Documentation on Awareness Programme for Children on Safe use of Social Networks

School Student Helpline, OSEPA
School & Mass Education Department
Govt of Odisha

Introduction:

Fast-paced technological innovation and widespread accessibility of information and communication technology (ICT) have transformed societies around the world. **ICT** refers to technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums. Most of the Children have access to computers and mobile technologies from an early age which makes it easier for criminals to target children in ways that were not previously possible. Children are particularly vulnerable to the exploitation of online predators because they rely heavily on networking websites for social interaction. Offenders use false identities in chat rooms to trap victims into physical meetings, thus connecting to the worlds of cyber and physical crime. When this happens, virtual crime often leads to traditional forms of child abuse and exploitation such as trafficking and sex tourism.

Objective:

Cyber-crimes against children are on the raise. Some illegal persons try to defame children by sending obscene e-mails, by online chatting, developing pornographic videos where children are depicted in compromising positions mostly created without their consent, spoofing e-mails, altering of images for pornographic content etc. In order to keep the children away from such incidents, School Student Helpline, OPEPA has organized an awareness programme regarding the safe use of Mobile Phones, Computers, Internet and other social networks.

Strategy & Target Group:

Direct sharing with the children will have a better result than any other means. In order to disseminate the message directly to the target group, a detail discussion points were developed and circulated to all the Upper primary as well as High schools with a clear cut instructions regarding mode of transaction. The said programme was organized in all upper primary schools as well as in High schools on 17th April 2018. All the children from class VI to X along with their parents participated in the programme. A total 22679 number of schools have been covered under this programme. Different issues regarding safety of the children on use of social network are given below:
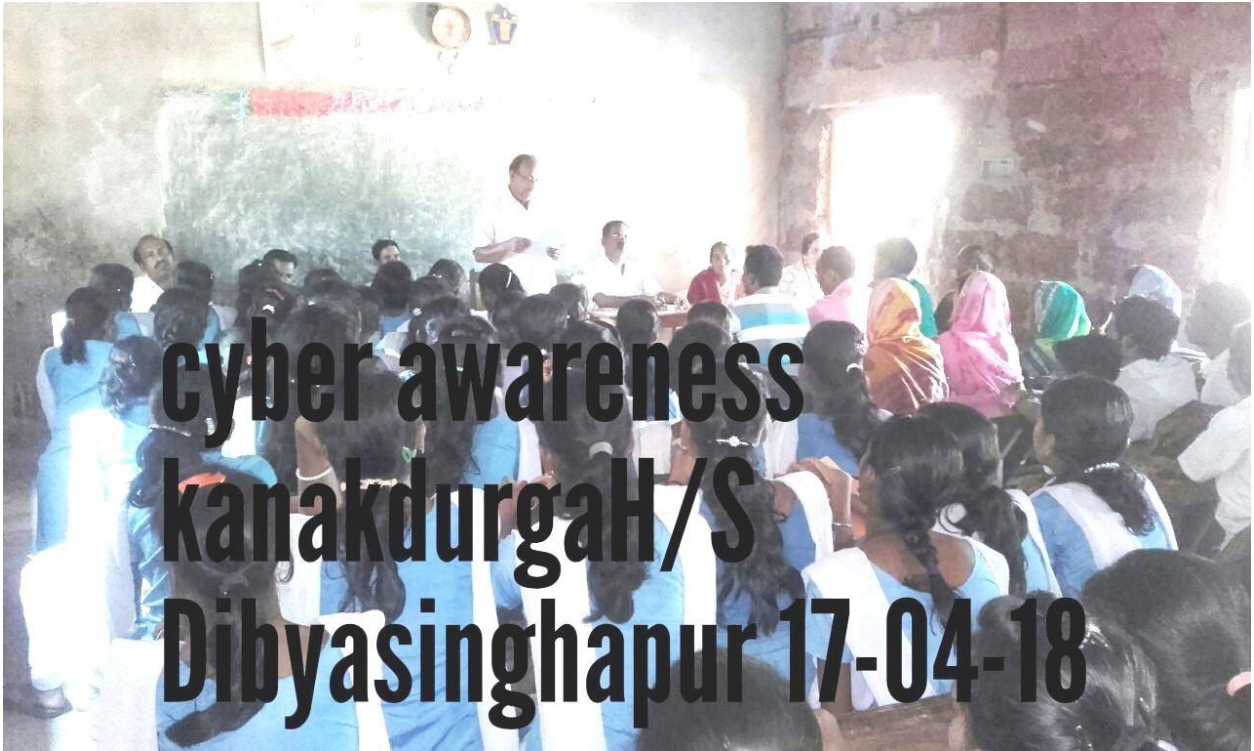

Boxma High School, Sambalpur

Safety Measures

- Usually children use to access others computer. While using somebody else's computer, open the file with due permission of the owner & don't try to steal information.

- The users should keep secrecy of their User ID and Password. Otherwise if it is accessible to any outsider then he may misuse the account by posting vulgar messages as a result of which there is possibility of being ashamed in the friends circle.

- Don't put any personal and sensitive information about one's family details, addresses, photographs which may be misused.

Bilana Sahayog Nodal High School, Bhadrak, Odisha

- Most of the sites provide option for privacy settings to keep the personal information secure. As a network user one should use them to prevent attackers from viewing the personal information. Set the privacy settings accordingly.(whatsapp/instagram/face book)

- If any one wants to meet social networking friends personally, he/she should think before meeting the person as it may not be a true identity posted on the website. Further one should meet the person during day time and with intimation to the parents.

- Before accepting friend request in Facebook one should ensure how far the person is known. If he/she is an unknown person there is possibility of developing intimacy, get into his confidence and later start blackmailing taking the weak points. Sometimes he never hesitates to pressurize for doing illegal things without the knowledge of ones parents.

- Use at least 8 characters or more to create a password.The more number of characters we use, the more secure is our password. For example, create a password consisting of a combination of lowercase, uppercase, numerical and special characters etc. Change the password at once whenever it is felt that the account is accessed by somebody else.

- One or single password should not be used for different networks.

- Never share the password with Cyber Cafe Owner or anyone else to access your mail. One should know the use of computer before going to the cyber café.

- All the downloaded materials to be deleted soon after the work is over in cyber café.

- Use of public Wi-Fi Installed in public places like railway station, bus stand, aerodrome etc. should be avoided as they are ripe for exploitation by hackers. Further never access online banking transactions in Public Wi-Fi Zone.

Kanakdurga High School, Ganjam, Odisha

- During surfing the Internet, one should always check about the browser security to avoid risks of exposing personal information. Very often before leaving the computer one can notice display of "Remember my ID /Password on this computer" with two options such as ' Save' and ' Never' on the screen. In such case 'never' option to be clicked to keep the password secured. Always make sure to logout properly before leaving the Cyber cafe.

- While using the computer in the cyber cafe don't leave the computer unattended with any information on the screen.

- In cyber café always ensure to use the computer having loaded with anti-virus.

- All the applications that are running on the computer are to be closed to avoid any error while downloading any file otherwise there is possibility of corrupt of those files.

- Never download any file like music, video, games etc. from untrusted sites. Otherwise the computer may be affected with virus.

- Every site has a prefix either // https // or //http//. //https// is a secure one. Hence before opening any site check its authenticity and proceed.

- Sometimes while working on the computer some dirty words/pictures appear on the website which is for the promotion of illegal sites. If such things happen just close the window no matter how important the work is, otherwise spyware may be installed in your PC from such websites as a result of which your data can be transformed easily to other computers.

Jagannath Vidyamandir, Jagatsinghpur, Odisha

- Don't accept anything that offers free download because that may contain malicious software.

Bahada Jhola Govt ME, Nayagarh, Odisha

- Read carefully before you click on install or run application. That means one should go through the **terms and conditions** of the software prior to install of any application.
- Prior to download any information from the website, ensure its originality first and then proceed.
- Bluetooth connection in mobile to be kept in an inactive mode, and should be activated at the time of data transfer.
- MMS messages received from unknown user should be deleted without opening it otherwise there is possibility of hacking of mobile

- **Don't keep** the **Tethering Mode / Hot Spot (Wi –Fi) always ON**. If so when one enters into the open Wi-Fi zone, mobile will be automatically accessed to it which may cause hacking of personal data of the mobile.

- It is advisable not to store important information like credit card No, bank account No, pass word etc. in a mobile phone. It is dangerous if it falls in the hands of a stranger.

- The IMEI code which is written on the backside of the cell phone should be noted in a safe place. **(*#06#).** If the mobile is missing, the owner can block the phone by using the IMEI code and prevent access to the stolen mobile.

- Regularly backup of important data in mobile phone or laptop is to be done to avoid loss of data due to software problem.

- Prior to open any given link, its authenticity is to be verified.

- Before sharing any information to any person or organization one should ensure the purpose for which it is collected.

- Reply to the unknown messages received through mail or mobile should be avoided. If so the phone number or mail ID may be automatically added with the unknown group that may create problem in future.

- All financial benefits (Lottery) received through mail or mobile are fake which may lead to bankruptcy.

- Please don't use mobile when it is in charging

Behavioural Changes of an Addicted Child:

Excess use of anything will be reflected on the behavior of the person . Similarly when a child is addicted to social network a number of behavioral deviations are found .The Resource persons had a vivid discussion on the above issue the detail of which is given below:

- Spends more and more time with the computer or mobile
- The child seems excited while he/she is with computer or mobile in comparison to other things.
- Most of the times it becomes difficult to divert the child from the computer. If so he/she will be aggrieved, depressed or irritated.

Govt. Upgraded High School, Mandasahi, Jagatsinghpur

- The child ignores family and friends.
- The child habituated in telling lie as well as hide things.
- The child remains inattentive in classroom.

Role of Parents

Parents at home have the responsibility to keep an eye on their ward regarding use of social network. The resource persons have shared the following points with the parents how to monitor the use of social network by the children. If it is felt that the child's performance in school is declining, maintaining distance with the family members, avoiding friends etc, then it is the first duty of the parents to identify the reason. If it is due to use of

social network, according to the gravity of the issue following steps are to be taken:

- If the child is demonstrating strong symptoms of Internet addiction, advice of any professional counselor is to be taken.

- Parent should assess his/her own online habits. Before cautioning the child parents are to check their habit as they are the role model of the children.

- Instead of putting complete ban on Internet, guide them which sites they can access,

- The computer should be placed in common place so that one can know the sites the child is accessing.

- Encourage and support your child's participation in other activities - particularly physical activities.

Conclusion: As per the feedbacks received from the field, it reveals that the programme has a good response. Both children and parents have actively participated in the programme. Most of the school head masters have opined that in the present society such type of awareness is very much essential to prevent children from misuse of social networks.

****