AARAMBH

Online Safety Handbook: Safe Digital Hygiene

Small habits. Stronger digital safety.

A practical handbook for protecting accounts, devices, personal information and digital transactions.

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. Protect Your Accounts

Use long, unique passwords and enable multi-factor authentication where available.

Never share OTPs, passwords, UPI PINs or recovery codes.

2. Protect Your Device

Use a screen lock, install updates and download apps only from trusted sources.

Avoid unknown USB devices, suspicious files and remote-access software requested by strangers.

3. Protect Your Information

Share only the information necessary for the task. Be careful with Aadhaar/PAN images, banking details and personal documents.

Review privacy settings on social media and be cautious about public posts, location information and unknown contacts.

4. Respond to Incidents

If you suspect account compromise, change credentials from a trusted device and contact the relevant service provider.

For online financial fraud, report quickly through 1930 and cybercrime.gov.in.

Remember

Good digital hygiene is a daily habit, not a one-time setting.

Your Action Checklist

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

- Update important devices.
- Review account security settings.
- Remove unused apps.
- Back up important files.
- Check bank/payment alerts daily.
- Know how to report cyber fraud.

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

Is public Wi-Fi safe for banking?

Avoid sensitive financial activity on untrusted networks. Prefer a trusted connection and verify the website/app.

Can a genuine-looking website be fake?

Yes. Check the domain carefully and navigate through a known official source rather than a suspicious message link.

Where can cybercrime be reported?

The National Cyber Crime Reporting Portal is the Government of India's reporting platform; 1930 is listed for immediate online financial-fraud reporting.

Trusted starting points

• National Cyber Crime Reporting Portal / I4C Cyber Security Awareness Booklet.

• NPCI UPI safety guidance.

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.