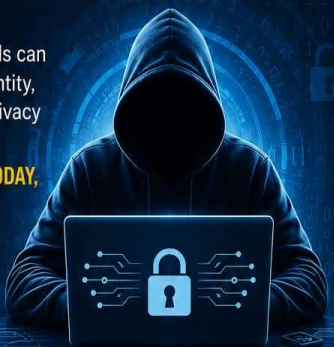


# CYBER CRIME AWARENESS

BE AWARE. BE SAFE. BE SECURE.

Cyber criminals can steal your identity, money and privacy in a \*click\*.

STAY ALERT TODAY, SECURE YOUR TOMORROW.



## TYPES OF CYBER CRIMES



**PHISHING**  
Tricking you to share personal or financial information.



**ONLINE FRAUD**  
Fake offers, scams and cheating for money.



**IDENTITY THEFT**  
Stealing your personal data and using it illegally.



**MALWARE / VIRUSES**  
Malicious software that damages your device or steals data.



**CYBERBULLYING**  
Harassment, threats or humiliation using digital platforms.



**ONLINE SCAMS**  
Fake websites, lottery scams, job scams and more.



THINK BEFORE YOU CLICK!  
YOUR AWARENESS IS YOUR **BEST DEFENSE.**

## STAY SAFE ONLINE – FOLLOW THESE TIPS



**USE STRONG PASSWORDS**

Use a mix of letters, numbers and symbols. Change passwords regularly.



**KEEP SOFTWARE UPDATED**

Regular updates fix vulnerabilities and keep you protected.



**BEWARE OF SUSPICIOUS LINKS**

Don't click on links or attachments from unknown senders.



**USE SECURE NETWORKS**

Avoid public Wi-Fi for banking or sharing sensitive information.



**PROTECT YOUR PERSONAL INFO**

Don't share OTPs, PINs or personal details with anyone.



**ENABLE TWO-STEP VERIFICATION**

Add an extra layer of security to your accounts.

A SECURE YOU  
BUILDS A  
SECURE  
NATION

BE RESPONSIBLE. BE RESPECTFUL. BE SAFE.



Spread Awareness



Report Cyber Crimes



Make The Internet  
A Safer Place

TOGETHER,  
WE CAN FIGHT  
CYBER CRIME.



**REPORT IT. DON'T SUPPORT IT.**  
Report cyber crime at the nearest police station or on the National Cyber Crime Portal

[www.cybercrime.gov.in](http://www.cybercrime.gov.in)



Stay Informed.  
Stay Alert.  
Stay Secure.



## CYBER SECURITY AND CYBER CRIME AWARENESS

**B K Chaudhary**

Director (SPB)

Home (Police) dept.

Bihar Police Headquarter

# What is Cyber Security?

## Simple Definition

Cyber Security means protecting your computers, smartphones, networks, and personal data from unauthorized access or digital attacks by hackers.

🔒 Just like you lock your home door to stay safe, Cyber Security locks your digital life!



# Why Cyber Security Matters



## Protect Financial Data

Keeps your bank accounts, credit cards, and online UPI payments safe from thieves.



## Protect Personal Identity

Prevents bad actors from stealing your identity, photos, and private messages.



## Keep Devices Working

Protects your phone and computer from getting damaged or locked by dangerous viruses.

# Major Cyber Threats

---

Understanding the most common danger zones on the internet

# Threat 1: Phishing Attacks

## Fake Messages & Emails

Phishing is a trick where hackers send fake emails, SMS, or messages pretending to be your bank or trusted brand to steal your passwords or card numbers.

**⚠ Warning: Never click on random links promising free gifts or urgent bank alerts!**

# How to Identify Phishing Links

- ! **Urgent Threats:** Messages saying "Your account will be blocked in 2 hours!"
- ! **Strange Sender Address:** Sender email looks unusual (e.g. support@banhk-sec.com).
- ! **Unbelievable Offers:** "You won \$10,000 lottery! Click here to claim."
- ! **Requests for Secrets:** Asking for PIN, OTP, or passwords directly.

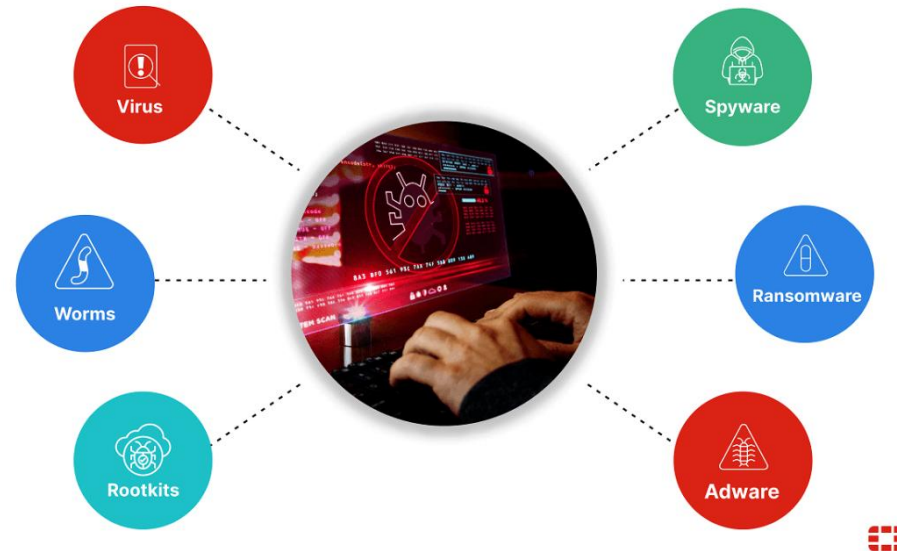
## Threat 2: Malware & Viruses

### Harmful Software

**Malware** (Malicious Software) is any software designed to harm, steal data from, or secretly control your device.

It usually enters your system when you download free movies, apps from unknown websites, or open email attachments.

### What is **Malware**?



# Common Types of Malware



## Virus & Worms

Spreads quickly across files and slows down or crashes your entire computer.



## Ransomware

Locks your personal files and demands money (ransom) to unlock them.



## Spyware

Secretly tracks what you type, reads messages, and steals password information.

## Threat 3: Social Engineering

### Manipulating Human Trust

Social Engineering is the art of tricking people into giving up confidential information by gaining their emotional trust.

👤 Hackers target human fear, greed, or helpfulness rather than hacking technology!



# Examples of Social Engineering

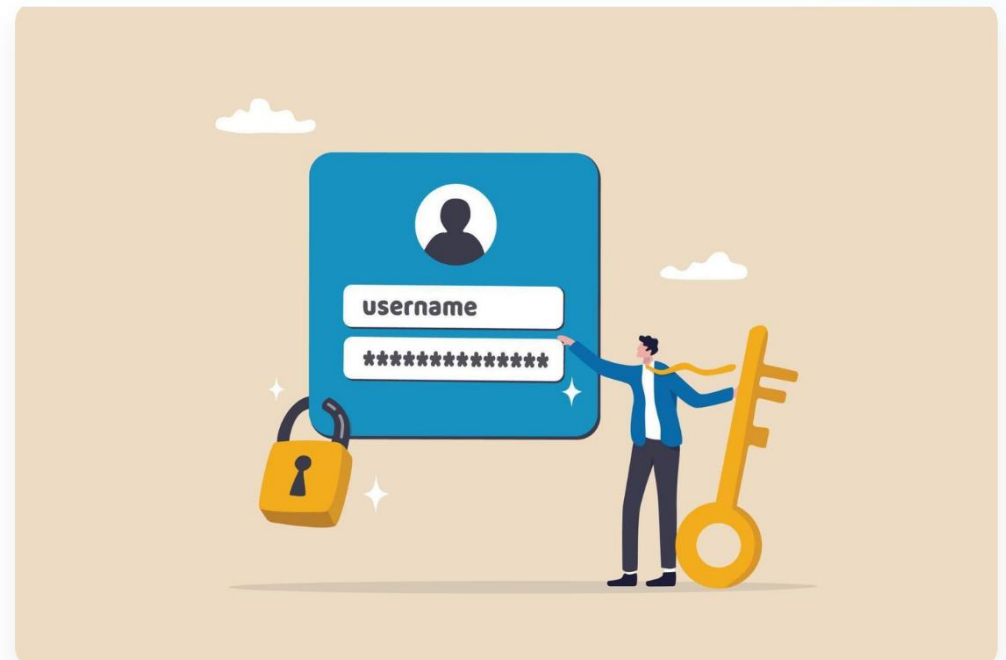
-  **Fake Customer Care:** Scammers posing as support executives asking for remote screen access.
-  **Impersonation:** Pretending to be your manager, police officer, or relative needing emergency cash.
-  **Baiting:** Offering free downloads, prize rewards, or jobs to collect your personal details.

## Threat 4: Password Attacks

### Cracking Your Login Keys

Password attacks happen when attackers try to guess, steal, or crack your passwords to gain access to your private accounts.

🔑 Simple passwords like "123456" or "password" can be cracked in less than 1 second!



# How Hackers Attack Passwords

## Brute Force Attack

Hackers use automated software programs that try millions of password combinations until they hit the right one.

## Credential Stuffing

If you use the same password everywhere, hackers use stolen passwords from one site to unlock all your other accounts.

# Golden Rules of Cyber Security

---

Follow these simple rules to stay 100% safe online

# Core Security Habits

## Essential Rules to Follow

1. Use strong, unique passwords for every site.
2. Enable Two-Factor Authentication (2FA).
3. Keep your software & apps updated daily.
4. Never share OTPs or banking PINs with anyone.

# Daily Cyber Safety Rules



## Use Antivirus

Install reliable security software on your mobile and laptop to block virus threats automatically.



## Avoid Public Wi-Fi

Do not perform banking or online shopping on open, free public Wi-Fi networks without a VPN.



## Backup Your Data

Regularly save important files to Google Drive, iCloud, or an external hard disk drive.

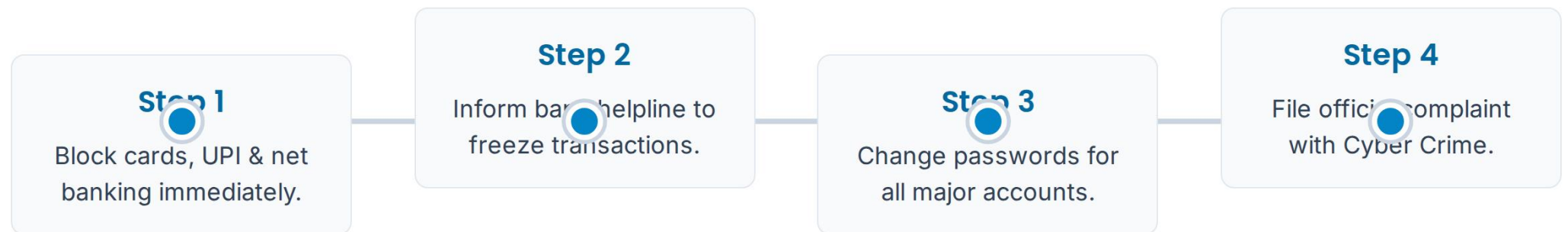
# In Case of Online Fraud

## Act Fast! Every Second Counts

If you lose money or get hacked online, don't panic. Following rapid response steps can save your funds and stop further damage.

 Reporting financial fraud within 1 hour gives the highest chance of freezing lost funds!

# Immediate Action Plan After Fraud



# Where to File Fraud Complaints

| Channel               | Contact / Details                                               | Action Required                                      |
|-----------------------|-----------------------------------------------------------------|------------------------------------------------------|
| Cyber Helpline Number | Dial 1930 (National Cyber Crime Helpline)                       | Report financial fraud immediately over call         |
| Official Cyber Portal | Visit <a href="https://cybercrime.gov.in">cybercrime.gov.in</a> | File online complaint with screenshots & proof       |
| Local Police Station  | Visit nearest Cyber Crime Cell                                  | Submit written application along with bank statement |

# Quick Safety Checklist

- ✓ Never share OTP, PIN, or Passwords with anyone.
- ✓ Verify sender identity before clicking any link.
- ✓ Keep 2-Factor Authentication ON for WhatsApp, Gmail & Banking.
- ✓ If scammed, dial 1930 immediately!

 DIGITAL SAFETY & AWARENESS

# Cyber Crime Awareness

A Comprehensive Guide to Understanding Cyber Threats, Real Police Case Studies,  
and Essential Protection Rules

---

# MODULE 1

Digital Footprint, Impersonation & Online Harassment

# 1. Internet Never Forgets

## Definition & Concept

Everything you upload, comment, share, or search online creates a permanent record called a **Digital Footprint**.

- **Permanent Storage:** Even if you delete a photo, post, or video, servers, archives, and screenshots keep a copy.
- **Data Aggregation:** Cyber criminals gather old social media posts to guess passwords, answer security questions, or target individuals.
- **Impact on Future:** Past online activity can affect personal privacy, academic admissions, and professional career opportunities.



# 1. Internet Never Forgets

## ⚠️ REAL POLICE CASE STUDY

**Old Photos Used for Blackmail:** A college student in Delhi deleted her private social media account. However, scammers had already scraped her photos months prior and created fake profiles to demand money from her contacts. Police arrested the culprit through IP tracking.

## Key Takeaway

Deleting a post from your profile screen does not mean it is deleted from the web infrastructure.

## 🛡️ PREVENTION & SAFETY TIPS

- Think carefully before posting personal images or sensitive opinions online.
- Keep all social media profiles set to strictly **Private**.
- Periodically google your name and review connected third-party apps.
- Avoid uploading official IDs, residence photos, or daily location tags.

## 2. Digital Arrest Fraud

### Definition & Modus Operandi

A high-tech extortion scam where cyber criminals impersonate law enforcement officers (CBI, Customs, Police, ED) over video calls.

- **Fake Illegal Parcels:** Fraudsters claim a parcel containing drugs or fake passports in your name was seized.
- **Confinement over Video:** Victims are forced to remain on Skype/WhatsApp video call continuously in "Digital Arrest".
- **Money Extortion:** Threatening arrest warrants unless money is transferred into fake "verification bank accounts".



## 2. Digital Arrest Fraud

### REAL POLICE CASE STUDY

**Senior Citizen Scammed of ₹50 Lakhs:** A retired professor in Bengaluru received a video call from fraudsters wearing fake police uniforms. They held him on video call for 48 hours in "digital arrest" until police cyber cell intercepted the bank transfer and froze the accounts.

### PREVENTION & SAFETY TIPS

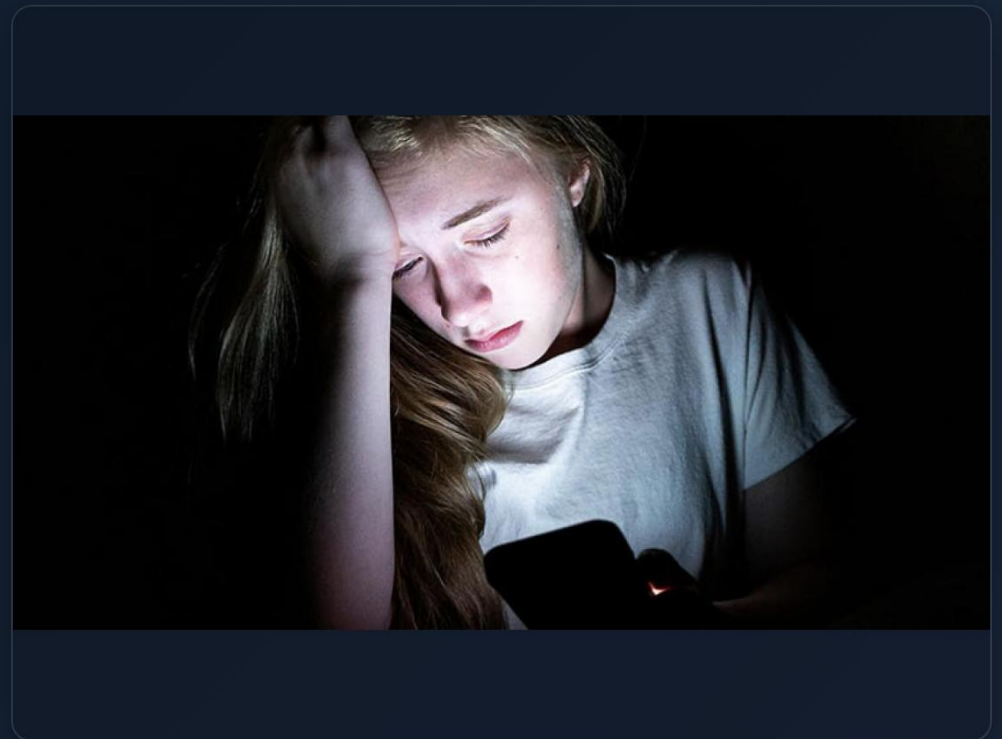
- **NO** Law Enforcement Agency in India conducts "Digital Arrest" over video calls.
- Police will never demand money transfer for verification or clearance.
- Immediately disconnect suspicious police impersonation video calls.
- Report instantly on **1930** or local cyber police station.

# 3. Cyber Bullying

## Definition & Forms

Cyber bullying is the intentional and repeated use of digital platforms to harass, humiliate, intimidate, or demean an individual.

- **Harmful Content:** Sending hateful messages, posting false rumors, or sharing embarrassing altered images online.
- **Exclusion & Trolling:** Deliberately excluding someone from online groups or organizing massive negative comment attacks.
- **Severe Mental Impact:** Causes extreme anxiety, depression, isolation, and loss of self-confidence.



## 3. Cyber Bullying

### REAL POLICE CASE STUDY

**School WhatsApp Group Harassment:** A 15-year-old student was targeted by classmates who created morph images and posted offensive comments in public groups. Cyber police identified the group admins and perpetrators, offering counseling and legal warnings under IT Act.

### PREVENTION & SAFETY TIPS

- Do not respond or retaliate to bullies; it encourages further harassment.
- Take clear **screenshots** of messages, comments, and profile URLs as evidence.
- Use "Block" and "Report" tools on social media platforms immediately.
- Inform parents, teachers, or report to cyber police if harassment continues.

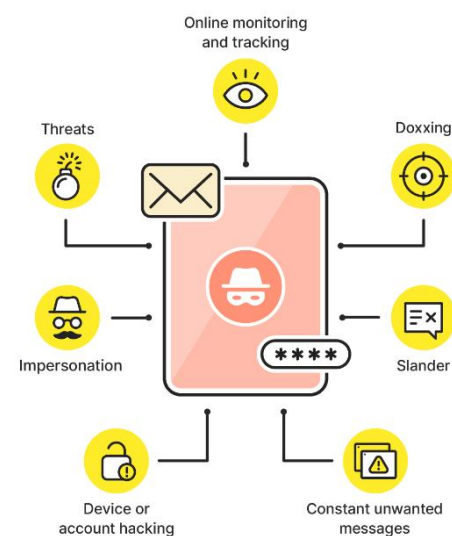
## 4. Cyber Stalking

### Definition & Threat Signs

Cyber stalking involves persistent, unwanted surveillance, tracking, and monitoring of a person's online activity and real-time location.

- **Obsessive Tracking:** Constantly checking posts, comments, location check-ins, and online status.
- **Unwanted Contact:** Sending dozens of messages daily across multiple created accounts despite being blocked.
- **Spyware/Stalkerware:** Installing hidden tracking software or GPS tools on victim's device without consent.

### Examples of cyberstalking



## 4. Cyber Stalking

### REAL POLICE CASE STUDY

**Location Tracking via Spyware:** A working woman in Mumbai received creepy messages detailing her daily travel routes. Cyber cell investigation found stalkerware installed on her phone by a former colleague. The suspect was arrested under Section 354D of IPC.

### PREVENTION & SAFETY TIPS

- Disable real-time location tagging on public social media posts.
- Never accept friend requests from unknown or suspicious profiles.
- Scan mobile phones for unauthorized or hidden background tracking apps.
- File a formal complaint under Indian Penal Code (IPC) Section 354D for stalking.

---

# MODULE 2

AI Scams, Social Engineering & Financial Frauds

## 5. Online Friendship Fraud

### Definition & Romance Traps

Scammers build fake emotional or romantic relationships online to gain trust and ultimately extort money or sensitive information.

- **Fake Wealthy Persona:** Fraudsters pose as wealthy NRI doctors, defense officials, or overseas business experts.
- **Customs / Gift Trap:** Fraudster claims to send expensive gifts or foreign currency stuck at airport customs.
- **Sextortion Traps:** Inducing victims into private video calls, recording them secretly, and demanding blackmail money.

 Online Friendship Honeytrap Scam Illustration

## 5. Online Friendship Fraud

### ♥ REAL POLICE CASE STUDY

**Customs Clearance Scam:** A resident in Hyderabad lost ₹18 Lakhs to an online "friend" met on social media who claimed a luxury gift box was held by Delhi Customs officer. Fake customs fee receipts were used until police busted the scam ring.

### 👤 PREVENTION & SAFETY TIPS

- Never transfer money to someone you have only met online.
- Customs authorities never request personal bank deposits for gift releases.
- Avoid engaging in private video calls with unverified online profiles.
- Perform reverse image searches on profile pictures to check fake identities.

## 6. Voice Cloning AI Fraud

### Definition & AI Technology

Criminals use Artificial Intelligence (AI) algorithms to clone the exact voice of your relatives or friends using short audio clips from social media.

- **Emergency Distress Calls:** Fraudsters call pretending to be your child, friend, or relative in urgent trouble (accident, arrest, hospital).
- **Identical Voice Tone:** AI mimics tone, pitch, and emotion so accurately that victims panic immediately.
- **Immediate Cash Demand:** Urgently asking for immediate UPI/bank transfer to pay medical bills or bail.



## 6. Voice Cloning AI Fraud

### REAL POLICE CASE STUDY

**Fake Accident Emergency Call:** A father in Lucknow received a distressed call sounding exactly like his son screaming that he met with an accident. The scammer asked for ₹50,000 immediately. The father verified directly with his son and avoided loss, reporting to cyber cell.

### PREVENTION & SAFETY TIPS

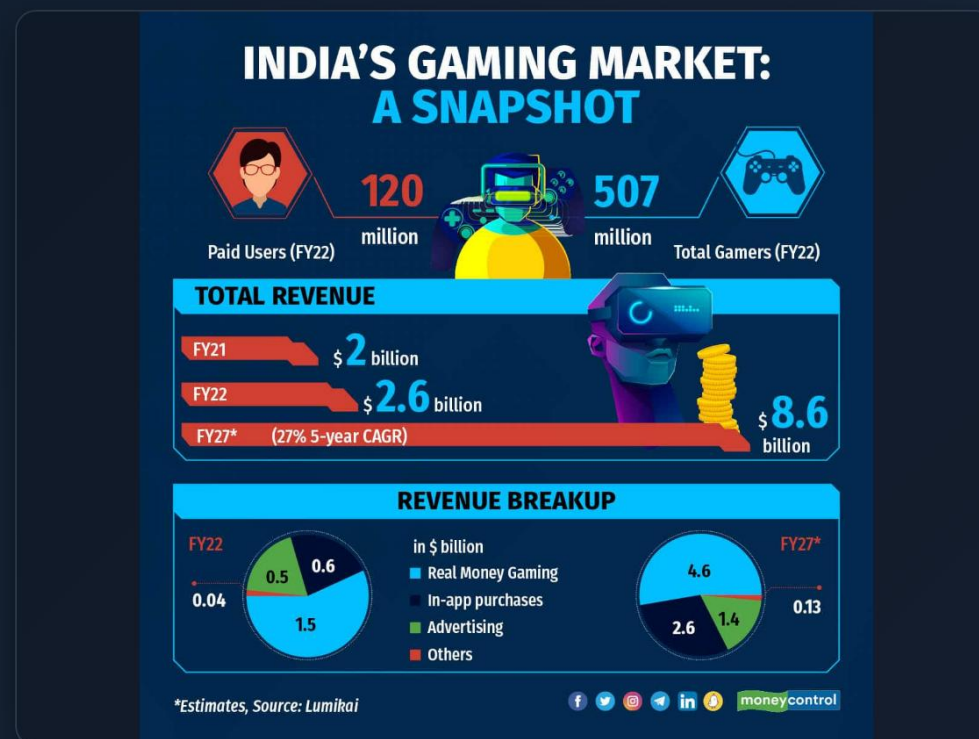
- Always hang up and call back your relative directly on their regular phone number.
- Establish a private **Family Secret Code Word** to verify true identity during emergencies.
- Ask specific personal questions that only your real family member would know.
- Do not post public audio or video clips on open social media profiles.

## 7. Online Gaming Fraud

### Definition & Mechanics

Targeting youngsters and online gamers through fake game currency, skin hacks, fake tournaments, and unauthorized in-app purchases.

- **Free Diamonds / Coins Scam:** Links promising free game passes, skins, or weapons that ask for parent's credit card or UPI PIN.
- **Account Theft:** Phishing login screens stealing high-value gaming accounts to resell online.
- **Malware Links:** Downloading game cheat codes or MOD APKs containing trojans that steal banking data.



## 7. Online Gaming Fraud

### REAL POLICE CASE STUDY

**Un-authorized In-Game Spending:** A minor boy in Punjab used his mother's linked bank account to buy gaming diamonds via a fraudulent third-party website, losing ₹2.5 Lakhs. Police arrested the fraud operators hosting fake game top-up sites.

### PREVENTION & SAFETY TIPS

- Disable auto-saved payment cards and single-click purchases on mobile devices.
- Never download modified game APKs or hack tools from unknown websites.
- Enable purchase password confirmation and parental controls on Google Play / App Store.
- Buy game items only through official in-game stores.

# 8. Online Shopping Fraud

## Definition & E-Commerce Scams

Fake online shopping websites or social media storefronts offering branded products at unrealistically low prices (e.g., 90% discount).

- **Fake Websites:** Cloning famous brand layouts with slightly altered domain names (e.g., flipkart-discounts-sale.com).
- **Advance Payment Only:** Demanding online payment before delivery, then shipping empty boxes or nothing at all.
- **No Customer Care:** Fake contact numbers that redirect to cyber fraudsters who siphon bank accounts.

### FraudWear: Anatomy of a Global Shopping Scam

FraudWear creates sophisticated, fake fashion e-commerce websites impersonating trusted brands to defraud consumers globally, using social media ads and deep discounts to steal money and data.

#### THE GLOBAL SCALE OF FRAUDWEAR

**30,000+**  
Malicious  
E-Commerce Sites

Identified across a vast, resilient, and constantly regenerating scam ecosystem.

**350+**  
Trusted Global Brands  
Impersonated

Includes major names like Nike, Adidas, and Puma, as well as lesser-known brands.

#### A Global Operation Across 104 Countries

Campaigns are highly localized with regional languages, currencies, and social media promotions.



Copyright © CTM360



#### ANATOMY OF THE ATTACK: A 4-STEP PROCESS



**1. RESOURCE DEVELOPMENT: FAKE STORES ARE BUILT**  
Scammers register lookalike domains and host impersonated websites that appear professional and legitimate.

**2. TRIGGER & DISTRIBUTION: VICTIMS ARE LURED**  
Deceptive ads on Meta and social media promote fake deals to drive traffic.



**3. MOTIVE: CREDENTIALS & DATA ARE HARVESTED**  
Fake checkouts collect personal details, account credentials, and financial data for identity theft.

**4. MONETIZATION: FUNDS ARE STOLEN**  
Victims are redirected to either genuine or fraudulent payment gateways, resulting in funds being sent to money-mule accounts and the compromise of payment credentials.



## 8. Online Shopping Fraud

### REAL POLICE CASE STUDY

**Fake iPhone Discount Store:** Over 100 buyers were cheated by a fake Instagram shop offering iPhones at 80% off. Payments were taken via UPI, but no goods were delivered. Cyber Police traced the bank accounts and arrested 3 fraudulent operators.

### PREVENTION & SAFETY TIPS

- Check website domain URL carefully (Look for **https://** and correct spelling).
- Avoid buying high-value items from unverified social media advertisement links.
- Choose **Cash on Delivery (COD)** when buying from new shopping platforms.
- Verify official customer service numbers through official mobile apps only.

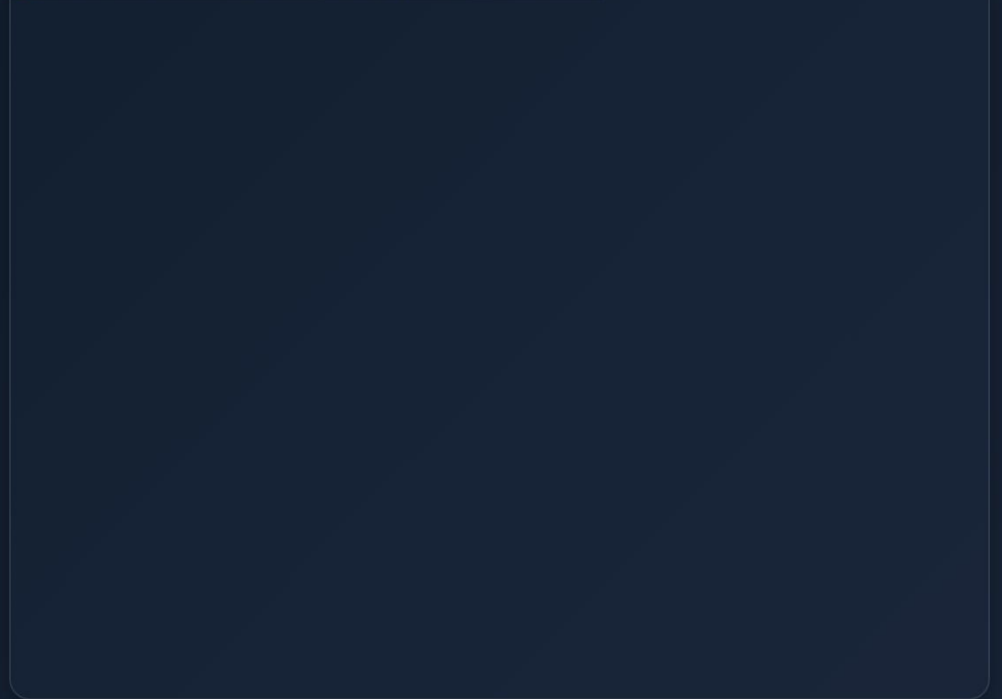
## 9. Fake Social Media Profile

### Definition & Identity Theft

Cyber criminals copy your photos, name, and bio to create a duplicate fake profile on Facebook, Instagram, or LinkedIn.

- **Urgent Money Request:** Scammers message all your friends claiming an urgent medical emergency or wallet loss.
- **Reputation Damage:** Posting vulgar content or scam links under your identity to spoil your personal goodwill.
- **Friend Request Spam:** Sending friend requests to mutual friends to make the profile look authentic.

 Fake Social Media Profile Scam Illustration



## 9. Fake Social Media Profile

### REAL POLICE CASE STUDY

**Government Officer Profile Cloned:** A duplicate profile of a government officer was created on Facebook asking his colleagues for ₹20,000 emergency loan. Police issued a public alert and blocked the cloned account within hours.

### PREVENTION & SAFETY TIPS

- Lock your social media profile guard (e.g., Facebook Profile Lock feature).
- Always double-check with your friend via phone call before sending emergency money.
- Report cloned profiles immediately on the social media platform's abuse portal.
- Inform your contacts publicly if a fake profile is operating in your name.

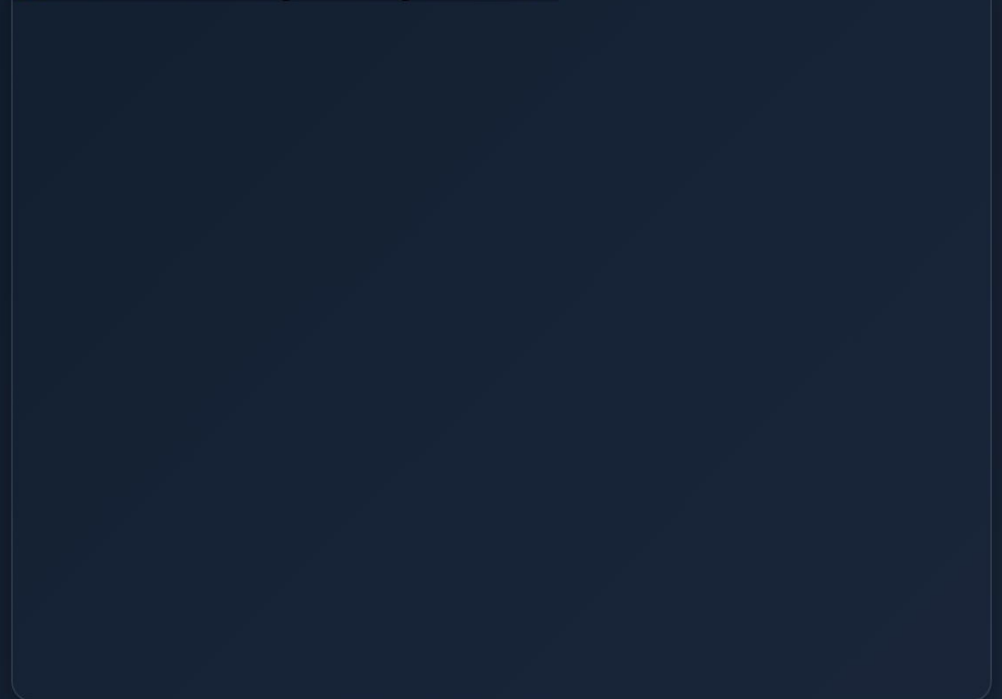
# 10. OTP Fraud & Phishing

## Definition & Financial Theft

Stealing One-Time Passwords (OTPs) or bank credentials through manipulative phone calls (Vishing) or fake SMS links (Smishing).

- **Fake Banking Alerts:** Calls claiming your debit card, SIM card, or electricity connection is expiring today.
- **Screen Sharing Apps:** Convincing victims to install apps like AnyDesk, TeamViewer, or RustDesk to control their phone remotely.
- **UPI Pin Misconception:** Tricking victims into entering UPI PIN on money request links (Remember: UPI PIN is ONLY for sending money!).

 OTP Fraud Banking Phishing Illustration



## 10. OTP Fraud & Phishing

### REAL POLICE CASE STUDY

**Electricity Bill KYC Update Fraud:** A resident received an SMS stating electricity will be disconnected tonight due to unpaid bills. On calling the given number, victim shared OTP and lost ₹1.2 Lakhs. Police traced the jamtara-linked phishing network.

### PREVENTION & SAFETY TIPS

- **NEVER** share your OTP, CVV, or passwords with anyone, including bank employees.
- Entering your **UPI PIN** means **MONEY DEDUCTION**, not money receiving.
- Never install remote desktop screen sharing apps on caller's instructions.
- Banks never ask for sensitive credentials or card numbers over telephone calls.

# Cyber Safety: Golden Rules



## Strong Passwords & 2FA

Use unique 12+ character passwords with numbers and symbols. Always enable Two-Factor Authentication (2FA) on all apps.



## Verify Before Trusting

Double-check emergency phone calls, prize offers, gift claims, and police threats independently before making payments.



## Zero OTP Sharing

Treat your OTP like your ATM PIN. Never disclose it on call or SMS. Remember: UPI PIN is required ONLY to debit money.

# How to Report Cyber Crime

## National Emergency Steps

If you or anyone you know becomes a victim of cyber fraud, take action within the **Golden Hour (First 2 Hours)** to freeze stolen money.

### **CYBER CRIME HELPLINE: 1930**

Dial toll-free number **1930** immediately to report financial fraud to Ministry of Home Affairs Cyber Crime Unit.

### **OFFICIAL NATIONAL PORTAL**

File online complaints at: [www.cybercrime.gov.in](http://www.cybercrime.gov.in)

## Cyber Crime Helpline Report Emergency

 Digital Safety Guide

# Cyber Security & Awareness

Simple Do's and Don'ts to Stay Safe Online

# Why Is Cyber Security Important?



## Major Online Threats

Online fraud is increasing rapidly. Common threats include:

- Fake banking calls and OTP scams
- Phishing links on WhatsApp and SMS
- Theft of personal photos and private data



## How Security Protects You

Basic awareness keeps you safe and worry-free:

- Protects your hard-earned money
- Keeps your identity and photos secure
- Ensures a safe and stress-free digital experience

# Key Safety Rules: Do's



## Strong Passwords

Combine letters, numbers, and symbols (@, #). Always enable Two-Factor Authentication (2FA) for extra protection.



## Regular Updates

Keep your mobile, apps, and computer software updated to fix security flaws and protect against virus attacks.



## Secure Websites

Check for 'https://' and the padlock symbol (🔒) in the address bar before entering personal details.

# Important Warnings: Don'ts

- ✗ **Never Share OTP or PIN:** Banks or officials will never ask for your OTP, CVV, or PIN on phone calls.
- ✗ **Don't Click Unknown Links:** Avoid clicking links offering "Free Rewards", "Lotteries", or "Urgent KYC Updates".
- ✗ **Avoid Public Wi-Fi for Payments:** Never perform banking or enter passwords on free public Wi-Fi networks.
- ✗ **Don't Install Unknown Apps:** Only download apps from official platforms like Google Play Store or App Store.



# Quick Summary: Do's vs Don'ts

| Category         | Do's (Safe Habits)                                         | Don'ts (Avoid Risks)                                   |
|------------------|------------------------------------------------------------|--------------------------------------------------------|
| Passwords        | Use strong, unique passwords (e.g., P@ssw0rd#2026)         | Don't use easy details like your name or birthdate     |
| Calls & Messages | Stay alert to unknown callers and block suspicious numbers | Don't transfer money or share OTP under panic or greed |
| Online Payments  | Use official banking apps and verified QR codes            | Never enter your UPI PIN to receive money              |

# Stay Alert & Stay Safe!

If you encounter any cyber crime or fraud, report it immediately:

**National Cyber Crime Helpline**



Website: [www.cybercrime.gov.in](http://www.cybercrime.gov.in)