INDSMART

इंडियन बैंक Indian Bank

BEWARE OF COMMON CYBER FRAUD TACTICS

STAY VIGILANT, STAY SAFE

Common Cyber Frauds at a Glance

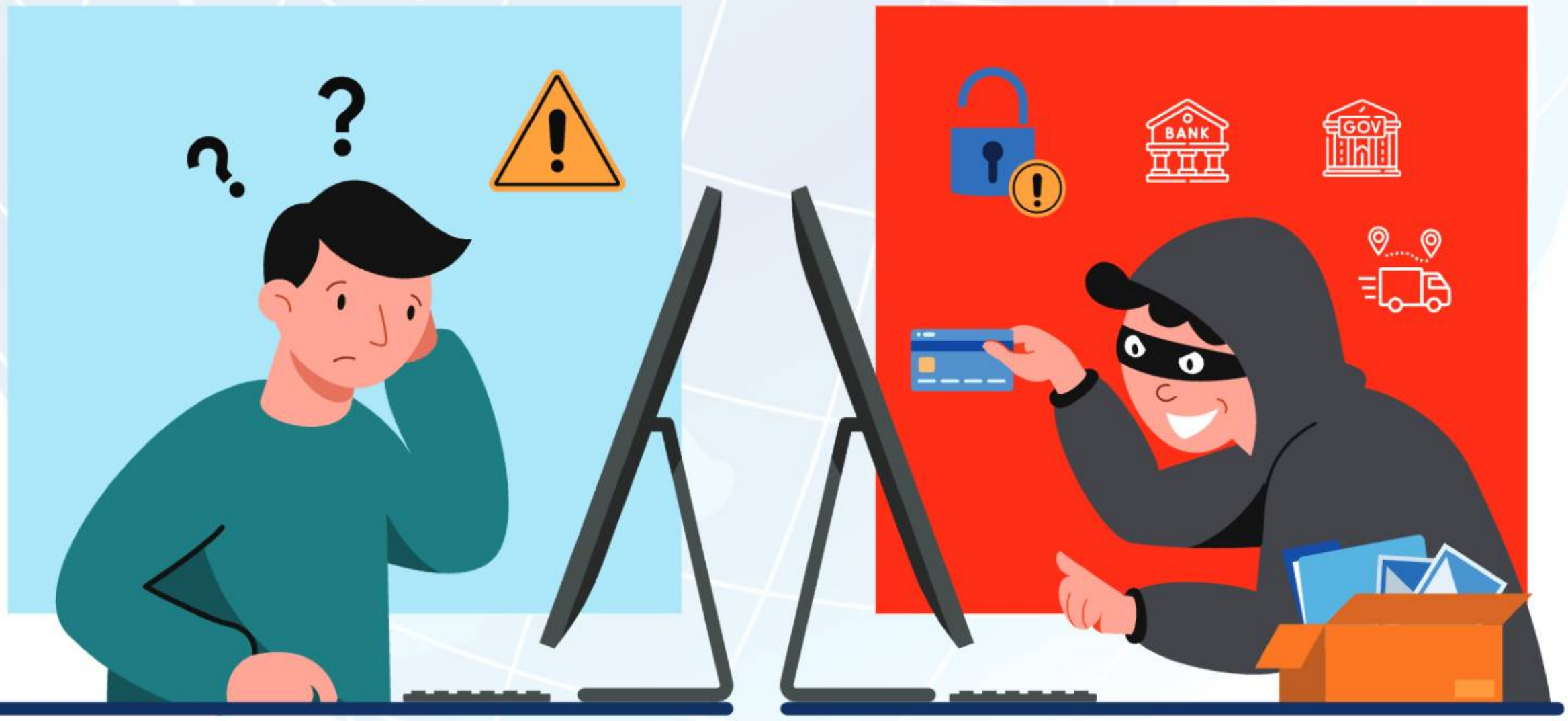
KHABAR NAHI KHABARDAR BANO

Cybercrime helpline

1930

Introduction

In today's digital world, scammers use increasingly sophisticated tricks to deceive people. One common tactic involves impersonating trusted entities like banks, government agencies, or delivery services. They might call you with urgent-sounding issues - claiming your account is at risk, ATM Card needs renewal, KYC needs updation, your Aadhaar needs verification, or your phone service will be disconnected. These calls often play on fear and urgency, pushing you to act quickly without thinking.



The golden rule is simple:

Don't fall for it. If you receive a suspicious call, don't engage. Hang up immediately, block and report the number. Legitimate institutions **will never ask for sensitive information** like your Aadhaar, PAN, date of birth, or bank details over the phone. **Don't press any buttons or follow any instructions** during such calls - they are often designed to keep you connected longer and exploit your trust.

Remember,

Every fraudster plays upon three basic human emotions : Greed, Fear and Innocence. So, **be wise and act calmly.**

Identity Theft:
Don't Let Them Become You

What is identity theft?

The illegal use of your personal information (name, aadhar card number, credit card details) to commit fraud or other crimes.

How does it happens?

Data breaches, lost wallets, phishing scams, malware

Signs of identity theft:

Unexpected bills, unfamiliar charges on accounts, denied credit applications, strange calls from debt collectors.

What to do if you're a victim:

Act fast – contact your bank, file a police report

Mind Games: How Scammers Trick You

Urgency: They create a false sense of urgency to push you into making a quick decision ("Act now or the offer expires!").

Authority: They impersonate someone in a position of power (government agency, bank, tech support) to intimidate you.

Social Proof: They make it seem like "everyone else is doing it" to make you feel like you're missing out.

Scarcity: They claim the item or offer is limited to make you think you need to act fast or lose out.

Greed and Fear: They play on your desire for a big reward or your fear of loss to manipulate your emotions.

Modus Operandi

Sneaky Tricks They Use

Phishing emails: Fake emails that look like they're from your bank or a store you like.

Bad websites: Sites designed to trick you into giving up your passwords.

Phone scams: People pretending to be from your bank to get your information.

Digital Arrest: Scammers impersonate police officers and claim the victim is involved in a fake crime. They threaten the victim by providing fake FIR and do online interrogation and then they ask the victim to send amount to verify victim's account.

Parcel Stuck at Customs/Delivery point: Fraudsters claim a parcel addressed to the victim is stuck at customs due to illegal goods/ for the want of proper address etc., They threaten legal consequences and demand a fine to "release" the parcel/ send a link or ask to download app from a link for paying token amount of Rs.5/ Rs.10 for updating Customer's details to deliver the parcel.

Product Sale on Instagram or Facebook: Scammers offer the products on social media websites like Facebook/Instagram at extremely low prices. Often they demand advance payments and subsequently, either they send counterfeit items or disappear from the platform after receiving the money.

Social Media Attacks: How Scams Spread Online

Fake Profiles

Too-Good-To Be-True Offers

Phishing Links

Exploiting Emotions

Viral Spread Scams

Don't Fall Victim: Recognizing Digital Banking Scams

Phishing Attacks: Fraudulent emails/texts pretending to be from your bank, asking for login details or personal information.

Malware: Harmful software on your device that can steal passwords or monitor activity.

Smishing: Scam text messages leading to fake banking websites or requesting sensitive data.

Vishing: Fraudulent phone calls from someone posing as a bank representative.

KYC Expired: Scammers ask for KYC updates via links/phone calls.

Protecting Yourself from Mobile Banking Scams

Fake Banking Apps: Fraudulent apps designed to look like your bank's official app to steal login details.

Smishing Attacks: Text messages containing links to download malicious apps or visit fake banking websites.

QR Code Fraud: Scammers replace legitimate QR codes with their own, leading to fraudulent websites or malware downloads.

Remote Access Scams: Fraudsters trick you into granting them remote access to your phone, allowing them to control your device and steal information.

Virus Attacks: How Malware Can Steal Your Banking Info

Keyloggers: Viruses that record your keystrokes, including passwords and credit card numbers.

Banking Trojans: Malicious software specifically designed to target online banking activities.

Man-in-the-Browser Attacks: Malware intercepts and modifies communication between you and your bank's website.

Ransomware: Viruses that encrypt your files and demand payment to unlock them, threatening to release sensitive data.

Watch Out for Job Scams

Unsolicited job offers: Too-good-to-be-true opportunities that contact you out of the blue.

Upfront fees: Requests for payment for training, certification, or background checks.

Requests for sensitive information: Asking for bank details or Aadhaar number early on.

Poorly written communications: Job postings or emails with lots of grammatical errors and typos.

Pressure to act quickly: Urgent deadlines or trying to rush you into a decision.

Investing options to double the money

Promises of doubling your money quickly or with little effort are almost always scams.

Common tactics: Claims of "secret" systems, insider information, or limited-time offers.

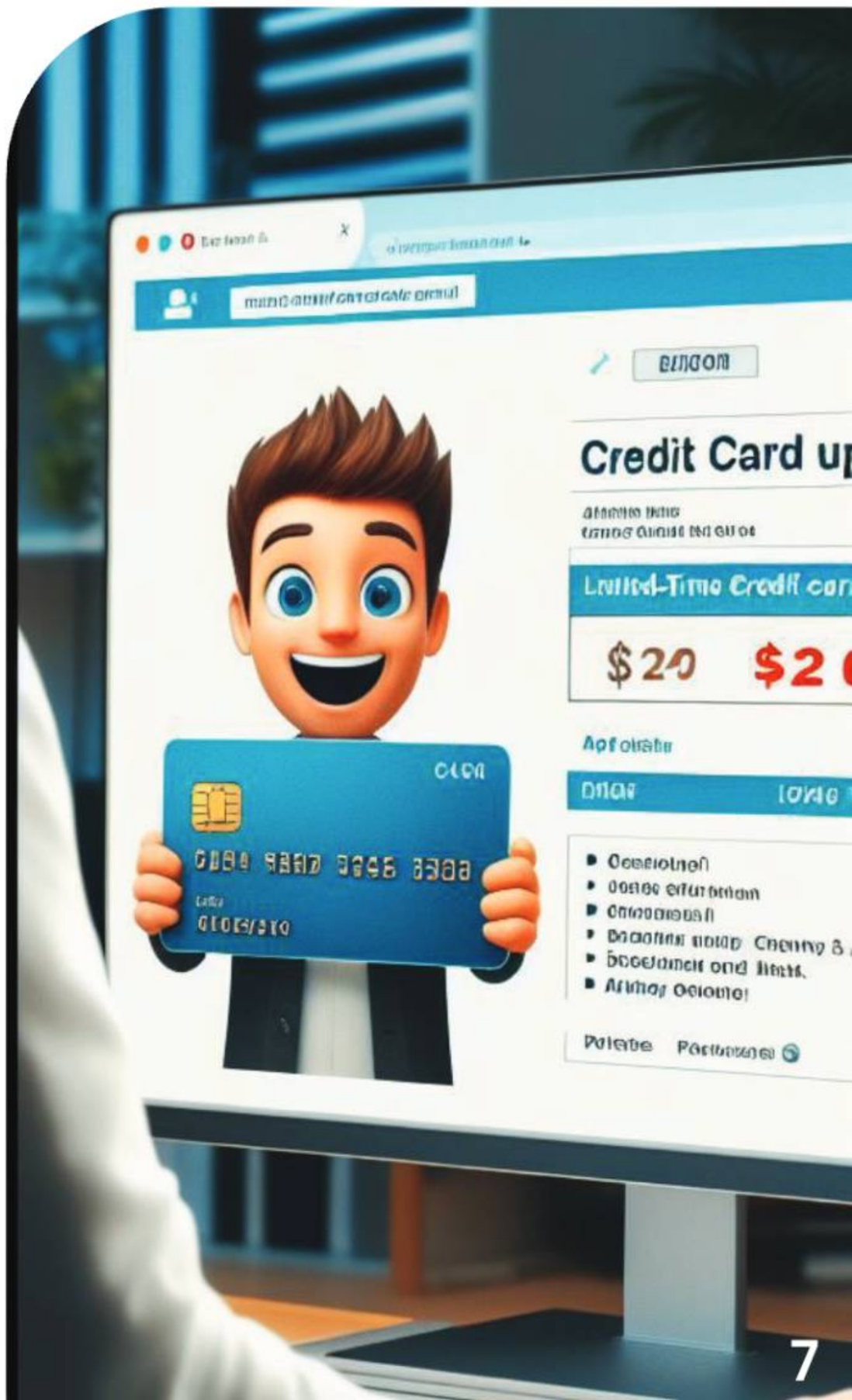
High-pressure sales tactics designed to create urgency and limit time for critical thinking.

Be wary of unsolicited investment opportunities through email, social media, or phone calls.

Fake Enhancement Offers

Fake Enhancement Offers:
Emails or calls promoting "better rates" or "increased limits" that require personal information.

Lottery in your Name:
SMS/email stating you've won a lottery and asking for account details or a security desposit.



Too Good to Be True? Beware of Fake Discount Websites

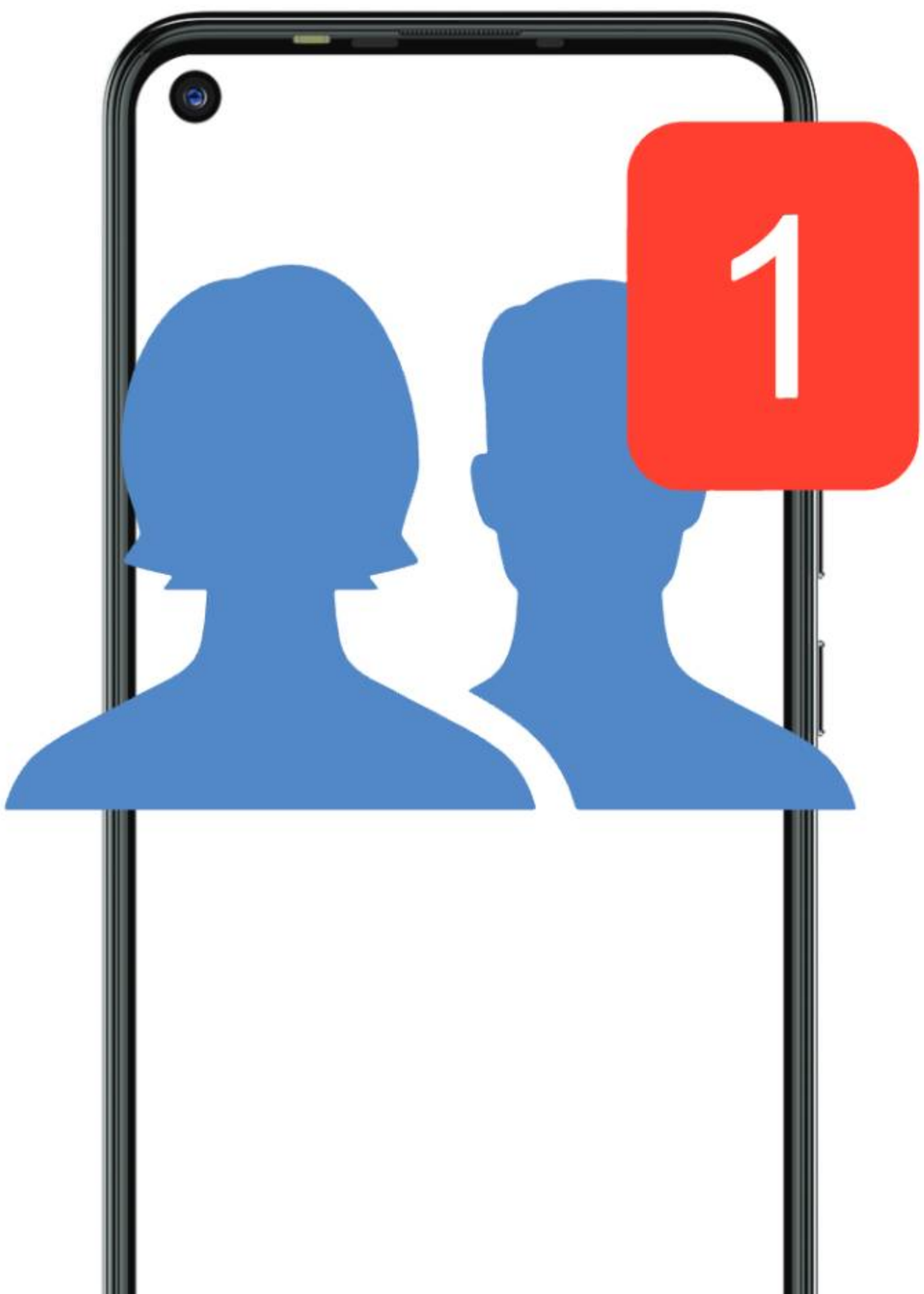
Fake Websites: Designed to look like legitimate retailers but created to steal your information.

Unbelievable Discounts: Prices far below what legitimate retailers offer.

Sense of Urgency: Limited-time offers or countdown timers pressuring you to buy quickly.

Poor Website Quality: Spelling and grammatical errors, unprofessional design, broken links.

Unfamiliar Payment Methods: Requests for payment via gift cards, wire transfers, or unusual payment apps.



Don't Get Fooled! Fake Friends and Money Requests

Emotional appeals: Fake profiles may invent emergencies or hardships to elicit sympathy and a quick financial response.

Urgency: They often pressure you to act fast, claiming they urgently need money and can't wait for traditional means.

Familiar language: They might use personal details extracted from social media to appear convincing.

Mistaken Money Transfer: Scammers claim incorrect credit transactions and ask for refunds.

Impersonation in form of Government Officers:

TRAI Phone Scam: Scammers threaten to suspend your mobile services, citing illegal activity or KYC non-compliance.

Family Member Arrested: Scammers claim a relative has been arrested and demand payment.

Generous Tax Refund: Fraudsters pose as tax officials asking for bank details.

Life Certificate Scam: Fraudsters may call you for Jeevan Praman Patra upda-tion pending to be from pension offices.

Tips to stay safe

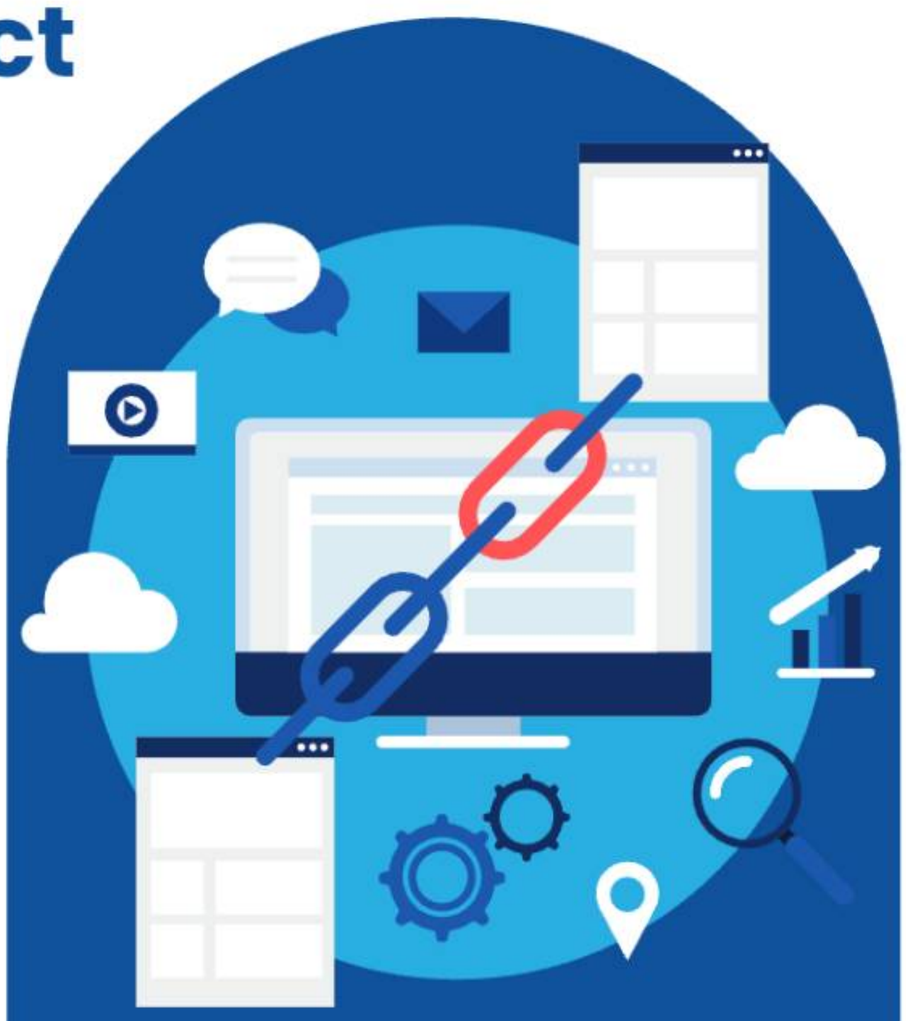
Your Password: The Key to Online Security

- Your password is your first line of defense against hackers.
- A strong password is difficult to guess or crack.
- Unique passwords for each important account are essential.
- Never Write or Save your passwords in unsecured systems.

Level Up Your Security: Two-Factor Authentication (2FA)

- Requires two ways to prove your identity when logging in.
- Even if a thief steals your password, they can't log in without your second factor.
- Its safe to always logout from the Browser once the financial transactions are complete.

Think Before You Click: Protect Yourself From Unsafe Links



- Hover to preview: Put your mouse over the link (don't click!) to see the real destination.
- Search for it: Type the website name in your browser instead of clicking the link.
- Never Share your personal credentials like PIN,OTP with anyone.
- Never perfrom Financial trasanctions on Untrusted WiFi networks.

Safe use of Mobile Device Prevent Financial Frauds

Keep Your Device and Apps Updated

Regularly update your phone's operating system (Android / iOS)
Updates often include security patches that fix known vulnerabilities. Enable auto-lock and Find My Device (Android) or Find My iPhone (iOS). Don't share your phone unlock PIN with anyone.

Review app permissions regularly (*Settings → Apps → Permissions*).
Revoke unnecessary access to contacts, SMS, storage, or location.

Avoid downloading unwanted apps
Do not install unnecessary or unverified apps on mobile devices used for banking or financial transactions as they may access sensitive data or install malware.

Avoid Using Public Wi-Fi for Financial Transactions
Public Wi-Fi can be easily intercepted by hackers. Use mobile data or a secure home network for banking.

Avoid sharing of SIM or Mobile Phone
Do not share or handover your mobile SIM or device to unknown person.

Make sure that your mobile connection is active always
Department of telecommunication may disconnect the connection which is not active for a specific period and the number may be re-allotted to a different person.
Such re-allotted which was your old number can also be misused by scamsters in multiple ways to commit various types of online frauds.

Inform Bank about contact number change immediately

Inform your bank in case of any change in your registered mobile number to ensure uninterrupted receipt of OTPs and transaction alerts and to avoid reaching your bank related information to unknown person.

Update all banking, UPI, and payment apps through official app stores only

Before installing, check developer name, reviews, and permissions. Logout after each transaction. Avoid saving passwords or card details in browsers or apps.

Access your bank only via official app or websites

Avoid searching for customer care numbers on Google

Fraudsters often post fake ones on search engines.
Use verified helplines listed on your bank's website.

Do not accept any credit if you are not supposed to

Monitor Accounts Frequently

Check your SMS/email alerts for every transaction
Enable instant notifications for your banking and UPI apps.
Report any unauthorized transaction immediately to the bank.

Register your email ID with the bank to receive notifications.

If You Suspect Fraud, Immediately block your debit/credit card, UPI and other digital channels through Digital Banking apps provided by your Bank or through your bank's helpline number.

Fell prey to a Digital fraud or scam? How to report?

HELPLINE

Call Toll free Number:1800 1700

Visit Bank's website www.indianbank.bank.in ,
Customer Corner > Lodge a Complaint >
Unauthorised Electronic Banking Transaction (UEBT)

Type “complaint” & send SMS to 56677

Request a call back through Bank's Website,
Internet Banking or Mobile Banking by visiting
Customer Grievances page

Drop an e-mail to cfrm@indianbank.bank.in

Along with reporting to Bank also report to
Cyber Police by calling Toll Free No. **1930** or
through website www.cybercrime.gov.in

Think before you act

KHABAR NAHI KHABARDAR BANO

Scan here to watch Cyber Security Awareness Videos