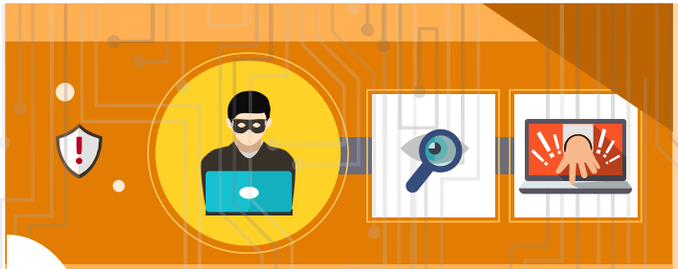


Cyberbullying

Cyberbullying includes sending, posting or sharing negative, harmful, false or mean information and content about someone. It is a serious offence which is punishable under Cyber Law

Cyber Bullying includes

- Nasty comments on your posts or posts about you
- Someone creating a fake profile in your name and trying to defame you
- Threatening or abusive messages online or on the mobile phone
- Being excluded from online groups and forums
- Embarrassing photographs put online without your permission
- Rumours and lies about you on a site
- Stealing your account password and sending unwanted/inappropriate messages from your account
- Offensive chat
- Fake online profiles created with an intent to defame you

Do the following If Cyberbullied

Do not Respond
If someone is cyber bullying you, do not respond or retaliate by doing the same thing back. Responding or retaliating to cyber bullying may make matter worse or even get you into trouble

Screenshot
Take a screenshot of anything that you think could be cyber bullying and keep a record of it.

Block and Report
Most online platforms have this feature, if someone bothers you, make sure you block and report the offender to the social media platform.

Talk about it
Cyber bullying may affect you in many different ways. Do not feel that you are alone. Let your parents and teachers know what is going on. Never keep it to yourself.

Be Private
Keep your social media privacy settings high and do not connect with anybody who you do not know offline. You would not talk to random people on the street, so why do it online?

Be Aware
Remain updated with all the preventive and security measures in the cyber world.

Be Safe in Cyber World

विद्ययाऽमृतमश्नुते
एन सी ई आर टी
NCERT

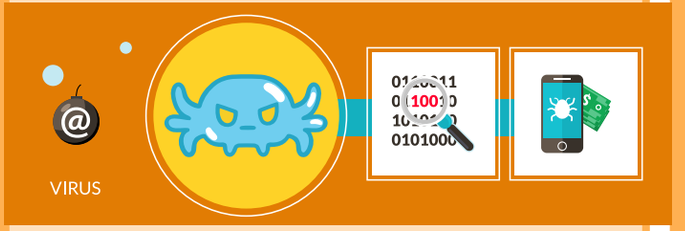
Central Institute of Educational Technology (CIET),
National Council of Educational Research and Training (NCERT)
Sri Aurobindo Marg, New Delhi-110016

Tel. : 011-26962580, Fax : +91 112686 4141
Email: jdciet.ncert@nic.in, jointdirector@ciet.nic.in
ncert.nic.in | ciet.ncert.gov.in

Basics of Cyber Safety and Security

What is Cyber Safety and Security?

Cyber safety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful to other people online, and using good Internet etiquette. It includes body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.



Computer Safety and Security

- Log off your computer when not in use and don't leave it un-attended
- Do not plug the computer directly to the wall outlet as power surges may destroy computer. Instead, use a stabilizer to plug a computer
- Do not install pirated software
- Do not connect unknown devices to your computer as they may contain viruses
- Use only verified open source or licensed software and operating systems
- Check that antivirus software in each system is regularly updated
- Invest in a robust firewall
- Consider blocking of file extension such as .bat, .cmd, .exe, .pif by using content filtering software
- Have a password protocol with specific strong password guidelines, frequently change your passwords, prevents reuse of old passwords
- Ensure that computer system and labs are assisted only by authorized personnel
- Discourage use of personal devices on the network, such as personal USBs or hard drives

Internet Safety and Ethics

- Respect other people's privacy
- Follow proper protocol in language use while chatting, blogging and emailing
- Do not log in to other people's email accounts
- Do not download and use copyrighted material
- Enable automatic browser update to ensure detection of malicious sites

Safe Email Practices

- Do not reply to emails from unknown sender even if it looks like a genuine email
- Do not provide personal information like name, date of birth, school name, address, parent's names or any other information
- Do not fall for lucrative offers/discounts as they might be coming from unknown source and it may not be reliable. Ignore/delete those mails
- Do not open attachments or click on links from unknown senders, since they may contain malicious files that might affect your device. Only click the links and downloads from websites that you trust
- Beware of phishing websites - check the URL to confirm if the website is secure
- Do not forward spam or suspicious emails to others

Safe Social Networking

- Avoid revealing too much of your personal information like your age, address, telephone number, school name etc. as this can lead to identity theft
- Set your privacy settings very carefully on social networking sites
- Never reveal your password to anyone other than your parent or guardian
- Communicate and collaborate only with people known to you
- Do not post anything which hurts others' feelings
- Always be careful while posting photographs, videos and any other sensitive information in social networking sites as they leave digital footprints which stay online forever
- Do not post your friends' information on networking sites, which may possibly put them at risk. Protect your friends' privacy by not posting the group photos, school names, locations, age, etc.
- Avoid posting your plans and activities on networking sites
- Do not create fake profiles for yourself on any social networking sites. If you suspect that your social networking account details have been compromised or stolen, report immediately to the support team of networking site
- Do not forward anything that you read on social media without verifying it from a trusted source
- Always avoid opening links and attachment through social networking sites
- Never leave your account unattended after login, log out immediately when you are not using it