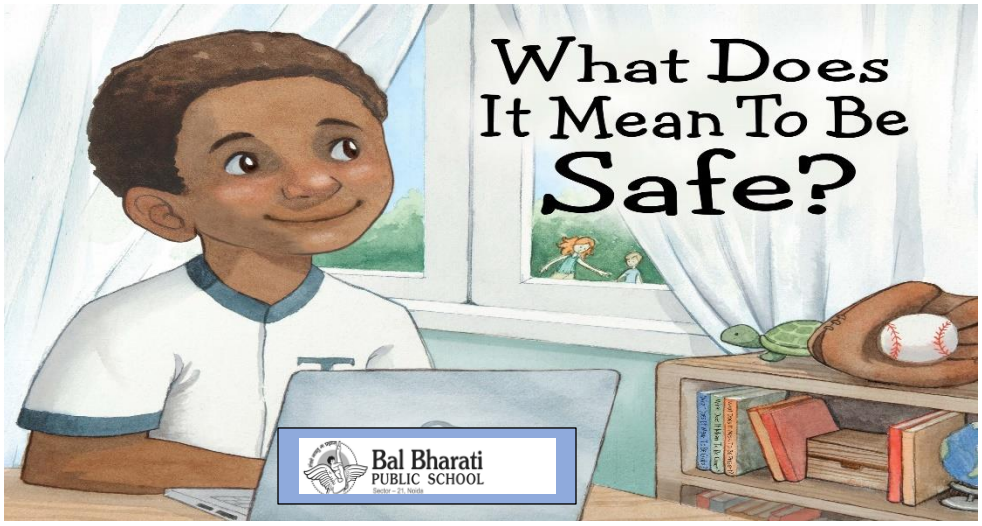
HANDOUTS ON CYBER AWARENESS

CLASS VI TO VIII (TERM I)



UNDERSTANDING INTERNET

Cybersecurity

What is Cyber Security?

Cyber security is a branch of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damages or unauthorized access.

The concept of Cyber security has become very relevant as the users of these devices are prone to direct or an indirect attack in a friendly or not so friendly way from those who have intentions to exploit them physically, financially, on account of terrorism or to the extent beyond imagination of these individuals.

Types of cyber risks:

Cyber risks can be divided into three distinct types:

Cyber crime

- Conducted by individuals or organized groups. Cyber criminals are intent on extracting money, data or causing disruption. Cybercrime can take many forms, including the acquisition of credit/debit card data and intellectual property, and impairing the operations of a website or service.

Cyber war

- A nation or a state conducting a sabotage or an espionage against another nation in order to create a law and order problem or to disrupt economy.

Cyber terror

- An organization, working independently of any nation or a state, conducts terrorist activities through the medium of cyberspace.

Major Issues concerning children:

- Almost every child in the urban or semi urban society is hooked to the internet
- These children start using internet as early as at the age of 7yrs
- These Children are very inquisitive and thus, try everything new
- The Internet offers them a world of glamorous opportunities

CYBERSPACE

What is Cyber Space?

CYBERSPACE**,** is a "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure..

cyberspace as a term was taken to describe the "location" in which people interact with each other while using the Internet. This is the place in which online games occur, the land of chat rooms, and the home of instant-messaging conversations.

How to protect your cyberspace?

1. Before entering our username and password in a website to logon, always check the URL of the website. If it is a fake webpage it will be showing a different URL.
2. Never store passwords in an email account as these are most often broken into.
3. If you think a website is unsafe, you can check it on the webpage by entering the URL safewebnorton.com in your browser's webpage.
4. Keep your broadband connection off when not in use and close the cover of your laptop when not in use to avoid misuse of its webcam.
5. Always secure your WiFi modem with passwords. Also avoid getting connected to Free Internet WiFi access zones that may leak your personal information to anyone.
6. Beware of Card readers at a store or petrol pumps. Use your debit/credit card at trusted places only. Also beware while using them on the Internet.Use them only at trusted websites.
7. Avoid using pen drives with data in computers that you do not trust. If you have to take data there, take formatted pen drives with only the required data in it.
8. Always install a legally purchased good antivirus on your computer. It will save you from all spywares and other harmful programs.

E-crime It occurs when computers, or any other electronic communication equipment or devices (such as mobile phones or the internet), are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

E-crime may be bank theft, identity theft, sending offensive messages or cyber bullying through newsgroups, chat rooms etc.

PROTECTING YOURSELF

It has become as easy to fall prey to a cyber crime as it is to press the 'like' button on Facebook. Given below are few ways to prevent you from being hacked and scammed.

When online

- **Personal Information**. Don't give out personal information without your parents' permission. This means you should not share your last name, home address, school name, or telephone number. Remember, just because someone asks for information about you does not mean you have to tell them anything about yourself!
- **Screen Name**. When creating your screen name, do not include personal information like your last name or date of birth.
- **Passwords**. Don't share your password with anyone but your parents. When you use a public computer make sure you logout of the accounts you've accessed before leaving the terminal.
- **Photos**. Don't post photos or videos online without getting your parents' permission.
- **Online Friends**. Don't agree to meet an online friend unless you have your parents' permission. Unfortunately, sometimes people pretend to be people they aren't. Remember that not everything you read online is true.
- **Online Ads**. Don't buy anything online without talking to your parents first. Some ads may try to trick you by offering free things or telling you that you have won something as a way of collecting your personal information.
- **Downloading**. Talk to your parents before you open an email attachment or download software. Attachments sometimes contain viruses. Never open an attachment from someone you don't know.
- **Bullying**. Don't send or respond to mean or insulting messages. Tell your parents if you receive one. If something happens online that makes you feel uncomfortable, talk to your parents or to a teacher at school.
- **Social Networking**. Many social networking websites (e.g., Facebook, Twitter, Second Life and MySpace) and blog hosting websites have minimum age requirements to signup. These requirements are there to protect you!
- **Research.** Talk to your librarian, teacher or parent about safe and accurate websites for research. The public library offers lots of resources. If you use online information in a school project, make sure you explain where you got the information.

While Playing games Create a family e-mail address for signing up for online games.

1. Use antivirus and antispyware programs.
2. Be cautious about opening files attached e-mail messages or instant messages.
3. Verify the authenticity and security of downloaded files and new software.
4. Use a firewall.
5. Never download softwares and games from unknown websites.
6. Beware of clicking links, images and and pop ups in the websites as they may contain a virus and harm the computer
7. Never give personal information over the Internet while downloading games.
8. Some free games may contain virus, so be cautious and refer while downloading them.
9. Patch and update your application software.

Against Social Engineering

Social engineering is the art of manipulating people so they disclose confidential information.

1. Don't open attachments or click on links in emails from people you don't know.
2. Be particular about what you install on your computer.
3. Learn to trust your instincts and believe in yourself.

Against Cookies.

Cookies are data sent from a website and stored in a user's web browser while a user is browsing a website. These cookies contain your personal information and allow the website company to build a profile of sites that you visit over time.

1. Disable cookies by going to the web browser→ Tools button→Internet Options→Privacy tab→ Block all cookies by Slider rule.

Your Computer

1. Keep your systems free of vulnerabilities by using licensed Operating System.
2. Installing Antivirus software.
3. Running Antivirus software regularly
4. Using a firewall.

WHEN TO GO ONLINE?

Age for going online

Children live and breathe this environment as "digital natives". Excluding them from the digital world could prove to be a disadvantage for their development.

We, therefore, need to ensure that minors are able to use online services under adequate supervision of their parents and teachers and are even further protected with the help of suitable safety tools, such as parental controls, as well as adherence to good practices. Remember, Children normally access those various online services – such as social networks or other adult oriented sites which have not been developed for them. Also services, such as email, prohibit children under the age of 13 from creating an account. However, in both cases, no mechanisms have been put in place to enable the user's age to be verified, given that any date of birth can be used to fulfill the requirements. Additionally, the checks used can be easily sidestepped.

Digital Footprints

Digital footprint or digital shadow refers to one's unique set of traceable digital activities, actions, contributions and communications that are manifested on the Internet or on digital devices.

There are two main classifications for digital footprints: passive and active. A passive digital footprint is created when data is collected without the owner knowing, where as active digital footprints are created when personal data is released deliberately by a user for the purpose of sharing information about oneself by means of websites or social media

COPPA

The main reason why children under 13 are not allowed to have an email address or a social network profile is the law protecting child privacy, commonly known as COPPA (Children's Online Privacy Protection Act), which companies have to comply with.

So, there is an urgent need to inculcate safe online habit. Since Internet is a reality & cannot be wished away and you cannot block sites exclusively for the children, so

- Children must learn how to Pause & Think before they connect online.
- Children must learn to be safe and alert on the Internet.

The Mantra of online safety is **'Pause & Think before you Connect!'**

Precautions That Children Must Take

Limit your online friends to people you already know.

Change privacy settings to restrict who can see and post on your profile on Face book, Whatsapp etc. Don't stick with the defaults.

While online …

Seek guidance before participating in any online activity.

Most Apps are interested in your personal data.

You decide whether they are worth the privacy loss ?

Don't think that instagram, whatsapp, facebook or snapchat are free. If you create your account on any of these social networking apps or, games, you are giving your personal data, chats, pics and personal videos to these companies which later on sell to the other companies for purposes like sending ads, schemes etc. Even from your chats, they analyze your taste, your interest and the group opinions about popular eating points, movies, places, dresses, etc. Not only this data is used by the entrepreneurs to expand or start a new business but can also become a real security threat for the user.

Children need to be aware of loading up PCs, tablets, phones, with applications that have not been approved or checked out.

Be careful on pop up messages like "you won" or "you will get free", just ignore the message.

While installing any app or software always read the instructions carefully.

HANDOUT 5

CYBER BULLYING

“Cyber Bullying is the use of the Internet and related technologies to harm other people in a deliberate, repeated, and hostile manner."

Types of Cyber Bullying

Flaming

Online fights using electronic messages with angry and vulgar language.

Aman and Abhay online exchange got angrier and angrier. Insults were flying. Aman warned Abhay to watch his back in school the next day.

Harassment

Repeatedly sending nasty, mean, and insulting messages.

Sara reported to the Principal that Kayla was bullying another student. When Sara got home, she had 35 angry messages in her e-mail box. The anonymous cruel messages kept coming - some from complete strangers.

Denigration

"Dissing" someone online. Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.

Some boys created a "We Hate Joe" Web site where they posted jokes, cartoons, gossip, and rumors, all dissing Joe.

Impersonation

Pretending to be someone else and sending or posting material to get that person in trouble or danger or to damage that person's reputation or friendships.

Laura watched closely as Emma logged on to her account and discovered her password. Later, Laura logged on to Emma's account and sent a hurtful message to Emma's boyfriend, Adam.

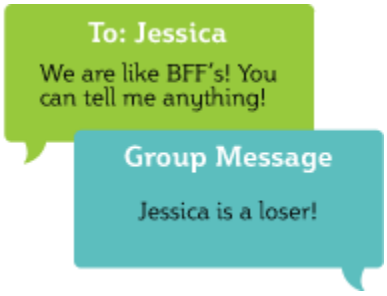
Outing

Sharing someone's secrets or embarrassing information or images online.

Greg, an obese high school student, was changing in the locker room after gym class. Matt took a picture of him with his cell phone camera. Within seconds, the picture was flying around the phones at school.

Trickery

Talking someone into revealing secrets or embarrassing information, then sharing it online.



Katie sent a message to Jessica pretending to be her friend and asking lots of questions. Jessica responded, sharing really personal information. Katie forwarded the message to lots of other people with her own comment, "Jessica is a loser."

Exclusion

Intentionally and cruelly excluding someone from an online group.

Millie tries hard to fit in with a group of girls at school. She recently got on the "outs" with a leader in this group. Now Millie has been blocked from the friendship links of all of the girls.

Cyberstalking

Repeated, intense harassment and denigration that includes threats or creates significant fear.

When Annie broke up with Sam, he sent her many angry, threatening, pleading messages. He spread nasty rumors about her to her friends and posted a sexually suggestive picture she had given him in a sex-oriented discussion group, along with her e-mail address and cell phone number.

Laws of Cyber Bullying

Common Cyberbully targets are kids in their pre-teen years. Online conflicts will sometimes start in the real world and then transfer into the virtual world. Bullying is pushed to the virtual world because cyberbullies are mostly, if not completely, anonymous.

This gives the cyberbully the false idea that their actions have no repercussions. Now that more and more kids have cell phones, cyberbullying often takes place through texting and picture messaging as well.

Civil Laws

In this case, a victim should try to resolve this problem by seeing a bully's parents or asking an attorney for advice on how to handle the situation.

Criminal Laws

When a bully is accused of breaking criminal laws, they can be subject to prosecution and even arrest.

How to prevent Cyber bullying?

Guidelines to use the internet safely:

I. Don't give out personal information such as your address or phone number.
II. Do not share passwords, user names, account IDs or PINs with anyone besides your parents.
III. Do not share other people's personal information or say things that might violate the safety or rights of others, even if you mean it as a 'joke'.
IV. Do not leave the ICT devices unattended.
V. Don't become online 'friends' with people you don't know.
VI. Don't open emails or attachments from people you don't know.
VII. Never arrange to meet someone in person who you have met online.
VIII. If anything you see or read online worries you, tell your parents/teachers about it.
IX. Never give out personal details in messenger or in personal profiles.
X. Remember that people may not be who they say they are.
XI. Don't send pictures to strangers.
XII. Most reputable chat rooms allow you to block messages from a particular sender.
XIII. Be careful about who you share photos with.
XIV. Use social network's privacy settings so only your friends can see your stuff.
XV. What you do not do in real life, don't do on the internet. This includes all kinds of cyber bullying using text, photos and videos.

HANDOUT 6

CYBER ETHICS & SOFTWARE PIRACY

What is Computer Ethics?

Ethics is a set of moral principles that govern the behavior of a group or individual. Therefore, computer ethics is set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society.

Ten rules of Computer Ethics that one should follow

1. Do not use a computer to harm other people.
2. Do not interfere with other's computer work.
3. Do not snoop around in other's compute files.
4. Do not use a computer to steal.
5. Do not use a computer to bear false witness.
6. Do not copy or use proprietary software for which one has not paid.
7. Do not use other's computer resources without authorization or proper compensation.
8. Do not use appropriate other's intellectual output.
9. Be aware of the social consequences of the program written or system designed by you.
10. Use a computer in ways that insure consideration and respect for one's fellow humans.

What is Software Piracy?

Software Piracy is the illegal reproduction and distribution of the software applications
End User Piracy. All softwares are licensed. When someone copies software without the appropriate license for each copy, it is called end-user piracy
Internet Piracy- Unuathorised copies downloaded over the Internet falls under Internet piracy
Pre-Installed Software Piracy – When a computer manufacturer takes one copy of a particular software and illegally installs it on more than one computer, it performs pre-installed software policy.
Counterfeiting- People making duplicate CDs of original software and sell them low price This activity falls under counterfeiting.
Online Auction Piracy- This is selling of software that is never authorized for resale by a third party.

HANDOUT 7

CYBER POLICY

What is the Need for Cyber Policy?

"To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation".

School Cyber Policy

This policy applies whenever students are using Bal Bharati Public School Information Technology equipment, services and/or resources, whether such equipment, service and/or resources is being used at school or home.

I. Students must not eat/drink near the IT devices.
II. Must respect school equipment and should not indulge in moving the IT equipments and/or cables.
III. Students must not cause damage to any equipment. If they spot any damage, they must inform the teachers immediately.
IV. Must not use flash drives or any other external media(Cell phone, hard disk, CD, camera etc.) for the purpose of
    a. Saving or transferring the work
    b. Installing new software without due permission from the computer faculty.
V. Viewing social media sites/registering on any website/downloading any material for use must be under the strict supervision of the teacher.
VI. In the computer lab, Internet access is allowed only after permission from computer faculty and the computer faculty reserved the right to check IDs of the users.
VII. Students are not allowed to bring equipment such as iPad, iPod, PSP, mobile phones etc. to the school. Any such equipment confiscated from the students will be kept in the school.
VIII. Students must report incidents of Cyber Bullying and misuse of IT resources to their teachers/parents immediately.

What happens if a student breaches the Bal Bharati Public School's Cyber Policy:

If you breach this policy, you will be subjected to Bal Bharati Public School Behavior Management Policy.

I. Minor breaches (like installing new software, accessing internet, brining IT devices to devices without prior permission of the concerned teacher etc.) of this policy will result in the suspension period of two weeks.
II. Major breaches (like cyber bullying, identity theft etc.) of this policy will result in the suspension period of up to ten weeks.
III. If you behave online in a manner that threatens the well being of another child, student, parent or member of the school community, even if this occurs off-site and or out of the school hours, the Principal/VP/HM has the authority to take appropriate action.
IV. When it is suspected that a personal electronic device such as a mobile phone is used to capture images of a crime (such as an assault), or contains any other evidence of a crime, the device will be confiscated and handed to the police.
V. If the Principal suspects an electronic crime has been committed, this will be reported to the Police Department. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device such as a notebook, computer etc., and the device will be confiscated and handed to the investigating police officer. The police will determine any further action.
VI. These actions may be taken even if the alleged incident occurs off site and /or out of school hours.