

AARAMBH

Top 10 Financial Scams & How to Spot Them

Pause. Verify. Then act.

Recognize common fraud patterns affecting banking, payments, investments, loans and online services.

LEARN Understand the basics	THINK Compare risks and choices	ACT Use official channels
--------------------------------	------------------------------------	------------------------------

Educational resource • Simple language • No product endorsement

Important: This booklet is for education only. Financial products, rates, eligibility, rules and scheme terms can change. Verify current information from official sources before acting.

The Guide

1–5: Common Patterns

Fake investment schemes promising unrealistic returns.

KYC/identity scams asking for OTP, Aadhaar, PAN or banking details.

UPI/payment scams using fake collect requests or QR-code tricks.

Lottery/prize scams asking for fees or personal details.

Fake job/work-from-home offers demanding registration or security deposits.

6–10: More Warning Signs

Phishing links and fake websites designed to steal credentials.

Malicious loan apps with hidden charges, harassment or data misuse.

Impersonation of bank, government, police or other trusted officials.

Matrimonial/relationship scams that build trust before requesting money.

Fake property/investment listings asking for advance payments or deposits.

If You Are Targeted

Stop the transaction if possible. Contact your bank/payment provider immediately.

For financial cyber fraud, report quickly through 1930 and the National Cyber Crime Reporting Portal. Keep transaction IDs, dates, screenshots and other evidence.

Do not pay another person who promises to 'recover' your lost money for an upfront fee without verifying them.

Remember

If someone creates urgency, asks for secrets or promises unrealistic returns, pause and verify.

Your Action Checklist

Use this page during a workshop or at home. Tick each item only when you understand it.

Stop and verify.

Never share OTP/PIN/passwords.

Do not click unknown links.

Check official websites independently.

Keep transaction evidence.

Report financial cyber fraud quickly.

Questions to Ask Before You Act

1	What exactly am I buying, joining, borrowing or authorizing?
2	What could go wrong, and what would I lose?
3	What are the fees, penalties, exclusions or conditions?
4	Who regulates or officially administers this product/scheme?
5	Where can I verify the information independently?

My Notes

Quick Questions & Trusted Sources

What is the biggest red flag?

Pressure combined with secrecy, urgency, unrealistic returns, requests for credentials, or demands for upfront payment.

Should I trust a caller claiming to be from my bank?

Do not rely on the caller ID alone. End the call and contact the bank through an official number or app.

What is 1930?

The National Cyber Crime Reporting Portal lists 1930 as the helpline for immediate reporting of online financial fraud.

Trusted starting points

- National Cyber Crime Reporting Portal / I4C.
- SEBI Investor — Safeguarding against Securities Market Frauds.

Aarambh Note

Aarambh creates simple educational resources to help families and communities understand important financial and digital topics. This booklet does not provide personalized financial, legal, tax or insurance advice and does not endorse any product, provider or scheme.

For current rules, rates, eligibility and official application processes, always check the relevant government, regulator, bank, insurer or other official source.