Online Safety

Pause and think
Before you connect

Primary wing

Class: 3 to 5

Content:

INTERNET – A BLESING IN DISGUISE

Introduction:

The internet is one of the most important changes that have happened in the way we live and work. It began life in an American military research agency. Its inventors would not have foreseen how it would develop over time. The internet now spans the world connecting billions of people in their everyday life.

What is Internet?

The Internet, sometimes called “the Net," is a network of networks in which users at any one computer can, if they have permission, get information from any other computer. Today, the Internet is a facility accessible to hundreds of millions of people worldwide.

Note that no one owns the internet. This is because each part of it is made of individual networks that someone has put together and then connected to the internet. However each network has to obey the internet standards in order to connect.

Uses of the internet

Internet has many uses some of the major ones include:

- **Research and Homework**

The internet is a fantastic place to research information for a project or a piece of work. It does not matter what topic you are looking for you can guarantee that you will find something on the subject.

- **Communication:**

The internet opens up many different possible ways to communicate with others.

- emails
- Social networking sites
- Chatrooms
- Forums etc

❖ **Shopping**

Whatever you want to buy you can pretty much guarantee that you will definitely get it on the computer at competitive prices.

❖ **Leisure and Entertainment**

There are many activities that you can choose to do online in your leisure time. They include

- Playing games
- Listening to music
- Reading online books e-books.
- Keeping yourself updated with news and sports and events
- Watching TV programs o the computers, etc.

❖ **Exploring the world**

The internet has many services that help you in exploring the world. Like:

- Satellite and mapping applications
- Travel sites providing details of other places
- Live web cameras showing other parts of the world
- Almanacs and encyclopedias.

Benefits of the Internet:

- **Always available.**

  The internet is always available for you to use. You don't have to wait for it. It is just there when you need it and for whatever you need.
- **Vast range of information**

  Think of any search term and type it on to the search engine. You will end up finding websites with information on the search term.
- **Easy to contact people**

  The internet enables us to be in touch with our near and dear ones with options like emails, chat rooms, VoIP and video calls.
- **Up to date**

  One of the main advantages of the internet is how fast things are updated and made available.in case of the newspaper's we have to wait for the next day to get information on the topic. Even news on the television takes longer to get to us than the internet.

Computer Ethics:

Computer ethics is a set of moral principles that govern the usage of computers. Some of the rules that the individuals should follow while using the computer are:

1. Do not use computers to harm other users.
2. Do not use computers to steal others information.
3. Do not access files without the permission of the owner.
4. Do not copy copyrighted software's without the author's permission.
5. Respect the privacy of others
6. Complain about illegal communications and activities.
7. Always safeguard your personal information.

Cyber Ethics:

Cyber ethics is a code of behavior for using the internet .acceptable behavior on the internet is very much the same as the acceptable behavior in everyday life.

Basic cyber ethics includes:

1. do not send email or chat with strangers .
2. do not forward the content received from a stranger.
3. never pretend to be someone else on the internet.
4. avoid bad and abusive language.
5. do not download the copyrighted material.

Threats involving the internet:

Students today are growing up digital. They are increasingly using digital technologies to learn, socialise and communicate, challenging the traditional concept of a school.

When students develop internet behaviours without guidance, problems are sure to occur. We hope that teaching students some key messages from a young age will help them navigate their way safely through the internet as they grow older.

Some of the threats associated with Internet are:

- Privacy
- Exposing your computer to unwanted softwares
- Contracting computer viruses
- Infringing Copyrights

Internet safety – dos and donts

1. Always ask an adult if you're unsure of anything when you are online.
2. Don't sign up for sites that are 13+ if you are not old enough (Facebook, YouTube, Instagram etc).
3. Remember YAPPY (the personal information you should **not** share online) – **Y**our full name, **a**ddress, **p**hone number, **p**asswords, **y**our plans.
4. Don't add people as online friends unless you know them in real life or have parent permission. Never arrange to meet an online friend without talking to a parent.
5. Remember that you cannot believe everything you read on the internet and you can't trust everything online friends tell you.
6. Choose sensible names for usernames, email addresses etc.
7. Talk to your parents about what you're doing online and let them know when you're going on the internet.
8. Know what cyber bullying is and tell someone if you think it's happening to you. Cyber bullying is when someone picks on you, annoys, embarrasses, or threatens you over and over again using technology, such as the internet or a phone.
9. Protect your digital footprint: don't put anything online that you wouldn't want all your friends, family, teachers and future employers to see.
10. Treat others online the way you'd like to be treated.

Cyber space:

Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks l to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to your friend, you could say you sent the message to her through cyberspace.

Major Challenges

The three major challenges that are associated with cyber space are:

- Inappropriate conduct
- Inappropriate content
- Inappropriate contact

How to overcome the challenges:

A child must always:

- Seek guidance before participating in any online activity.
- Do not get involved in any unethical activity. Remember you are leaving behind your DIGITAL FOOTPRINTS.
- Be careful on pop up messages like "you won" or "you will get free", just ignore the message.
- Most Apps are interested in your personal data, so while installing any app or software always read the instructions carefully.
- Do not befriend or respond to messages from strangers.

Cyber security

What is Cyber Security?

Cyber security is a branch of technologies, 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 extend beyond imagination of these individuals.

Cybersecurity involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people.

The various threats associated with cybersecurity are:

- **Cyber crime**

  Conducted by individuals or organized groups. Cyber criminals are intent on extracting money, data or causing disruption. Cyber crime 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 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. **:** A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer bases attack against computers, network, and the information stored on them.

Cyber Threat:

What is Cyber threat ?

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet.

a**.** Inappropriate Content

The Internet is chock-full of "inappropriate content." Your children may try Searching for such content, or they may stumble upon it accidentally. Regardless, it's very easy to find if the websites containing the content are not Blocked.

b. Chat Room "Friends"

Some predators enter chat rooms or use social media to find young children. They befriend them by pretending to be their age, and usually try to meet up at some point. Online Scams. Children are very vulnerable to them as well. Common scams include emails claiming you've won large sums of money and requesting payments to receive said "winnings," websites offering something for a low price but never explaining what it is exactly; and essentially anything that's extremely cheap or free.

What is Spam Mail?

Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware.

What is Phishing?

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

What is Spyware?

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as keylogging), passwords, and other valuable data.

What is malware?

This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner.

What is a Virus?

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

What is Cyber Crime?

Criminal activities carried out by means of computers or the Internet.

Here are just a few of the ways that kids could fall for the tricks of cybercriminals:

- **Search engine links.** Typically when something big happens in the world – breaking news, a long-awaited movie, the latest iPhone or video game – we rush to the web to find out more. Finding information on a search engine like Google is a great way to get the information you're looking for fast. Cybercriminals pay attention to these types of events and set up camp right in the midst of the results of your search. They'll create fake but legitimate-looking websites that mimic a site that would likely have the information you're looking for, and will make sure that when you search, their link is one of the first you'll see and hopefully click. By going to these links, you might be further tricked into downloading something you never intended to, or your system could be infected by malicious software simply by visiting the link.

- **Enticing offers.** Kids might be drawn to online offers for popular products, movies, music, or games which cybercriminals offer using cleverly designed tactics to get kids to click, download, or enter personal information for the chance to get their hands on one of these things. Sometimes the offers are sent via text, as a fake "like" that one of their friends supposedly posted on their Facebook stream, or as an ad that looks like a game so they will click on it.

- **Fake mobile apps.** With the enormous popularity of apps, it's no surprise criminals have found a way to wiggle onto smart phones by creating false versions of popular, legitimate apps. In the app stores, it's sometimes tough to tell which ones might be fake because they're disguised so well.

Cyber laws

Here is some basic guidance to give your kids i.e Cyber safety:

- **Practice thinking critically** about the things you read, post, and download. Not everything you come across online is necessarily as it might appear. Take the time to consider this before you do anything online.
- **Stick to well-known websites and online services** for downloading music, games, or movies. If you're unsure if a site is fake or safe, it's best not to visit it. Or ask your parents or other adult before visiting it.
- **Choose online passwords that are not easy** for someone to figure out. Pick a word or phrase that mixes letters, numbers, symbols, uppercase and lower case letters to make it as strong as possible. Don't use the same password for every site or service. One way is to come up with a pattern and change 1-2 characters in the pattern for each site or service you use a password for.
- **Use privacy settings** wherever they are available and use the strongest level possible. And resist sharing personal information online such as home address, phone number, and birth date in emails, texts, blogs, or social network updates. Even with privacy settings, anything you post can still be shared by those who see it, so think before you say or do anything online.
- **If you need to enter personal information** online, enter the least amount necessary. Make sure the website begins with "https" (not http) which is more secure. Also look for information at the bottom of the webpage verifying that the site is secure or has been verified by an outside party to be secure
- **If you think you may have done something** wrong and may have fallen for a cybercriminal's trick, let your parent or other adult know so they can check and fix things if necessary.
- Sending pictures to strangers is the biggest NO!
- Do not download any content. If something needs to be saved or downloaded for school work, you should always check with either of your parents. Otherwise you might download malware as well.
- Computers and internet services should always be used as tools for gaining knowledge and wisdom.

- Parents should discourage the use of any unnecessary websites. One can contact the internet service provider (ISP) regarding any possibility of filtration or blocking such websites.
- It is responsibility of parents to teach children about the importance of password use on the internet. Passwords should never be disclosed to a third person.
- At the time of registration, several websites ask for important information about the user that includes family address, telephone number, school/college name, credit card or calling card number and picture of the user. One should abstain from providing such personal and family information to anyone on the computer network who is not known personally. There are people who can use this information for trapping children.
- Children and teenagers can use internet for a variety of purposes including using it to complete schoolwork, visiting museums located in faraway places and learning more about universities and colleges. However, one should be really careful about downloading programs from the internet.
- It is important to consult a parent regarding the websites to browse on the internet. Parents should always know about their child's online activities. It is important to talk to the child about the possible dangers on the internet.

What to do if you Encounter Illegal Material

- If you come across content that you consider to be illegal such as child abuse images or criminally obscene adult material, you should report this to the IWF: **www.iwf.org.uk.**
- If you come across content that you consider illegal such as racist or terrorist content, you should report this to the **Police.**

Cyber policy of bbps Noida:

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 equipment's 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.

Guidelines for Parents:

I. Place the computer in an open area in your home – not in your children's bedroom.
II. Set clear expectations for your children, based on age and maturity.
III. Install parental control (content filtering) software.
IV. Learn internet basics, be approachable and lead by example.

Tips for parents to avoid and identify cyber bullying:

I. Discuss any changes in mood or behavior with them. If you concerned, help your child to stay connected to friends and family they trust.
II. Talk to your child about cyber bullying before it happens.
III. Be aware of what your child is doing online and explore it with them.
IV. Keep the lines of communication open so your child will be comfortable talking about if something is worrying them. Help your child to develop the skills they need to interact safely and respectfully online. Guide their online activities and help them learn to communicate appropriately with friends and family.
V. Help your child to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly.

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.