



CERT-IN • CYBER SWACHHTA KENDRA (CSK) • RBI MASTER DIRECTIVE COMPLIANCE

INDIAN CYBER SECURITY GUIDELINES • TEAM AWARENESS

Standard Operating Procedures for Banking Systems, Employee Hygiene & Customer Safety

MANDATE: 6-Hour Incident Reporting to CERT-In (IT Act Sec 70B)

RBI CS FRAMEWORK: Zero-Trust Architecture

CITIZEN PROTECTION: Golden Hour Intervention (1930)

1 PREVENTING DIGITAL FRAUD

Vishing, Smishing & OTP Theft

Scammers pose as bank staff, electricity boards, or TRAI. **Bank officials NEVER ask for OTP, CVV, or UPI PIN.** Never disclose codes.

Digital Arrest & Impersonation Scams

Impostors pose as Police/CBI over Skype alleging illegal parcels. **Indian law enforcement NEVER conducts arrests or interrogations via video calls.**

Lookalike Domains & Phishing URLs

Always check sender domains. Never click links claiming KYC expired. Verify only on **nkgbsb-bank.com**.

Illegal Lending & Fake IPO Platforms

Never download unauthorized loan apps or transfer money into individual personal accounts for stock market/crypto "guaranteed returns."

2 SECURE PAYMENT PRACTICES

QR Code Golden Rule: Pay vs. Receive
Scanning a QR code and entering your UPI PIN is **STRICTLY** for **DEBITING/SENDING** money. Receiving money never requires a PIN.

ATM Skimming & Shoulder Surfing
Always cover the keypad while entering ATM PINs. Inspect card readers for loose skimming attachments before inserting cards.

Card Controls & Daily Limits (RBI Rule)
Use mobile banking to disable international/online POS usage when idle. Set conservative daily transaction thresholds.

Sanchar Saathi & Chakshu Verification
Verify suspicious incoming SMS/calls on **sancharsaathi.gov.in (Chakshu)** and report malicious numbers to disconnect fraudsters.

3 ACCESS CONTROL & ID HYGIENE

Proactive Password Reset Directive
Reset personal & official passwords every 60-90 days. Never reuse passwords across portals; an external breach can compromise banking logins.

Mandatory App-Based 2FA / MFA
Enable Authenticator apps (Google/Microsoft Authenticator) or hardware tokens. Avoid relying purely on SMS OTPs vulnerable to SIM swap.

Workstation & Session Management
Always lock terminals with **Win + L** when stepping away. Terminate unrecognized active sessions in account settings immediately.

Safe Masked Aadhaar Usage
Share only **Masked Aadhaar** (where only the last 4 digits are visible) for offline verifications to protect against identity theft.

4 MALWARE & DEVICE DEFENSE

Block APK Sideloads
Never install **.APK files** received via SMS or WhatsApp (e.g., fake e-Challan, courier updates). Use official Google Play / App Stores only.

Cyber Swachhta Kendra (CSK) Tools
Utilize free government cleaning tools & **USB Pratirodh** at **csk.gov.in** to scan and disinfect botnets and removable media.

Zero Remote-Access App Permission
Never install AnyDesk, TeamViewer, or screen-sharing tools on instructions from callers, and never dial forwarding strings like ***401***.

Operating System & Antivirus Updates
Keep smartphones, bank terminals, and antivirus definitions updated to protect against active zero-day vulnerabilities.

MANDATORY INCIDENT ESCALATION:
Bank InfoSec Helpdesk: **infosec@nkgbsb-bank.com**
Official Compliance Portals: **cert-in.org.in** • **csk.gov.in**

ACT IN GOLDEN HOUR
Within 2 hrs to freeze defrauded funds!

National Cybercrime Portal:

cybercrime.gov.in

HELPLINE: 1930