Online Safety Guide

Online Safety Guide

Protecting yourself online is essential for safe digital transactions and communication.

Recognizing Fraud

Common Fraud Tactics:

- Fake calls claiming to be from bank asking for PIN/password
- Messages with links saying "you won a prize" or "urgent action needed"
- Requests to install "security apps" or remote access apps
- Fake job offers asking for money upfront
- Too-good-to-be-true deals or offers

Creating Strong Passwords

- Use at least 8 characters
- Mix uppercase and lowercase letters
- Include numbers (0-9)
- Add special symbols (@, #, $, %, etc.)
- Avoid using birthday, name, or simple patterns (123456, password)
- Use different passwords for different accounts

What NEVER to Share

- **OTP (One Time Password)** - Do not share with anyone, ever
- **UPI PIN** - This is like your ATM PIN, never share
- **Bank Password** - Keep it completely private
- **CVV Number** - 3 digits on back of debit/credit card
- **Full Card Details** - Never send card photos on WhatsApp

Safe Social Media Usage

- Do not post personal information publicly (phone number, address, bank details)
- Set privacy settings to "Friends Only"
- Be careful about accepting friend requests from strangers

• Do not share photos of valuable items or money

• Avoid posting when you are away from home

If Something Goes Wrong

Immediate Actions:

• 1. Call your bank immediately and block your account/card

• 2. Call Cyber Crime Helpline: 1930

• 3. Change all your passwords

• 4. Report to local police station

• 5. File online complaint at cybercrime.gov.in

Remember: Banks and government agencies will NEVER ask for your password, PIN, or OTP over phone, email, or SMS. If in doubt, hang up and call the official customer care number yourself.