



TRAIN THE TRAINERS

CYBER SECURITY, AI & SOFT SKILLS



PARTICIPANTS

COSMO TEACHERS & SHALINIS



DATE

22 - 24 DECEMBER, 2025



TIME

9:00 AM - 05:00 PM



LOCATION

Nath School of Business & Technology, MGM University, Chh. Sambhajinagar, Maharashtra

Your Cyber Guide

NATH SCHOOL OF BUSINESS & TECHNOLOGY

What is Cyber Crime



👉 Cybercrime means crime using computer, mobile or internet.

Examples:

- Someone hacks your Facebook/Instagram account
- Sending threatening messages online
- Using your photo without permission
- Online fraud (money scams, fake calls, QR fraud)

📌 Remember: Cybercrime happens online, but it harms real people

WHY CYBER AWARENESS ?



- Everyone face increasing risks online cyberbullying, stalking, sextortion, identity theft, online scams.
- Teenagers are often targeted because they are active on social media, gaming platforms, and messaging apps.
- Being cyber-smart builds confidence, safety, and digital independence.

We carry our world inside our phone



Passwords & OTP

Rule:

1. Use strong passwords
2. (mix letters, numbers, symbols).
3. Never share OTP.

Weak vs Strong Passwords



🔑 Weak Passwords (Easy to Guess)

- 1234
- password
- teacher123
- abcd
- Birthdate: 15081990

🔒 Strong Passwords (Hard to Guess)

T3ach@2025!

My\$chool#45

Arya!P@ss789

Use mix of:

- ✓ Capital letters (A-Z)
- ✓ Small letters (a-z)
- ✓ Numbers (0-9)
- ✓ Symbols (! @ # \$)



Mobile Safety



Do's:

- Download only from Google Play Store.
- Keep Bluetooth/WiFi off when not in use.

Don't:

- Install unknown “free” apps.

Online Payments Safety

WRONG QR CODE



SAFE QR CODE



- UPI: Never share PIN/OTP.
- Beware of QR code frauds.

What is CYBER THREAT?

- Cyber threats are online dangers ways in which bad people try to harm you, your devices, or steal your personal information.
- They Can Attack You By:
 1. Tricking you into clicking dangerous links
 2. Stealing your passwords or photos
 3. Damaging your phone or laptop
 4. Pretending to be someone you trust

Be the Change

Common Online THREATS



- Cyberbullying
- Cyberstalking
- Grooming
- Online Harassment
- Identity Theft
- Deepfake & Morphing
- Sextortion
- Dating scams

CYBER STALKING

- Cyber stalking is when someone repeatedly uses the internet or digital platforms to harass, monitor, or intimidate a person. It includes sending unwanted messages, tracking online activities, creating fake profiles, or using private information to threaten or blackmail the victim.

Be the Change

ONLINE SAFETY: UNWANTED ATTENTION

1. What It Is



Someone you don't know keeps watching you, asking too many questions, or sending weird messages online.

2. How It Feels



It can feel scary, confusing, or make you feel shy and sad.

3. What To Do!



BLOCK & REPORT.
Tell the app!



BLOCK & REPORT.
Tell the app.



TELL A TRUSTED ADULT!
A parent, teacher, or guardian.



SAVE PROOF!
Take screenshots.
It's not your fault!

Picture Morphing

- Picture morphing is the misuse of someone's photo by editing or altering it often to create fake or inappropriate images. These morphed images are then used to embarrass, blackmail, or defame the person. It's a serious cybercrime, especially targeting girls.

Be the Change



**AISHWARYA IS A HAPPY GIRL.
18 YEARS OLD, LIVING IN
MUMBAI**



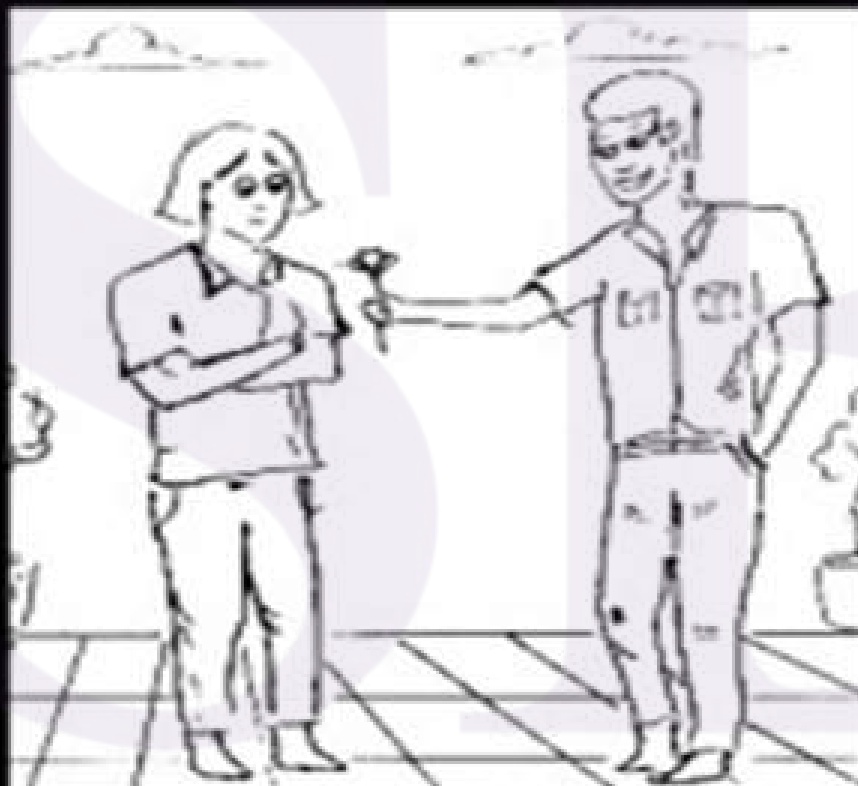
**SHE ALWAYS CLICKED PHOTOS
AND UPLOADED ON INSTA. ALSO,
WAS CRAZY ABOUT TIKTOK**



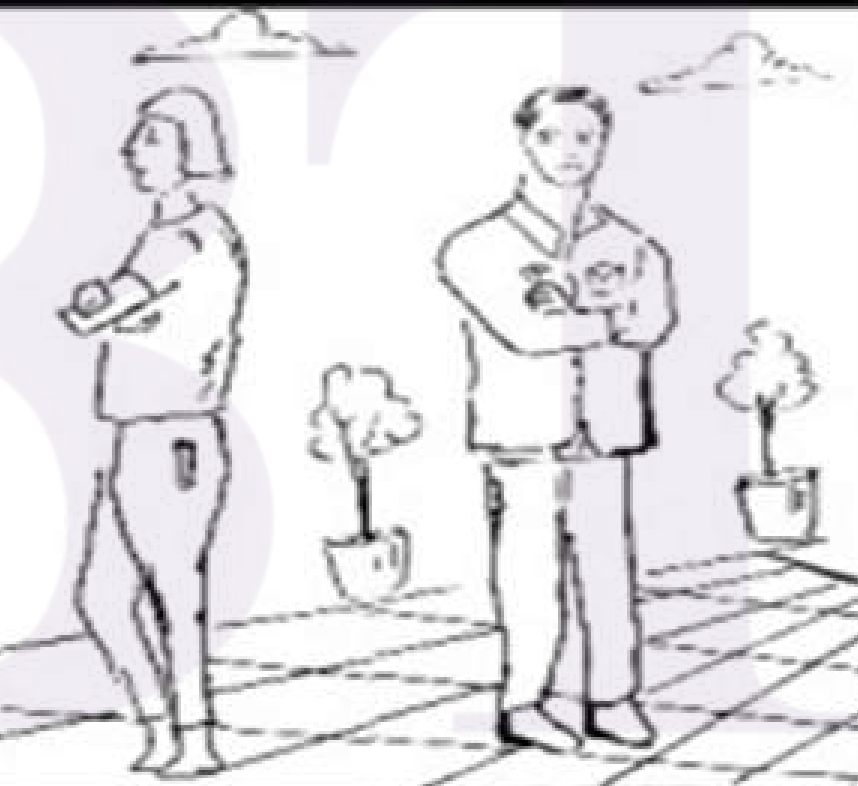
**SHE USED TO GET THOUSAND
LIKES AND HUNDRED
COMMENTS FOR EVERY
PIC POSTED.**



**ONE DAY, SHE GETS A REQUEST
FROM A RANDOM GUY. SHE
ACCEPTS.**



**THE GUY, ARYAN FOLLOWS HER
WHILE SHE IS ON HER WAY TO
COLLEGE AND PROPOSES TO HER**



**AISHWARYA OUTRIGHTLY
REJECTS HIS PROPOSAL
AND SHOUTS AT HIM**



**ARYAN GOES BACK HOME,
DOWNLOADS HER PICTURES,
AND MORPHED HER WITH
NAKED BODY**



**HE SENDS IT TO HIS
FRIENDS AND UPLOADS
ON RANDOM WEBSITES
WITH HER PHONE NUMBER**



**AISHWARYA IS DEPRESSED AND
REGRETS FOR UPLOADING HER CLEAR
PHOTOS ON SOCIAL MEDIA AND
ACCEPTING RANDOM REQUESTS.
YOU BE VIGILANT**

IDENTITY THEFT

- When someone whoever fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any woman commits identity theft.
- Fraudsters create face social media profiles using one's photos to impersonate them, often for fraud, defamation, or to harass their contacts.
- Scammers use personal details for financial fraud - such as Aadhar numbers, pan cards or banking information for scams or unauthorized transactions.

CYBER REVENGE

- Using digital platforms to get back at against someone, often through harassment or sharing private information without consent to cause harm or humiliation.

SAFETY TIPS:

- Avoid sharing personal photos with your close ones, intimate photos with your partners. Deleted files can be recovered.
- Limit who can see your posts, information, photos.
- Report any blackmail incidents.

CYBER GROOMING

- Cyber Grooming is the act of using the internet to build a relationship with someone with the intent of luring and harassing them to perform some acts. These acts are often sexual in nature.

NSBT
Be the Change

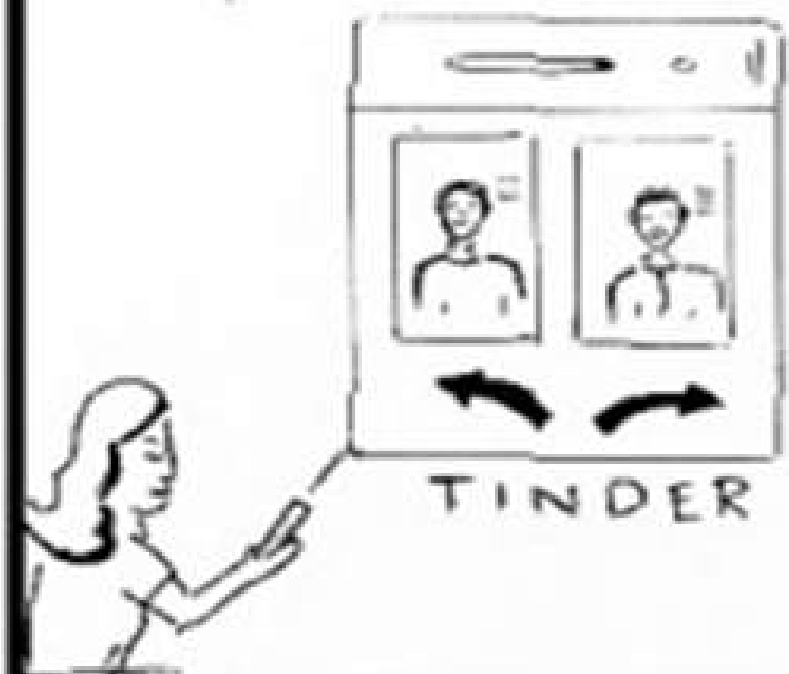
CYBER GROOMING



RASHMI IS A FIRST YEAR MBBS STUDENT. SHE WAS RECENTLY CROWNED AS MISS FRESHER..



SHE USED TO ALWAYS TALK TO HER FRIENDS ONLINE. BUT SHE WAS BORED OF TALKING TO THE SAME PEOPLE.



ONE DAY SHE REGISTERS ON TINDER AND STARTS SWIPING LEFT AND RIGHT.



SHE HAPPENS TO COME ACROSS SHAKS, A VERY GOOD LOOKING GUY, CLASSY, HAS LUXURIOUS CARS, PARTIES, TRAVELS ETC.



SHAKS WAS A SMOOTH TALKER. HE INSTANTLY IMPRESSED RASHMI AND GOT LUCKY TO TAKE HER OUT.



HE TOOK HER FOR A CANDLE LIGHT DINNER. RASHMI FEELS, HE IS THE ONE FOR HER!



AFTER A COUPLE OF DAYS, SHAKS TELLS RASHMI THAT HE URGENTLY NEEDS 2 LAKHS AS IT OFFICERS HAVE FROZEN HIS ACCOUNT. SHE SELLS HER GOLD CHAIN AND GIVES HIM THE MONEY.



SHAKS BLOCKS HER. LATER, THROUGH ONE OF HER FRIENDS SHE GETS TO KNOW THAT SHAKS WAS A MARRIED MAN AND HE USED TO CON WOMEN LIKE THIS.



SHE REGRETS TRUSTING THIS STRANGER THRU' DATING SITE AND FOR SENDING HER PRIVATE PICS & VIDEOS. STAY ALERT

Beware of AI Deepfake Scams!



- Deepfake uses Artificial Intelligence (AI) to create fake videos or voice messages that look or sound like someone you know like your mom, dad, teacher, or best friend.
- It Looks Real -But It's Fake!
- You may hear or see someone you trust but it's a scammer using AI tools
- Even adults fall for it.

How Do Scammers Trap You?

- Clone your parent's voice and call you saying:
- "I'm in trouble, send money fast!"
- Send a fake video of your friend asking for urgent help
- Create fake social media videos of you to blackmail or shame you

How To Stay Safe:

- Don't trust just voice or video. Verify by calling back on their known number.
- Never share OTP, passwords, or money just because you feel pressure.
- Tell a trusted adult immediately if something feels wrong.

Be Careful with your DOCUMENTS

- Never Share Documents with Strangers or Untrusted Sources
- You should PROTECT your Aadhar card, PAN card, Bank Statements, Receipts, ATM Card.

If Shared Carelessly, These Can Be Misused For:

1. Identity Theft: Someone can pretend to be you
2. Financial Fraud: Your bank or wallet can be hacked
3. Blackmail or Harassment: Private info used to threaten you
4. Fake Profiles: Used to defame your name online

Be the Change

How to get Masked Aadhaar?

- How to Get Masked Aadhaar:
- Visit It is a safer version of your Aadhaar card where the first 8 digits are hidden and only the last 4 digits are visible.
- Go to “Download Aadhaar”
- Select “Masked Aadhaar” option before downloading
- PDF will be password protected — use the first 4 letters of your name + year of birth to open it

Be the Change

What is Masked Aadhaar?



- It is a safer version of your Aadhaar card where the first 8 digits are hidden and only the last 4 digits are visible.

Gaming Safety

Protecting Your Personal Info

- Remember that the people you play with online are strangers in real life.

Be careful what you share.

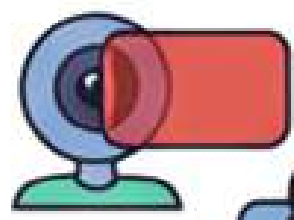
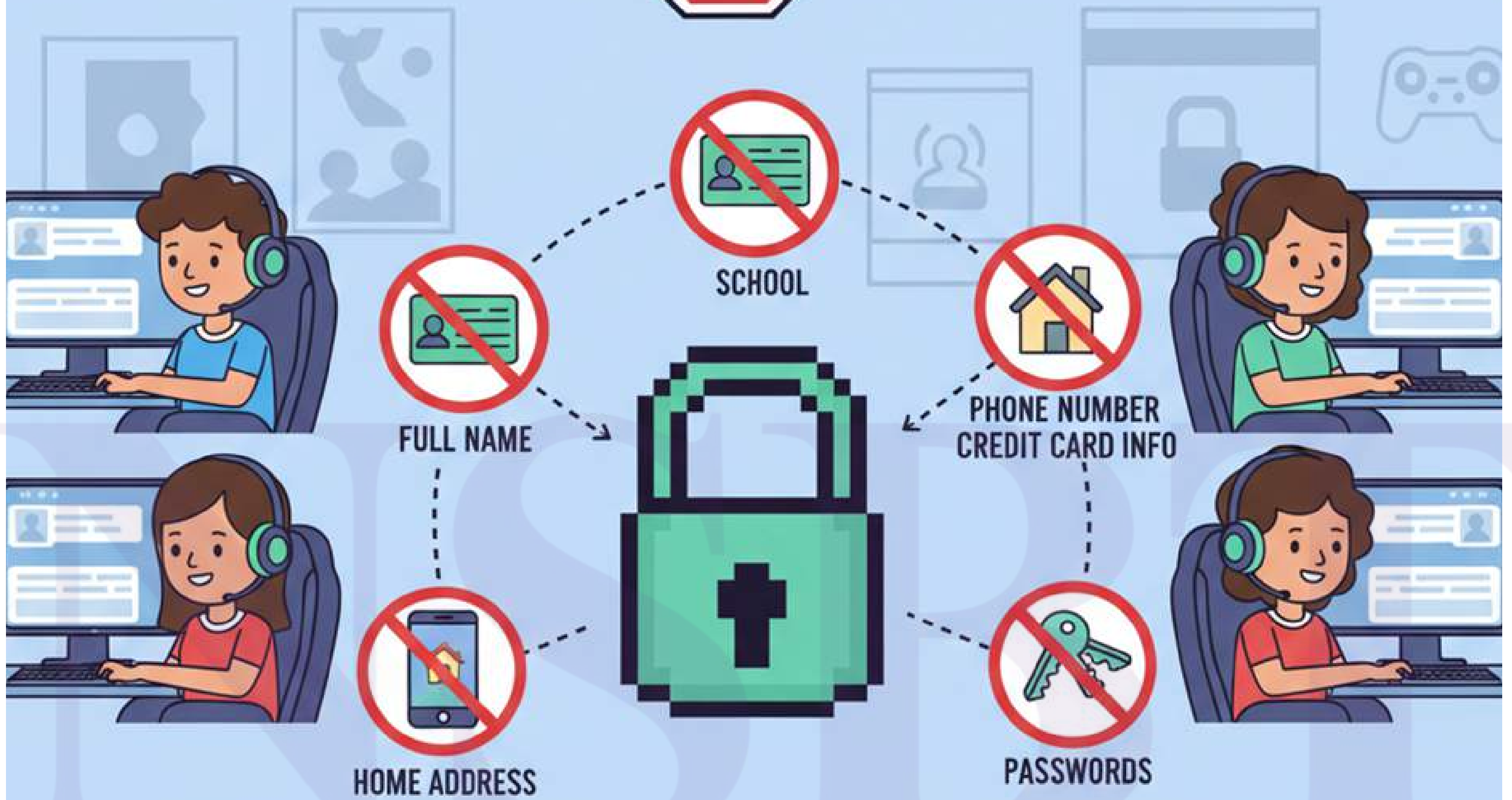
Keep it Private: NEVER share your:

- Full Name
- School Name or Location
- Home Address
- Phone Number
- Passwords or Credit Card Info
- Watch the Webcam: Be careful about using a webcam with people you don't know well.
- Setting Boundaries: If someone asks for personal information or makes you feel uncomfortable, block them and report them to the platform or tell a trusted adult.

PROTECT YOUR



PERSONAL INFO



WATCH THE
WEBCAM



MEK OHY



REPORT &
TRUSTED ADULT



What should a Cyber Crime Victim do?

1. Stay Calm: Don't panic. It's not your fault.
2. Stop Using the Affected Account or Device:
Disconnect from the internet temporarily.
3. Collect Evidence: Take screenshots, note down messages, dates, usernames, and URLs.
4. Change Passwords Immediately: Start with the affected account, use strong new passwords.
5. Tell a Trusted Adult: Talk to your parents, teacher for support.

Be the Change

Where to Report?

CYBERCRIME HELPLINES & RESOURCES



Call Cybercrime Helpline: 1930
(24x7 toll-free support)



2. Report Online: www.cybercrime.gov.in

National Commission for Women (NCW):

- Helpline Number: **7827170170**
- **<https://ncw.nic.in>**
- **Contact: 1930** For Financial Fraud
- **1945** For other Cyber Fraud
- Visit the Nearest Cyber Cell: Every district has a **cyber police station**. Carry your ID and evidence.

The “3-Hour Golden Rule”

What is it?

- If you face a cyber-attack or crime, try to report it within 3 hours.

! Why Is It Important?

- Early reporting increases the chance of tracing the attacker
- Quick action can help recover hacked accounts
- Reduces damage like money loss, data leaks, or blackmail

Digital Discipline



- Teach students safe internet use.
- Don't forward fake news.
- Free recharge link.
- Lottery call.

The Big Picture: Common Dangers

Cyberbullying & Harassment

Unwanted messages, mean comments, and digital exclusion from groups.

Privacy Invasion

Strangers finding your personal info like your school, location, or phone number.

Scams & Phishing

Fake accounts, "free" offers, and links that are designed to steal your password.

How It's Harmful: Insta & Snap

"Vanishing" Content Isn't Gone:

- Snaps and Stories can be screen-recorded and saved by anyone, without you always knowing.

Location Dangers:

- Instagram's "Add Location" and Snapchat's "Snap Map" can tell strangers **exactly** where you are, or where you live.

Fake Profiles & Catfishing:

- People pretending to be someone they're not (like someone your age) to gain your trust or get information.

How It's Harmful: The "Forever" Problem

- Your Digital Footprint: Everything you post, like, and comment on builds a "digital footprint" that colleges and future employers **will** look at.
- Account Hacking: Losing control of your account, where hackers can post as you or send scam messages to your friends and family.
- Blackmail & Sextortion: A serious crime where someone threatens to share a "private" photo or message unless you do what they say.

INSTAGRAM SAFETY SHIELD



Enable

(Two-Factor Authentication)

2FA

Step 1: Secure Your Login

This is your #1 defense.

- Even if a hacker steals your password, they can't log in without a special code from your phone. It's like a deadbolt on your digital door.
- Also, use a strong, unique password for every account. Use a password manager to keep them straight!

Step 2: Master Your Privacy Settings

- **Go Private (Instagram):** Set your account to "Private." This is the easiest and biggest win. Only followers you approve can see your posts.
- **Use "Ghost Mode" (Snapchat):** Go to Settings -> "See My Location" -> turn on "Ghost Mode". Don't share your live location with anyone.
- **Control Your Stories:** Use the "Close Friends" feature on Instagram. On Snapchat, set "Who Can... View My Story" to "My Friends" only.
- **Limit DMs & Tags:** In your settings, set who can message you, tag you, or add you to groups to "Friends Only" or "People You Follow."

WhatsApp Security: Control Your Privacy

1. Two-Step Verification (2FA) - Your Account Lock

- This is the most important security feature for WhatsApp. It prevents a hacker from taking over your account, even if they get your SMS code.
- Action: Go to Settings > Account > Two-Step Verification > Enable.
- Create: Set a unique 6-digit PIN that you will remember (don't use common numbers like your birth year).
- Add an Email: Add a recovery email address. If you ever forget your PIN, WhatsApp can send a reset link to this email.

WhatsApp Security: Control Your Privacy

2. Auto-Download Settings - Stop Malicious Files

Disabling auto-download prevents your phone from automatically saving potentially malicious images, videos, or documents sent by strangers or groups.

- Action: Go to Settings > Storage and Data > Media Auto-Download.
- Set All to "No Media" or "Wi-Fi Only": Under 'When using mobile data' and 'When connected on Wi-Fi', uncheck Photos, Audio, Videos, and Documents.
- Benefit: You must manually tap to download media, giving you time to vet the sender.

WhatsApp Security: Control Your Privacy

3. Status Privacy - Control Your Audience

Ensure only people you trust can see your updates.

- Action: Go to Settings > Privacy > Status.
- Choose: Select "My Contacts Except..." or "Only Share With..." to precisely control who views your status updates. Avoid leaving it set to "My Contacts" if you have contacts you don't fully trust.

Telegram Security: Misuse Prevention

Telegram's powerful features require extra vigilance to ensure they are used safely and responsibly.

1. Enable Two-Step Verification (2FA) - Double Protection

Like WhatsApp, this adds a crucial password layer to your account, protecting it from SIM-swap attacks.

- Action: Go to Settings > Privacy and Security > Two-Step Verification (Cloud Password).
- Set: Create a strong, unique password and a recovery email. This is requested when you log in on a new device.



Telegram Security: Misuse Prevention

2. Manage Active Sessions - Check for Intruders

Telegram allows you to be logged into multiple devices. Regularly check this list to remove old or unrecognized sessions.

- Action: Go to Settings > Privacy and Security > Devices (or Active Sessions).
- Review: Look for any unfamiliar devices and tap 'Terminate' to log them out immediately.

Telegram Security: Misuse Prevention

3. Adjust General Privacy Settings - Limit Exposure

Control who can contact you and see your details.

- **Phone Number:** Set Settings > Privacy and Security > Phone Number to 'My Contacts' or 'Nobody'. This prevents strangers from finding your profile by simply knowing your number.
- **Last Seen & Online:** Set this to 'My Contacts' or 'Nobody' under Settings > Privacy and Security > Last Seen & Online.
- **Groups & Channels:** Set 'Who can add me' to 'My Contacts' under Settings > Privacy and Security > Groups & Channels to stop random invites.

Telegram Security: Misuse Prevention

4. Be Cautious of Public Groups, Links, and Bots

Telegram's open environment means higher risk from unverified content.

- **Never Click Suspicious Links:** Malicious links (phishing) are often spread in public groups or by unknown users. If a link looks unusual or promises something too good to be true, do not click it.
- **Avoid Unverified Bots:** Only interact with bots from official or highly trusted sources. Bots can be used to spread malware or collect your data.
- **Beware of Scams:** Be skeptical of messages asking for money, personal information, or promising investment returns, even if they appear to come from a contact (their account might be compromised).

Awareness of Fake News

- Always verify news before sharing.
- Teach students “Check before you forward.”

Responsible Sharing

- Share only trusted apps and verified websites.
- Don't click on “free recharge/lottery” links.

Content Filtering

- Guide students to watch/use educational apps & safe websites.
- Stop students from accessing inappropriate content.

Basic Safety:

Device Integrity and Maintenance

The first line of defense is ensuring your phone's software is free of vulnerabilities and running as intended by the manufacturer.

- **Enable App and System Updates:** Always enable automatic updates for your device's operating system (iOS/Android) and all your apps. Updates often contain crucial security patches that close loopholes (vulnerabilities) hackers could otherwise exploit.
- **Download Official Apps Only:** Only install apps from the official Google Play Store or the Apple App Store. Third-party sources carry a high risk of distributing malicious or compromised applications.

- Do Not 'Root' or 'Jailbreak': Never gain administrator or root access to your device. This process removes the critical built-in security architecture that protects your data, making your device highly vulnerable to malware and data theft.



Account Protection and Credentials

- Your accounts are only as secure as the weakest password protecting them. Strong credentials are non-negotiable.
- Use Unique and Complex Passwords: Use a password manager to generate and store unique, complex passwords (long, with a mix of letters, numbers, and symbols) for every single account. Never reuse passwords.
- Monitor Account Activity Alerts: Enable and actively monitor alerts (via email, SMS, or in-app notifications) for login attempts, password changes, or unauthorized access, especially on financial and primary email accounts. This allows you to respond instantly to a potential breach.

- **Do Not Log In on Unknown Devices:** As a rule, never log into your personal or sensitive accounts (like email, banking, or social media) on a shared, public, or unfamiliar device. You cannot guarantee that the device is free of keyloggers or malware designed to steal your credentials.

NSBT
Be the Change

Network and Data Privacy

- Control who can see your activity and what data is being shared while you use the internet.
- Avoid Public Wi-Fi: Never connect to public, unsecured Wi-Fi networks (like those in cafes or airports) for sensitive tasks like banking or entering passwords. These networks can be easily intercepted by a technique called a "Man-in-the-Middle" attack. Use a Virtual Private Network (VPN) or your mobile data instead.
- Use Mail Privacy Protection (iPhone/iOS): If you use the native Mail app on iPhone, enable Mail Privacy Protection. This feature helps prevent email senders from tracking when you open their email and shields your IP address, enhancing your privacy against marketing trackers.

5 Golden Rules



1. Don't share OTP/PIN.



2. Use strong passwords



3. Prioritize Real-Life Activities



3. Update your phone



5. Report fraud immediately



What is Digital Footprint?

- Everything you post online leaves a permanent trace.
- Colleges & companies check online profiles.
- “Delete” does not fully erase screenshots & backups exist.
- Think twice before posting: Would I be okay with this going public?

Open Wi-Fi = Open Danger

- Hackers can read your data on open networks
- Anyone on the same network can steal your data.
- Your passwords, photos, UPI details can be stolen
- Fake WiFi hotspots (Evil Twin Attack) look like real networks
- Never log in to banking apps on public WiFi
- Prefer mobile data
- Turn off WiFi when not in use

Incognito Mode Myths

- Incognito does not hide your activity from:
- WiFi owner
- College network
- Government
- Websites
- It only hides history on your phone.

Phishing – How to Identify Fake Messages

- Poor spelling, urgent tone, threats, “click fast!”
- Unknown number or email ID.
- Links that look slightly different: amaz0n.com, paytm-help.xyz
- Ask students to STOP → CHECK → VERIFY before clicking.

QR Code Fraud Awareness

- Scanning QR always makes YOU pay them, not the opposite.
- QR codes can be changed secretly on shops/boards.
- Scammers send QR on WhatsApp saying “scan for refund.”
- Teach: Never scan unknown QR codes.

Fake Job / Money Making Scams

- “Earn ₹5000 per day from home!” posters are scams.
- Fake HR interviews asking for registration fee.
- Instagram & Telegram “task scams” target youth.
- Students must verify job/company before sharing documents.

Identity Theft Examples for Students

- Fake Facebook/Instagram account created with your photo.
- Misusing Aadhaar/PAN details for loans.
- Using your mobile number to target others.
- Pretending to be you to ask money from your contacts.

Ransomware Explain Simply

- Your files (photos, documents) get locked with a password.
- Hacker asks for money to unlock them.
- Happens through infected apps, pen drives, and fake links.
- Teachers should encourage students to backup important files.

Email Spoofing

- Email spoofing is a cyber attack where a fake email is sent that looks like it came from a trusted person or organization.
- Why do hackers use Email Spoofing?
- To steal personal information (passwords, OTPs, bank details)
- To spread malware or viruses
- To cheat people into sending money
- To gain trust and trick the user

How to Identify a Spoofed Email

- Email asks for passwords, OTPs, or bank details
- Message creates panic or urgency
- Poor spelling or grammar
- Email address looks similar but slightly different (example: support@paytm-secure.com)
- Suspicious links or attachments

Fake Link

- Fake links look similar to real websites but have small changes.
- Hackers use them to steal passwords, OTPs, banking info.

◆ Spelling mistakes:

example: instagrarn.com (r + n instead of m)

◆ Extra words added:

paytm-support-login.online

◆ Wrong domain extensions:

.xyz, .online, .fun, .live, .shop, .work

◆ Unusual characters:

amaz0n, faceb00k, snap-verify

◆ Link sent with urgent pressure:

“Click fast! Account will be blocked!”

◆ HTTPS is not enough:

even fake sites can show a lock icon.

Voice Cloning Scam Awareness

- AI can copy your parents' or friends' voice.
- Calls saying: "I'm stuck, send money!"
- Students must verify by calling back on the real number.

Reporting Safety How to Guide Students

- Screenshot everything
- Save chats, profile links, phone numbers
- Block the attacker
- Report to [cybercrime.gov.in](https://www.cybercrime.gov.in)
- Inform parents or teachers immediately

Where to Report?

CYBERCRIME HELPLINES & RESOURCES



Call Cybercrime Helpline: 1930
(24x7 toll-free support)



2. Report Online: www.cybercrime.gov.in

National Commission for Women (NCW):

- Helpline Number: **7827170170**
- **<https://ncw.nic.in>**
- **Contact: 1930** For Financial Fraud
- **1945** For other Cyber Fraud
- Visit the Nearest Cyber Cell: Every district has a **cyber police station**. Carry your ID and evidence.