SECURE BENGAL

Secure Citizens. Strong Digital Bengal.

Cyber Hygiene for Daily Life

Stay Safe • Stay Smart • Stay Secure

Presented by **SECUREDBENGAL** — Digital Safety Awareness Initiative

What is Cyber Hygiene?

Just as personal hygiene keeps our bodies healthy, **cyber hygiene** refers to the regular, safe digital habits we practise to protect our online lives. In today's connected world, nearly every aspect of life — banking, communication, shopping, and identity — exists in digital form. Protecting these assets requires consistent, conscious action.

Mobile Phones

Your primary digital gateway

Bank Accounts

Financial security at stake

Social Media

Your digital identity and reputation

Personal Identity

Guard sensitive personal data

Family Information

Keep loved ones protected

Why Cyber Hygiene Matters

Today's Reality

Cyber crime is rising at an alarming rate across India. Every citizen who owns a smartphone is a potential target — regardless of age, education, or income. Criminals are sophisticated, organised, and constantly evolving their tactics.

Common Threats You Face Every Day

- **OTP Fraud** — Tricking you into sharing one-time passwords
- **UPI Scams** — Fraudulent payment requests and fake QR codes
- **Fake Calls** — Impersonating banks, police, or government
- **Phishing Links** — Malicious URLs that steal your data
- **WhatsApp Hacking** — Account takeover via social engineering
- **Social Media Fraud** — Fake profiles and impersonation attacks

⚠ 📱 Every citizen using a smartphone is a potential target. Awareness is your first line of defence.

Strong Password Habits

Your password is the first barrier between a criminal and your personal data. Weak or reused passwords are responsible for a significant proportion of account breaches. Creating strong, unique passwords for every account is one of the simplest and most effective cyber hygiene habits you can adopt.

✅ A Strong Password Should Include

- Uppercase letters (A–Z)
- Lowercase letters (a–z)
- Numbers (0–9)
- Special symbols (!@#$%)
- At least 10–12 characters

Good example: Bengal@Safe2026!

❌ Never Use These as Passwords

- 123456 or password
- Your date of birth
- Your mobile number
- Your name or family name
- The same password across multiple sites

ⓘ Use a password manager to store unique passwords safely for every account.

OTP & Banking Safety

One-Time Passwords (OTPs) are the last line of defence protecting your bank account. Fraudsters use clever social engineering — posing as bank officials, delivery agents, or government representatives — to convince you to share these codes. Once they have your OTP, your account can be emptied within seconds.

🚫 Never Share These — Ever

- OTP (One-Time Password)
- ATM PIN or debit card PIN
- CVV number on the back of your card
- Net banking username and password

⚠️ The Golden Rule

No legitimate bank, payment gateway, or government body will **ever** call you to ask for your OTP, PIN, or password. If someone asks — **it is fraud. Hang up immediately.**

Phishing Awareness

Phishing is the practice of sending deceptive links or messages designed to look legitimate, tricking users into revealing passwords, financial details, or downloading harmful software. These attacks arrive via SMS, email, WhatsApp, or social media — and they are becoming increasingly convincing.

Check the Website URL

Look carefully at the spelling of any website address. Fraudsters use names like "sbi-bank-secure.com" to mimic real sites. Always verify the domain before entering any personal information.

Look for the HTTPS Lock

A genuine, secure website will show a padlock symbol and begin with **https://** in the browser bar. If it shows "Not Secure," do not enter any passwords or payment details.

Avoid Unknown APK Files

Never download or install **.apk** files sent via WhatsApp, SMS, or email from unknown sources. These files often contain malware that can steal data or take control of your device silently.

Social Media Safety

Social media platforms hold vast amounts of personal information — your location, daily routine, family details, and more. Without proper settings and habits, this information becomes a treasure trove for scammers, stalkers, and identity thieves.

✅ Secure Your Accounts

- Enable **Two-Factor Authentication (2FA)** on all platforms
- Set your profile to **private or friends-only**
- Regularly review app permissions and connected accounts
- Use a strong, unique password for each social platform

❌ Habits to Avoid

- Sharing your **live location** publicly or with strangers
- Posting sensitive personal details (Aadhaar, address, phone)
- Accepting **unknown friend requests** — even if they look familiar
- Over-sharing daily routines — criminals learn your patterns

📸 Think before you post. Once online, information is very difficult to erase.

Mobile Security

Your smartphone is your digital identity. It contains your banking apps, personal messages, photos, contacts, and government credentials. Keeping it secure is not optional — it is essential. Most mobile security breaches occur due to outdated software or apps downloaded from unofficial sources.

✅ Keep Software Updated

Software updates patch known security vulnerabilities. Enable **automatic updates** for your operating system and all apps to stay protected against the latest threats.

✅ Use a Screen Lock

Set a **strong PIN, fingerprint, or face lock**. This prevents physical access to your device if it is lost or stolen. Avoid simple patterns like "L" or "Z."

✅ Official App Stores Only

Download apps exclusively from the **Google Play Store** or **Apple App Store**. Avoid mod APKs, cracked apps, and third-party download sites — these often contain hidden malware.

Public WiFi Dangers

Free public WiFi networks in cafés, railway stations, airports, and shopping centres are convenient — but extremely risky. These networks are often unencrypted and can be monitored by attackers who are connected to the same network. A technique called a **"man-in-the-middle attack"** allows criminals to intercept everything you send and receive.

❌ Never Do This on Public WiFi

- Open banking or UPI apps
- Make online payments
- Log in to email or social media
- Enter passwords or PINs
- Access government portals with credentials

✅ Safer Alternatives

- Use your **mobile data** for sensitive transactions
- Enable a **VPN** (Virtual Private Network) on public networks
- Always log out after using shared or public computers

ⓘ Your mobile data connection is encrypted by default — far safer than open WiFi for banking and payments.

WhatsApp & Messaging Scams

Messaging platforms like WhatsApp have become the primary channel for fraud in India. Scammers craft emotionally compelling messages — fake lotteries, urgent job offers, family emergencies — designed to bypass your rational thinking and prompt immediate action. The cardinal rule: **verify before you trust.**

1

Fake Lottery Wins

"Congratulations! You've won ₹10 lakh. Share your bank details to claim." — Always a scam. No legitimate lottery contacts you this way.

2

Fraudulent Job Offers

Too-good-to-be-true job opportunities requiring an "advance registration fee." Legitimate employers never ask for payment upfront.

3

Fake KYC Updates

Messages claiming your bank or SIM KYC has expired and asking you to click a link or share an OTP. Your bank will never do this via WhatsApp.

4

Emergency Money Requests

A message from a "friend" or "family member" claiming to be in trouble and needing urgent funds. Always call the person directly to verify.

The Digital Arrest Scam

⚠️ HIGH ALERT — LATEST INDIAN CYBER THREAT

The **"Digital Arrest" scam** is one of the most sophisticated and frightening frauds targeting Indian citizens today. Criminals impersonate law enforcement and government officials, using video calls and official-looking props to create an atmosphere of terror, coercing victims into paying large sums of money.

Who Do They Pretend to Be?

- Police officers and commissioners
- CBI or ED (Enforcement Directorate) agents
- RBI (Reserve Bank of India) officials
- Court representatives or judges
- Customs or narcotics department officers

How to Protect Yourself

- Remain **calm** — fear is their most powerful weapon
- No legitimate agency demands money over a phone or video call
- Disconnect and call **1930** (National Cyber Crime Helpline) immediately
- Inform a trusted family member before taking any action

⊗ No government agency will ever arrest you via a phone call or demand payment to avoid prosecution.

Safe Online Shopping

Online shopping offers unmatched convenience, but it also attracts a disproportionate share of fraud. Fake e-commerce websites, counterfeit products, and payment scams are rampant. A few simple checks before every purchase can save you from significant financial loss.

→ Verify the Website

Stick to well-known platforms like Amazon, Flipkart, Meesho, or verified brand websites. For unknown stores, check for customer reviews on independent platforms and look up the seller's contact information and return policy before purchasing.

→ Use Secure Payment Gateways

Always pay using trusted gateways — UPI apps, credit or debit cards with OTP protection, or cash on delivery. **Never transfer money directly to a personal bank account** for an online purchase. Avoid paying via gift cards or cryptocurrency.

→ Be Sceptical of Extreme Deals

If a deal seems **too good to be true, it almost certainly is.** Fraudulent sites lure shoppers with impossibly low prices. If a brand-new iPhone is listed for ₹5,000, you will either receive nothing, or a counterfeit item.

Cyber Safety for Children & Seniors

Children and senior citizens are the most vulnerable members of our digital society. Children face threats such as cyberbullying, grooming, and exposure to harmful content. Seniors are disproportionately targeted by financial frauds and impersonation scams. As responsible family members, we have a duty to protect them.

👧 Protecting Children Online

- Teach them about **stranger danger** in online spaces
- Set parental controls on devices and apps
- Encourage open conversations about online experiences
- Explain that not everyone online is who they claim to be
- Monitor screen time and app usage

👴 Supporting Senior Citizens

- Teach them to **never share OTP or PIN** over the phone
- Help them identify fake caller IDs and impersonation calls
- Set up a verification system: all unknown calls must be verified with a family member first
- Remind them: if a call creates urgency or fear, it is likely fraud

Your Daily Cyber Hygiene Checklist

Good cyber hygiene is not a one-time event — it is a daily practice. These small, consistent habits compound over time to create a powerful shield around your digital life. Make these part of your everyday routine, just as you would lock your front door before leaving the house.

Update Devices

Keep your phone and apps updated to patch security vulnerabilities

Back Up Files

Back up important photos and documents to a secure cloud or external drive

Use Strong Passwords

Create unique, complex passwords for every account

Verify Links

Always check URLs and sender identity before clicking any link

Enable 2FA

Activate two-factor authentication on all important accounts

Think Before Sharing

Pause and reflect before posting or forwarding any message or image

Small daily habits = Big long-term protection. 🛡️

What To Do If You've Been Hacked

Discovering that your account or device has been compromised can be frightening — but acting **quickly and calmly** can significantly limit the damage. Time is critical. Follow these steps immediately if you suspect you have been a victim of cyber fraud or hacking.

01

Change All Passwords

Immediately change the password of the compromised account and any account that shares the same password. Start with your email, as it is the master key to all other accounts.

02

Block Bank Cards

Call your bank's emergency helpline and block your debit and credit cards if any financial account was involved. Most banks offer instant blocking via their app or SMS.

03

Inform Your Bank

Report the incident to your bank branch or their fraud helpline. Request a transaction reversal if any unauthorised transfers have occurred — speed is essential here.

04

Report the Cyber Crime

File a complaint on the **National Cyber Crime Reporting Portal** at **cybercrime.gov.in** or call the national helpline **1930**. Available 24/7.

05

Preserve Evidence

Take screenshots of all suspicious messages, transaction alerts, and call records. Do not delete anything — this evidence is vital for the investigation and any potential recovery of funds.

"Cyber Security Starts With Awareness"

A safe digital Bengal begins with each responsible citizen making informed, conscious choices every single day. Together, we build a community that criminals cannot easily exploit.

🛡️ Stay Alert

Question every unexpected message, call, or link

🔒 Stay Safe

Practise your daily cyber hygiene checklist

📢 Stay Secure

Share this knowledge with family and friends

SECUREDBENGAL — Creating a Cyber Aware Society

National Cyber Crime Helpline: **1930** | cybercrime.gov.in