



इलेक्ट्रॉनिक्स एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

certin
Enhancing Cyber Security in India



Information Security
Education & Awareness



साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

CYBER SMART KIDS: SURAKSHA GUIDE



#Cyber
Jagrit
Bharat

**NATIONAL CYBER SECURITY
AWARENESS MONTH
(October 2025)**

**INDIAN COMPUTER EMERGENCY
RESPONSE TEAM --- [CERT-In]**

TABLE OF CONTENTS



Preface

3

Protect Personal info

4

Strong Password

5

Social Media

6

Phishing

7

Online Safety

8

Cyber Grooming & Stalking

9

Safe Digital Habits

10

Reporting Cyber Security Incidents

11

PREFACE



The Indian Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology (MeitY), Government of India is established with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

CERT-In has been designated to serve as the national agency for incident response under Section 70B of the Information Technology Act, 2000. As part of services of CERT-In, for the creation of awareness in the area of cybersecurity as well as training/upgrading the technical know-how of various stakeholders, CERT-In is observing the National Cyber Security Awareness Month 2025.

This Cyber Security Best Practices Booklet for Kids is released as a part of CERT-In's awareness initiatives to educate the children on the best practices that needs to be followed for using the internet in a safe and secure manner.

**YOUR INFO IS
PRECIOUS – PROTECT IT!**



HOW ATTACKERS TARGET KIDS

Cybercriminals often trick children online by pretending to be friendly strangers, offering gifts, games, or fake contests to gain trust and steal personal information.

(How They Operate)

- Create fake profiles on games or social media to befriend kids.
- Ask for personal details like name, school, or photos.
- Send suspicious links or files that can steal data.
- Use flattery or threats to manipulate kids into sharing more.
- Misuse shared info to impersonate or harm the child or family.

BEST PRACTICES

1. Never share personal info online without a parent's permission.

– *Personal Identifiable Information, such as your full name, address, phone number, school name, or photos.*

2. Keep your accounts private.

– *Only accept friend requests from people you know in real life.*

3. Don't click on unknown links or download random files.

– *They might contain harmful software or lead to fake websites.*

4. Tell a trusted adult if something feels wrong or scary online.

– *Don't try to handle it alone.*

5. Use strong passwords and never share them with friends.

– *A good password keeps your account safe like a secret code!*

**A STRONG PASSWORD IS
LIKE A SUPERHERO SHIELD
– IT PROTECTS YOUR
ONLINE WORLD!**



HOW ATTACKERS TARGET KIDS

Cybercriminals try to guess weak passwords or trick kids into sharing them. They may pretend to be friends, send fake login pages, or offer free games to steal account access.

(How They Operate)

- Use common passwords like "123456" or "password" to break into accounts.
- Send fake messages or links asking for login details.
- Pretend to be someone you know and ask for your password.
- Hack one account and use the same password to access others.
- Use stolen passwords to change settings, send messages, or steal personal info.

Strong Password! BEST PRACTICES

1. Create strong passwords using a mix of letters, numbers & symbols.
– Example: *Tiger!42Dance* is better than *tiger123*.
2. Never use the same password for different accounts.
– Each account should have its own unique password.
3. Don't share your password with anyone except your parents.
– Even best friends shouldn't know your secret code.
4. Avoid using personal info in passwords.
– No names, birthdays, or pet names — they're easy to guess!
5. Change your passwords regularly.
– It's like changing the locks to keep intruders out.

**THINK BEFORE
YOU POST!**



HOW ATTACKERS TARGET KIDS

Cybercriminals look for photos, videos, or posts that reveal personal details. They use this information to stalk, impersonate, or manipulate kids online.

(How They Operate)

- Scan social media for posts showing school uniforms, home addresses, or locations.
- Use shared content to guess passwords or security questions.
- Create fake profiles using kids' photos and reposted content.
- Track location tags or check-ins to monitor movements.
- Trick kids into resharing harmful or misleading posts.

Social Media!

BEST PRACTICES

- 1. Never post pictures or videos showing your school uniform, home, or location.**
 - *These details can help strangers find you in real life.*
- 2. Avoid tagging your location or checking in publicly.**
 - *Keep your whereabouts private.*
- 3. Think before you reshare or retweet.**
 - *Make sure the content is safe, kind, and true.*
- 4. Keep your social media accounts private.**
 - *Only allow people you know to see your posts.*
- 5. Ask a parent before posting anything personal.**
 - *If you're unsure, it's always better to check first.*

**THINK BEFORE YOU CLICK!
NOT EVERY LINK IS SAFE
– SOME ARE TRAPS!**



HOW ATTACKERS TARGET KIDS

Cybercriminals send fake messages, emails, or pop-ups that look real. They trick kids into clicking links that steal personal info or install harmful software.

(How They Operate)

- Send messages pretending to be from games, schools, or friends.
- Use urgent language like “Click now to win!” or “Your account will be deleted!”
- Link to fake websites that look real but steal login details.
- Attach files that secretly install viruses or spyware.
- Ask kids to enter personal info or passwords on fake forms.

Phishing! BEST PRACTICES

1. **Never click on links from strangers or unknown sources.**
 - Always ask a parent before opening anything unfamiliar.
2. **Look closely at the link before clicking.**
 - Fake links often have weird spellings or extra characters.
3. **Don't trust messages that sound too good to be true.**
 - Free gifts, prizes, or threats are common phishing tricks.
4. **Use trusted websites and bookmarks.**
 - Don't search for login pages – go directly to the official site.
5. **Report suspicious messages to a parent or teacher.**
 - If something feels off, don't click – speak up!

**STAY SMART,
STAY SAFE ONLINE!
ONLY VISIT WEBSITES THAT ARE
SAFE, AGE-APPROPRIATE, AND
APPROVED BY PARENTS.**



HOW ATTACKERS TARGET KIDS

Cybercriminals often pose as friendly strangers or create fake websites and games to trick kids into sharing personal information or clicking harmful links.

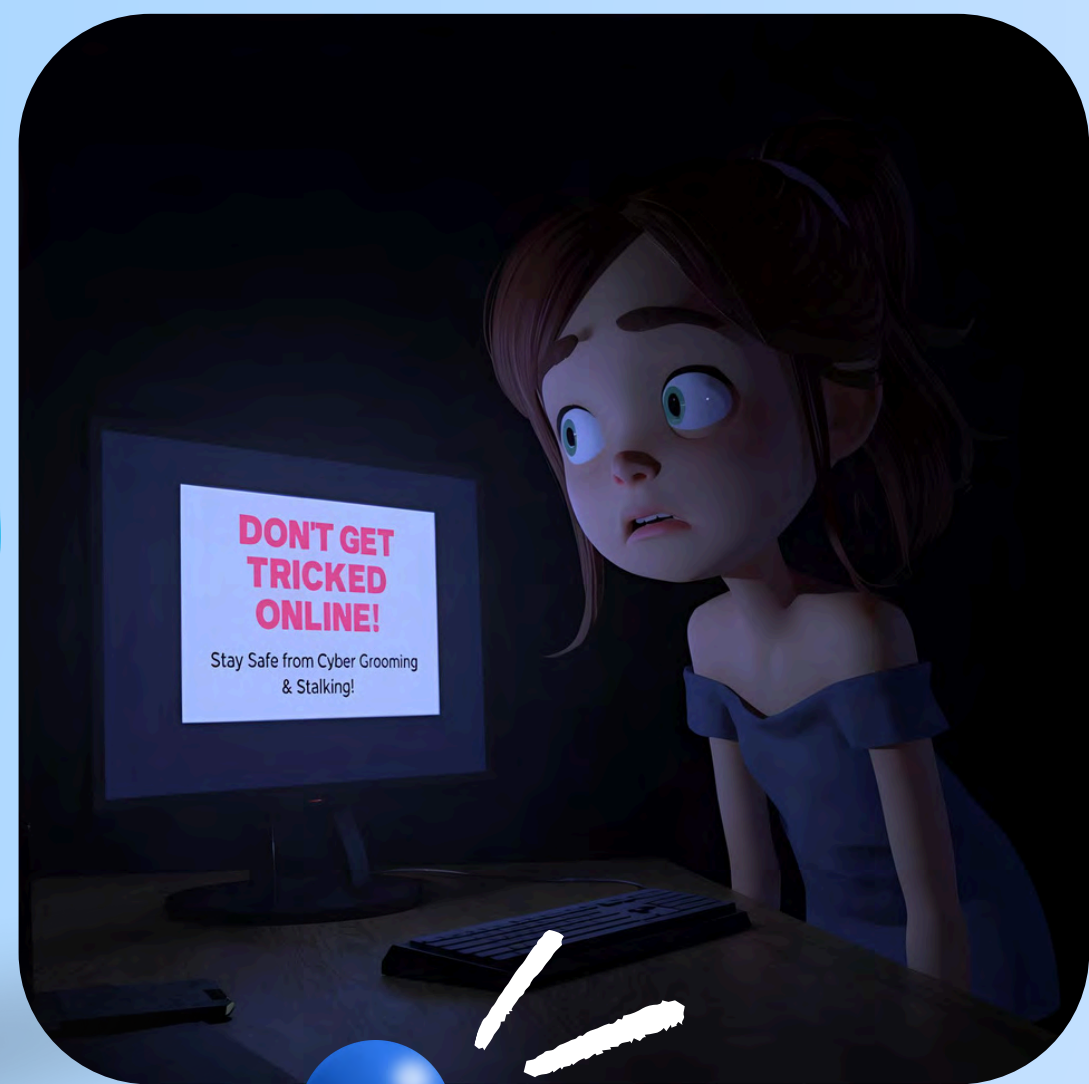
(How They Operate)

- Pretend to be kids or gamers to build online friendships.
- Share links to unsafe or fake websites that look fun or familiar.
- Ask for personal details like name, school, or photos.
- Use chatrooms or games to lure kids into unsafe conversations.
- Trick kids into downloading harmful apps or files.

Online Safety! BEST PRACTICES

1. Only use websites and apps approved by your parents.
 - Age-appropriate platforms are safer and designed for kids.
2. Don't talk to strangers online – even if they seem friendly.
 - Online friends should be people you know in real life.
3. Avoid clicking on ads or pop-ups.
 - They might lead to fake or dangerous websites.
4. Check the website address carefully.
 - Genuine sites usually start with “https” and have no spelling mistakes.
5. Tell a parent if something online feels weird or scary.
 - Never keep secrets about online experiences.

**DON'T GET TRICKED ONLINE –
STAY SAFE FROM CYBER
GROOMING & STALKING!**



HOW ATTACKERS TARGET KIDS

Cybercriminals build trust with kids online by pretending to be friendly. They slowly gather personal information, manipulate emotions, and may even threaten or follow kids digitally.

(How They Operate)

- Pretend to be kids or teens on games, chats, or social media.
- Start friendly conversations and offer compliments or gifts.
- Ask for personal details, photos, or secrets over time.
- Use emotional manipulation to gain control or silence the victim.
- Monitor online activity, send repeated messages, or track location posts.

Cyber Grooming & Stalking! **BEST PRACTICES**

1. **Never talk to strangers online – even if they seem nice or fun.**
–Real friends are people you know in person.
2. **Don't share personal info, photos, or secrets with online friends.**
–What feels private can be misused.
3. **Avoid posting your location, school name, or daily routine.**
–Stalkers use this info to track you.
4. **Block and report anyone who makes you uncomfortable.**
–Don't respond – tell a trusted adult immediately.
5. **Speak up if someone online asks you to keep secrets.**
–Safe adults never ask kids to hide things.

**DON'T GET TRICKED BY
TECH – USE IT RIGHT!**



SAFE DIGITAL HABITS

DO'S



&

DON'TS



- Visit genuine websites approved by parents.
- Use a genuine operating system and keep it updated.
- Download apps and games from trusted sources.
- Install software that's legal and safe.
- Take regular breaks and limit screen time.
- Don't browse unknown or suspicious websites.
- Don't ignore software updates.
- Don't download pirated or illegal content.
- Don't use cracked software or OS – it can harm your device.
- Don't spend too many hours online without breaks.

Report Cyber Security Incidents to CERT-In

For reporting Cyber Security Incidents to CERT-In:

Visit website: <https://www.cert-in.org.in>

Email: incident@cert-in.org.in

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

Information Desk

Phone: +91-11-22902657

For Collaboration with CERT-In in the area of Cyber Security:

Visit website: <https://www.cert-in.org.in>

Email: collaboration@cert-in.org.in

Phone: +11-22902600 Ext: 1012, +91-11-24368572

For Trainings/ Awareness programmes:

Email: training@cert-in.org.in

Official social media handles of @IndianCERT

 <https://www.facebook.com/IndianCERT/>

 <https://twitter.com/IndianCERT>

 https://www.instagram.com/cert_india/

 <https://www.linkedin.com/company/indiancert-cert-in/>

 <https://youtube.com/@indiancert>



csk@cert-in.org.in

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre



Announcements

<https://www.csk.gov.in/announcements/index.html>



Security Tools

<https://www.csk.gov.in/security-tools.html>