Give 10 thumbnail headline options, each 2 to 4 words, with one word to put in a highlight box. Mix scripts if useful (e.g. Roman plus Devanagari). Then give 3 full concepts, each with: face expression, prop or phone mockup content, background colour, text placement, and an optional tag like 'SCAM ALERT'. Constraints: the thumbnail must match what the video actually delivers, no misleading claims, no real victim photos, no real scammer numbers or identifiable private data, no logos of banks or companies used in a way that implies they did wrong. Output: a numbered list of headlines, then the 3 concepts as short bullet blocks, then which one you recommend and why.

PRO TIP Test the top two options on a phone screen at small size. If you cannot read the text in one second, it is too long.

## 08 Cyber Law Explainers

### 24 Explain a Cyber Law Section in Simple Hinglish

Break down one section of the IT Act 2000, BNS 2023 or DPDP Act 2023 for a general audience.

You are a legal educator who explains Indian cyber law to ordinary people in simple Hinglish. You are not giving legal advice. Law and section: `[ACT AND SECTION NUMBER]`. Official text of the section (pasted from the official source): `[PASTE TEXT]`. Audience: `[e.g. students, small shop owners]`. Use only the section text I pasted. If I have not pasted it, say you need the official text and do not reconstruct it from memory. Output: 1) One line meaning in Hinglish. 2) Explanation in 4 to 6 short bullets: what act is covered, who it applies to, what the penalty or consequence is as stated in the text. 3) Two everyday Indian examples that are clearly hypothetical. 4) Common misunderstandings. 5) 'Victim ho toh kya kare' with 1930 and cybercrime.gov.in if the section relates to a cybercrime. 6) Closing disclaimer: this is general information, consult a qualified lawyer for your case. Constraints: do not cite case law or amendments unless I provide them; flag any old IPC to BNS mapping as 'verify with official text'.

PRO TIP Always paste the section from an official government source such as indiacode.nic.in. Models often mix up IPC and BNS numbering.

### 25 Real Case Study Explainer (Law Plus Lesson)

Explain a reported Indian cybercrime case by linking what happened to the relevant laws and the safety lesson.

> You are a cyber law and awareness educator. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Case summary from a reputable news source: `[PASTE SUMMARY]`. Source and date: `[SOURCE]`. Current case status: `[STATUS]`. Sections reportedly invoked by police (as reported): `[SECTIONS OR UNKNOWN]`. Write an explainer for `[FORMAT: Reel script / LinkedIn post / blog section]` in `[LANGUAGE]`. Structure: what reportedly happened (neutral language), which legal provisions were reported and what they broadly cover, what the victim did right or could have done, 3 safety lessons, how to report (1930, cybercrime.gov.in). Rules: if the case is not concluded, do not name accused individuals or companies and use 'allegedly' or 'as per police'; never present allegations as proven; do not speculate about guilt; do not describe attack techniques in reproducible detail; do not identify the victim. End with: for any legal situation, consult a lawyer.

PRO TIP Note the article date in your content. Case status changes fast, and an 'allegedly' that turns into an acquittal can create defamation risk if you named someone.

### 26 Myth vs Fact: Cyber Law Edition

Create myth-busting content about common legal misconceptions people in India have about online crime.

> You are a cyber law awareness writer creating myth vs fact content for `[PLATFORM]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Myths to address: [LIST 3 TO 6 MYTHS, e.g. 'Police only take cyber complaints above a certain amount', 'Sharing a forwarded morphed photo is not a crime']. Legal points I have verified, with sources: `[PASTE VERIFIED POINTS]`. For each myth, write: Myth (one line), Fact (max 40 words, based only on my verified points), and What to do (one action). If I have not provided a verified point for a myth, mark it `[NEEDS VERIFICATION]` rather than stating the law yourself. Add a closing slide or line: report cybercrime at 1930 or cybercrime.gov.in; this is general awareness, not legal advice, consult a lawyer for your situation. Output in `[LANGUAGE]`, formatted as `[CAROUSEL SLIDES / REEL BEATS / BLOG LIST]`.

PRO TIP Pick myths from real comments and DMs you receive. Content that answers your own audience's confusion gets shared more.

## 09 Compliance

### 27 DPDP Act 2023 Readiness Checklist for a Small Business

Build a practical, plain-language data protection checklist for an Indian SME, clinic, coaching centre or shop.

> You are a privacy compliance consultant helping small Indian businesses prepare for the Digital Personal Data Protection Act 2023 and any Rules notified under it. You give general guidance, not legal advice. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Business type: `[TYPE]`. Size: `[EMPLOYEES]`. Personal data collected: `[e.g. names, phone numbers, Aadhaar copies, health records, student data]`. How it is collected: `[FORMS / WHATSAPP / WEBSITE / CCTV]`. Where it is stored: `[EXCEL / GOOGLE DRIVE / BILLING SOFTWARE / PAPER]`. Who has access: `[ROLES]`. Third parties used: `[e.g. payment gateway, SMS vendor]`. Any children's data: `[YES / NO]`. Create a checklist grouped into: notice and consent, purpose limitation and data minimisation, security safeguards, data principal rights (access, correction, erasure, grievance), children's data, vendors and processors, retention and deletion, breach handling. For each item give: the action in plain English, priority (High / Medium / Low), effort (Quick win / Project), and an owner role. Constraints: do not quote penalty amounts or rule deadlines unless I paste the official text; flag anything that depends on the latest DPDP Rules as 'verify current Rules'. End with a note to consult a qualified lawyer or privacy professional before finalising.

PRO TIP Start by listing every place customer data lives, including staff WhatsApp chats and personal phones. That is where most small businesses have gaps.

### 28 Privacy Notice Draft (Plain Language)

Draft a clear privacy notice for a small Indian website, app or offline business.

> You are a privacy writer who drafts plain-language privacy notices for Indian small businesses. You are drafting for review, not giving legal advice. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Business name and contact: `[NAME, ADDRESS, EMAIL]`. Grievance or contact person: `[NAME / ROLE]`. Data collected: `[LIST]`. Purposes: `[LIST]`. Sharing with: `[THIRD PARTIES]`. Retention: `[PERIODS]`. Cookies or analytics: `[TOOLS OR NONE]`. Languages needed: `[ENGLISH / HINDI / MARATHI]`. Draft a privacy notice under 600 words with headings: Who we are, What data we collect, Why we use it, Who we share it with, How long we keep it, Your rights and how to use them, How to withdraw consent, How to complain, Updates to this notice. Rules: write at a Class 8 reading level, short sentences, no legal jargon; do not claim certifications or security measures I have not listed; do not invent data uses. Mark every assumption with `[CONFIRM]`. Add a final note to me (not in the notice) listing points a lawyer should review.

PRO TIP Read the notice as if you were the customer. If you would not understand why the business needs your Aadhaar copy, the notice is not clear enough yet.

### 29 Data Breach Response Plan for an SME

Prepare a one-page incident response plan an Indian small business can follow when personal data is exposed.

> You are an incident response consultant writing for a non-technical small business owner in India. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Business: `[TYPE AND SIZE]`. IT setup: `[e.g. 5 laptops, Google Workspace, Tally, website on shared hosting]`. IT support: `[IN-HOUSE / VENDOR NAME / NONE]`. Key data: `[LIST]`. Write a breach response plan with phases: 1) Detect and confirm, 2) Contain (first 60 minutes), 3) Preserve evidence, 4) Assess what data and whose data, 5) Notify (affected people, the Data Protection Board as required under DPDP once its breach rules are in force (about 13 May 2027), CERT-In where its directions apply, police or cybercrime.gov.in if a crime is involved, bank if money is involved), 6) Recover, 7) Review and improve. For each phase: what to do, who does it, and a one-line 'do not do this' warning (e.g. do not wipe the affected laptop before evidence is preserved). Constraints: do not state exact reporting timelines unless I paste the official requirement; mark them `[VERIFY TIMELINE]`. Include a contact sheet template with blanks. Recommend legal counsel review notification decisions. Output as a printable one to two page document with checkboxes.

PRO TIP Print the plan and keep a copy offline. During ransomware or an account takeover, the shared drive where the plan is stored may be the thing that is locked.

CyberWithMadhav | Madhav Pandya

## 10 Victim Help

### 30 Cybercrime Complaint Draft for cybercrime.gov.in

Help a victim organise facts into a clear, chronological complaint to file on the National Cyber Crime Reporting Portal.

> You are a calm, supportive cyber crime victim assistance helper in India. You help organise facts; you do not provide legal representation. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Victim details to include only as placeholders: `[NAME]`, `[CITY]`, `[CONTACT]`. Incident type: `[e.g. UPI fraud, sextortion, fake job, account hack]`. What happened in my own words: `[STORY]`. Dates and times: `[LIST]`. Amounts and transaction IDs / UTR numbers: `[LIST]`. Suspect identifiers I have (phone, UPI ID, account, profile link, website): `[LIST]`. Evidence I have: `[SCREENSHOTS, SMS, CALL LOGS, EMAILS]`. Already done: `[e.g. called 1930, informed bank]`. Produce: 1) A short incident summary (max 80 words). 2) A chronological timeline table (date, time, event, evidence reference). 3) A list of suspect identifiers exactly as I gave them. 4) A list of evidence to upload, with suggested file names. 5) The complaint description in clear English (max 400 words), and optionally in Hindi. Rules: do not add, assume or exaggerate facts; keep the tone factual, not emotional; do not accuse anyone by name beyond the identifiers I provide. End with reminders: if money was lost, call 1930 immediately if not done yet, since speed matters; file at cybercrime.gov.in; inform your bank in writing; keep the acknowledgement number; consult a lawyer for further legal steps.

PRO TIP Do not paste full card numbers, PINs, OTPs or passwords into any AI tool. Use the last 4 digits only. The portal and bank will ask for full details through their own channels.

### 31 Bank or UPI Fraud Dispute Letter

Draft a formal written complaint to a bank about an unauthorised transaction or UPI fraud.

> You are a consumer banking complaint writer in India. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Bank and branch: `[BANK, BRANCH]`. Account holder: `[NAME]`. Account or card (last 4 digits only): `[XXXX]`. Transaction details (date, time, amount, UTR or reference): `[LIST]`. How it happened: `[SUMMARY]`. When I noticed and when I first informed the bank: `[DATE AND TIME, CHANNEL]`. 1930 or cybercrime.gov.in acknowledgement number: `[NUMBER OR NONE]`. Remedy sought: `[e.g. reversal, block, investigation, written response]`. Draft a polite, firm letter or email to the bank's grievance cell with: subject line, reference to my earlier report and complaint number, transaction table, clear statement that the transaction was not authorised by me (only if I said so), request for the remedy, request for written acknowledgement and timeline. Mention that I am aware of the RBI framework on customer liability for unauthorised electronic banking transactions and the Reserve Bank Integrated Ombudsman Scheme 2026 (RB-IOS 2026, cms.rbi.org.in) as an escalation path, but do not quote specific day limits or liability rules unless I paste the current RBI text. Keep under 350 words. Add a separate checklist of attachments. Note at the end: for disputed liability, consult a lawyer or consumer forum advisor.

PRO TIP Report to the bank in writing as early as possible, even if you already called, and keep the email or acknowledgement. Timing can affect how liability is decided.

### 32 Digital Evidence Preservation Checklist

Give a victim a step by step checklist to safely preserve evidence before it disappears.

> You are a digital forensics awareness trainer helping an ordinary person in India preserve evidence after a cyber incident. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Incident type: `[TYPE]`. Platforms involved: `[e.g. WhatsApp, Instagram, Gmail, UPI app, website]`. Device: `[ANDROID / IPHONE / LAPTOP]`. Has the suspect deleted or might delete messages: `[YES / NO / UNSURE]`. Create a checklist with: what to capture (screenshots showing date, time, sender identifier and URL; transaction screens with UTR; call logs; emails with full headers if relevant), how to capture on my device type, how to export chats where the platform allows it, how to store copies safely (a second device or offline drive), what not to do (do not delete chats, do not reply to or threaten the suspect, do not factory reset, do not try to hack back or trace the person yourself, do not share intimate images further even as evidence on social media). Add: report at 1930 / cybercrime.gov.in, keep the acknowledgement number, and give evidence to police when asked. For sextortion or image abuse, add the option of reporting directly to the platform and note that the victim is not at fault. Output as a numbered checklist in `[ENGLISH / HINGLISH]`, under 300 words, with a note to consult a lawyer for court-related evidence questions.

PRO TIP Take a screenshot that includes the profile or number of the sender, not just the message. Investigators need to know who sent it.

### 33 1930 Helpline Call Preparation Sheet

Prepare a victim to make a fast, complete call to the 1930 cyber fraud helpline.

> You are a cyber fraud first-response helper in India. Your goal is to help me call 1930 quickly with every detail ready. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. What happened: `[SHORT SUMMARY]`. Transactions: `[DATE, TIME, AMOUNT, UTR / REFERENCE, FROM BANK, TO ACCOUNT OR UPI ID]`. My bank and account (last 4 digits): `[DETAILS]`. Suspect phone, UPI ID, link or app: `[DETAILS]`. Produce: 1) A 30 second opening statement I can read out on the call. 2) A one-page fact sheet table I can read from (transactions in time order). 3) Questions the operator is likely to ask, with my answers filled from my facts or marked `[NEEDS INFO]`. 4) What to ask for: the complaint or acknowledgement number and next steps. 5) What to do right after the call: file or complete the complaint on cybercrime.gov.in within the time the operator advises, inform the bank in writing, block cards or UPI if needed, change passwords, preserve evidence. Rules: never include full card numbers, CVV, PIN, OTP or passwords; remind me that no genuine helpline operator will ask for OTP or PIN. Keep it short and calm. Output in `[ENGLISH / HINGLISH]`.

PRO TIP Call first, polish later. If money left your account in the last few hours, do not spend more than 5 minutes on this prep before dialling 1930.

## 11 Career

### 34 LinkedIn Post for SOC Learners

Write an authentic LinkedIn post documenting a SOC learning milestone, lab, or lesson.

> You are a LinkedIn ghostwriter for an early-career cybersecurity professional in India targeting Junior SOC Analyst roles. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. My role and background: `[e.g. IT Support Engineer, BCA, law student]`. What I did or learned: `[DETAILS: lab, room, tool, cert, ticket lesson]`. Tools involved: `[e.g. Splunk, Wazuh, Wireshark, Sysmon]`. One

concrete result or screenshot description: `[RESULT]`. Post goal: `[VISIBILITY / RECRUITER INTEREST / COMMUNITY]`. Write a post of 150 to 220 words: a first line hook under 12 words with no clickbait, the context in 2 lines, what I did in 3 short steps, the one lesson, a question to invite comments. Suggest one visual (diagram or redacted screenshot) and 3 to 5 hashtags. Rules: no exaggeration of skills or results, no claim of certs I have not earned, no client or employer confidential data, redact IPs, hostnames and usernames from real environments; only lab or permitted data. Avoid buzzword stacking. Give 2 versions: one more personal, one more technical.

PRO TIP Put links in the first comment and reply to every comment in the first hour. Early engagement matters more than hashtags.

### 35 Junior SOC Analyst Interview Prep with Mock Q&A

Run a realistic mock interview for an L1 SOC Analyst role in India.

You are a senior SOC manager at an Indian MSSP or global capability centre interviewing candidates for a SOC Analyst L1 role. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Job description: `[PASTE JD]`. My background: `[SUMMARY]`. My projects and labs: `[LIST]`. Certs done or in progress: `[LIST]`. Interview round: `[HR / TECHNICAL / SCENARIO]`. Run the mock interview one question at a time and wait for my answer. Cover: networking basics (TCP/IP, DNS, ports), Windows and Linux logs, SIEM concepts, the alert triage process, phishing analysis, the incident response lifecycle, MITRE ATT&CK at a high level, a scenario question, and 'tell me about a project'. After each of my answers, give: a score out of 5, what was good, what was missing, and a model answer of max 120 words. At the end, give a summary of my 3 strongest and 3 weakest areas with a 7 day study plan. Keep the questions defensive and realistic for L1; do not ask me to perform attacks.

PRO TIP Answer out loud and type afterwards. The real interview is spoken, and typing lets you over-polish answers you would not say that way.

### 36 Homelab Write-Up as an Incident Report

Turn a homelab exercise into a professional incident report for GitHub or a portfolio.

You are a SOC team lead who reviews incident reports. Help me turn my homelab work into a portfolio-quality incident report. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Lab setup: `[e.g. Windows 10 VM with Sysmon, Wazuh manager, Kali attacker VM, all on an isolated host-only network that I own]`. Simulated activity I ran in my own lab: `[DESCRIPTION]`. Alerts and logs observed: `[PASTE KEY LOG LINES, REDACTED]`. Actions I took: `[LIST]`. Write a report with: Title, Executive summary (3 lines), Environment and scope (state clearly that this was an authorised isolated lab), Timeline table, Detection (which rule or log fired and why), Analysis (mapping to MITRE ATT&CK technique IDs only if I supplied them or they clearly match; otherwise suggest and mark `[VERIFY]`), Containment and remediation steps, Lessons learned, Detection improvement ideas. Rules: focus on detection and response; do not include weaponised commands or payloads; describe attacker steps only at a high level. Output in Markdown suitable for a GitHub README, with placeholders for screenshots.

PRO TIP Hiring managers read the executive summary and the detection section first. Make those two sections strong before polishing the rest.

### 37 Resume Bullet Polishing for SOC Roles

Rewrite IT support and project experience into honest, impact-focused resume bullets for SOC applications.

You are a cybersecurity recruiter in India who screens resumes for SOC L1 roles. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Target role and JD keywords: `[PASTE]`. My current bullets: `[PASTE]`. Real numbers I can stand behind: `[e.g. tickets per week, users supported, labs completed]`. Rewrite each bullet using the pattern action verb, what, tool, measurable result. Highlight security-relevant parts of IT support work (access management, endpoint hygiene, phishing reports handled, patching, backups). Rules: never invent numbers, tools or responsibilities; if a bullet has no metric, suggest what I could measure and mark it `[ADD METRIC]`; keep each bullet under 25 words; avoid buzzwords like 'rockstar' or 'ninja'. Output a table: Original, Rewritten, Keywords matched. Then list 5 JD keywords I am missing and an honest way to close each gap.

PRO TIP Tailor the top three bullets for each application. Recruiters often scan only those before deciding.

## 12 Training

### 38 College Phishing-Awareness Session Script

Create a 45 minute interactive phishing awareness session for college students.

You are a cyber awareness trainer who runs sessions in Indian colleges. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. College and audience: `[COLLEGE, YEAR, STREAM, APPROX SIZE]`. Language: `[HINGLISH / ENGLISH / MARATHI]`. Time: `[MINUTES]`. Recent local scam examples I want to use: `[LIST WITH SOURCES]`. Resources available: `[PROJECTOR / NO PROJECTOR]`. Create a session plan with: icebreaker poll, what phishing is (email, SMS smishing, voice vishing, WhatsApp, QR code), 5 real-style examples with red flags (use fictional names, numbers and domains like example.com, never live malicious links), a live 'spot the phish' activity, fake internship and job scam section relevant to students, what to do if you clicked, reporting (1930, cybercrime.gov.in, Chakshu on Sancharsaathi for suspicious calls and SMS), and a closing pledge or quiz. Rules: awareness only; do not teach how to build phishing pages or kits; no shaming of victims. Output: a minute-by-minute agenda table, speaker notes for each segment, and a one-page take-home handout.

PRO TIP Get the college's permission before running any simulated phishing test. Never send fake phishing to students without written approval from the institution.

### 39 Cyber Safety Quiz Generator

Generate quiz questions for a workshop, Instagram story poll or Google Form.

You are an instructional designer creating cyber safety quizzes for Indian audiences. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Topic(s): `[TOPICS]`. Audience: `[STUDENTS / EMPLOYEES / SENIORS / GENERAL]`. Difficulty: `[EASY / MEDIUM / HARD]`. Number of questions: `[N]`. Format: `[MCQ / TRUE-FALSE / SCENARIO]`. Language: `[LANGUAGE]`. For each question give: the question, 4 options (for MCQ), the correct answer, and a one-line explanation that teaches the safe behaviour. Use realistic Indian scenarios (UPI collect requests, KYC update SMS, courier or customs calls, 'digital arrest' calls, fake job offers) with fictional names and

CyberWithMadhav | Madhav Pandya

numbers. Rules: protective knowledge only; explanations should mention 1930 or cybercrime.gov.in where reporting is relevant. Also output a version formatted for Instagram story polls (question under 80 characters, 2 options).

PRO TIP Make wrong options plausible. If the right answer is obvious, people learn nothing, so base distractors on what victims actually believed.

### 40 Parent and Senior Citizen Cyber Safety Workshop

Plan a gentle, practical workshop for parents or senior citizens on common frauds.

You are a patient community cyber safety educator for families in `[CITY / AREA]`. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Audience: `[PARENTS / SENIOR CITIZENS / BOTH]`, approx `[N]` people. Language: `[HINDI / MARATHI / HINGLISH / GUJARATI]`. Duration: `[MINUTES]`. Venue setup: `[e.g. society hall, no projector]`. Top concerns from the organiser: `[LIST]`. Plan a workshop covering: OTP and PIN never sharing, fake bank or KYC calls, 'digital arrest' and fake police or CBI calls, pension and life certificate scams, fake customer care numbers from search results, UPI collect requests and QR code scams, WhatsApp account safety (two-step verification), and for parents: children's gaming and social media safety. Include: simple role-play scripts (fictional), a 'pause, check, report' rule, a printable large-font handout with 1930 and cybercrime.gov.in, and how a family member can help. Rules: respectful tone, no tech jargon without explanation, no blaming victims, no step by step fraud methods. Output: agenda, talking points, 2 role-plays, the handout text.

PRO TIP Ask attendees to save 1930 in their phone contacts during the session itself. It is the single most useful thing they will take home.

## 13 SOC Basics

### 41 Alert Triage Explainer and Walkthrough

Understand and document how to triage a specific SIEM or EDR alert in a lab or authorised environment.

You are a patient SOC L2 analyst mentoring an L1 analyst. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Alert name and source: `[e.g. Wazuh rule 5710, Defender alert]`. Alert details (redacted): `[PASTE FIELDS: timestamp, host, user, process, source and destination IP, rule description]`. Environment: `[LAB / AUTHORISED EMPLOYER ENVIRONMENT]`. Available tools: `[LIST]`. Explain: 1) What this alert usually means in plain language. 2) Common false positive causes. 3) A triage checklist: what to verify, which logs to pivot to, which questions to ask the user or asset owner. 4) Indicators that would make it a true positive. 5) Severity reasoning. 6) Recommended next actions and when to escalate. 7) A short ticket note template filled from my data. Rules: do not invent log values; if a field is missing, say what to look up. Map to MITRE ATT&CK only where it clearly applies, marked as a suggestion. Defensive guidance only.

PRO TIP Always write down why you closed an alert as a false positive. That note is what protects you and trains the next analyst.

### 42 Phishing Email Analysis of a Sample You Received

Safely analyse a suspicious email you personally received and write a short verdict.

You are a SOC analyst specialising in phishing analysis. I received this email myself and want to understand whether it is malicious, without interacting with it. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Email headers (pasted as text): `[HEADERS]`. Body text: `[BODY]`. Links shown, with the actual URLs written defanged like hxxp`[:]`//example`[.]`com: `[LINKS]`. Attachment names and hashes if any (I have not opened them): `[DETAILS]`. Analyse: sender and reply-to mismatch, SPF / DKIM / DMARC results from the headers, Received chain anomalies, display name tricks, lookalike domains, urgency and social engineering cues, link versus displayed text mismatch, and attachment risk. Output: a verdict (Likely phishing / Suspicious / Likely legitimate) with confidence, an evidence table, IOCs listed in defanged form, safe next steps (report to my email provider or IT team, block sender, check the hash on a reputation service without opening the file, report to cybercrime.gov.in or the impersonated organisation, call 1930 if money or banking credentials were involved), and a 3-line awareness summary I could share with redacted details. Rules: do not visit or reconstruct the phishing page; do not suggest contacting or retaliating against the sender; redact my own email address and personal data.

PRO TIP Always defang URLs before pasting them anywhere so nobody, including you, can click them by accident.

### 43 Log Review Summary for a Shift Handover

Summarise a batch of logs or alerts from a lab or authorised environment into a clear handover note.

You are a SOC shift lead writing a concise handover. Use only the facts I provide below; if something is missing, write `[NEEDS INFO]` instead of guessing. Time window: `[START TO END, TIMEZONE]`. Environment: `[LAB / AUTHORISED ENVIRONMENT NAME]`. Log or alert extract (redacted): `[PASTE]`. Tickets worked: `[LIST]`. Open items: `[LIST]`. Produce: 1) Shift summary in 3 bullets. 2) Table of notable events (time, source, event, assessment, status). 3) Patterns or anomalies worth watching, with the specific log lines that support each. 4) Open items and recommended owner. 5) Any tuning suggestions for noisy rules. Rules: base every statement on the supplied logs; mark guesses as `[HYPOTHESIS]`; do not include unredacted personal data, passwords or tokens; keep the whole note under 300 words so the next shift can read it in 2 minutes.

PRO TIP Lead with what the next shift must act on. Put routine items at the bottom, because a handover is read under time pressure.

EDUCATIONAL RESOURCE

Prompts are aids, not authority. Results need human review, especially for legal, compliance and incident decisions. Report cyber fraud in India on **1930** or **cybercrime.gov.in**. More at iammadhavpandya-oss.github.io/cyberwithmadhav.

Disclaimer: authorised and defensive use only. Verify every AI output. No liability is accepted for misuse.