POCKET GUIDE · MINI

₹49 EDITION

Digital Privacy & Safety, in 20 Minutes

The plain-English defence plan against phishing, UPI fraud and deepfakes — before the scam call comes. Sourced from CERT-In, I4C, RBI, NIST, the FBI and the FTC.

WEKNOWWHATYOURELOOKINGFOR.COM

Pocket Insight Guide

WHAT'S INSIDE

Everything that matters, in pointers

This mini gives you the honest map of digital safety in 20 minutes: what actually threatens you in 2026, how to lock your passwords and phone, how to spot AI-written phishing and UPI scams, and exactly what to do the moment you're defrauded. Read it once and you're already harder to scam than most people online.

THE ONE IDEA TO HOLD THE WHOLE WAY

Most fraud succeeds on basic gaps: a reused password, a clicked link, a shared OTP. Close those three doors and you're harder to scam than the overwhelming majority of people online.

CHAPTER 01

The 2026 threat landscape

- **Two different questions, two answers:** what loses the most money is investment/"pig-butchering" fraud; what hits the most people is phishing.
- **India in numbers:** ₹22,495 crore lost to cyber fraud in 2025 (I4C). A widely-cited ₹1.2-lakh-crore figure is an unreported-loss projection, not the booked total.
- **The global picture:** $16.6B in US internet-crime losses in 2024 (FBI IC3); 3.8M phishing attacks tracked worldwide in 2025 (APWG).
- **Deepfakes are fastest-growing:** US deepfake-fraud losses hit $1.1B in 2025 — triple 2024. The $25M Arup case: 15 transfers approved on a video call where every other "person" was AI-generated.
- **The honest counter-trend:** classic file-locking ransomware is actually declining for individuals — criminals shifted to stealing and threatening to leak data instead.

REALITY CHECK

~60% of breaches involve a human element (Verizon DBIR 2025). That's bad news and good news: a careful human is a real defence.

CHAPTER 01 · CONTINUED

Where the money actually goes

$6.57B	$2.77B	$1.46B
US investment-fraud losses, 2024 (FBI IC3)	Business-email-compromise losses, 2024	Tech-support scam losses, 2024

Investment scams are rare but catastrophic per victim. Phishing is constant but usually cheap to defeat — one careful pause before you click. You need defences against both.

- **AI cut the cost of attack:** generative AI cut the time to write a phishing email from 16 hours to 5 minutes (IBM).
- **"Shadow AI" is a new cost driver:** it featured in 20% of breaches, adding $670,000 to the average breach cost.

REMEMBER

Judge messages by what they ask you to do — click, pay, share a code, act urgently — not by how polished they look.

CHAPTER 02

Passwords & authentication

- **NIST rewrote the rules:** length beats complexity. No more forced 90-day rotation — change only on evidence of compromise (SP 800-63B, Rev.4).
- **The passphrase wins:** a four-word passphrase like river-copper-lantern-42 beats P@ss1! — support at least 64 characters.
- **Password managers use zero-knowledge:** everything encrypts/decrypts on your device. The provider never sees your vault — but your master password is the one point of failure.
- **The honest LastPass caveat:** the 2022 breach stole encrypted vaults; encryption held, but weak master passwords later cost 150+ victims $35M+.
- **Passkeys are the biggest login upgrade in years:** a key pair bound to the real site's address — phishing-resistant by design. ~5 billion already in use worldwide.

2FA, RANKED WEAKEST TO STRONGEST

SMS OTP (breaks under SIM-swap) → Authenticator app (TOTP) → Passkey (domain-bound) → Hardware key (gold standard). Turn on any 2FA today; upgrade the ladder on email and money accounts first.

Check your exposure first

OLD RULE	WHAT NIST SAYS NOW
Force a change every 90 days	No rotation unless compromise is known
Symbols, digits, mixed case	No composition rules — passphrases OK
Short "complex" strings	Length wins: support 64+ characters

- **haveibeenpwned.com:** a free, trusted tool by researcher Troy Hunt — indexes ~2 billion addresses. Search every email you use.
- **Why SIM-swap breaks SMS 2FA:** a fraudster ports your number to their SIM. FBI IC3 logged $25.98M in US SIM-swap losses across 982 complaints in 2024 alone.

SO DO THIS

Change any reused or breached password now, subscribe to HIBP alerts, and put MFA on the vault itself.

CHAPTER 03

Phishing, quishing & India's scam playbook

- **"Spot the bad grammar" is dead:** AI-assisted phishing jumped from 4% to 56% of reports in a single month (Hoxhunt) — and it converts ~60% better.
- **Quishing rose 5×:** QR-code phishing hides its destination and slips past filters — Microsoft saw a 146% jump in early 2026. Treat any QR like a stranger's link.
- **Fake KYC — India's biggest banking scam:** no bank ever asks for KYC via a link, app download or call. Genuine KYC is in-branch, the official app, or video-KYC only.
- **Digital arrest is not real:** no agency arrests you on a video call or over an OTP-sharing "crime." ~9% of India's 2025 fraud losses, 123,672 cases in 2024.
- **Pig-butchering is the costliest con:** $5.8B in US crypto-investment fraud (2024, FBI IC3) — built on weeks of manufactured trust, not urgency.

THE TELLS THAT STILL WORK

Hover/long-press a link before tapping · assume any "share this OTP" request is a scam · verify urgent asks on a second, known channel · never scan a QR to receive money.

CHAPTER 03 · CONTINUED

Red flags that scream "scam"

3.8M	+85%	640
Phishing attacks tracked worldwide, 2025 (APWG)	UPI fraud rise in FY24, staying high (I4C)	Mumbai deepfake-investment cases, 2025 (₹400cr)

- **The receive-money rule:** a PIN or QR scan is only ever needed to send money. Anyone asking you to "enter PIN to receive a refund" is scamming you.
- **Job & loan scams:** fake offers and task-based "earn money" traps flagged by I4C as a major 2025 vector for harvesting data and cash.

CUT THE CALL, CUT THE LOSS

You cannot be arrested for sharing an OTP — you are the victim. Hang up and report to 1930.

CHAPTER 04

Devices, networks & the VPN question

- **Updates beat almost everything:** turn on automatic updates on every device — most mass hacks exploit bugs that already have a patch available.
- **Sideloading is a 50× risk:** internet-sideloaded Android apps carry 50× more malware than Google Play. Never install an APK sent in a message.
- **Public Wi-Fi is mostly fine now:** 95%+ of web traffic is HTTPS-encrypted, so classic packet-sniffing doesn't work anymore. The real danger is fake login pages.
- **What a VPN actually does:** hides which sites you visit from the local network/ISP and your IP from sites. It does NOT make you anonymous — the VPN provider can now see instead.
- **Router in 10 minutes:** change the default admin password, turn on WPA3, update firmware, disable WPS.

THE HONEST BOTTOM LINE

For everyday HTTPS browsing you don't need a VPN. Its real value is hiding domains from the network, reaching work systems, or a network you distrust.

Fence off your smart devices

	VPN DOES	VPN DOES NOT
Identity	Hides IP from sites	Make you anonymous
Logins	—	Hide you from any site you log into
Scam pages	—	Protect data typed into a fake form

- **The average home runs 25+ connected devices.** Put smart TVs, plugs and cameras on your router's Guest network — a hacked gadget can't then reach your banking laptop.
- **Google's 2026 change:** every Android developer must verify identity, even for sideloaded apps — rolling out from September 2026.

CHAPTER 05 · THE MOST IMPORTANT CHAPTER

The UPI golden rule & the golden hour

- **The one sentence to remember:** your UPI PIN is only ever used to send money. You never enter it to receive money — receiving needs zero action.
- **The collect-request scam:** a fake "refund" arrives as a collect request; you enter your PIN to "receive" it — and it authorises a payment out.
- **RBI zero-liability:** report in writing within 3 working days of the bank's alert and your liability is zero; 4–7 days and it's capped (₹5,000–₹25,000).
- **Tokenisation protects saved cards:** since Oct 2022, merchants can't store your real card number — only a useless token.
- **Freeze credit at all four bureaus:** CIBIL, Experian, Equifax, CRIF High Mark in India — free, 24–48 hours, doesn't touch your score.

THE GOLDEN HOUR

The first ~60 minutes are decisive. Call 1930, file at cybercrime.gov.in, and notify your bank in writing — speed, not paperwork, recovers money.

CHAPTER 05 · CONTINUED

Your rights, in one glance

YOU REPORT WITHIN…	YOUR LIABILITY
3 working days of alert	**Zero**
4–7 working days	**Capped ₹5,000–₹25,000**
Bank negligence, no fault of yours	**Zero**

- **India's DPDP Act 2023:** gives you access, correction, erasure, grievance and nomination rights over your data — enforced by the Data Protection Board.
- **SIM-swap: the 24-hour response:** block the rogue SIM, lock UPI, dial 1930, file an FIR under IT Act 66C/66D.

CHAPTER 06

Family, kids & elders

- **Financial sextortion is surging:** 50,000+ NCMEC reports in 2025 (~137/day) — overwhelmingly teen boys aged 14–17. Money is the goal, not images.
- **The teen script:** don't pay — not once · stop replying and block · save evidence first · report to 1930/NCMEC · say "you are not in trouble."
- **Teens need trust, not spyware:** covert monitoring breaks trust and pushes risk underground; safety scaffolding with agreed rules works better.
- **Elders: four scams to brief by name:** fake customer care, digital arrest, refund/UPI-PIN traps, OTP/KYC calls.
- **Two rules stop most elder fraud:** never share an OTP or PIN with anyone; never enter a PIN to receive money.

SET IT UP FOR THEM (10 MINUTES)

Turn on transaction alerts · teach "pause and verify" · check TAFCOP at sancharsaathi.gov.in for stray SIMs · save 1930 as "CYBER FRAUD — CALL FIRST."

CHAPTER 06 · CONTINUED

The privacy hygiene checklist

- **A unique passphrase** for every important account, stored in a password manager.
- **Passkeys or an authenticator app** for 2FA — never SMS where you have the choice.
- **Automatic updates on** for phone, laptop, browser and apps.
- **Never enter a UPI PIN to receive money** — only to send it.
- **1930 saved in your phone and your family's,** before you ever need it.

THE 80/20 OF STAYING SAFE

Most fraud succeeds on basic gaps: a reused password, a clicked link, a shared OTP. Close those and you're harder to scam than nearly everyone online.

YOU'VE GOT THE MAP. NOW GET THE TERRAIN.

This was the 20-minute version. The full playbook is the whole defence.

You now know more than most people who get scammed. The complete **Digital Privacy & Safety — 2026 Playbook** takes every chapter above and adds the diagrams, the step-by-step settings walkthroughs, and the full emergency scripts.

- **The full 8 chapters** — threat landscape, passwords, phishing, devices, tracking, money, family and breach response.
- **Every settings walkthrough** for Google, Apple and Meta privacy dashboards, screen by screen.
- **The complete scam encyclopedia** — fake KYC, digital arrest, quishing, sextortion, SIM-swap, with red flags for each.
- **The full emergency playbook** — account hacked, card stolen, identity misused, SIM-swap — exact sequences.
- **FAQs & glossary** — every term in plain English, plus your DPDP and GDPR rights explained.

UPGRADE TO THE FULL EDITION

~~₹199~~ **₹99**

Complete illustrated guide · instant download

SCAN / TAP
to upgrade

GO FURTHER, PAY LESS

Two ways to keep going

THE AI & TECH STACK BUNDLE

Digital Privacy + AI Skills + Crypto & Web3 + more

Everything you need to stay safe and sharp in the AI era, in one download.

~~₹396~~ **₹199**

THE COMPLETE LIBRARY

All 30 Skill Series books

Spirituality, money, career, health, tech — the entire collection, one price.

₹499

GET EVERY NEW BOOK FREE

Follow **@weknowwhatyourelookingfor** and join our WhatsApp list — buyers get first access and reader-only pricing on everything we publish next.

weknowwhatyourelookingfor.com

NOTICE

This guide is for **general educational purposes only**. Individual results vary with effort and circumstances, and no specific outcome is warranted.

Published by weknowwhatyourelookingfor.com · For queries, corrections, or licensing, visit weknowwhatyourelookingfor.com.