Children's Guide to Online Safety

CYBER SKOOL (स्कूल)

"Shaping Cyber Scouts in Schools"

An Initiative By:

Edistys

About Edistys Foundation:

Edistys Foundation is a Non-Governmental Organization registered under the Telangana Societies Registration Act based out of Hyderabad, working towards initiating change in society for a better tomorrow.

Our Aims and Objectives:

- *To work towards establishing a gender-equal society*
- *To create awareness on rights and duties given to the citizens*
- *To impart legal education and extend necessary assistance to the victims of crime*
- *Promoting need for mental health awareness and reducing the stigma surrounding it*
- *To facilitate socio, economic, medical and educational support to backward and vulnerable sections of the society.*

Contact us: edistysfoundation@gmail.com

What is Cyber Skool?

Cyber Skool is an initiative to train a team of students from different schools along with teachers where the team is empowered to handle the online threats to children and also to promote the positive use of Internet & Mobile. This project will create ***Cyber Scouts*** *who will be trained on all aspects of cyber safety and will in turn educate everyone in their school and community circles on how to be safe from cybercrimes.*

Objectives of Cyber Skool:

- *To create* ***awareness*** *on online safety among adolescent children and facilitate discussions to identify challenges and opportunities in order to prepare our youngsters in the digital world.*
- *To establish '****Cyber Safety Club****' in the school with a progressive classic team who will act as torch bearers doing awareness sessions about cyber safety among other students & public.*
- *Create a* ***pool of young and well aware Cyber Scouts*** *who will act as a catalyst in spreading awareness on Cyber Safety to their immediate communities.*

WHY?

To make Cyber Space Safer for Women and Children

WHAT?

It is a 6 month-long initiative where students will be enabled as Cyber Scouts and Agents of Change in their respective communities.

WHO?

Cyber Safety and Security Experts (Knowledge Partner) would be conducting the training sessions.

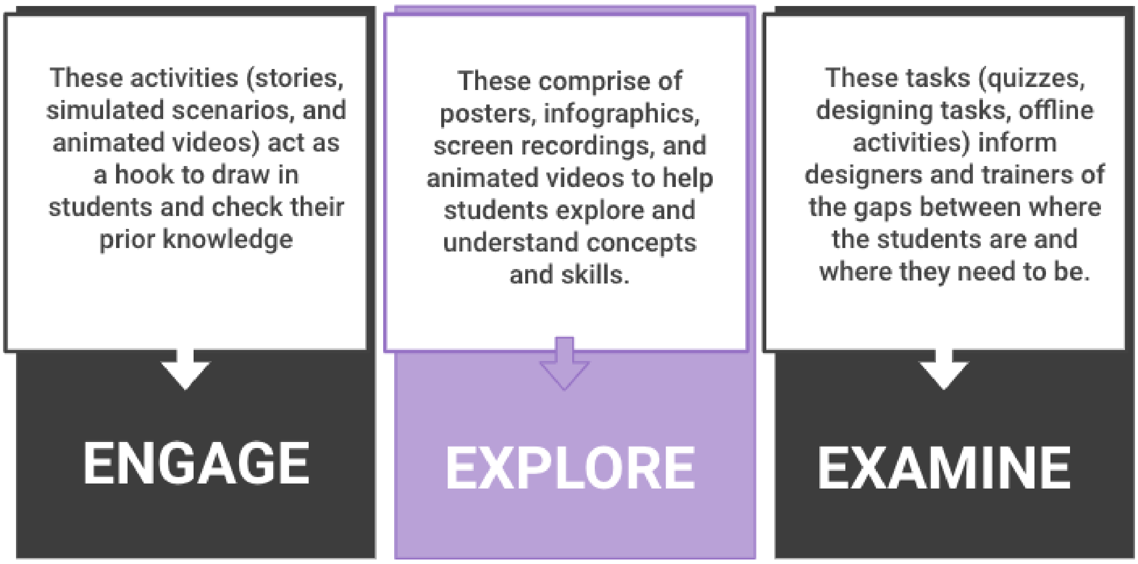
WHEN?

The training sessions are scheduled with a gap of at least 30 days from Class 1 to Class 2. During this period, students will be engaged in Activities.

HOW?

2 students from each section and 1 teacher for every three sections will be selected as cyber volunteers for working closely to enable and engage children

Learning Tasks & Activities:



These activities (stories, simulated scenarios, and animated videos) act as a hook to draw in students and check their prior knowledge

ENGAGE

These comprise of posters, infographics, screen recordings, and animated videos to help students explore and understand concepts and skills.

EXPLORE

These tasks (quizzes, designing tasks, offline activities) inform designers and trainers of the gaps between where the students are and where they need to be.

EXAMINE

Chapter. 1

Basic Rules - Digital Citizenship & Netiquettes

What is Cyberspace?

Cyberspace is a place where **people and information can interact** without worrying about any physical limitations. In cyberspace, we can find websites, social media platforms, online services, games, and various resources. It's a kind of **informational digital library**. You may get any information you want on any subject on the internet.

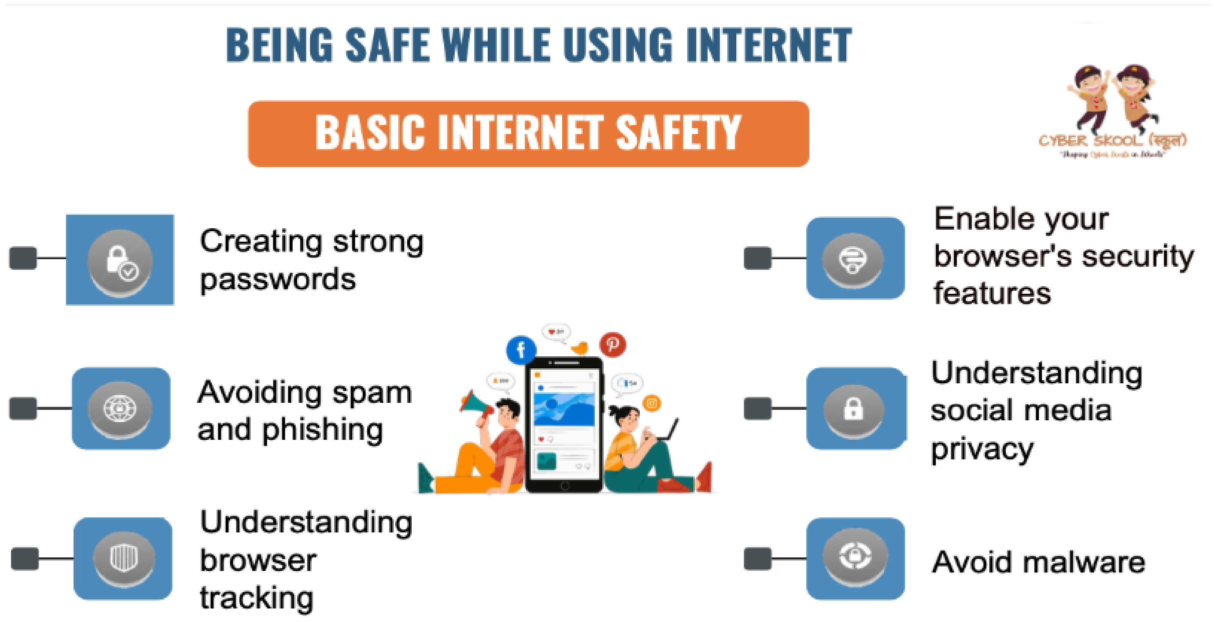
Here we can see some examples:

- Facebook
- Instagram
- Snapchat
- WhatsApp
- Twitter

Digital Citizenship

Digital Citizenship is an important role in ensuring online safety and protecting digital assets. Here's how Digital Citizenship relates to cybersecurity:

- **Reporting Inappropriate Content,** knowing how and when to report harmful or inappropriate content encountered online.
- **Maintaining a healthy balance** between online and offline activities to avoid excessive screen time.
- Developing the **ability to evaluate the credibility and reliability** of online information and sources.
- Recognizing and taking steps to prevent or address any form of online harassment.



BEING SAFE WHILE USING INTERNET

BASIC INTERNET SAFETY

- Creating strong passwords
- Avoiding spam and phishing
- Understanding browser tracking
- Enable your browser's security features
- Understanding social media privacy
- Avoid malware

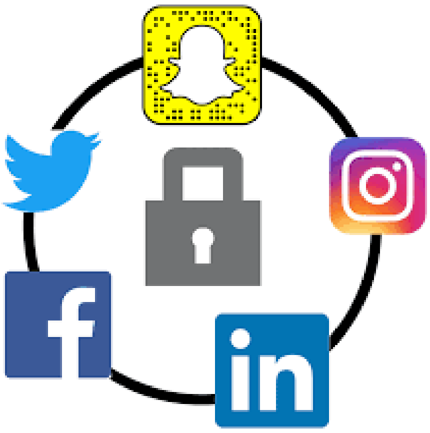
Netiquettes:

Netiquette is essential to maintain a safe and secure online environment.

- **Staying updated** about the latest online threats, which helps to take necessary precautions.
- **Reporting** helps in addressing and reducing cyber threats effectively.
- Updating software and **using strong passwords**.
- It helps to **recognize and report suspicious** messages, which could be attempts at social engineering or cyber scams.

Chapter. 2
Safe Browsing & Privacy Settings

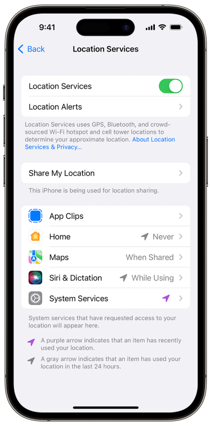
Social Media Security Settings:



- **Privacy Settings:** Setting your social media accounts to private can protect your personal information from people you do not know in real life

- **Password Security:** Having a strong password can prevent other people from hacking into your account. Enable two-factor authentication on all social media.

- **Location Settings:** In order to stay safe, make sure you look in your settings and turn off any feature that shares your location.



9:41

Back Location Services

Location Services ●

Location Alerts >

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location >

This iPhone is being used for location sharing.

App Clips >

Home Never >

Maps When Shared >

Siri & Dictation While Using >

System Services >

System services that have requested access to your location will appear here.

A purple arrow indicates that an item has recently used your location.

A gray arrow indicates that an item has used your location in the last 24 hours.

How to Protect Your Privacy on Social Media?

Use **different passwords** on all your different social media accounts and keep changing your passwords frequently

While adjusting your privacy settings, never forget to **turn off your gadget's location sharing**

Avoid logging into public computers or using friends phones to log in to your social media accounts

Use **caution with public wireless connections** when accessing your social media accounts.

Before you post any photos, **think twice**. Posting photos on social media has been identified as one of the risky social networking activities

When prompted to 'comment below to see magic' or 'check which celebrity you share a birthday with,' avoid clicking these **random baits**. They are third-party apps that try to capture and misuse your private information

You don't have any obligation to accept a "friend or follow" request of anyone on social media, particularly those you do not know

VPN (Virtual Private Network):

VPN establishes an opportunity to establish a **protected network** connection when using public networks. VPNs **encrypt** your internet traffic and **disguise** your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

Clickbait:

Clickbait is a text or a thumbnail link that is designed to **attract attention** and to **entice users** to follow that link and read, view, or listen to the linked piece of online content, being **typically deceptive, sensationalised, or otherwise misleading**.

Auto-Fill:

Auto-Fill automatically fills in information for you in web browsers and apps. It remembers details like your name, email address, and phone number. Saves time by suggesting completed information while typing. **Be cautious with sensitive information** and use it on secure websites.

Cookies:

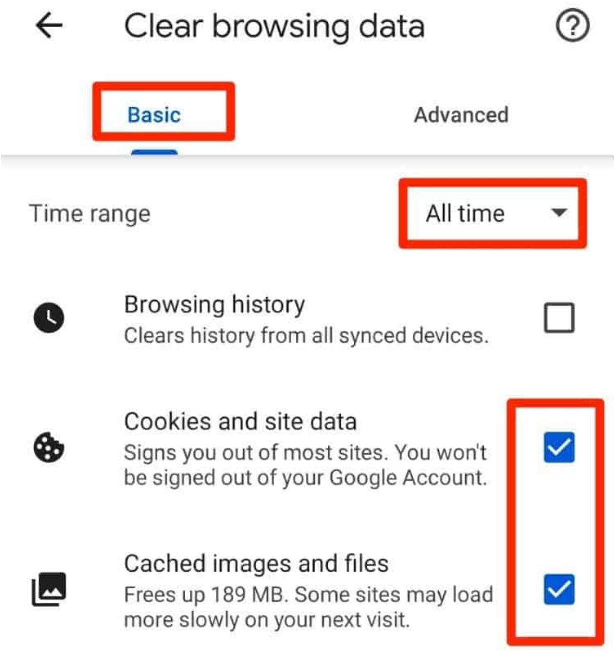
Cookies are small files that websites store on your computer or device. They contain information like preferences, login details, and browsing habits. It helps websites remember you for personalised and efficient experiences. Some cookies may track your behaviour, so you can adjust browser settings for more control.

Cache:

Cache is a temporary storage area in your computer or device. It stores website data like images, videos, and pages to speed up future visits when you visit again. Clearing the cache occasionally frees up space and makes sure you see the latest content.

Browsing History:

Browsing history is a record of websites you've visited in your web browser. It helps you find sites you visited before. Clear your browsing history regularly to ensure privacy of your data.



Clear browsing data

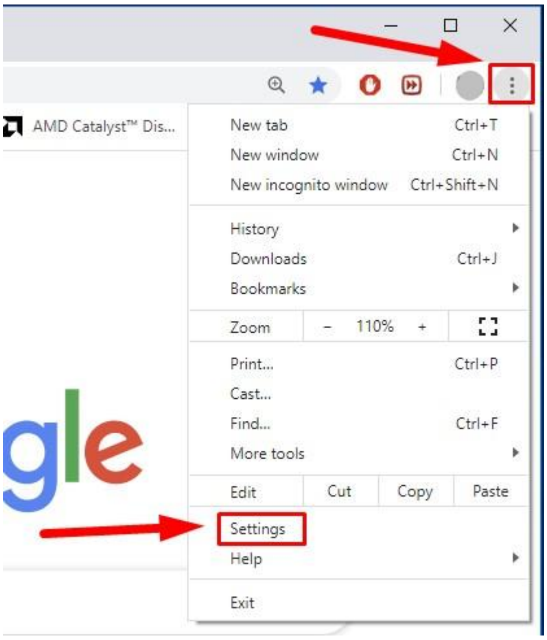
Basic | Advanced

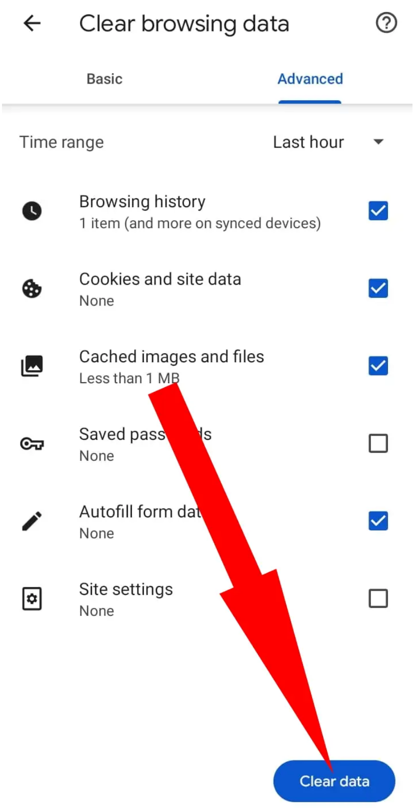
Time range: All time

Browsing history ☐
Clears history from all synced devices.

Cookies and site data ☑
Signs you out of most sites. You won't be signed out of your Google Account.

Cached images and files ☑
Frees up 189 MB. Some sites may load more slowly on your next visit.





Clear browsing data

Basic | Advanced

Time range: Last hour

Browsing history ☑
1 item (and more on synced devices)

Cookies and site data ☑
None

Cached images and files ☑
Less than 1 MB

Saved pass…ds ☐
None

Autofill form dat… ☑
None

Site settings ☐
None

Clear data

Rules to Set Strong Passwords:

Length: Make your passwords at least 16 characters long. Longer passwords are generally more secure.

Complexity: Use a mix of uppercase and lowercase letters, numbers, and special characters (e.g., @, !, #) in your passwords.

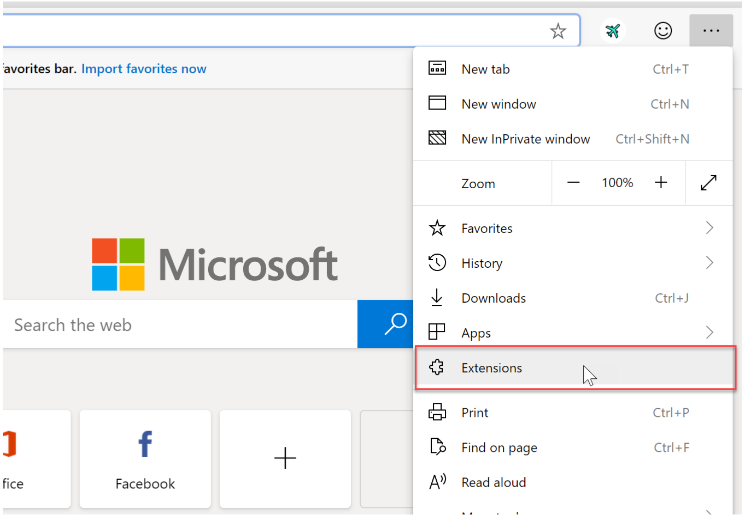
Avoid Common Words and Patterns: Avoid using easily guessable words like "password," "123456," or sequential patterns like "abcd" or "qwerty."

Avoid Personal Information: Don't use personal details like your name, birthdate, or any publicly available information as passwords.

Unique Passwords: Use a different password for each online account. Reusing passwords across multiple accounts increases the risk if one account gets compromised.

Extensions:

Browser extensions offer additional features and functionalities to enhance the browser capabilities. But be very careful while you add them & know what to add.



Anti-Virus:

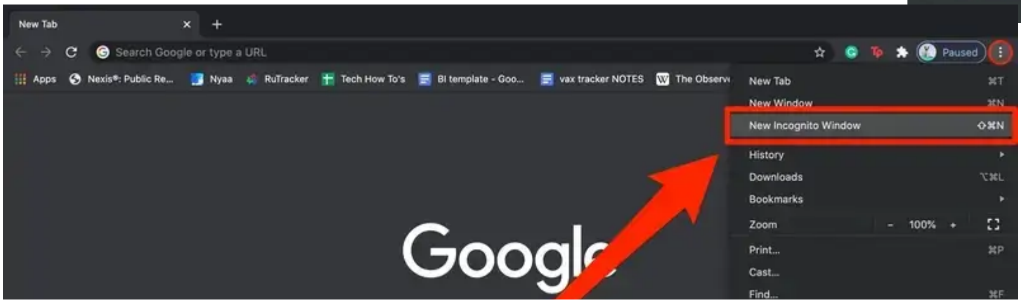
An anti-virus is a special program that protects your computer or device from bad software called "malware." This bad software can cause harm, steal your information, or make your device not work properly. The anti-virus scans everything on your computer to find this bad software and get rid of it, keeping your device safe and secure.

Incognito Mode:

Incognito mode, also known as private **browsing or privacy mode**, is present in all web browsers that allows users to browse the internet privately and discreetly. When you use incognito mode, your browsing activity is not recorded, and the browser doesn't store cookies, temporary files, or your browsing history.

Some special features about private/Incognito are:

- Privacy
- No History Tracking
- Temporary Data
- No Autofill
- Private Searches



Chapter. 3
Cyber Crimes & Preventive Measures

Cyber Bullying:

Cyberbullying is a type of bullying that takes place online, using digital communication such as social media, messaging apps, emails, or online forums.

Examples includes :

- Hateful text messages or emails
- Rumours sent by email or posted on social media networks.
- Embarrassing pictures, videos, websites, or fake profiles posted online.

What to do, if you are bullied?

Tell someone: Make sure you tell a trusted adult, such as a parent or teacher, and they will help you to decide what to do

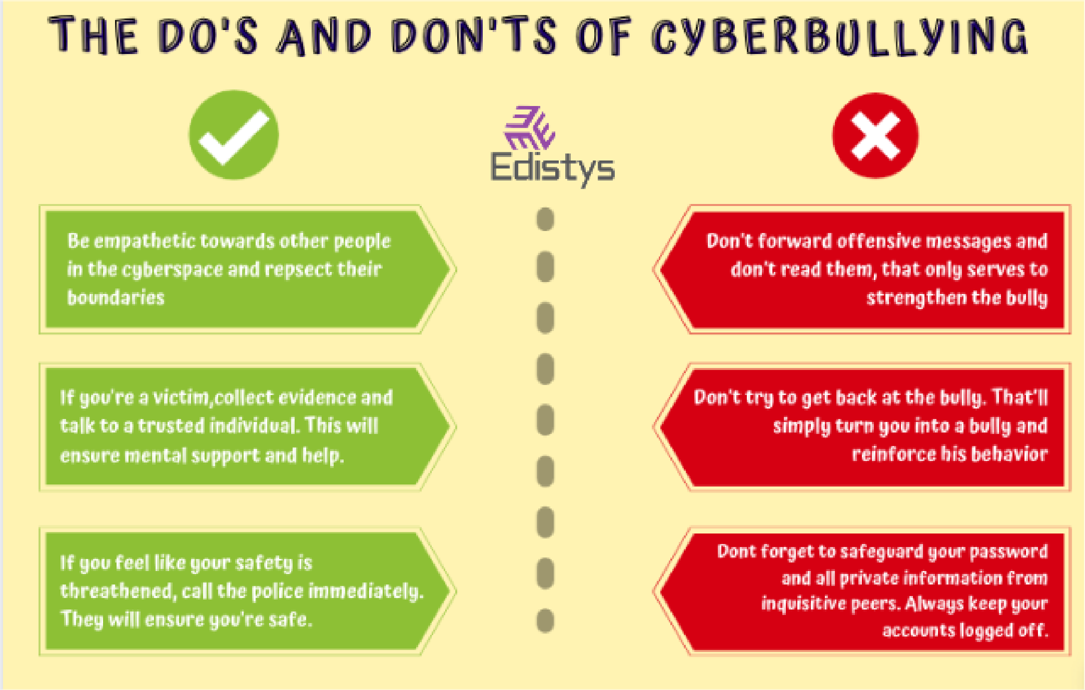
Save the evidence: It is really important to have evidence of the cyber bully to show it to the concerned authorities (Screenshots..)

Block the person/group: Most social media sites will give you the option to block the person/group cyber bullying you.

Don't reply or answer back: Don't become a cyber bully yourself. Deal with the bullying by blocking and reporting the abuser.

Report: Cyber bullying is never acceptable and you should report such content

Stay positive: Although it may feel like you do not have any control of the situation, you can by following the right measures. You are not alone.



THE DO'S AND DON'TS OF CYBERBULLYING

Be empathetic towards other people in the cyberspace and repsect their boundaries

If you're a victim,collect evidence and talk to a trusted individual. This will ensure mental support and help.

If you feel like your safety is threathened, call the police immediately. They will ensure you're safe.

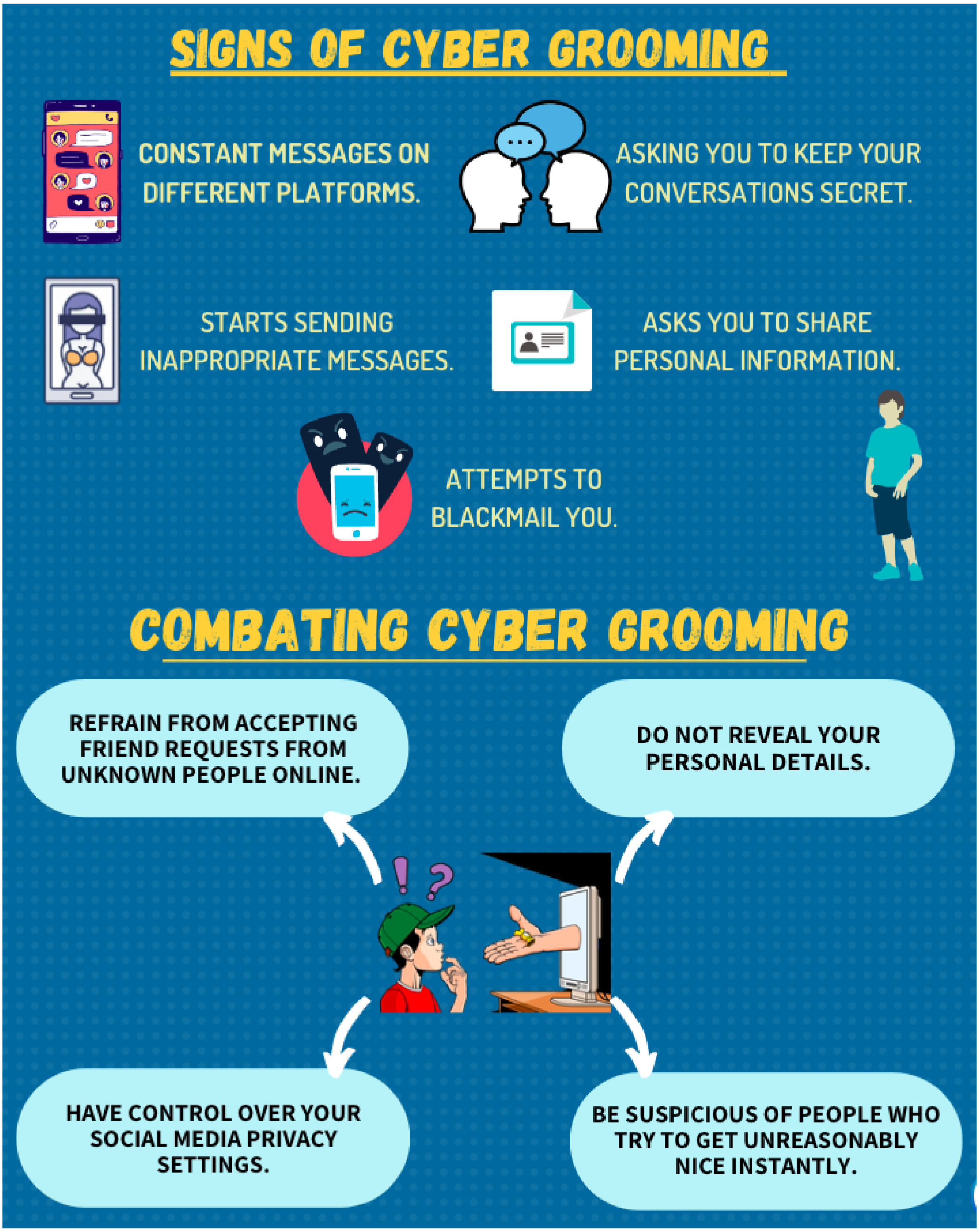
Don't forward offensive messages and don't read them, that only serves to strengthen the bully

Don't try to get back at the bully. That'll simply turn you into a bully and reinforce his behavior

Dont forget to safeguard your password and all private information from inquisitive peers. Always keep your accounts logged off.

Cyber Grooming:

Cyber grooming is the manipulation of a child or a teenager often by an adult on online communicative gaming platforms, apps and social media. This manipulation is done to gain the trust of vulnerable individuals. After gaining the trust of the individual, the predator begins to normalise sexual conversations or introduce vices. Further, the predator may ask the victim to send personal pictures of themselves or even ask them for a personal meeting.



SIGNS OF CYBER GROOMING

CONSTANT MESSAGES ON DIFFERENT PLATFORMS.

ASKING YOU TO KEEP YOUR CONVERSATIONS SECRET.

STARTS SENDING INAPPROPRIATE MESSAGES.

ASKS YOU TO SHARE PERSONAL INFORMATION.

ATTEMPTS TO BLACKMAIL YOU.

COMBATING CYBER GROOMING

REFRAIN FROM ACCEPTING FRIEND REQUESTS FROM UNKNOWN PEOPLE ONLINE.

DO NOT REVEAL YOUR PERSONAL DETAILS.

HAVE CONTROL OVER YOUR SOCIAL MEDIA PRIVACY SETTINGS.

BE SUSPICIOUS OF PEOPLE WHO TRY TO GET UNREASONABLY NICE INSTANTLY.

Phishing:

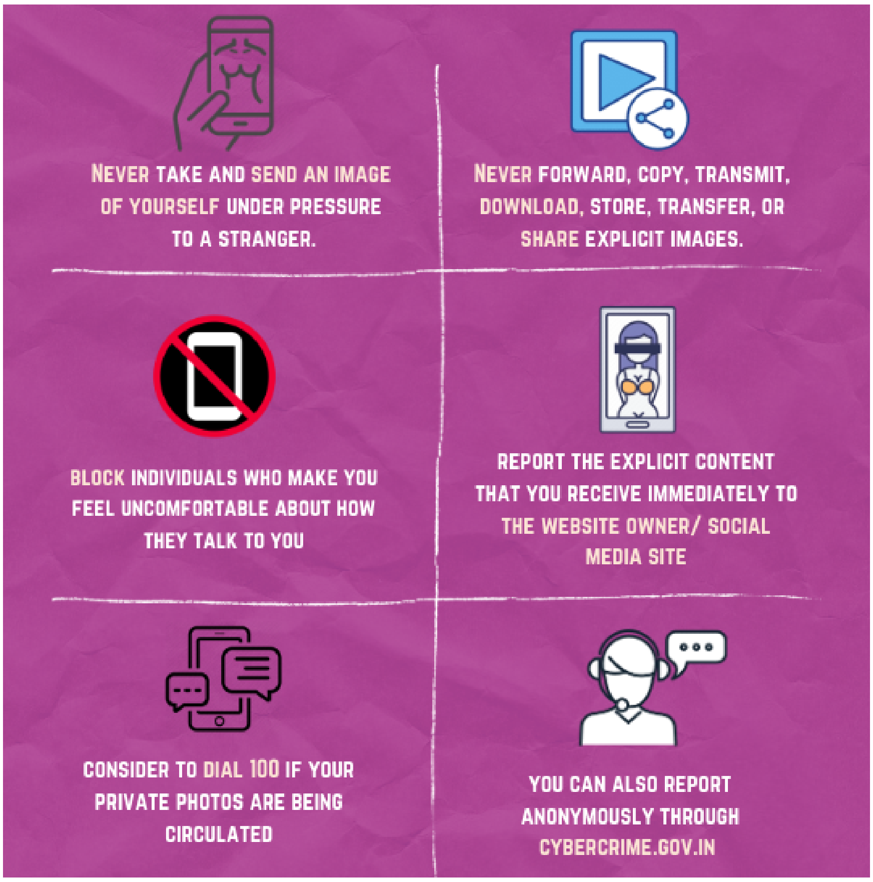
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

How to stay away from Phishing?

- Create unique-complex passwords that include a dozen letters, numbers, and symbols.
- Enable two-factor authentication.
- Check your financial accounts often for unauthorised transactions.
- Set up alerts on your banking and credit card accounts.
- Never give out your personal information.
- Don't click links from unTRUSTED sources.

Sexting:

Sexting is a combination of "sex" and "texting". Sexting refers to sending, receiving, or forwarding sexually explicit messages, photos, or videos through text messages, social media, or messaging apps.



NEVER TAKE AND SEND AN IMAGE OF YOURSELF UNDER PRESSURE TO A STRANGER.

NEVER FORWARD, COPY, TRANSMIT, DOWNLOAD, STORE, TRANSFER, OR SHARE EXPLICIT IMAGES.

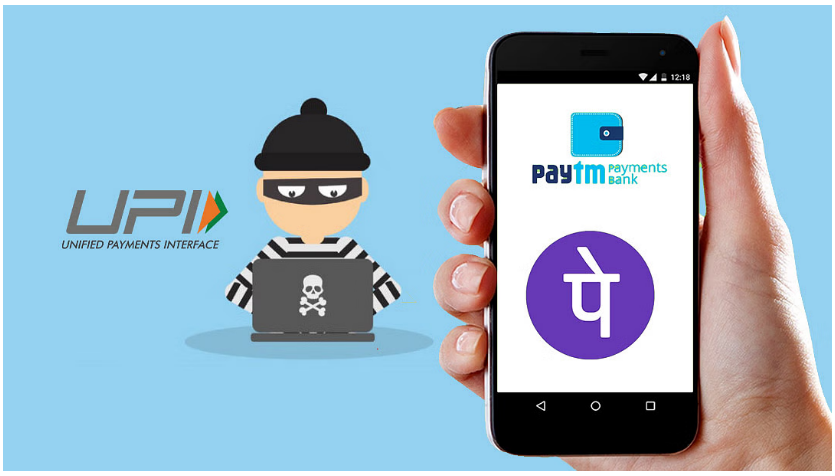
BLOCK INDIVIDUALS WHO MAKE YOU FEEL UNCOMFORTABLE ABOUT HOW THEY TALK TO YOU

REPORT THE EXPLICIT CONTENT THAT YOU RECEIVE IMMEDIATELY TO THE WEBSITE OWNER/ SOCIAL MEDIA SITE

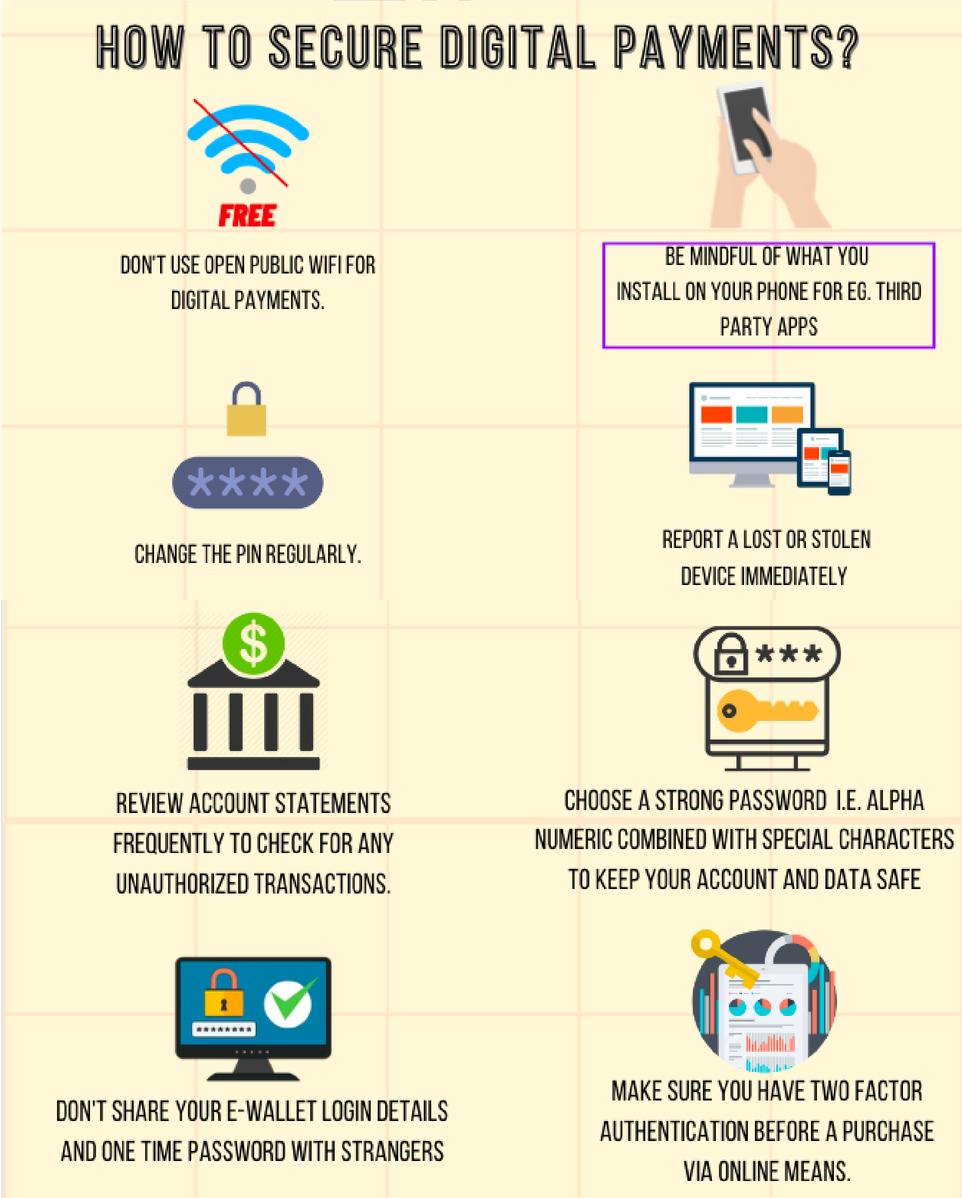
CONSIDER TO DIAL 100 IF YOUR PRIVATE PHOTOS ARE BEING CIRCULATED

YOU CAN ALSO REPORT ANONYMOUSLY THROUGH CYBERCRIME.GOV.IN

UPI Scams:



UPI is instant money transfers between bank accounts through mobile devices using apps or online banking platforms. Scammers take advantage of UPI's convenience to deceive people and steal money or sensitive information.



HOW TO SECURE DIGITAL PAYMENTS?

FREE

DON'T USE OPEN PUBLIC WIFI FOR DIGITAL PAYMENTS.

BE MINDFUL OF WHAT YOU INSTALL ON YOUR PHONE FOR EG. THIRD PARTY APPS

CHANGE THE PIN REGULARLY.

REPORT A LOST OR STOLEN DEVICE IMMEDIATELY

REVIEW ACCOUNT STATEMENTS FREQUENTLY TO CHECK FOR ANY UNAUTHORIZED TRANSACTIONS.

CHOOSE A STRONG PASSWORD I.E. ALPHA NUMERIC COMBINED WITH SPECIAL CHARACTERS TO KEEP YOUR ACCOUNT AND DATA SAFE

DON'T SHARE YOUR E-WALLET LOGIN DETAILS AND ONE TIME PASSWORD WITH STRANGERS

MAKE SURE YOU HAVE TWO FACTOR AUTHENTICATION BEFORE A PURCHASE VIA ONLINE MEANS.

Chapter. 4

Making Online Spaces Safer for Children

Online Gaming:

Online gaming describes any video game that offers online interactions with other players. Gaming is a fun and sociable way to spend time, encouraging teamwork and developing skills.

All good stuff, but there are a few things you need to be aware of:

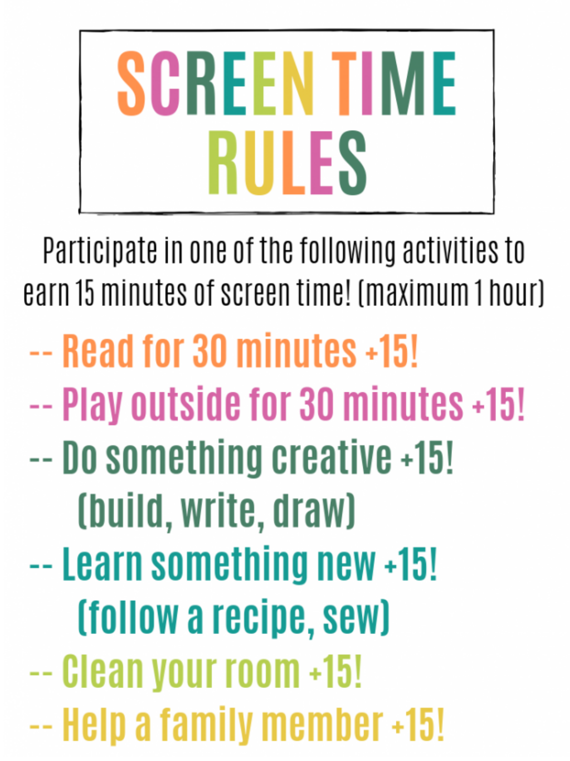
- Children might become mentally or physically ill resulting in issues like anxiety, short attention span, obesity, etc.
- Children do not understand the concept of privacy and might end up sharing personal information and fall victim to hacking and identity theft.
- If the gaming habits are not controlled the players might take over other aspects of a child's life.
- Online gaming exposes children to offensive language and acts.
- Most children's first interaction with someone they don't know online is now more likely to be in a video game.

Do's & Don'ts of Online Gaming:

Do's	Don'ts
Use Official Game Platforms	Don't use third party applications for downloading games
Be Careful with Personal Information	Never reveal your real name, location. gender, age or any other personal information
Never trust on the popups that may ask you to pay for items in the game	Don't add any credit card or debit card information in online gaming platforms.
Report Suspicious Behaviour	Don't trust or make friendships with any person you meet on gaming platform

Screen Time Management:

Creating time limits and boundaries for the use of the internet can be very effective. It improves your mental health and leaves you feeling productive. The Internet is a boon but screen time management is the key.



SCREEN TIME RULES

Participate in one of the following activities to earn 15 minutes of screen time! (maximum 1 hour)

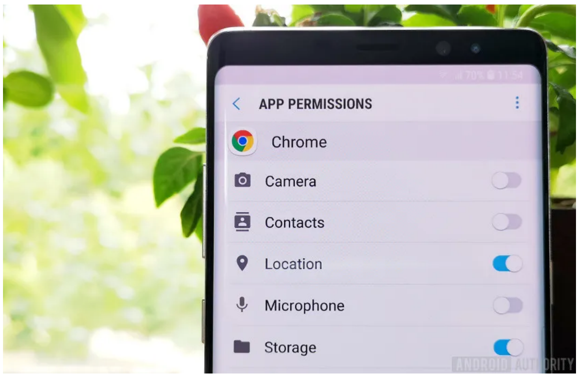
-- Read for 30 minutes +15!
-- Play outside for 30 minutes +15!
-- Do something creative +15! (build, write, draw)
-- Learn something new +15! (follow a recipe, sew)
-- Clean your room +15!
-- Help a family member +15!

Mobile App Permissions:

When you download and install an app, it may ask for specific permissions to function properly. These permissions grant the app access to various parts of your device.

Don'ts:

- Don't give permission to any third-party applications that are not downloaded from the Play Store.
- Do not download any apk's or applications from third party sites.



APP PERMISSIONS

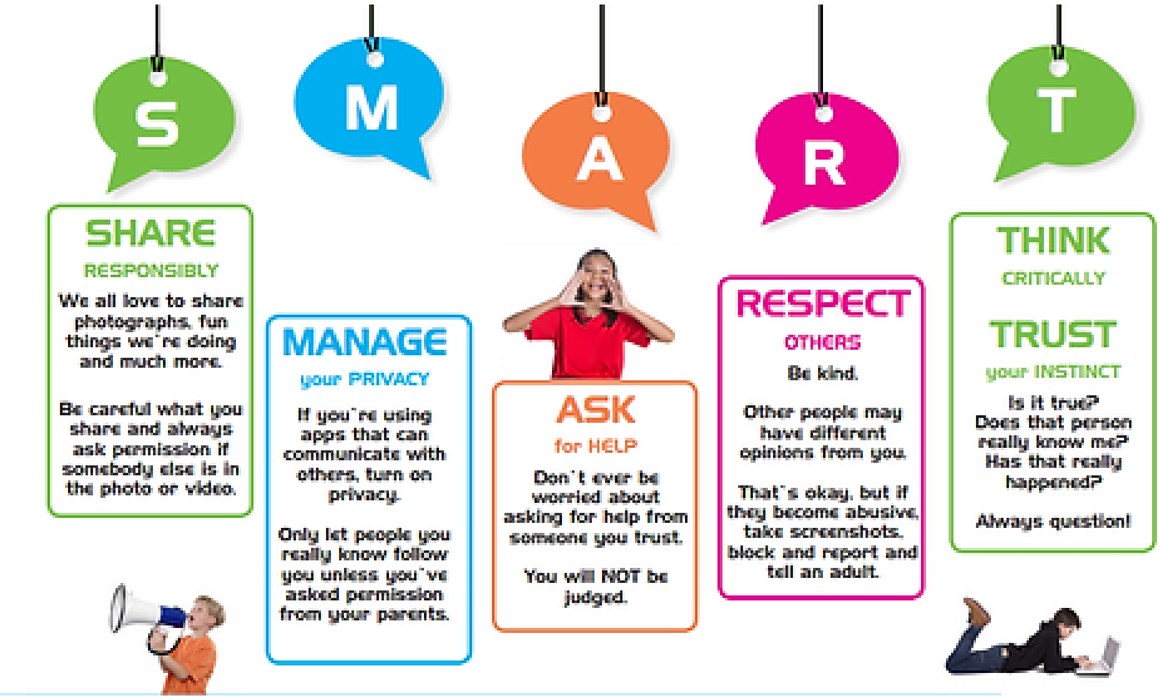
Chrome

Camera: off
Contacts: off
Location: on
Microphone: off
Storage: on

Laws to Ensure Online Safety for Children:

- Indian Penal Code, 1860
- Information Technology Act, 2000
- Protection of Children from Sexual Offences Act of 2012

BE CYBER:



SHARE RESPONSIBLY

We all love to share photographs, fun things we're doing and much more.

Be careful what you share and always ask permission if somebody else is in the photo or video.

MANAGE your PRIVACY

If you're using apps that can communicate with others, turn on privacy.

Only let people you really know follow you unless you've asked permission from your parents.

ASK for HELP

Don't ever be worried about asking for help from someone you trust.

You will NOT be judged.

RESPECT OTHERS

Be kind.

Other people may have different opinions from you.

That's okay, but if they become abusive, take screenshots, block and report and tell an adult.

THINK CRITICALLY

TRUST your INSTINCT

Is it true?
Does that person really know me?
Has that really happened?

Always question!

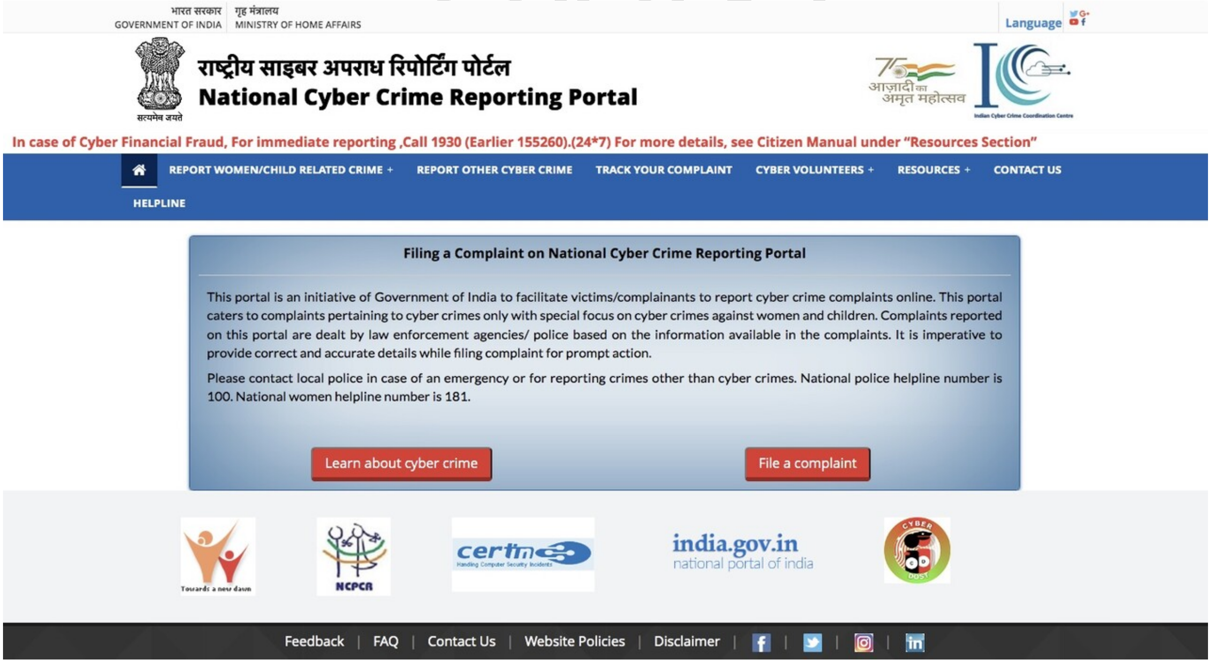
How to Report Cyber Crimes?

- Dial ‘100’ - FIR with local police or Cyber Crime Police Station

- To report cyber fraud call

  National Cyber Crime Helpline - 1930

- **Visit https://www.cybercrime.gov.in/**
  - “REPORT WOMEN/CHILDREN RELATED CRIME” .
  - Select “REPORT ANONYMOUSLY” or “REPORT AND TRACK”.
  - Fill in all the required details and submit.
  - To report “CYBER CRIME” Visit “REPORT CYBER CRIME”.
  - Select “FINANCIAL FRAUD” or other “CYBER CRIME”.
  - Fill in all the required details and submit.



राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

In case of Cyber Financial Fraud, For immediate reporting ,Call 1930 (Earlier 155260).(24*7) For more details, see Citizen Manual under “Resources Section”

Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

Edistys

Printed by: Edistys Foundation

First edition, 2023

Edited by: Sriharshitha Chada & Naguru Vema Sunny

CYBER SKOOL (स्कूल)

"Shaping Cyber Scouts in Schools"