Be Safe in Cyber World

DO's & DON'Ts

for Students

विद्यया ऽमृतमश्नुते

एन सी ई आर टी
NCERT

DEVELOPMENT COMMITTEE

Chairperson

Prof. Amarendra Behera, Joint Director, Central Institute of Educational Technology (CIET), NCERT, New Delhi.

Member Coordinator

Dr. Angel Rathnabai, Assistant Professor, Central Institute of Educational Technology (CIET), NCERT, New Delhi.

Member

Prof. M.U. Paily, RIE-NCERT, Mysuru, Karnataka

Dr. Indu Kumar, Associate Professor and Head, DICT&TD, CIET - NCERT, New Delhi.

Dr. Mohd. Mamur Ali, Assistant Professor, CIET- NCERT, New Delhi.

Dr. Rejaul Karim Barbhuiya, Assistant Professor, DESM - NCERT, New Delhi.

Dr. Ramanujam Meganathan, Associate Professor, DEL - NCERT, New Delhi.

D. Varada M. Nikalje, Associate Professor, DEE - NCERT, New Delhi.

Ms. Surbhi, Assistant Professor, CIET - NCERT, New Delhi.

Mr. I L Narasimha Rao, Project Manager II, Center for Development of Advanced Computing (CDAC), Hyderabad, Telangana.

Ms. Sujata Mukherjee, Global Research and APAC Outreach Lead, Google India Pvt Ltd, Hyderabad, Telangana.

Capt. Vineet Kumar, Founder and President, Cyber Peace Foundation, Ranchi, Jharkand.

Ms. Chandni Agarwal (National ICT Awardee), Head, Department of Computer Science, Maharaja Agrasen Model School, New Delhi.

Ms. Vineeta Garg, Head, Department of Computer Science, Shaheed Rajpal DAV Public School, New Delhi.

Internet, the most interactive technological platform of this century, has become an integral part of our daily lives. It is a learning and communication tool that offers us a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination. Internet ethics involves our approach while using it for different purposes. We should be aware that we should always be honest and respect the rights and property of others on the web.

Cybersafety is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). Here are some tips to keep you safe online.

DO's

1. Respect the privacy of others.
2. Report and flag content that is abusive or illegal.
3. Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.
4. Use an alias/ alternate name as username when you interact/ chat with others online.
5. Report online bullying immediately to the teacher and parents/ or some one whom you trust.
6. Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s).
7. Keep the browser, operating system and antivirus up-to-date.
8. Obtain software from trusted sources. Always scan files before opening them.

DO's

9. Lock your screen when you're finished using your computer/ tablet/ phone. Further, set it to lock automatically when it goes to sleep.
10. Check to see if the web address begins with https:// whenever you sign in online.
11. Make privacy settings in social media accounts in such a way that profile and posts are visible only to close friends and acquaintances.
12. Connect only with known individuals.
13. Be mindful of your digital reputation - think twice before you post something embarrassing, harmful or inappropriate.
14. Report to the service provider immediately if the account is hacked. If possible deactivate your account.

DON'Ts

1. Don't share your personal information: real name, date of birth, phone number etc. unnecessarily.
2. Don't send your pictures to unknown persons or share them on social media.
3. Don't open emails and attachments from strangers.
4. Don't respond to any suspicious email, instant message or web page asking for personal information.
5. Don't enter a password when someone is sitting beside you as they may see it.
6. Don't share your password with anyone.
7. Don't save your username and password on the browser.
8. Don't steal other's information.
9. Don't access or use files without the permission of the owner.

DON'Ts

10. Don't copy software which has copyright without the author's permission.
11. Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
12. Don't use someone else's password even if it is shared with you.
13. Don't log in as someone else to read their emails or mess with their online profiles.
14. Don't attempt to infect or in any way try to make someone else's computer unusable.
15. Don't meet unknown (even if they are known only through online interaction) people alone; always inform an adult or a friend.
16. Don't open or download any attachments from an unknown source as they may contain viruses.

For more details visit

www.ncert.nic.in
www.ciet.nic.in
www.ictcurriculum.gov.in
www.infosecawareness.in
www.cyberswachhtakendra.gov.in

Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Aurbindo Marg, New Delhi-110016

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

विद्यया ऽ मृतमश्नुते
एन सी ई आर टी
NCERT

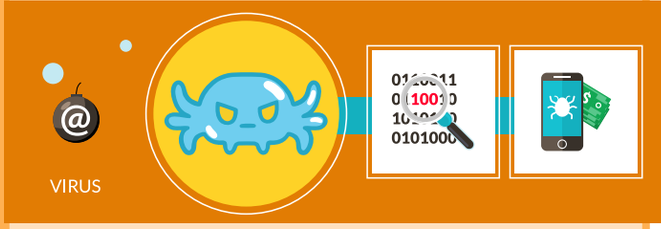
Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Aurobindo Marg, New Delhi- 110016

Tel. :- 011-26962580 | Fax :- 011-26864141
E-mail:- jdciet.ncert@nic.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 & don't leave them 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 assist 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
- Do 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