NAVIGATING THE DIGITAL FRONTIER

A Guide to Digital Fraud Awareness

Digital fraud isn't just one thing .
It's any deception powered by technology.
From email, SMS, WhatsApp, or Telegram to your bank account – think before you click, tap, or pay, and stay one step ahead of fraudsters.

Stay one step ahead of digital criminals.

Understanding "Digital Fraud"

What Is Digital Fraud?

Digital fraud refers to any deceptive activity carried out using **mobile phones, computers, the internet, or digital payment platforms** to steal money, data, or identity.
It commonly appears in the following forms:

Phishing

Fraudulent emails or messages that trick users into clicking fake links or sharing login details.

Vishing

Fraud calls pretending to be bank officials, government agencies, or company executives.

Smishing

Scam messages or WhatsApp texts containing fake offers, refunds, or account warnings.

Quishing (QR Code Phishing)

Fake QR codes that redirect users to malicious websites or unauthorized payment pages.

Impersonation Fraud

Criminals pose as bank staff, police, delivery agents, or known contacts to gain trust.

Identity Theft

Stealing personal details to open accounts, take loans, or conduct transactions.

Account Takeover

Gaining control of bank, email, or social media accounts using stolen credentials.

Key Fact:

Most digital frauds succeed not because technology fails, but because **trust is exploited**.

The New Wave of Threats

The 2026 Digital Fraud Landscape

- **AI Deepfakes**
  Fraudsters use artificial intelligence to clone the voice or face of a senior officer, employer, or family member.
  If an urgent request for money is received through an unusual channel, **disconnect and verify using a known contact number.**

- **Malicious APK Install Frauds**
  Links shared via SMS or WhatsApp lure users into installing fake apps(e-challan/bank schemes).
  These apps secretly capture OTPs, screen activity, and banking credentials.
- **"Digital Arrest" Scams**
  Fraudsters impersonate police, CBI, or cybercrime officials and threaten arrest over video or phone calls.
  No law-enforcement agency conducts arrests or investigations digitally.
- **SIM Swap Fraud**
  Fraudsters obtain a duplicate SIM using stolen personal details, due to which the actual SIM gets disabled. The victim loses control over communication services.
  Report sudden loss of network and secure accounts immediately.
- **Fake Customer Care Number Scam**
  Fraudsters publish fake customer care numbers to trick people into sharing OTPs and banking details. Always use official contact details and never share OTPs.
- **Investment & Trading Scams**
  Fake stock tips, crypto schemes, and "guaranteed returns" are promoted on social media platforms.
  Assured profits are a strong warning sign.
- **Job & Work-From-Home Frauds**
  Victims are offered online jobs and later asked to pay fees or complete paid tasks.
  Legitimate employers **do not charge for recruitment.**
- **AePS Frauds**
  Misuse of Aadhaar and biometric data leads to unauthorized transactions.
  Do not share Aadhaar details or fingerprints with unknown persons.
- **NACH / Auto-Debit Frauds**
  Unauthorized mandates result in recurring debits from customer accounts.
  Regularly review bank statements and active mandates.
- **Loan & Instant Credit Frauds**
  Fake loan apps collect personal data and use illegal recovery methods.
  Verify lenders before sharing documents or installing apps.
- **BBPS Frauds**
  Fake bill payment links or unauthorized agents collect money without bill settlement.
  Use only official **BBPS-enabled banking channels.**
- **Card Frauds (Debit / Credit Cards)**
  Card details stolen through phishing, skimming devices, or fake customer care calls lead to unauthorized usage.
  Never share **card number, expiry date, CVV, or OTP.**
- **Lost or Stolen Card Misuse**
  Lost cards with PIN can be misused immediately.
  Block your card instantly using the banking app or bank-helpline.

- **ATM Helper Fraud**
  Fraudsters pose as helpful strangers at ATMs and observe PIN entry or swap cards. Never accept help from strangers and always shield your PIN.

Money Mule Frauds

What Is a Money Mule?

A **money mule** is a person who is **knowingly or unknowingly used by fraudsters** to move or receive illegally obtained money through their bank account.

How Customers Get Trapped

- Asked to **receive money and transfer it further**
- Offered **easy commission / quick income**
- Lured through **job offers, online tasks, or acquaintances**
- Requested to **share bank account, debit card, or credentials**

Why It Is Dangerous

- The **account holder is held responsible** for suspicious transactions
- Accounts may be **frozen or closed**
- May attract **regulatory action and legal consequences**

RBI Safety Message

Never allow your bank account to be used by others. Do not receive or transfer money on someone else's instructions.

Stay Safe – Advised Precautions

- Do not share account details, ATM cards, or QR Codes
- Do not accept money for "routing" or "temporary holding"
- Be cautious of job offers/investment scams involving bank transactions
- Report suspicious requests immediately to your bank.
- Do not share sensitive personal information like your Aadhaar number, bank details, or passwords.
- Always confirm the bill status directly from your electricity provider's official app, website, or customer service before making any payments.
- Do not click on links in unsolicited messages.
- Download apps only from official app stores and verify their legitimacy

The "3-Second Rule"

Before You Tap, Click, or Pay

Pause for **3 seconds** and ask yourself:

Was I expecting this?

Unexpected calls, messages, refunds, prizes, or account warnings are **common fraud tactics**.

Is there panic or urgency?

Fraudsters create fear, urgency, or threats to prevent you from thinking clearly.

Is the payment method unusual?

No legitimate bank, government authority, or company will demand payment **only through whatsapp calls, installation of APKs under pressure**.

PIN is never required to receive money.

Bank never asks to enter sensitive credentials for product related information.

A 3-second pause can prevent a lifetime of loss.

Technical Self-Defense

How Digital Frauds Operate And How to Stop Them

Fraud Modus Operandi	Effective Defense	Why It Works
Fake Links & Websites (Phishing / Smishing)	Verify URLs & use official apps	Fake links mimic bank pages to steal login details. Official apps and websites block this risk.
Fake Calls Posing as Bank / Police (Vishing / Impersonation)	Never share OTP, PIN, CVV,passwords	Fraudsters need these to complete transactions. Banks never ask for them. Police, CBI, ED, or any government agency never conduct arrests, inquiries, or demand money over video calls or phone calls; such "digital arrest" threats are always a fraud.
Malicious APK Installation	Install apps only from official app stores	Fake APKs secretly steal banking credentials, read OTPs and control screen activity.
SIM Swap Fraud	Never share SMS OTP	OTP allows fraudster to activate SIM.
Account Takeover	Enable 2FA and step-up Authentication	Multifactor and step-up authentication add extra layers, making it harder for fraudster to access the account.
Social Media Data Mining	Restrict privacy settings	Scammers use personal posts to guess security questions.
QR Code & Refund Scams	Never Enter UPI PIN to receive money.	Scanning someone else's QR code or Entering UPI PIN cannot credit money in your account, it is used to send money.
ATM Helpers	Shield PIN & avoid assistance from strangers	Fraudsters secretly exchange the cards by distracting the customer during transaction. Observing PIN entry enables immediate card misuse.

Fraudsters don't break systems , they exploit behavior.
Awareness breaks the fraud chain.

Reporting & Recovery

If You Are a Victim of Digital Fraud

Act Immediately. Early reporting helps prevent further loss.

Report to J&K Bank (TMC – Transaction Monitoring Cell)

- **Call Contact Centre: 1800-890-2122**
- **Block debit / credit cards instantly through mPay**
- **Report fraudulent transactions via mPay**
- **Report online through the official website of J&K Bank(https://jkb.bank.in)**
- **Visit the nearest J&K Bank branch** for assistance

All digital fraud complaints reported to the Bank are examined and handled through the **Transaction Monitoring Cell (TMC)**.

Report to National Cybercrime Authorities

- **National Cybercrime Helpline: 1930**
- **Online Reporting Portal: www.cybercrime.gov.in**

Keep the Following Details Ready While Reporting

- Bank **account number / card number**
- **Transaction reference number / UTR**
- **Date, time, and amount** of the fraudulent transaction
- **Mobile number / email ID** used by the fraudster
- Screenshots of **messages, calls, links, QR codes, emails**
- **Brief description of the fraud modus operandi** (how the fraud occurred — call, link, APK, QR scan, impersonation, etc.)

Transaction Monitoring Cell (TMC)

Protecting customers through timely detection, response, and reporting.
J&K bank's Transaction Monitoring Cell contacts customers only through **1600-00-8000.**
Remember: Report early. Stay alert. Stay protected.