



Rotary
District 3131



a handbook on CYBER SAFETY



BE CYBER
SAFE!



BY ROTARY CLUB OF POONA WEST

Foreword

This book has been designed for standard eighth and ninth students to help them understand the basics of Cyber Safety. With the growth of Internet, it has become essential for students to know the dangers of Cyber Safety and also become good Netizens. The language of this booklet is simple supported by clip art to help students to grasp the subject and at the same time sound interesting.

The subject matter of the booklet has been divided into three parts. The first part talks about basic Cyber Safety practices, the second part lets the students become aware about different types of Cyber Crimes and the third gives information about the different reporting Channels.

We hope the children will find this booklet interesting and informative.

Rtn Dr Madhuri Ghate
Cyber Suraksha,
Rotary Club of Poona West.

INDEX

S.NO	CONTENTS	PAGE NO
1.	Device Safety	4
2.	Safe Internet browsing	8
3.	Keeping Online Accounts safe - Password safety	13
4	Social media safety precautions.	18
5.	App safety	22
6.	Hacking	27
7.	Cyber Bullying	32
8.	Gaming & Cyber Grooming	37
9.	AI Challenge	41
10.	Internet Addiction & Cyber Footprint	44
11.	Basic Online financial safety	49
12.	Reporting Channels	53

Device Safety



Cyber Safety for Your Devices

Your phone, tablet, or laptop is like your **digital notebook**. Just like you protect your books and bag, you must **protect your devices** too!



1. Use a Strong Password or Lock Screen



Always set a **strong password, PIN, pattern, or fingerprint** to unlock your device.



Don't use simple passwords like "1234" or your name.



2. Connect Only to Safe Wi-Fi



Use **trusted and known Wi-Fi** (like your home Wi-Fi).



Don't connect to **free or open Wi-Fi** in public places—they may not be safe.



3. Update Your Device Regularly



Updates fix bugs and keep your device safe from hackers.



Always allow software updates.

4. Don't Download Unknown Apps or Games

 Download apps only from **official stores** (Google Play Store or Apple App Store).

 Unknown apps may have viruses or steal data.

5. Use Antivirus or Security Apps

 Install a **good antivirus app** to protect your device from viruses or hacking.

6. Cover Your Webcam When Not in Use

Sometimes hackers can **turn on your webcam** secretly.

 Keep it covered when not in use.

7. Back Up Your Data

 Save your important photos, files, or notes to Google Drive or a USB.

If your device gets damaged or hacked, your data will still be safe.

8. Don't Charge Your Phone on Public Ports

 Avoid using public USB charging ports (like in malls or buses).

They can be unsafe and steal your phone data.

9. Ask for Help if Something Feels Wrong

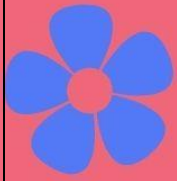
If your device is:

- Acting weird
- Slowing down suddenly
- Showing pop-ups or unknown apps

 Tell a **parent, teacher, or trusted adult** immediately.

 **Be Smart. Be Safe. Be Cyber-Secure!**

Your device is smart—you should be **smarter!**



SAFE INTERNET BROWSING



SAFE INTERNET BROWSING

Contents

1. Safe vs unsafe sites
2. Downloading material
3. Use of cookies
4. Clicking on links
5. Use updated browser
6. VPN & Incognito mode

How to Identify Safe vs Unsafe Websites

Before entering any personal information online, always check the website's safety:

1. Look for HTTPS and a Padlock

- **Safe Website:** Starts with `https://` and shows a padlock symbol in the address bar. This means the site is secure and uses encryption to protect your data.
- **Unsafe Website:** Starts with `http://` (without the "s") or has no padlock. This indicates the site is not secure.

Example: `https://www.amazon.in` is safe. `http://example.com` is not.



2. Check the Domain Name

- **Legitimate Sites:** Use familiar domain names like .com, .in, .org.
- **Suspicious Sites:** May have misspelled names or unusual characters, like amaz0n.com instead of amazon.com.



3. Verify Contact Information

- **Trustworthy Sites:** Provide clear contact details, including a physical address, phone number, and email.
- **Fake Sites:** Often lack contact information or provide vague details.



4. Watch for Typos and Strange Characters

- **Real Websites:** Have professional design and correct spelling
- **Fake Websites:** May contain spelling errors, unusual fonts, or strange symbols.



5. Use Browser Security Features

- **Modern Browsers:** Warn you if a site is suspicious or known for phishing.
- **Always:** Pay attention to these warnings and avoid entering personal information on such sites.



6. Be Cautious with Downloads

- **Safe Downloads:** Only download files from trusted websites.
- **Unsafe Downloads:** Avoid downloading files from unknown sources or clicking on suspicious links.

7. Be Aware of Fake Websites

- **AI Technology:** Hackers can create websites that look exactly like real ones.
 - **Tip:** Always verify the website's URL and look for signs of authenticity.
-

Understanding Cookies

Cookies are small files stored on your device that help websites remember your preferences.

- **Safe Use:** Most websites use cookies to enhance your experience.
 - **Managing Cookies:** You can delete or manage cookies through your browser settings.
 - **Privacy Tip:** Be cautious when accepting cookies from unknown websites.
-

Downloading Material Safely

Follow these steps to download files safely:

1. **Use Secure Websites:** Ensure the website is secure (https://).
2. **Give Credit:** Always credit the source when using downloaded material.
3. **Avoid Third-Party Apps:** Do not download apps from untrusted sources.
4. **Follow Browser Warnings:** Pay attention to any security alerts from your browser.

5. **Avoid Unknown Links:** Do not click on suspicious links to download software.
 6. **Verify New Browsers:** If a site asks you to download a new browser, verify its authenticity before proceeding.
-

Using a Virtual Private Network (VPN)

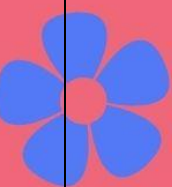
A VPN encrypts your internet connection, providing greater privacy.

- **Benefits:** Masks your IP address, making your online actions untraceable.
 - **Use Cases:** Ideal for secure browsing on public Wi-Fi networks.
-

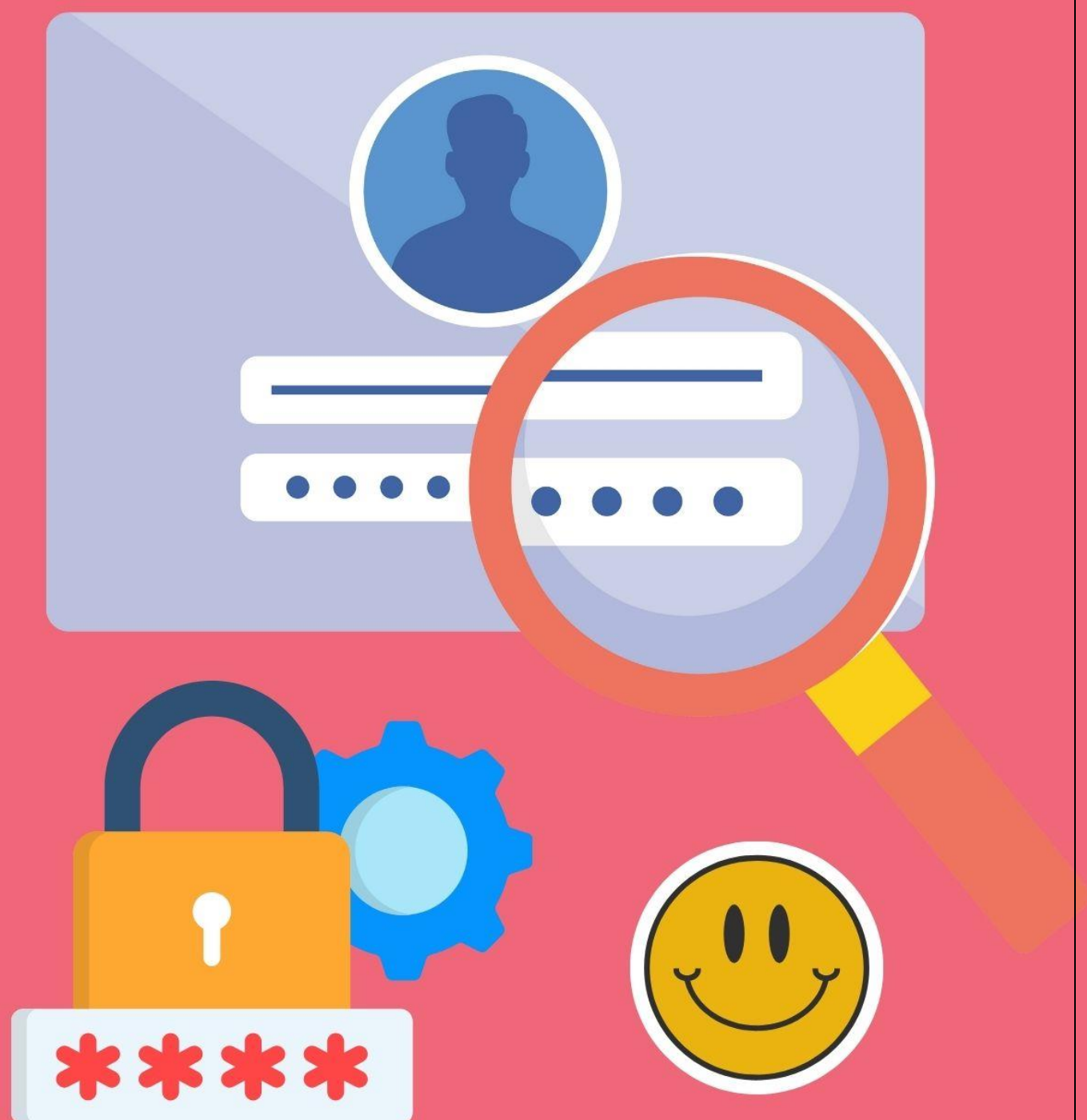
Incognito Mode Explained

Incognito mode allows you to browse the internet without saving your browsing history, cookies, or site data.

- **What It Does:** Prevents your browser from storing your activity locally.
 - **Limitations:** Does not hide your activity from websites, your internet service provider, or employers
 - **Best Use:** Useful for private browsing on shared devices.
-



KEEPING ONLINE ACCOUNTS SAFE – PASSWORD SAFETY



PASSWORD SAFETY

Contents

1. **Creating a strong word password for accounts and devices**
 2. **Passphrase instead of password.**
 3. **Rules for password safety.**
 4. **Password Manager.**
 5. **Two factor authentication or multi factor authentication.**
-

Why Passwords Matter

A **password** is like a **key** to your online accounts and devices. If someone guesses your password, they can access your personal information. That's why it's important to create strong passwords to keep your accounts safe.

How to Create a Strong Password

1. **Use at least 12 characters:** The longer your password, the harder it is to guess
 2. **Mix it up:** Include uppercase letters (A–Z), lowercase letters (a–z), numbers (0–9), and special characters (!, @, #, \$, etc.).
 3. **Avoid personal information:** Don't use your name, birthdate, phone number, or pet's name.
 4. **Make it random:** The more unpredictable, the better
-

What is a Passphrase?

A **passphrase** is a sequence of words combined into a phrase. It's longer and more secure than a simple password.

Example: If you enjoyed a holiday in Goa in 2023, you could create a passphrase like:

Holiday@Goa2023

This passphrase is easy to remember but hard for others to guess.

Rules for Password Safety

1. **Use different passwords for different accounts:** Don't use the same password everywhere.
 2. **Don't share your passwords:** Keep them private
 3. **Change your passwords regularly:** It's a good habit to update them every few months.
 4. **Don't save passwords in browsers or on your phone:** It's safer to remember them or use a password manager.
-

Password Manager

A **password manager** is a tool that securely stores your passwords. You only need to remember one master password.

Note: Always choose a strong master password for your password manager.

Two-Factor Authentication (2FA)

2FA adds an extra layer of security. Even if someone knows your password, they can't access your account without the second factor.

Example: After entering your password, you'll receive a code on your phone that you need to enter to access your account.

Check if Your Information Was Leaked

Visit [Have I Been Pwned](#) to see if your email or password has been part of a data breach.

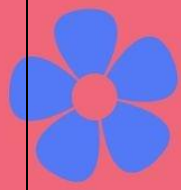
Tips for Remembering Passwords

- **Use a password manager:** It stores all your passwords securely.
 - **Create a memorable passphrase:** Think of a sentence or a combination of words that are meaningful to you.
 - **Write it down securely:** If you must write it down, keep it in a safe place.
-

Quick Recap

- **Strong Password:** At least 12 characters, mixed with letters, numbers, and symbols.
- **Passphrase:** A memorable phrase that's hard to guess.
- **2FA:** Adds extra security to your accounts.

- **Password Manager:** Helps you store and manage your passwords securely.
-



SOCIAL MEDIA SAFETY



SOCIAL MEDIA SAFETY

Contents

- 1.What is social Media**
- 2.Managing friend requests**
- 3.Privacy settings**
- 4.Social media accounts hacked**
- 5.Inappropriate content**
- 6.Identifying fake accounts**

What is social media?

Social media is a place on the internet where people can:

- Talk to each other
- Share ideas, thoughts, pictures, and videos
- Make new friends
- Build businesses or personal brands

Popular social media apps:

- Facebook
 - Twitter
 - Instagram
 - WhatsApp
 - Snapchat
 - Tinder
-

How to Stay Safe on social media

1.  **Don't accept friend requests from strangers.**
Only talk to people you know in real life.
2.  **Keep personal information private.**
Don't post your:
 - Photos or videos
 - Address or phone number
 - Date of birth or travel plans
3.  **Use a strong password.**
Use **two-factor authentication (2FA)** for extra safety.
4.  **Be careful with apps.**
Don't download unknown apps from social media.
5.  **On dating apps:**
Don't share private or revealing photos.
Block and report people who act strangely.

Privacy Settings

Many social media platforms allow **parents and children** to use **child safety settings**.

Use these to stay safe.

Inappropriate Content

1. Report **rude or abusive** posts.
2. Don't share **fake news** or **unverified messages**.
3. Be careful with **AI-made photos or videos**.
Not everything is real!

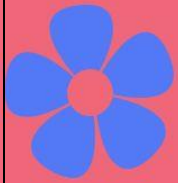
4. Don't forward content that can hurt **religious or political feelings**.
 5. Be polite and kind on social media.
 6. Your social media shows your **digital footprint**.
Colleges and employers may check it.
-

What if Your Account Gets Hacked?

1.  Change your password quickly.
 2.  Change your email password too.
 3.  Tell your friends your account was hacked.
 4.  Ask them not to click any strange messages from your account.
 5.  Use the "Help centre" of the app to get your account back.
-

How to Spot a Fake Account

1. No bio, no profile picture.
 2. New account with very few posts.
 3. Follows many people but has few followers.
 4. Tries to scam you with fake offers.
 5. Use **Google Images** to check if the profile photo is stolen.
-



APP SAFETY



APP SAFETY

Contents

- 1.Points to be kept in mind before downloading an app.**
 - 2.Managing App permissions including location services.**
 - 3.Updating apps.**
 - 4.Deleting an app.**
-

What is an App?

App is short for **Application**.

It is a **small program** that runs on your **phone, computer, or tablet**.

Apps help you:

- Chat with friends (WhatsApp)
 - Watch videos (YouTube)
 - Study (Google Classroom)
 - Play games
 - Get work done
-

Think Before You Download an App

Before you download an app, **check these things**:

1.  **Only download from** trusted stores like **Google Play Store** or **iPhone App Store**.
 Don't download from unknown websites.
 2.  **Check app ratings.**
Too many 1-star or 5-star ratings may be a sign of fake reviews.
 3.  **Check number of downloads.**
More downloads usually mean the app is safe.
 4.  **Read app reviews** on websites to know if it works well.
 5.  **Check app maker (vendor) details.**
 6.  **APK files (Android)** are special files for installing apps.
Only download APKs from **safe websites**.
-

Managing App Permissions (Access)

Apps often ask for **permissions**, like:

-  Your location
-  Your camera
-  Your microphone

 **Allow only the permissions the app really needs.**

For example, a photo editor needs camera access — but not your location!

 Go to your **phone settings** and check what each app can access.

You can **turn off permissions** anytime.

Updating Apps

 When your phone says an **update is available**, don't ignore it!

Updating apps:

- Fixes problems (bugs)
 - Adds new features
 - Makes your app run better
-

Deleting Apps You Don't Use

If you haven't used an app for **3 months**, it's time to delete it.

Safe Steps to Delete an App:

1. Uninstall the App

- **iPhone:** Press and hold app → Tap  Remove App
- **Android:** Press and hold → Drag to  Uninstall
Or go to **Settings > Apps > [App Name] > Uninstall**

2. Backup Important Data

- Save your notes, photos, or files.
- Make sure data is synced to **cloud** if needed.

3. Unlink Accounts

- Remove social media or email links.
- Delete saved **payment methods**.

4. Clear App Data

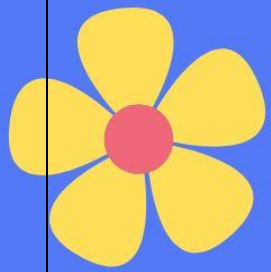
- Go to settings → clear **cache and data**
This removes leftover files.

5. Revoke Permissions

- Remove access to your camera, contacts, location, etc.

6. Check Device Security

- After deleting, make sure your phone works normally.
If it acts strange, get it checked.
-



HACKING



HACKING

Contents

1.Hacking

2.Phishing & Vishing and Smishing attacks

3.Signs of malware attacks on devices and accounts

4.Getting rid of malware if account is compromised.

What is Hacking?

Hacking means breaking into a computer or phone system **without permission to steal data or cause harm.**

Real Example:

People received fake messages that their **MNGL gas bill** was pending.

The message had a **link** asking them to pay or download an app.

This was a **fraud** to steal their money.

Phishing, Vishing, and Smishing

Phishing

- You get a **fake email or message** that looks real.

- It may ask for your **password, ATM PIN**, or other private info.
 - Never click on suspicious links.
-

Vishing

- **Fake phone calls** from scammers pretending to be your **bank or government**.
 - They ask for your **bank details**.
 - **Don't tell anyone** your PIN or OTP.
-

Smishing

- You get a **fake SMS** that says something urgent.
 - It asks you to **click a link** or **reply** with details.
 - Don't click. **Delete the message**.
-

How to Stay Safe from Malware Attacks

Malware is a bad software that can:

- Steal your information
- Damage your device
- Send spam from your account

Tips to Stay Safe

1.  Be careful with **attachments** in emails.
2.  Scan **pen drives** before using.
3.  Don't click on strange **links**.

4.  Never download **pirated software**.
5.  Don't click "OK" on pop-up ads or fake prizes.
6.  Install **Anti-virus** software.
7.  Back up your data to **cloud** or USB drives.

Signs Your Computer May Have Malware

-  It becomes **slow** and unresponsive.
 -  It **freezes** or crashes often.
 -  You see **weird pop-up ads**.
 -  Your account sends messages on its own.
 -  Strange apps open by themselves.
 -  Your storage space suddenly becomes full.
-

How to Remove Malware from Your Computer

1.  Disconnect your computer from the internet.
 2.  Start in **Safe Mode**
(*A special way to open the computer with only needed programs*)
 3.  Install or **update antivirus**, then scan your computer.
 4.  Delete apps you recently installed that look suspicious.
 5.  Clear your browser **cache**.
For Chrome: Chrome → History → Clear Browsing Data → All Time → Clear
 6.  Restart to **exit Safe Mode**.
-



Still Not Fixed?

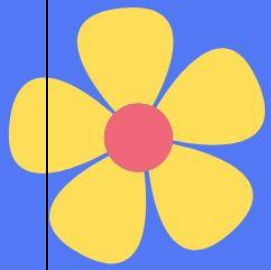
If the malware won't go away, you may have to:

- **Reinstall your operating system**
 - **Ask a tech expert for help**
-

Always Remember:

- Never share personal info online.
- Think before you click.
- Ask an adult if you're not sure.

Stay safe. Stay smart. 



CYBER BULLYING



CYBER BULLYING

CONTENTS

1. What is bullying
2. Impact of bullying
3. Precautions to be taken
4. Reporting

What is Cyber Bullying?

Cyber bullying is when someone uses phones, computers, or the internet to **hurt, tease, threaten, or embarrass** another person.

It can happen on:

- Social media (Instagram, WhatsApp, Facebook)
- Chat rooms or messaging apps
- Online games

Real-Life Case

A girl from Class 9 who was very good in studies suddenly became quiet and sad. She stopped talking, eating, and smiling. Her teacher told her parents, and they took her to a counsellor. It was found that some classmates were calling her names and making fun of her weight online.

She got help just in time, and the teacher explained to the other students how dangerous cyber bullying is.

Types of Cyber Bullying

1. **Flaming / Roasting / Name Calling:** Saying mean things online to hurt someone.  *Example:* Calling someone by a rude nickname.
 2. **Outing:** Sharing private photos or secrets without asking.
 3. **Trolling:** Posting upsetting messages just to make others angry.
 4. **Spreading Rumours:** Telling lies about someone online.
 5. **Sending Inappropriate Images:** Sending or sharing personal pictures without permission.
 6. **Cyber Stalking:** Constantly messaging someone to scare or threaten them.
-

How Cyber Bullying Affects Victims

- Stress and anxiety
 - Depression (feeling very sad)
 - Feeling bad about oneself
 - Skipping school
 - Getting angry or upset easily
-

Who Are Cyber Bullies?

Cyber bullies may:

- Want to feel powerful
 - Have poor behaviour or mental health issues
 - Lack empathy (don't care about others' feelings)
-

What to Do and What Not to Do

Do's:

1. Take a screenshot of the mean message.
2. Block the bully.
3. Talk to your teacher, parent, or any trusted adult.
4. Report to the website or app.
5. Report to Cybercrime Cell if needed.

Don'ts:

1. Don't reply to the bully.
2. Don't feel ashamed or blame yourself.
3. Don't stay silent.

Cyber Bullying is a Crime. It can be punished by law.

Final Message

Say **NO** to bullying.

Be kind online. If you see someone being bullied, speak up and help.

What is Bullying?



Cyber bullying is bullying that takes place when someone uses technology to harass, threaten, or target another person.

Impact of Bullying



A 9-year-old girl student stopped participating, crying and became depressed.

Teachers and parents took action and counseled students on impact of cyber bullying

Precautions to be taken



Don't respond to bullies



Take a screenshot of the post

Block the bully



Talk to a trusted adult

Report to the social media site

REPORT

Reporting

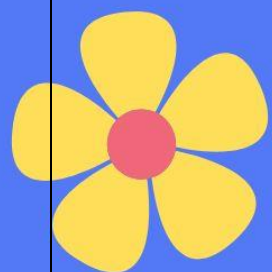


Cybercrime is a cyber crime

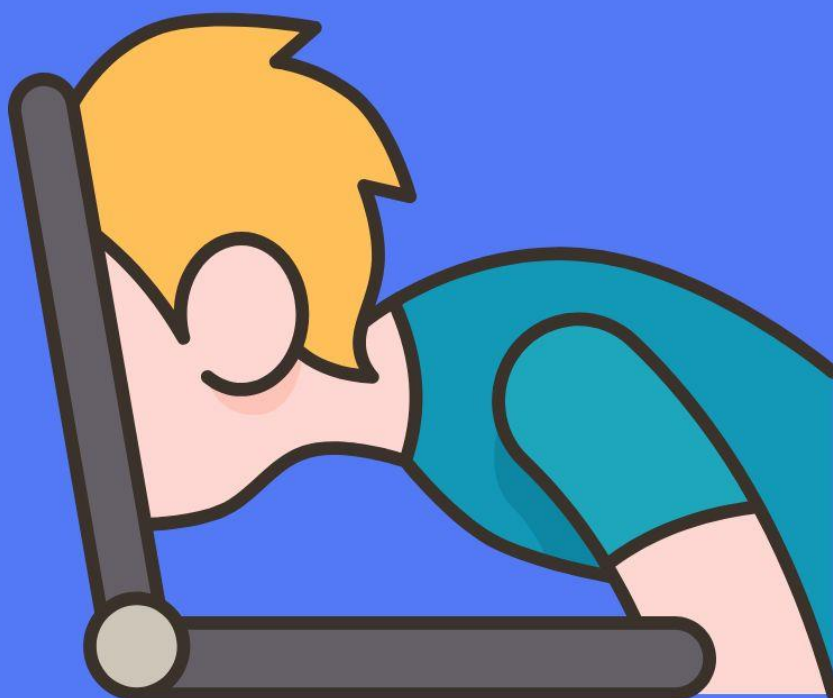
Cyber bullying is

Say No to Bullying

Cyber Bullying is a cyber crime



GAMING & CYBER GROOMING



ONLINE GAMING & CYBER GROOMING

CONTENTS

1. Risk involved with online gaming.
2. Task Games
3. Cyber Grooming
4. Precautions for Online Games and Cyber Grooming

Online Gaming – Fun with Risks

Dangers of Online Gaming

1.  **Hacking** – Bad links or files may steal your personal info.
 2.  **Cyber Bullying** – Hurting others using chats or messages.
 3.  **Cyber Grooming** – Strangers pretending to be friends to harm you.
 4.  **Stealing Financial Info**
 5.  **Using You for Cyber Crime**
-

Dangerous Task/Challenge Games

Some games ask you to complete dangerous challenges like hurting yourself or others.

Examples:

- ◆ PUBG
- ◆ Blue Whale
- ◆ Pink City
- ◆ Pokémon Go

 **Real Story:** A 14-year-old boy in Pimpri Chinchwad jumped off a balcony as part of a game challenge.

Safety Tips for Online Gaming

1. Play games meant for your age. 
 2. Limit your play time. 
 3. Never play with strangers. 
 4. Don't download games from unknown sites.  
 5. Don't share your personal info.  
 6. Keep card/bank info private.  
 7. Avoid voice chat or webcam.  
 8. Don't meet online friends alone. 
 9. If something feels wrong, BLOCK and REPORT!  
-

What is Cyber Grooming?

Cyber Grooming is when someone online builds trust to take advantage of a child—often in a harmful or abusive way.

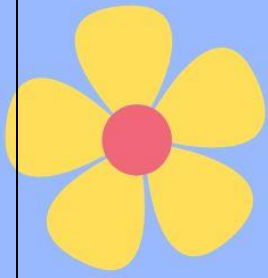
Tips to Stay Safe from Cyber Bullying & Grooming

1. Don't share personal details online.
 2. Only talk to people you know.
 3. Watch out if someone is too friendly too fast.
 4. If anyone asks for pictures or odd favours – BLOCK them.
 5. Never meet online friends alone.
 6. Talk to a parent or teacher.
 7. Report to **Cyber Crime Police** or **cybercrime.gov.in**.
-

Why Outdoor Games are Better!



- ✓ Builds **teamwork**
 - ✓ Improves **physical strength**
 - ✓ Makes **real-life friends**
-



AI CHALLENGE



The AI Challenge

1. What is Artificial Intelligence?
 2. Dangers of AI in Cyber World.
 3. Precautions to Stay Safe from AI Misuse
-

AI and Cyber Safety – Be Smart, Be Safe!

AI (Artificial Intelligence) is a technology that helps machines think and act like humans. It is used in games, social media, and apps. But it can also be misused. So, we must stay alert and safe!

Dangers of AI in Cyber World

1. Fake Messages or Calls

 AI can create voice messages or calls that sound real.

2. Deepfake Videos or Photos

 AI can create fake videos or photos to trick people.

3. AI Chatbots Pretending to be Real People

 Some AI bots chat like real people and try to get your info.

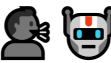
4. Personal Info Stealing

 AI can collect your data from your online activities.

Precautions to Stay Safe from AI Misuse

-  Never give your name, school, phone number, or address to strangers online.

Check if You're Talking to a Human or a Bot

-  Ask simple questions. If replies feel robotic, stop chatting.

2. Think Before You Believe

-  Don't trust every photo, video, or message. It could be AI-made.

3. Don't Click on Strange Links

-  AI bots may send dangerous links that steal your data.

4. Use Parental Controls and Security Apps

-  Ask your parents to use filters to block bad websites or bots.

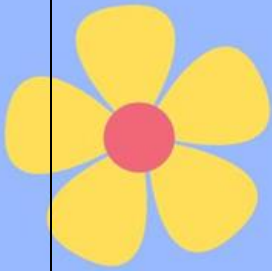
5. Report Fake or Suspicious Activity

-  If someone is acting weird online, tell a **teacher or parent**.

 **REMEMBER!**

- AI can be helpful but also harmful if misused.
- Always stay alert and follow cyber safety rules.

 **Stay Smart, Stay Safe, Stay Happy Online!**



INTERNET ADDICTION & CYBER FOOTPRINT



INTERNET ADDICTION.

CYBER FOOT PRINT

CONTENTS

1. Internet addiction
2. Gaming addiction
3. Selfie addiction.
4. How to overcome addiction
5. Cyber footprint

Internet Addiction, Selfie Addiction & Your Digital Footprint

What is Internet Addiction?

When someone spends **too much time online**, it affects their:

- Health 
- Studies 
- Family & Friends 
- Daily Routine 

If they don't get to use the internet, they feel **angry or anxious**.

A person can get addicted to:

1. Browsing websites 
2. Playing games 
3. Social media (Instagram, YouTube) 
4. Watching bad content 

Why do people get addicted?

Online activities release a chemical in the brain called **Dopamine**, which makes us feel happy. We want that feeling again and again—this creates addiction.

How to Overcome Internet Addiction

1. Set time limits on phone/computer use.
 2. Replace screen time with hobbies like art, music, or sports.
 3. Avoid using devices before sleep.
 4. Spend time with supportive friends & family.
 5. Don't use devices while eating.
 6. If it gets serious, talk to a counsellor or psychologist.
-

What is Selfie Addiction?

Selfie addiction means taking too many selfies and sharing them just to get likes or attention.

It can:

- Lower your confidence
- Make you feel bad about yourself
- Cause risky behaviour

 **Real Case:** A social media influencer in Maharashtra died after slipping while taking a selfie near a waterfall.

How to Overcome Selfie Addiction

 Set a limit on selfies you take & post.

1. Enjoy the moment instead of capturing it.
 2. Build confidence through hobbies or sports.
 3. Ask friends/family for help if needed.
 4. Get professional help if it becomes too much.
-

What is a Cyber Footprint? (Digital Footprint)

Just like your feet leave prints in the sand, everything you do online leaves a **digital footprint**.

 Your footprint includes:

- Websites you visit
- Posts you like/share
- Search history
- Personal info you share

 **Others can see your digital trail, including:**

- Colleges
 - Companies (for jobs)
 - Visa officials (for travel)
 - Even future marriage partners!
-

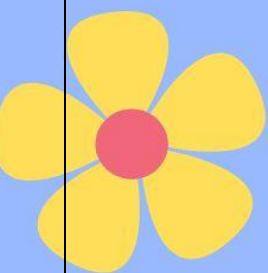
Tips to Keep Your Digital Footprint Clean

1. Be careful what you post or share.
2. Don't give personal details online.

3. Don't visit unsafe websites.
4. Think before you comment or message.
5. Google yourself to see what others can find about you.

 **Final Tip: Use the Internet wisely. It's a tool, not your boss!**

:



BASIC ONLINE FINANCIAL SAFETY



Cyber Safety While Doing Online Money Transactions

Contents

1.What is a Financial Transaction?

2.Why Be Careful?

3.Cyber Safety Rules for Money Transactions



What is a Financial Transaction?

A financial transaction means sending or receiving money online, like:

- Using UPI (Google Pay, Phone Pe, etc.)
- Online shopping
- Using debit/credit cards
- Paying school fees online



Why Be Careful?

If you're not careful, hackers and fraudsters can:

- Steal your money 
 - Get your personal information 
 - Use your account for illegal things 
-

Cyber Safety Rules for Money Transactions

1. Use Secure & Trusted Apps Only

 Use only **official apps** like Google Pay, PhonePe, Paytm, or your bank's app.

 Don't use unknown or fake apps.

2. Never Share Your OTP or PIN

Never tell your:

- ATM PIN
 - UPI PIN
 - OTP (One-Time Password)
to anyone—not even friends.
-

3. Don't Click on Unknown Links

Fraudsters send fake links through messages or emails.

 Don't click on them.

 Visit official websites for payments.

4. Never Save Card Details on Public Devices

Don't save your card details on:

- Cyber cafés
- Friend's phone

- Shared computers
-

5. 👁️ Always Check Before Paying

✅ Double-check the name and number before sending money.

❌ A small mistake can send money to the wrong person.

6. 👤🏠 Inform Parents or Teachers

If something goes wrong or feels suspicious:

- **Tell your parents or teacher immediately.**
 - **Never try to hide financial mistakes.**
-

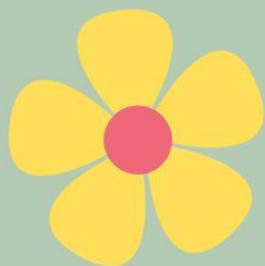
7. 🚨 Report if Scammed

If money is stolen:

- Call your bank customer care immediately.
 - Report it on **cybercrime.gov.in**.
-

★ **Smart Student = Safe Student!**

Using money online is useful—but only when you are **smart, safe, and alert**.



REPORTING CHANNELS



REPORTING CRIME CRIMES:

CONTENTS

1. Government portals
 2. Helpline numbers
 3. Social media sites.
 4. Telecom portals
-

Reporting Cyber Crimes

Cyber-crimes are increasing. Hackers and fraudsters use smart tricks to fool people — from India and other countries.

 So, it is important to **report cybercrimes**.

Here's **how and where** you can report, in simple steps 

Why Should You Report Cyber Crimes?

1.  You may get your problem solved faster (timely help).
 2.  It helps stop others from getting fooled.
 3.  If a financial fraud is reported within **1 hour**, you may get back **up to 90% of your money**.
 4.  Authorities can take action and protect more people.
-

Where to Report a Cyber Crime?

1. Offline: Go to the nearest Cyber Crime Police Station

Pune Police Cyber Cell

 Email: crimecyber.pune@nic.in

 Phone: 020-29710097

2. Online: Use Government Cyber Crime Portal

 Website: <https://cybercrime.gov.in>

 This is a **safe website** to report all cyber crimes.

 You can also report crimes against **women and children**, even without giving your name.

3. Cyber Crime Helpline Numbers

-  **1930** – National Cyber Crime Helpline
 -  **1945**-Maharashtra Cyber Crime Helpline
 -  **1098** – Childline India (for crimes against children)
-

4. Report on social media

Follow **Cyber Dost** – the official account for cyber safety tips.

(Started by the Ministry of Home Affairs)

-  x: [@CyberDost](https://twitter.com/CyberDost)
-  Facebook: [Cyber Dost](https://www.facebook.com/CyberDost)

-  Instagram: [Cyber Dost](#)
 -  Telegram: [Cyber Dost Channel](#)
-

5. Report to Telecom Department

 Website: <https://sancharsaathi.gov.in>

This portal helps you with phone-related frauds.

Features on Sanchar Saathi:

-  Check fake messages/calls (CHAKSHU)
-  Block lost or stolen phone (CEIR)
-  See your mobile number connections (TAFCOP)
-  Check IMEI number of phone (KYM)
-  Report fake calls using Indian numbers (RICWIN)
-  Know your internet service provider

 Helpline: 14022

Remember:

 Be alert online.

 Report anything suspicious to a trusted adult or teacher.

 Your quick action can **stop a cyber crime** and even **save someone's money or life!**

ACNOWLEDGEMENTS

- **We thank Pune Police for their full support to our Be Cyber Safe program.**
- **We thank Adv. Vaishali Bhagwat, Cyber Law Expert, for validating the content.**
- **We thank Dr Arati Sameer Nimgaonkar, Cyber Security co-ordinator, Assistant Professor, Department of Computer Sciences, FC College, Pune for her valuable inputs.**

Rotary Club of Poona West Team

- *President:* **Rtn Santosh Chiplunkar**
- *Service Director:* **Rtn Bhagyashree Bhide.**
- *Chairperson Cyber Suraksha:* **Rtn Rita Kothari**
- *Ideation, Content Development, Video Creation:* **Rtn Dr Madhuri Ghatе.**
- *Content Editing:* **Rtn Bhagyashree Bhide.**

THANK YOU!



**You have learnt to be
Cyber Safe!**



