

Table of Contents

Module 1: Getting Started with Cyber Wellness

Activity 1: Introducing Yourself	1.2
Activity 2: How Cyber Smart are You?	1.2
Activity 3: What is Cyber Wellness?	1.4
Activity 4: Cyber Wellness Values	1.7

Module 2: Threats to Cyber Wellness

Activity 1: Common Threats to Cyber Wellness	2.1
Activity 2: STOP. THINK. CONNECT.	2.7
Activity 3: Dealing with Threats to Cyber Wellness	2.10
Activity 4: Smartphone Safety	2.13

Module 3: Safety for Social Media

Activity 1: My Social Media Favourite	3.1
Activity 2: Social Media Interaction	3.3
Activity 3: Bystander or Upstander?	3.6
Activity 4: My Social Media Safety Card	3.8
Activity 5: Legal Protection in the Digital Age	3.10

Module 4: The Road Ahead

Activity 1: Take your Manners Along	4.1
Activity 2: What is your IIQ- Internet Intelligence Quotient?	4.2
Activity 3: Your Workshop Learning	4.4
Activity 4: Wrap-Up	4.4

Appendix

Appendix A- Copyright Infringement and Laws	A.01
Appendix B - Frequently Asked Questions	B.01
Appendix C- What is Personal Information?	C.01
Appendix D- Protective Measures for Cyber Safety	D.01
Appendix E- Popular Social Media Sites and Apps	E.01
Appendix F- Social Media Safety Tips	F.01
Appendix G- Scenario-based Questions	G.01

Module 1

Getting Started with Cyber Wellness

Welcome to the **Intel® Education Digital Wellness Workshop!**

Description: All of us today have a parallel existence. This shows up as our online identity on social media sites, gaming portals, discussion forums, learning communities and even personal blogs and websites. While using the Internet everyday has become more of a need than a choice in an ever-connected world, it can do more harm than good if we lose sight of the right motivations and values, and fail to create a balance between our online and offline life. We are also increasingly facing challenges such as cyber bullying, inappropriate behaviour, identity theft, gaming addiction, virus attacks and more. As we become more cyber-smart every day, we also become more cyber-endangered. In this module you will learn what cyber wellness implies, why it is needed in today's world and the values that promote cyber wellness.

Initiate a discussion by asking participants about how often they use the Internet. Ask simple questions like 'Do you have a computer or laptop at home?' 'How much time do you spend on the Internet?', 'Do you access the Internet on your mobile?' Direct their attention to their regular use of the Internet and how this makes it necessary for them to operate safely and responsibly in an online world. Introduce the objectives of the workshop.

Workshop Overview: The Intel® Education Digital Wellness Workshop focuses on how you can create, promote and enjoy a healthy and safe cyber-environment. This workshop is designed to help you build skills and inculcate values which will prepare you to navigate safely in cyberspace, act in a balanced and responsible manner while using the Internet, cultivate respect in your interactions with others and build a healthy cyber-culture.

This workshop will:

1. Make you aware of the benefits and dangers of using the Internet
2. Nurture a strong character through cyber wellness values
3. Familiarise you with types of cyber threats, consequences and protective measures
4. Prepare you to make responsible and informed decisions in cyberspace

Activity 1: Introducing Yourself (15 minutes)

This is an ice breaker activity. Direct the participants to interview their partners and then introduce them to the larger group. As they introduce, make appropriate comments to engage the participants. Note down some of the most commonly mentioned Internet activities on a whiteboard/flip-chart. Direct the attention of the participants to how each of them uses the Internet to talk, shop or play!

A good way to start any workshop is by getting to know the other participants. In this activity, you will have an opportunity to introduce yourself and meet other participants. So, let's start!

1. Divide into pairs as instructed by your facilitator.
2. Find out as much information about your partner as you can in 2-3 minutes: name, hobbies and favourite Internet activity. You can decide between yourselves which person gets to conduct the mini interview first. The second person can then follow with the same information about themselves.
3. When asked by the facilitator to introduce your assigned partner to the larger group, use only two descriptors to do so- a hobby and the favourite Internet activity. For example: "My partner today is Poornima. She loves to paint and her favourite Internet activity is *playing scrabble online*."

Activity 2: How Cyber Smart are You? (10 minutes)

We have already seen how often we use the Internet for schoolwork, recreation and even to seek information. Let's find out how much you already know about safe online behaviour. Answer the questions below:

1. While using a public discussion forum, you should ideally:
 - a. Use your real name
 - b. Use a Nickname
 - c. Use your friend's name

2. You should accept all friendship requests on social networking sites even if you don't know the person:
 - a. Always
 - b. Sometimes
 - c. Never
3. A group of users in a forum where you discuss television shows is asking you to share your photograph. You should:
 - a. upload your latest and best photograph
 - b. share someone else's photograph
 - c. politely decline to share photographs
4. A Webpal has invited you to meet in person. You should:
 - a. accept the invitation
 - b. inform a parent or trusted adult and take advice
 - c. take another friend along for the meeting
5. You have to write a report for a school project. You complete it by:
 - a. copy-pasting information from various websites
 - b. reading information on websites and rephrasing them
 - c. understanding information on websites and then writing in your own words

This activity has been included to assess the participants' awareness of cyber safety.

Guide the participants to answer the questions listed in the activity.

Discuss the questions and review their answers to gauge their knowledge. Conclude by pointing out how the frequent use of Internet makes it important for us to know about proper online conduct.

For your reference, answers to the quiz are as follows:

1. b
2. c
3. c
4. b
5. c

The Internet has completely changed the way we do things. Be it work, socialising, learning, having fun or even communicating, we have digital technologies to support us. While this makes our communication and interaction a lot easier and quicker, not everyone uses the Internet in an appropriate and lawful manner. We need to make an effort to ensure that, as Internet users, we act responsibly and make the Internet safe for ourselves and others.

Activity 3: What is Cyber Wellness? (15 minutes)

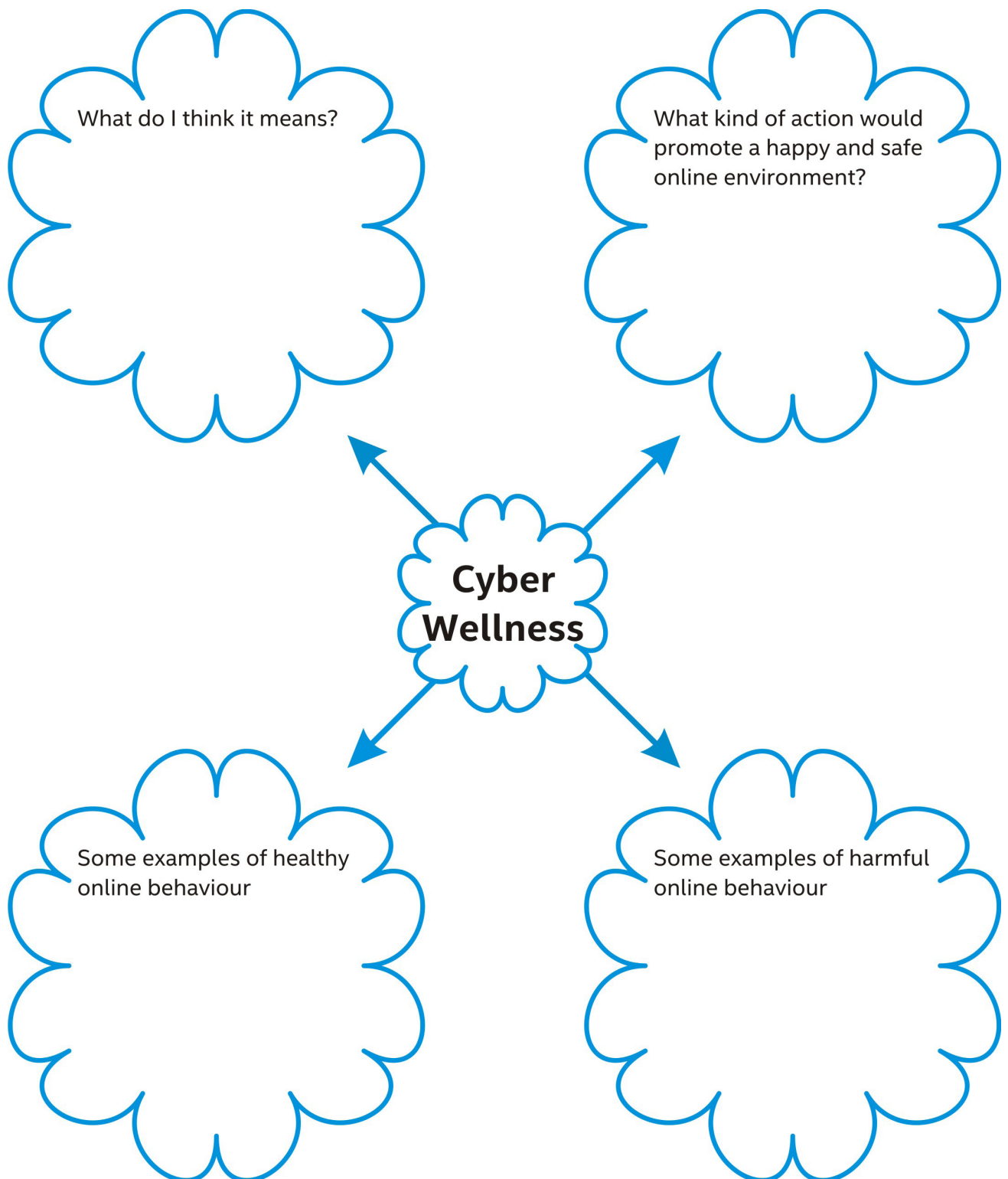
This activity has been designed to jump-start thoughts on the meaning of cyber wellness and what it implies. Discuss the meaning of wellness and encourage the participants to think of what it would imply in cyberspace. Once the participants have finished the word cloud template, spend a few minutes discussing the responses. Use the discussion as the springboard for the next activity.

Wellness is most commonly defined as an active process of becoming aware of, and making choices toward, a healthy and fulfilling life. The concept of wellness lays emphasis on the whole individual and the understanding that our health is affected by all that we do, think and believe. It is a proactive approach that promotes an optimum manner of physical and social functioning and leads to emotional well-being.

If we were to take the term wellness to cyberspace, what would it imply? Going by the definition of wellness, it would entail an awareness of and making such choices towards feeling good and safe in our online interaction with others and thereby living a more stress free life. How can we then define cyber wellness? What kind of choices would lead to cyber wellness?

In this activity, you will reflect on the term cyber wellness and what it means to you. How do you envision a state of cyber wellness?

Note down your thoughts in the Word Cloud Template on Cyber Wellness.



My Thoughts on Cyber Wellness

Now that you have some idea about Cyber Wellness and what kind of actions promote it, let us try and gain a more in-depth understanding of the term.

According to the Media Development Authority, Singapore, Cyber Wellness refers to the positive well-being of Internet users and a healthy cyber culture for the Internet community. It involves an understanding of the risks of harmful online behaviour, an awareness of how to protect oneself and other Internet users from such behaviour, and a recognition of the power of the Internet to benefit oneself and the community at large.

Cyber Wellness is a broad term that is inclusive of Cyber Ethics, Cyber Security and Cyber Safety.



The three aspects of Cyber Wellness can be understood as below:

- a.** Cyber Ethics- refers to appropriate, responsible and ethical online behaviour that governs all our interaction with other Internet users and emphasizes on the exercise of cyber values.
- b.** Cyber Security- refers to the protection of our computer systems, devices and networks from any unauthorized access or misuse by others.
- c.** Cyber Safety- refers to following safe practices that minimize the risks of being harmed by the dangerous behaviour of others such as cyber-bullying and stalking.

In a technology-driven society where we spend most of our time online participating in friendly chats or games, searching for information, reading posts or just watching videos, promoting cyber wellness is necessary for our safety and well-being.

Activity 4: Cyber Wellness Values (20 minutes)

We now understand what cyber wellness is and why it is needed. However, it is equally important to identify the values that promote cyber wellness. It is the practice of these values that will help us act in a manner that ensures a healthy environment for the Internet community.

In this activity, you will identify cyber wellness values and learn how they are practiced in an online environment.

There are five cyber wellness values hidden in the Values Grid. Can you find these values?

Cyber Wellness Values Grid



Start with examples of healthy and harmful online behaviour that participants have shared in the previous activity. Point out that if we want to promote cyber wellness we need to focus on healthy online behaviour and this is possible if we follow cyber wellness values. Ask the participants to search for the cyber wellness values in the grid. Conclude with linking these values to proper online conduct. Share the examples provided and encourage the participants to come up with some examples of their own. They can note them the space provided.

The Cyber Wellness values can be located in the grid as follows:



Can you find the Cyber Wellness Values hidden in the grid?

- 1) Responsibility
- 2) Compassion
- 3) Respect
- 4) Integrity
- 5) Resilience

Let us now see how these values promote cyber wellness.

Value 1- Responsibility

Responsibility is being accountable for your behaviour. An example of being responsible as an Internet user would be to play online games only for a fixed and reasonable amount of time.

Value 2- Respect

To respect others is to have a regard for them and be appreciative of them. An example of being respectful would be to communicate politely with others while writing emails or posting comments on a blog or in a discussion forum.

Value 3- Compassion

Compassion is a feeling of wanting to help someone in trouble. For example, you are being compassionate if you are supporting a friend who is being cyber bullied by reporting the act to parents, teachers or any other person of authority.

Value 4- Resilience

Resilience is the ability to recover from an undesirable change or incident. An example of being resilient would be to respond appropriately and not give up if you have faced any disturbing experience online.

Value 5- Integrity

Integrity is the quality of being honest and fair. For example, if you follow copyright regulations and do not copy-paste content from other sources for your school assignments then you are exercising integrity.

Write down an example of how you follow cyber wellness values when you are using the Internet.

Value 1- Responsibility

Value 2- Respect

Value 3- Compassion

Value 4- Resilience

Value 5- Integrity

The Internet today is an indispensable part of our lives. This makes it important for us to know not only how to protect ourselves but also be discerning about the online activities we participate in, what we read and watch and how we conduct ourselves. While you may take care to follow cyber wellness values, not everyone is favourably inclined towards proper conduct. Many Internet users do not engage in lawful and appropriate behaviour and may even try to cause harm to others.

In the next module you will learn about the risks you face in cyberspace and the forms they can take. You will also find out how you can minimize these risks and protect yourself from harmful online behaviour.

Conclude the module by telling that participants that though they may act properly in an online environment, others may not. There are people who harm others through their online activities. Hence, apart from an awareness of values to follow, there should also be an awareness of risks they may face in cyberspace. This awareness of risks and protective measures will prepare them to take informed decisions. In the next module they will learn about how they can keep themselves safe from those who may cause them harm.

Module 2

Threats to Cyber Wellness

Description: The Internet opens several opportunities that you would never be able to avail otherwise. You can see places you have never travelled to, communicate with friends across the globe, get information on anything anytime, and create an online reputation that allows you to present yourself as you desire to be seen by the world. However, with all of these come risks. You may stumble across a website that displays inappropriate content, your email or social networking account could be hacked and misused, someone could misinterpret what you posted and respond with hurtful comments or you could be embarrassed by photos or information that gets associated with your online profile. It is therefore very important to know how you can avoid risks and keep yourself safe on the Web. In this module, you will identify threats to cyber wellness, understand their implications and learn how to protect yourself from these threats.

Activity 1: Common Threats to Cyber Wellness (45 minutes)

Technology is so much a part of our lives today that it seems unimaginable to spend even a day, unplugged and away from our smartphones, laptops, tablets or other gadgets that drive our activities and interaction. While most of us feel life without the Internet is impossible, it is not too early to consider the consequences of spending most of our time online.

In this activity you will learn to identify the types of threats you may face on the Internet. All these threats obstruct cyber wellness and a healthy cyber culture.

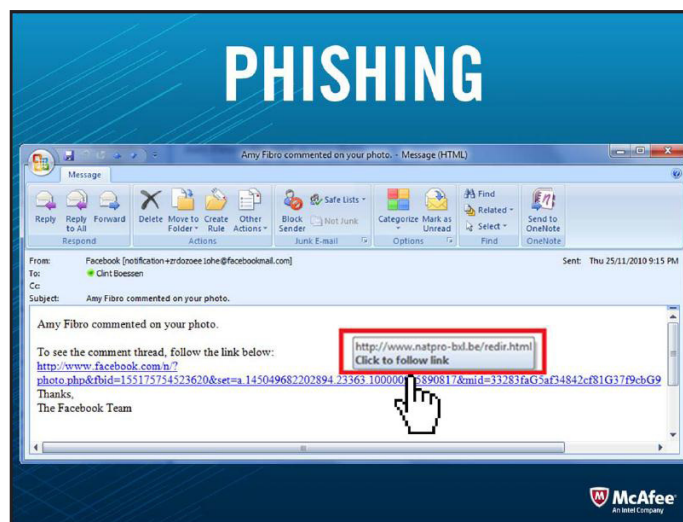
Step 1: Learning about Threats

Take a few minutes to read about some threats often faced in cyber space.

- **Cyber Bullying-** Cyber bullying is using technology to harass someone, by sending or posting mean, threatening and intimidating messages. Examples of cyber bullying include abusive emails, malicious posts on social networking sites, inappropriate image tagging, uploading of embarrassing photographs, creating fake profiles or Web sites designed to hurt another person and so on. Cyber bullying has serious emotional consequences and can leave the victims of bullying depressed and anxious with lowered self-esteem and suicidal thoughts.

Give the participants a few minutes to read the information given about the threats to cyber wellness. Encourage them to reflect on whether they have faced these threats while they were using the Internet.

- Cyber Predators-** Cyber predators are adults who exploit children and teenagers by using Internet communication tools such as mobile phones, chat rooms, social networking sites and even email. Their main motive is sexual abuse. They use attention, affection, kindness and sympathy while interacting to manipulate children and teenagers into thinking they care and thus build online relationships. Once trust is established and sensitive information is gained, they arrange for personal meetings often ending in great emotional and physical harm to the child or teenager.
- Gaming Addiction-** Gaming addiction is an excessive or compulsive use of online games at the cost of health, education, real life social engagements and even cleanliness. Last year it was added to the Diagnostic and Statistical Manual of Mental Disorders published by the American Psychiatric Association. Left untreated, gaming addiction can lead to social isolation, mood swings and an inability to cope with real life.
- Identity Theft-** Identity theft is a fast growing cyber threat where a person makes unauthorised use of someone else's name and personal information such as passwords, usernames, banking or financial data to commit theft or other crimes. It often occurs through a data breach, virus or phishing scams. Phishing scams are called so because they aim to 'fish' for personal information that will allow access to important data, money and other financial assets.



A phisher will masquerade as a trustworthy business or person, like Facebook for example. The 'bait' is in the electronic communication like this email. Sometimes you will see clues that it's a phony- like misspelled words, links, or buttons. If there is a link or button, hover your cursor over it, and the actual URL will appear. If they don't match, as in this example, DON'T click on the link, or you could mistakenly put your device, or your personal information at risk. Here's another good piece of advice: If you receive an email from an organization asking YOU to reset your password, chances are, it's a phishing attempt.

- **Copyright Infringement and Plagiarism-** Copyright Infringement takes place when a person copies, distributes, publicly performs or displays copyrighted work without the permission of the author or creator. Plagiarism is presenting someone else's work as your own. The work may or may not be copyrighted. For example, copying a sonnet written by Shakespeare and claiming it to be your work is plagiarism but not copyright infringement as it is a work in public domain. To know more about copyright infringement read **Appendix A- Copyright Infringement and Law**.
- **Malware-** A Malware, short for 'malicious software', is software that gets installed on your laptop, desktop computer or smartphone and performs a multitude of undesirable tasks such as stealing passwords, deleting files or reformatting the hard disk.



Common examples of malware include viruses, worms, Trojan horses and spyware:

- Virus: Computer program files capable of attaching to disks or other files and replicating repeatedly, without user knowledge or permission.
- Worms: Parasitic programs that replicate, but do NOT infect other computer program files. They can send copies to other computers via a network.
- Trojan Horse: A seemingly harmless program that you knowingly download. What you don't know is that it also conceals a destructive back door that will allow attackers access to your system.
- Spyware: Exploits infected computers for commercial gain, delivering unsolicited pop-up ads and monitor web browsing activity, among other things.

Some common ways by which a virus spreads include opening emails with harmful links or attachments, downloading infected mobile apps and clicking on mystery links shared at social networking sites. A good firewall and security software package can help protect against these types of threats. To protect your computer and keep it clean (free of infected files or contaminated software), you can check it with a [free virus scan](http://home.mcafee.com/downloads/free-virus-scan) (<http://home.mcafee.com/downloads/free-virus-scan>). You can also install the [McAfee Site Advisor](http://www.siteadvisor.com/) (<http://www.siteadvisor.com/>) which is a free and powerful, lightweight security app that secures your browsers and keeps you protected from all kinds of digital dangers. Its primary mission is to block and warn you of malicious sites that might be loaded with malware, or setup to steal your passwords.

In your spare time, do read through **Appendix B- Frequently Asked Questions** to learn more about Online Safety.

Think of the cyber wellness values you learned about in the previous module- Responsibility, Respect, Compassion, Resilience and Integrity. Do the threats that you have just read about violate these values? How?

Divide into small groups as instructed by your facilitator. Discuss your answers and note them in the space provided. Be prepared to share your answers with the other participants.

Step 2: Recognising Threats

Now that you know about various threats and how they violate cyber wellness values, read about Umesh's disturbing experience on the Internet and see if you can recognise the ones that he had to face.

Cyber Friends or Cyber Fiends?

Umesh was a bright 15 year old, moderately good at sports with a keen interest in debating activities till he was introduced to online gaming by some of his friends. In no time at all, Umesh became skilled at the games he was playing and started to win many of his role-playing bouts. He became emotionally attached to his gaming avatar and increasing scores kept him spending longer hours, day after day, hooked to the screen. His deep involvement led to joining gaming groups where he started to chat about his high scores and strategies and received admiration and appreciation for his skills. He started to spend more time with his friends in the forum than those in his school, finding greater acceptance in these online relationships. He stopped taking calls from his school friends and avoided hanging out with them. However, things soon started to go wrong. After an argument with some long time forum members who then ganged up against him, he began to receive threats and harassing messages. One of the forum members Rajan, however, has been very sympathetic and has asked for a private discussion on phone. A talk with Rajan to figure out a solution seems too hard to resist and the only way out to the depressed and scared Umesh. He does not want to tell his parents as he fears they will not let him use the Internet and he has already lost most of his close school friends due to his extensive gaming. He now feels he has no one.

Working in a small group, discuss and answer the questions that follow:

Which threats did Umesh expose himself to through his online activities?

How were these threats affecting Umesh's well-being?

What could Umesh have done differently?

Should Umesh talk to Rajan? Why or Why not?

What should Umesh do now?

Share your answers with the other participants.

Much like Umesh, many young Internet users across the globe leave themselves vulnerable to various threats. Umesh was not able to take the right steps at the right time to avoid his online experience turning from something he thought was fun to something he wished he hadn't started. Being able to decide what you must or must not do on the Internet requires thought, common sense and a commitment to cyber wellness values.

Activity 2: STOP. THINK. CONNECT. (30 minutes)

Whether you are using the internet for work or recreation, you will come across where several instances where you will have to decide whether you should perform certain actions or not. It is at these times that your ability to make a sensible choice will pave the way for a pleasant and safe online experience.

Staying safe on the Internet requires taking some common sense steps so that you can enjoy any online experience without negative consequences.

When you're about to cross the street you stop and check for oncoming traffic. The same rule applies when you're going on the Internet—you need to STOP and THINK before you CONNECT.

Start the activity by letting the participants know that we expose ourselves to threats through our online activities and behaviour. Hence it is very important to exercise judgment and be sensible while using the Internet. Ask them to review the list of activities and answer the questions for each of the steps of STOP, THINK and CONNECT.



Before you take any action on the Internet you must **STOP** to understand the risks that may be involved, **THINK** about the impact of the action on your safety and only then **CONNECT** or take the action. The three steps of STOP, THINK and CONNECT help you to guard and maintain your online safety.

Listed below are some of the most common online activities. Answer the questions for each step to decide whether you should engage in the activity or not. An example has been provided to help you get started.

Be prepared to share your decision and the reasons behind it with other participants.

For your reference, answers to the activity are as follows:

Online Activity 1- We should only click on links from trusted sources. Clicking on links that look suspicious, for example, those that have grammatical mistakes, awkward messages, grand announcements of a huge win and so forth, could infect the computer or device you are using with malware.

Online Activity 2- Do not download from any site unless you are sure it's a reputed one. Use free plugins that help you gauge the safety of a site. Downloading files from anywhere could infect you device with malware.

Online Activity 3- Yes, the Internet can be a valuable source of information on any topic. As long as you have a good anti-virus software installed, browsing different sites for information and resources on topics of interest is definitely helpful. Make sure you don't copy-paste all the content! Plagiarism and copyright violations can be serious offences.

Online Activity Example- Posting personal information such as the name of your school or phone number on social media sites. (To know more about what is considered personal information read **Appendix C- What is Personal Information?**)

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?
People other than friends and family could find out where I lived and studied.	It could lead to criminal acts such as theft or burglary at my house.	I will not post personal information on social media sites.

Online Activity 1- Clicking on a link in your email, or a Facebook post or smartphone message that announces a funny video of you.

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?

Online Activity 2- Downloading songs and movies from popular file sharing sites

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?

Online Activity 3- Researching various Web sites on environment protection for a school project assignment

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?

Online Activity 4- Uploading revealing selfies on Twitter that you think make you look attractive

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?

Online Activity 4- Uploading revealing selfies could bring unwanted attention and especially from people you don't know and who could be dangerous.

Online Activity 5- We shouldn't accept friend request from people we don't know as they maybe criminals, sex offenders or others who can cause harm.

Invite a few participants to share their decisions and encourage them to explain why they chose to go ahead and do something or not. Try and involve as many participants as you can. You can direct each participant to explain a decision s/he has taken for any one online activity. Ask the participants who are listening to raise objections and present their view point if they do not agree with what is being said.

Conclude the activity by stating that apart from thinking sensibly before we engage in online activities it is important to keep our devices safe by installing malware detection and anti-phishing software. Encourage them to use resources such as the McAfee free [virus scan](http://home.mcafee.com/downloads/free-virus-scan) (<http://home.mcafee.com/downloads/free-virus-scan>) or the [McAfee Site Advisor](http://www.siteadvisor.com/) (<http://www.siteadvisor.com/>)

Online Activity 5- Accepting friend requests from people you don't know

STOP	THINK	CONNECT
What could be the risks involved?	How could this affect my safety or my family's? What impact can this have?	Should I go ahead and do this?

Activity 3: Dealing with Threats to Cyber Wellness (30 minutes)

This activity has been included to assess the participants' ability to connect problems to the right solutions. It also gives them an opportunity to recognise the threat based on its description.

Instruct the participants to match the problem with the solution and name the threat being described (column A) in the last column.

Discuss the threats and their solutions. Encourage the participants to also offer alternate solutions that they feel may have worked for the incidents that have been mentioned.

For your reference, the answers to the activity are as follows:

1. Vikram can keep screenshots as evidence and report the incident. The threat he is facing is cyber bullying.
2. Tina can block the user. She may be facing a cyber-predator.
3. Priya can report to a person of authority as her work was copied. The threat she is facing is plagiarism and copyright infringement.
4. Jyoti should use a reputed anti-virus software and scan files before she downloads them. The threat she is facing is malware.
5. Raghav should ignore messages that ask for updating personal information via a link unless he has confirmed it is from the right source. The threat he is facing is identity theft via phishing.
6. Sameer should make a plan that regulates his internet time. The threat he is facing is gaming addiction.

As Internet users, all of us need to take a lead in creating a cyber-environment that promotes safety, mutual respect and positive communication. For all the actions that threaten cyber wellness, there are a number of protective measures that can be taken to control and minimize their occurrence and impact.

Match the threat described below (Column A) with the prevention strategy that can help minimize or eliminate it (Column B), then name the threat (Column C).

Column A What is happening?	Column B What can be done?	Column C Type of Threat
Akash has created a web site, posted mean comments and uploaded embarrassing pictures of Vikram after they had a big fight. The Web site also invites other students to state why they don't like Vikram.	Ignore any intimidating or supposedly official message that directs you to a link and requires the updating of personal information.	
Tina was in a chat room yesterday when a user who has been friendly to her for a while now asked her if she liked older men. He also expressed an interest in seeing her photograph.	Keep a look out for any suspicious activity and use a reputed anti-virus software to ensure that your machine is well protected. Scan files for viruses before you download them.	

Column A What is happening?	Column B What can be done?	Column C Type of Threat
<p>Priya was astonished to read one of her poems published on a popular poetry Web site under the name of another girl from her class. It had previously been published in the school magazine as a poem by Priya and therefore had been freely read and appreciated by many students.</p>	<p>Keep screenshots of content posted as evidence and report the incident to a parent or person of authority. Register an official complaint.</p>	
<p>Jyoti downloaded a greeting card sent to her yesterday. All through today she is unable to find some files she had stored on her laptop. She knows she did not delete them but cannot locate them.</p>	<p>Make a plan for a limited and reasonable amount of hours to be spent on the computer and do not keep your laptop or desktop computer in your bedroom.</p>	
<p>Raghav is a registered member of an online tutoring web site and has recently received an email with an update link that requires him to update all personal information on their Web site within a week failing which he will be blocked on the site.</p>	<p>Block the user that is making you feel uncomfortable with his/her comments and asking for personal information.</p>	

Column A What is happening?	Column B What can be done?	Column C Type of Threat
Sameer starts playing ConquerAll every night and continues till 4 in the morning. He has to start for school at 6:30 when his school bus arrives at the bus stop. He is always sleepy in class.	Make sure you report to a person of authority if you feel someone has stolen, copied or taken credit for your work as this is considered not just an unethical act but at times even an illegal one.	

Encourage the participants to reflect on their use of the Internet. Ask them to think of any instance where they were disturbed by their online experience. Ask them to note their thoughts on what happened and what they did or could have done in the space provided.

You now have a good idea about the Internet activities that can cause harm and how you can prevent the harm from growing. Think of a time when you or one of your friends felt disturbed by an online experience. Note down what you think you or anyone should do under similar circumstances.

A disturbing experience that I have faced

My prevention strategy

Give the participants some time to review the protective measures listed in Appendix D and attend to their queries, if any.

To know about other cyber safety measures, read **Appendix D- Cyber Safety**.

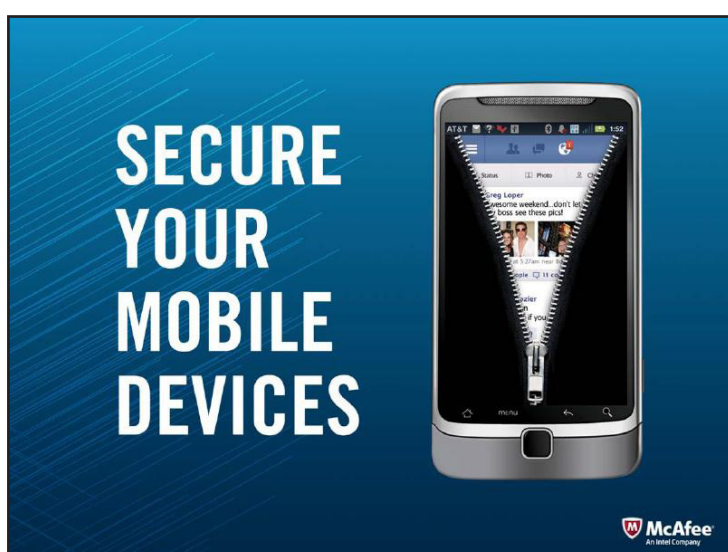
Also, share the **Tips for Parents** sheet with your parents. Prepared by McAfee it has useful tips that help make the Internet a safer place for you and your family. You may download it from the link below:

<http://www.mcafee.com/us/microsites/cybered/downloads/osk-parent-tips-resources-en.pdf>

You can also recommend the [McAfee Family safety blog](http://blogs.mcafee.com/category/consumer/family-safety) (<http://blogs.mcafee.com/category/consumer/family-safety>) to your parents. It provides the latest security tips and online trends to save you time, and keep your family safe.

Activity 4: Smartphone Safety(15 minutes)

Till a few years ago, mobile phones mainly came with the traditional SMS and Call features. With the advent of the mobile Internet or the ability to access the world wide Web through a phone, the risks that smartphone users face have increased. We regularly use our smartphones for surfing the Internet, downloading music and social networking apart from making calls. From private photos to videos and financial information along with a lot of information on our Contacts, there is plenty on our phones that could be misused in the wrong hands.



Spend a few minutes reading the Steps for Smartphone Safety.

S

Security Software- Use security software to protect your phone from malware attacks. Most malware apps also come with anti-theft options for your device. For example, you could use the [McAfee Mobile Security](https://www.mcafeemobilesecurity.com/) (<https://www.mcafeemobilesecurity.com/>), a reputed mobile security app, to protect your device, data, and your privacy.

M

Management of Settings- Explore the settings on your phone and customize them for location reporting, app installation, tracking online behaviour and also Wi-Fi Networking. Selecting strict options in settings allows you to fend off undesirable access to your personal information.

A

App Review- Avoid downloading apps that are not hosted at reputed app stores. If you download them from untested sites they may infect your phone with malware. When installing apps carefully review the terms and conditions of use to determine if you are giving access to information you don't want to share.



Restriction of Access- Lock your phone with a PIN Code or Pattern Lock. This ensures that even if your phone is stolen, the thief cannot immediately access information on it. You can then use security software to even remotely 'wipe off' or delete information on your phone.



Turn Off Public Wi-Fi- Do not use public Wi-Fi to shop or access emails. Public Wi-Fi hotspots can give hackers easy access to your phone. Use your network provider connection as it is much more secure.

Here are some safety tips offered by McAfee for your mobile device:

1. Set a passcode and configure it to automatically lock after a certain period of time. Keep it private.
2. Log out of your accounts like email and Facebook. (You should also remember to do this on your computer.)
3. DON'T keep ANY pictures on your phone that you wouldn't want others to see.
4. Read the user rating BEFORE downloading or installing apps and make sure they're from trusted sources. If the user ratings are negative, or if there aren't many ratings at all, it's a good indication that you shouldn't install it.

Give the participants some time to review the steps and invite them to share tips on how they ensure their phone remains safe to use.

What do you do to keep your smartphone safe? Use the space provided below to note down your tips for mobile security. Share your tips with the other participants.

Conclude the module by telling the participants that the most common use of technology devices such as smartphones and tablets is for social networking. This exposes users of social media tools to many risks. It is important to know how our social media activity can be protected from malicious or adverse actions of others. In the next module we will learn about safe use of social media sites and apps.

One of the most common uses of Internet today is connecting with others through social media tools. Most of us have Facebook*, Twitter*, LinkedIn* and Google* accounts. Instagram*, Snapchat*, Tumblr* and many other tools are also popular for sharing, viewing, commenting, collaborating and chatting. While this freedom to connect and share everything anytime is certainly welcome, it can often cause great harm to your online reputation if responsibility and discretion is not exercised. You need to be aware of safe social media practices and must understand the consequences of the choices you make and the decisions you take.

In the next module you will learn about how to use social media tools wisely so that your safety and well-being is ensured while connecting with others. You will also find out about the legal protection that is available to you in case you find yourself threatened by or are a victim of someone's malicious and harmful behaviour.

Module 3

Safety for Social Media

Description: The use of social media sites and apps continues to increase with their wide acceptance and popularity. Young users develop contacts, connect with friends, join groups based on common interest, share articles and personal information and even organize and host events, all of which leaves social networking sites continuously evolving and growing. With such fast expansion and adoption, however, comes greater risk. Racist, defamatory, abusive, provocative and inappropriate comments and content being published has become a regular and frequent occurrence. The threats to cyber wellness also extend to social media sites and because of their widespread use, are commonly faced by users of such sites. This makes it necessary to know how we can promote safe experiences and avoid the adverse effects of using social media. In this module you will learn about some popular social media sites and apps, understand how to use them responsibly and become familiar with the legal provisions that guard the safety of Internet users.

Start the module with a brief discussion on popular social networking sites and apps. Invite the participants to share how often and why they use social media sites and apps. Ask them if they have ever experienced or seen something on a social media site that made them uncomfortable. Lead them to realise that a lot of dangers lurk on such sites. Inform them that in this module they will learn about how they can make social networking safe and pleasant for themselves and others.

Activity 1: My Social Media Favourite (20 minutes)


Some of the commonly used social media tools by youth across the world are Facebook*, Twitter*, LinkedIn*, Google Plus*, Instagram* and Tumblr*. Take a look at some popular social media apps being used across the world in **Appendix E- Popular Social Media Sites and Apps**. Do you use any of these?

In this activity you will introduce your favourite social media site or app to the other participants and let them know why you prefer it over other alternatives.

Inform the participants that they will start this module with a short fun activity. Tell them to read about some popular social media apps commonly used across the world. Instruct them to pay attention to the age at which these apps can be used. Guide a brief discussion on which ones they use and what they like about it. They will then share their favourite social media site or app with others and also why they like using it and what they use it most for. Give them time to fill out the information required in the My Social Media Favourite Card. Invite the participants to share this information with others once they have completed the task. Note down the social media sites and apps that are mentioned most frequently, on a flip chart or whiteboard.

Which social media site or app do you use most often? What do you like most about it? What is the one feature that you would like to change in the app? Fill out the information required for the **My Social Media Favourite Card**. You can draw the logo in the box provided for the same.

My Social Media Favourite



(Site or App Logo)

Why I Like it Best-

What I Use it Most For-

What I would Like to Change-

Ask students if they know whether their favourite site/app is age-appropriate or not. Inform them that most popular sites/apps being used by kids all across the world are not meant for those less than 13 years of age. For those below 13, using these sites/apps is not legal. Guide them into a brief discussion on why it is important to use age-appropriate sites. Suggest alternate social networking sites/apps for kids below 13 years of age.

You are now familiar with the many ways in which social media sites or apps are used by you and others of your age. Many of these sites or apps, however, are not meant for those below 13 years of age. If you are younger than 13 and using certain popular social networking sites such as Facebook*, MySpace*, Twitter* and others, then you should know that this is not legally allowed. Although many of you may bypass the law to 'adjust your birthday' and gain access to these sites, it would be safer to use age-appropriate social networks. There are many other fun alternatives such as GiantHello*, KidSocial*, Kidzworld* and even Sweetie High* (a closed social network for girls and strong on privacy).

While using social media sites or apps for online activities you may come across instances where you may feel hurt, annoyed or disturbed because of how you have been treated by other users. You may also, at times, have participated in or initiated activities that targeted other users and made fun of them. The popularity of and easy access to social networking sites makes them a fertile ground for inappropriate activities such as sexting (sharing lewd messages and photos), cyber-bullying and identity theft. Because of the wide reach and impact of social media, it becomes important to know how to behave online such that it does not harm our reputation. Keep yourself up to date on the benefits and challenges of social networking by visiting educational sites like the [McAfee Security Advice Center](http://home.mcafee.com/AdviceCenter/Default.aspx) (<http://home.mcafee.com/AdviceCenter/Default.aspx>).

Activity 2: Social Media Interaction (30 minutes)

Not all activities on social media sites can be considered as safe and pleasant interaction. Some interactions leave us uncomfortable and looking for ways to avoid or end them. If what a user is doing makes you uncomfortable you need to trust your instinct and assume it may have harmful intent.

In this activity, you will use the **Social Media Interaction Matrix** to help you decide how you want to respond to an interaction. The horizontal axis of the matrix measures the risk you may associate with an interaction while the vertical axis measures the discomfort you may feel for the interaction.

DISCOMFORT	High	1. Avoid	2. Report
	Low	3. Carry On	4. Review
		Low	High

RISK

My Social Media Interaction Matrix

Inform the participants that this is a group activity and they will discuss the examples of social interaction, come to a consensus on the quadrants in which they would like to place these interactions and finally share their decisions with the other participants. Invite each group to share their filled out quadrant. You can ask participants to note down the activity numbers in the relevant quadrant.

For your references, answers are as follows:

Quadrant 1- Interactions 1, 2, 5 and 9

Quadrant 2- Interactions 3, 4, 6 and 10

Quadrant 3- Interaction 8

Quadrant 4- Interaction 7, verify by looking at the sender address to see if it is Facebook or not. Click on links only after verifying the source of the message.

In **quadrant 1**, you may note down activities that are not risky but make you uncomfortable. For example, you may feel uncomfortable being tagged in a picture that makes fun of an event or a person. These are activities you can then **Avoid** being a part of in the future and do what is needed to stop them for now such as blocking a user.

In **quadrant 2**, you may list the activities that are very risky and also make you very uncomfortable. For example, a stranger you recently met in a chat room and exchanged emails with is sending you intimate messages and insisting you meet. These are interactions you must **Report** to or tell a parent, teacher or a person of authority such as the concerned officer of the Web site security team and take their advice on dealing with them as they may become serious threats.

In **quadrant 3**, you may note down activities that are low on risk and don't make you uncomfortable. For example, sharing photo albums of your vacation with friends and telling them about the places you visited. These are activities we do most often and we can **Carry On** with them.

In **quadrant 4**, you may mention the activities that are very risky but do not make you uncomfortable. For example, opening a shopping Web site link in an email from an unknown person may not make you uncomfortable but it may carry high risk as it can be a phishing scam. These are interactions you must think about or **Review** before you act. Your review may lead to a change in your course of action or decision.

Given next are some interactions that may take place on any social networking site. Discuss with your group and place them in the relevant quadrant in the Social Media Interaction Matrix. Be prepared to share your opinion, with other groups, on why your group considered placing an interaction in a particular quadrant.

1. A Facebook friend you don't know very well suggests that you correct the grammar of your status message.

2. A friend tags you in a picture which makes fun of other classmates.

3. You receive a message with sexual overtones from a stranger you recently accepted as a friend on Facebook.

4. A person you met in a chat room claims to be a designer for a teen fashion magazine agent and is coaxing you to share your swim wear pictures for the next issue.

5. You commented on the dullness of a party. Some friends have now replied rudely and others are pressurizing you to remove your comment.

6. You have received a tweet. The message asks 'Do you remember this sexy one from your photos?' and provides you a link.

7. You have received a Facebook notification stating a friend has commented on your post. It has a button where you can click to see the comment.

8. You friends have recently started a book club and they have asked you to 'Like' the book club page on Facebook and post a comment.

9. You have received a tweet that you did not like as it mentioned that the user thought you had an attractive body.

10. You have been asked to look at a YouTube video by some of your friends. When you watch it you realise it is very violent and targets a minority community.

Give the participants a few minutes to reflect on their social media experiences. Encourage them to note down their thoughts in the space provided.

List some common interaction (s) that you have experienced on social media sites. Did any of them make you uncomfortable? Where would you place the interactions you have listed in the Social Media Interaction Matrix?

Activity 3: Bystander or Upstander? (20 minutes)

Ask the participants if they have ever faced instances where they were supported by their friends against others who were troubling them. Guide them to the realisation that everyone needs to stand up for the right actions and ensure that people are not treated harshly or unfairly. This is especially true for social media where anything posted or shared about a person can immediately be seen by millions of internet users. Discuss the terms Aggressor, Victim, Bystander and Upstander and give examples to ensure clarity.

It is undoubtedly important to know which social media interactions you need to avoid, ignore or review and which ones need a stricter response such as reporting or flagging. However, there are times when you may not be directly involved. Sometimes someone else may act in a manner that intends to hurt or harm others. At such times, we must strive to do the right thing. In every social media interaction that can be regarded as unpleasant, risky or harmful, there is usually an **aggressor** (person who targets others), a **victim** (the person who is targeted) and others who are simply observers. These observers have the choice to be **bystanders or upstanders**. They can choose to either ignore the incident (bystanders) or speak up for the victim (upstanders). The upstanders try and do the right thing. These upstanders help to spread cyber wellness, follow cyber wellness values, and promote a healthy cyber culture and environment that makes our online experiences safer and pleasant. For example, when upstanders see hurtful social media posts targeting someone, they try and be cyber-supportive by posting positive comments for the victim, asking the aggressor to stop, or if the incident seems to be escalating or becoming serious, reporting to social media sites, parents, teachers or other persons of authority.

Give the participants a few minutes to read the comic strip, reflect on the situation and formulate a response. Invite them to share their response with the other participants once they have completed the activity. Tell the participants to write their names on the Cyber Wellness Upstander badge once all the participants have shared their responses. They are now Cyber Wellness Upstanders!

Spend a few minutes looking at the comic strip that shows Sameer expressing what he has done to Anita, a girl he used to be once friendly with but now regards as a bitter enemy. Read what he has to say. The person in the comic strip with the blank call out is you. Your response is your choice of opinion in the matter. Write down your response in the space provided. What is happening here? Who is the aggressor? Who is the victim? Who are you- a bystander or an upstander?



My Response

Have you ever been in a situation where you saw an undesirable social media interaction take place? What did you do? What would you do if you faced a similar situation in the near future?



Cyber Wellness Upstander Badge

Activity 4: My Social Media Safety Card (30 minutes)

You now know the dangers that may lurk on social media sites and the choices you must make to keep yourself and others safe. In this activity you will design your very own Social Media Safety Card. It will contain content relevant for the social media site or app you use most often. Read some general tips given in **Appendix F- Social Media Safety Tips** to jumpstart your thinking.

Use the template provided to get started, unleash your creativity and create an eye catching card that educates other on safe social media practices. The best card wins a **Social Media Safety Star!**



(My Social Media Site/App)

My Profile Information

(Note down your thoughts on the information you would like to display if you had to create a profile on your chosen social media site. What and how much would like to divulge about your location, age, education, interests, friends and contact details? How would you like to present yourself to others? How would you keep your profile safe from misuse?)

My Privacy Settings

(Note down your thoughts on how you would like to customise the privacy settings. Would you like for your profile and all that you share to be public? If not, what would you like to share and with whom? What would you like to keep visible only to you?)

My Network

(Note down your thoughts on who you would like in your social network and why? Who would you accept as friends and which requests would you decline? What would you like to share with your network? How would you control the information posted about you by your network? What would you do about sharing of your pictures by others and tagging? What would you like to post? What would you like to hide or delete?)

Activity 5: Legal Protection in the Digital Age (20 minutes)

Apart from safety measures that we can adopt, the law also offers protection to ensure people are not harmed by the irresponsible and malicious behaviour and actions of others.

Section 66 of the IT Act acquires greater relevance for upholding safe social media practices. Under Section 66, the punishment for sending offensive messages through any communication service is as follows:

“Any person who sends, by means of a computer resource or a communication device-

- a. any information that is grossly offensive or has menacing character; or
- b. any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
- c. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages

-shall be punishable with imprisonment for a term which may extend to three years and with fine.”

Other cyber-crimes are punishable as follows:

Cyber Crime	Description	Relevant Section in IT Act	Punishments
Cyber Stalking	Stealthily following a person, tracking internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh
Cyber Pornography including Child Pornography	Publishing obscene content in electronic form involving children	67, 67 (2)	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, Piracy, Copyright Infringement and so forth	65	3 years, or with fine up to 2 lakh

Give the participants some time to read the information given about cyber laws in India. Explain the provisions of Section 66 briefly and what they imply for social media use.

Organise the participants into groups. Encourage the groups to discuss the issue, the legal provisions that apply and come to a consensus on the questions. Tell them to note down their thoughts in the space provided. Invite any one group to share the answers. Encourage the participants who are listening to raise objections to the answers shared if they do not agree. Guide the participants to a consensus on the case.

Cyber Crime	Description	Relevant Section in IT Act	Punishments
Cyber Terrorism	Protection against Cyber Terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, and so forth in computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Net banking and financial frauds	43, 65, 66	3 years, or with fine up to 2 lakh
Invading Privacy	Unauthorised access to a computer	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

(Source- <http://www.nair.indianrailways.gov.in/uploads/files/1380191818131-Primer%20on%20Cyber%20Laws%20in%20India%20-%20Rajnish%20Kumar.pdf>)

Now that you have some idea about cyber laws in India, read the scenario and discuss it with your group members. What did this person do that was wrong and punishable under law? Which section of the IT Act is relevant here? What protection is available to the victim?

23-year-old Rampally Ravi, an IT professional created a fake Facebook account of a married woman and posted obscene information and morphed images in order to defame and spoil her matrimonial life.

On what basis do you think this person can be arrested?

Note down your group's opinion in the space provided. Be prepared to share the opinion, with other groups.

Conclude the module by telling the participants that being aware of the kind of interactions that can be a dangerous, safety practices and legal protections prepares them to be strong and upright digital citizens. In the next module we will learn etiquettes that govern online behaviour and reflect on the learning from all the modules.

Self-governance or regulating your own online conduct and being aware of the legal protection that is available to you can go a long way in making your online experiences pleasant and welcome. In an age where technology advancement is extremely rapid and we are constantly exposed to new devices and platforms of interaction, knowledge of and adherence to safe social media practices can be the best armour against any threat to our cyber wellness.

In the next module you will learn about the etiquettes that govern proper online behaviour. You will also assess your learning from all the modules you have completed and reflect on how you are now better prepared to deal with cyber dilemmas you may face and ensuring your safety in this digital age.

Module 4

The Road Ahead

Description: Most of our communication in the digital age takes place through the Internet whether we use email, social networking sites, chat messenger apps or blogs to interact with others. Just like there are driving rules to follow on the road, there are netiquettes to follow on the Internet. Our online reputation is formed by what we communicate to others and how we do it. Netiquettes are essential for promoting cyber wellness and creating a healthy cyber-culture. In this module you will learn about the rules that govern online behaviour, assess your learning on cyber wellness and reflect on how the workshop has prepared you to lead a safer and better cyber life.

Activity 1: Take your Manners Along (30 minutes)

The word Netiquettes comes from a combination of two words- Internet and Etiquettes. It implies showing respect and courtesy to others when we communicate or interact with them on the Internet. Proper online behaviour is one of the most influential factors that promote cyber wellness. When on the Internet, it is important to take your manners along!

All through the previous modules you have learned about cyber wellness values, behaviour and activities that threaten cyber wellness, safe social media practices and even how to deal with challenging situations that you may face in cyber space. By now, you have a fair understanding of what should or should not be done while using the Internet.

In this activity, based on what you know of cyber wellness and healthy online interaction, you will design a poster on netiquettes. Your facilitator will share chart paper and sketch pens with each group. Reflect on your learning and collaborate with your group members to create an attractive and informative poster that tells people how they must behave, communicate and interact while using the Internet.

Your poster must have the following:

- A clear title that conveys what the poster is all about.
- A few illustrations that makes it attractive and interesting. Do remember that the illustrations should be relevant to the content.
- At least eight to ten netiquettes/guidelines on online behaviour.

Start the module with a brief recapitulation of the key learning from the previous modules. Guide the participants to the realisation that all the learning from earlier modules has prepared them to know what comprises proper and safe online behaviour and practices. This also develops their netiquettes. Inform them that in this module they will draw on their learning from the previous modules and identify the netiquettes necessary for promoting and maintaining cyber wellness. They will also assess their learning and reflect on how they have benefited from the workshop.

Inform the participants that they will start this module with a short fun activity. They will work in groups, collaborate and share their learning to design a poster on netiquettes that promote cyber wellness. Inform them that the successful completion of the poster and the quiz that follows rewards them with a Cyber Wellness Champion certificate!

In this activity, based on what you know of cyber wellness and healthy online interaction, you will design a poster on netiquettes. Reflect on your learning and collaborate with your group members to create an attractive and informative poster that tells people how they must behave, communicate and interact while using the Internet.

Your poster must have the following:

- A clear title that conveys what the poster is all about.
- A few illustrations that makes it attractive and interesting. Do remember that the illustrations should be relevant to the content.
- At least eight to ten netiquettes/guidelines on online behaviour.

Display the poster as instructed by your facilitator. Also, take a look at the posters made by other groups.

Activity 2: What is your IIQ- Internet Intelligence Quotient? (10 minutes)

This activity has been included to assess the participants' learning from previous modules.

Instruct the participants to answer the questions listed in the activity.

Discuss the questions, review their answers and announce the right answers. Congratulate the participants who have answered all the questions correctly.

For your reference, answers are as follows:

1. b
2. b
3. c
4. c
5. a

Let's find out how much you know about safe and proper use of the Internet and promoting cyber wellness. Answer the questions below:

1. You have a digital photo of yourself and someone you met online wants to see it. They mention that it is for their research on social media activities of people your age. Will you share the photo?
 - a. Yes
 - b. No
 - c. Maybe
2. You are a professional accountant and receive an email that contains financial details of a company. The email requests you to analyse their company finances and if the organization members are satisfied with your work, they will deposit 50,000 rupees in your account. This procedure requires that you share an account number where the money can be transferred, your name and address. Will you share the information?
 - a. Yes
 - b. No
 - c. Maybe

3. Select the password that you think is the strongest.
 - a. Tendulkar_mania
 - b. Buterchiken1
 - c. Yoi234@12

4. The act of acquiring usernames, passwords, and other personal information by posing as someone trust worthy is called:
 - a. spamming
 - b. flaming
 - c. phishing

5. Which of the following emails will you open?

	From	Subject of email
A	Divya	What are you upto?
B	xyz@thirsty.com	Hello from thirsty.com
C	Jackpot_guru	Congrats! You've won Rs.1500.
D	Shroff11	Sign up and win 2 tickets to IPL!
E	Sehgal	Coffee, this weekend?

- a. A and E
- b. B, C and D
- c. All of them

You have taken a quick assessment of your learning. Online behaviour and practices continuously evolve in accordance with advances in technology and therefore our preparation to meet new online expectations and challenges must also keep progressing.

For further assessing your knowledge about online safety, you may attempt to answer the scenario-based questions in **Appendix G- Scenario-based Questions** in your spare time. Each scenario presents an issue and is followed by a response to the issue. Remember to read the response only after you have noted down your own thoughts on the issue.

Activity 3: Your Workshop Learning (10 minutes)

Let the participants know that this is a very important activity as it helps them to know how the workshop has benefited them. Ask the participants to spend a few minutes and read the questions given. Ask them to reflect on the learning from each module and write the answers for the questions. Invite a few participants to share their answers.

Before the end of the workshop, reflect on the key learning from all the modules you have completed. Use the space below to capture your thoughts.

How has participating in the Intel® Education Digital Wellness Workshop benefited you?

How has the workshop prepared you to promote cyber wellness?

How will the learning from this workshop change your online practices? What kind of impact do you think this will have on the cyber environment?

Activity 4: Wrap-Up (10 minutes)

Certificates/Celebrations

Congratulate each participant on the successful completion of the workshop. Give the participants their Cyber Wellness Champion certificates. Wish them a safe and happy online experience whenever they use the Internet!

During this time, those who have successfully completed the workshop will receive their Cyber Wellness Champion certificates.

Congratulations on successfully completing the workshop!

Copyright Infringement and Laws

Appendix A- Copyright Infringement and Laws

When you wish to use somebody's work, you need to take permission from the creator. If you fail to do so and use the work without permission, it is called copyright infringement.

Read the examples of copyright infringement given below to better understand how it happens. Have you ever done anything like this? If so, you were violating copyright laws.

1. A new music album has been released. Harish really wants to listen to the songs so he finds an Internet source that lets you download new songs at no cost. After downloading, he shares the songs with his friends as well.
2. Reena buys an expensive book published by a foreign author. She likes the book and gets a few photostat copies of the book circulated among her friends.
3. Rahul has started a community project and require a logo for his group. He really likes the logo of a famous food chain and uses it for his group as well.
4. Abha has a blog where she reviews books. She copy pastes a big chunk of writing from a book on literary criticism and posts it as a new topic.
5. Saurabh often uses pictures, illustrations, drawings and paintings in his project work without crediting the author or mentioning the source.

Fair Practices

Follow the guidelines given below to avoid plagiarism or copyright violations:

- Cite references and source for the quotes used in your writing, if any.
- Do not forget to mention the author's name if you have used his findings or information in your article or post.
- If you put someone's ideas in your own words, even then, mention the source.
- Even if copyright is not mentioned on articles like the ones published on the Internet, do not present the content as your work.

Copyright Infringement and Laws

Copyright Laws in India

The Copyright Act 1975, allows us to keep our intellectual work protected and secure and provide us with the authority to demand an explanation in case of any illegal actions.

Copyright laws exist throughout India for (a) original literary, dramatic, musical and artistic works (b) cinematograph film and (c) sound recording (Section 13). These terms are defined in the Act.

Copyright does not exist forever. It applied only for a specific duration. After the expiry of the specified time, the work falls in the public domain and is then open to public for use without the permission of the owner. For literary, dramatic, musical and artistic works the term is 60 years from the death of the author; for photograph, cinematograph film, sound recording it is 60 years from the beginning of the calendar year following the year in which it is published/ released. In case of copyright infringements, the owner has the right to claim his/her authority and demand an explanation. It is a criminal offense to violate copyright Act. The minimum punishment for copyright infringement is imprisonment for six months and a fine of RS 50,000 (minimum).

Hence, while creating any kind of work that uses the work of others as a source; if you face any doubts, it is always better to consult an expert before you finalise and publish it as your work.



Appendix B - Frequently Asked Questions for Ages 11-18

Q1. What is a virus?

A1. A computer virus is a program file that can attach itself to other files, and replicate itself (copy itself) over and over without the user knowing that it's happening. It can spread from one computer to another, sometimes by using an email program, instant messenger, or even be disguised as an attachment. Some viruses are harmless pranks that display an annoying message, while others can destroy files and even erase an entire hard drive. McAfee's software currently detects more than 57,000 viruses, Trojans, and other malicious software.

Q2. What are pop-ups, and what should you do when you see one?

A2. A pop-up ad is a form of online advertising on the World Wide Web intended to attract web traffic or get email addresses. This form of online advertising is annoying for most Internet users because it interferes with what you're doing, and it appears without you wanting it or taking any action. They usually appear when a user is linking to a new Web site. Popup blockers are a web browser feature, software, or application that allows users to limit or block pop-up ads. A user can usually set their preferred level of blocking from minimal to total blocking of pop-up ads.

Q3. What is pirating (music and software)?

A3. The word "pirating" refers to the unauthorized copying of software, music, movies and other shared media files. Most programs are only licensed for use at just one computer, and by purchasing software/music/movies etc. you are allowed to make copies of the program for backup purposes only. You are not the owner of the software, you are a licensed user. It is illegal to give copies to friends.

Q4. What is peer to peer sharing?

A4. Peer to peer sharing (P2P) is a system of file sharing where any PC on the network can see any other PC on the network. Users can access each other's hard drives to download files. This type of file sharing can be valuable, for example when working on a homework assignment with others, but it can also lead to copyright issues for music, movies and other shared media files which are illegal to share without permission. Peer to peer sharing also can leave users vulnerable to viruses, Trojans, and spyware hiding in the shared files. McAfee – Online Safety for Kids Frequently Asked Questions for Ages 11-18

Frequently Asked Questions

Q5. Is YouTube bad?

A5. YouTube has a monitoring system to prevent the spread of potentially objectionable content, by asking its users to 'flag' videos that are offensive. YouTube staff members then review these flagged items and remove them if they are in violation of the Community Guidelines. YouTube might also add an age restriction on a video if it follows the guidelines, but still may not be appropriate for every viewer. Repeat offenders who continue to post inappropriate videos can have their YouTube accounts disabled.

Q6. What does hacking mean?

A6. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called 'hackers'. It's most common among teenagers and young adults. When hacking is done for negative reasons, it can be criminal as it often involves creating malware, which is software that is intended to damage or disable computers.

Q7. What does phishing mean?

A7. Phishing is a criminal activity that uses email or instant messaging to illegally acquire other people's information, such as passwords and credit card numbers. When someone is phishing they masquerade as a trustworthy person or business in what looks to be an "official" electronic communication. If you see a link in a suspicious email message don't click on it. Cybercriminals are not known for their grammar and spelling either, so look for obvious mistakes in an email because it could likely be a scam.

Q8. What is a firewall, and how do you set one up?

A8. A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier between all information passing between internal and external networks and systems. Firewall software analyzes information passing between these two and rejects it if doesn't conform to the requirements.

Q9. What kind of security do Apple products have and how can I keep my devices safe?

A9. Apple products have been designed with advanced technologies that work together to constantly scrutinize, encrypt and update to keep your Mac safer. Apple's products are known for having features designed to protect the information on their devices. Find My Mac helps you locate your missing Mac on a map and set a passcode remotely. A product called Gatekeeper makes it safer to download and install apps. Always use privacy settings to secure your personal information, and install the most current software updates as they become available.

Frequently Asked Questions

Q10. What is “jail breaking” and what does it do?

A10. Jailbreaking is the process of modifying the operating system running on an iPhone, iPod touch, or iPad to give the user more control over their device. One example of this would be removing Apple's pre-set restrictions allowing the user to install apps from sources other than the official App Store. While some people may feel that jailbreaking gives them more control over what is installed on their device, it can also cause problems like data corruption which allows access to malicious code. Apple does not support devices that have been damaged due to jailbreaking and this may also inactivate the warranty.

Q11. What should I do about chain e-mails?

A11. Chain letters and hoax messages are another type of Internet fraud. They persuade recipients to pass on the email to other email addresses, which clogs up in boxes and slow down the server. Chain letters also play on your emotions by scaring you with bad luck or falsely luring you in with chances of winning money. These kind of messages (known as email scams) often threaten or frighten you to pass on your personal information or a sum of money to the sender. They can also pass on computer viruses. Don't be fooled! Delete chain emails, and do not pass them along.

Q12. My art teacher wants me to create a Facebook account so I can share my artwork with him. Is this okay?

A12. Currently Facebook has a minimum age requirement of 13 years. Additionally, this is a question that should be addressed to a parent or guardian that can help you make that decision. Facebook is an amazing and useful social networking tool, and when used properly it has many benefits, but ALWAYS remember that what you post on Facebook is out of your hands and your control forever.

Q13. My family gets strange phone calls from an unmarked number. Can we block those?

A13. If your cellular device is receiving unwanted phone calls from an unmarked or 'blocked' number, there are now downloadable apps designed to reveal the caller's name and phone number as well as block (or blacklist) them. Just remember, it's important to read the user ratings on any app BEFORE installing it on your device as a safeguard to prevent you from downloading an unsafe application.

Q14. What is a bot?

A14. A 'bot' is a type of malware which allows an attacker to gain complete control over the affected computer. Computers that are infected with a 'bot' are generally referred to as 'zombies'. There are literally tens of thousands of computers on the Internet which are infected with some type of 'bot' and don't even realize it. Attackers are able to access lists of 'zombie' PC's and activate them to help execute attacks against Web sites, host phishing attacks on Web sites or send out thousands of spam email messages. If someone actually traces the attack back to its source, they will find an unwitting victim infected with a 'bot' rather than the true attacker.

Frequently Asked Questions

Q15. What is a Trojan?

A15. On the surface, a Trojan horse looks like a useful computer program, while it actually causes a great deal of damage to your computer. A Trojan's purpose is to stay hidden while downloading and installing a stronger threat on to your device such as a bot. Unlike viruses and worms, Trojan horses cannot spread by themselves. They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website. After it is installed it hides out invisibly carrying out its misdeeds such as downloading spyware.

Q16. Can you remove posts from Facebook wall permanently?

A.16. You certainly can remove Facebook posts from your OWN wall permanently, but as we've discussed, once you post something, it's out of your hands and you CAN'T control what others do with it. That's why it's so important to think before you post something that you might want to take back later.

Q17. Are all BitTorrent clients bad?

A17. BitTorrent is one of the most common peer-to-peer file sharing protocol used for distributing large amounts of data over the Internet. Not all BitTorrent clients contain malware, but many do. Installing one of these less reputable clients will result in a hijacked browser and numerous popups. Ignore catchy phrases like, "We use unique technology to increase the download speed of your torrents" to avoid accidentally downloading one of these clients.

Q18. What does "encryption" mean?

A18. Security is a major concern on the Internet, especially when you're using it to send sensitive information between parties. The most popular security methods all rely on encryption, the process of encoding information, or the scrambling of data, in such a way that only the person (or computer) with the key can decode it.

Q20. How can I protect my phone from viruses?

A20. People use a mobile device for all kinds of reasons like: calls, messages, contacts, photos, videos, games, social networking and shopping. If a device gets lost, stolen, or infected with a virus, personal data could be taken and one could be a target of fraud and identity theft. Antivirus/ anti-spyware/ anti-phishing software is available for mobile devices. It can give someone the ability to lock their device remotely, backup and restore their data, locate and track their missing device among other things. Always use a complex and creative password to lock your mobile device.

Q21. What should I do if my Facebook account gets hacked?

A.21. If your account has been hacked, you should (1) visit the Facebook Help Center and attempt to reclaim your account, and (2) make sure you change the password to your email address immediately. If you use the same password to access other accounts, especially banking, financial institutions. Make sure to change those passwords as well. (3) It is possible that the hacker gained entry to your computer through a virus or other malware. Make sure you have a current and up-to-date antivirus program installed on your computer, and do

Frequently Asked Questions

a thorough scan of your system. (4) Getting hacked can be an embarrassing and humiliating experience, but you must notify your friends and family of the incident. The hacker may use your account to send them malicious links and to phish for their personal information as well.

Q 22. I heard Macs can't get hacked. Is that true?

A22. In the past, Macs have been hacked, and though it is rare, there is malware out there (like viruses and worms) for Mac computers. Don't open suspicious files and links sent through email, and, if you're concerned you may have any viruses on your computer you should consider running an anti-virus scan. Sophos Anti-Virus and Kaspersky Anti-Virus are both supposedly quite good on the Mac. In the strictest sense of the word, there are no viruses affecting a computer running the latest version of Mac OS X (though there is a small amount of other malware for OS X on the internet). If you exercise caution and common sense in navigating the Internet, using email, etc. then chances are you will not ever have to worry. http://wiki.answers.com/Q/Do_mac_computers_get_hacked_and_get_viruses

Q 23. Is cyber-bullying against the law?

A23. The safety of schools is increasingly becoming a focus of state legislative action. School bullying and harassment policies are being supplemented to provide students protection from cyberbullying. This can be defined as the willful and repeated use of cell phones, computers, and other electronic communication devices to harass and threaten others. Most states have enacted legislation that addresses cyberbullying, with repercussions ranging from reassigning the bully to another school to separate them from the victim, school suspension/expulsion, all of the way to finding the student guilty of a misdemeanor. - NCSL (National Conference of State Legislatures)

Q 24. How do I change my privacy settings on Facebook?

A24. To edit the privacy settings for your own Facebook account, click the account menu at the top right of any Facebook page, and choose Privacy Settings. This page contains a group of general controls for your Facebook account, such as who can send you friend requests and messages. Your controls are right next to each thing you share. From this page you can personalize your privacy settings for Contact Information, Applications and Websites, and Search.

Q25. How do I create a safe, secure password?

A25. Length: make your passwords eight or more characters. **Complexity:** include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. **Variation:** to keep strong passwords effective, change them often (about every 3 months). **Variety:** don't use the same password for everything.

Frequently Asked Questions

Q26. What can I do to make sure I don't get viruses on any of my electronic devices?

A26. 1) even if you have a machine that isn't hooked up to the Internet, a reliable antivirus program is a low cost (sometimes free) addition to any machine. 2) Install antispyware and anti-malware programs; many of these are completely free. 3) Avoid suspicious websites, and if your anti-virus program gives you a warning, don't go back, 4) the most common way viruses are spread throughout the Internet is still via email. Make sure you use an email client that scans all email attachments before you are allowed to open them. This will help prevent computer viruses from getting into your machine. 5) Set your anti-virus software to run automatic scans, having daily scans run when nothing else is going on is a great way to prevent even the latest computer viruses from sticking around too long. 6) Watch Your Downloads – Part of the fun of the Internet is downloading music, movies and other items. Only download these files from trusted sites that you can count on, or at least scan them before you open them.

Q27. What is Everloop?

A27. Everloop is a social networking site for kids under 13 with special micro-networks or "loops" that safely connect kids. Everloop's privacy protection and monitoring technology (patent pending) guards young users against bullying, predators, bad language and sharing of personal information.

Q28. Why would someone want to steal my identity?

A28. Identity thieves take your personal information and use it to do things like rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector. This is why you should NEVER share information like your social security number, full name and birthday with strangers.

Q29. What is SiteAdvisor?

A29. Site Advisor software is an award-winning, free browser plugin that gives safety advice about Websites before you click on a risky site. With Site Advisor software installed, your browser will look a little different than before. We add small site rating icons to your search results as well as a browser button and optional search box. Together, these alert you to potentially risky sites and help you find safer alternatives.

What is Personal Information?

Appendix C- What is Personal Information?

Personal information is SO IMPORTANT that we should keep it as protected as if it were locked in a safe. It should always be kept private.

Now let's open the safe and see what's inside. Personal information is information related to:

- Your age
- Where you go to school
- Where your parents work
- Where you live
- Your phone number
- Passwords - Only you and your parents should know this!!!

Before sharing any personal information, always ask yourself the following questions:



Remember, before sharing ANY information online, STOP and THINK:

- WHO is asking for my personal information?
- WHAT information is being requested?
- WHY do they need this information?

Appendix C

What is Personal Information?

Even if there appears to be a good reason to give your information, you should ALWAYS ask your parent, guardian or a trusted person of authority FIRST.

In most cases, you can't really know who you're talking to online. You can't see them. You don't know them, which is why you should always ask a trusted adult before you give out any private information. The online bad guys are trying really hard to get it. Why? Because with your personal information, they can find ways to steal from you and your family or harm you in other ways.

Protective Measures for Cyber Safety

Appendix D- Protective Measures for Cyber Safety

Read the protective measures stated below to know what can prevent, control and stop the threats that create obstructions in cyber wellness.

Cyber Bullying	
1	If you receive any kind of unpleasant message or picture on your email, phone, through a social media app, do not respond to it or try to get back to the bully. The key is to avoid it.
2	If you are in a 'chat room' and receive an image or message that you think is inappropriate, do not respond. Just leave the room. Avoid joining such chat rooms but if you do, do not use your personal details anywhere in it.
3	If you are facing any kind of threat, save a picture or screen shot of the message or image and seek help from a trusted adult. If the bully continues to send such messages or threaten you, seek help from the police under some adult's guidance.
4	Make sure that you do not bully others unintentionally. Treat others the same way as you would treat them in real life interactions.
5	Do not consider being bullied your mistake or be ashamed. Change your social media account, if necessary.
Cyber Predators	
1	Follow age limit on social networking websites.
2	Cyber predators make use of our weaknesses and vulnerabilities and gradually bring unpleasant or sexually oriented matter into the conversation. Do not be scared or ashamed. Seek help.
3	Use email filters and never download images from unknown sources.
4	Do not get tempted or influenced by strange people claiming to do extraordinary tasks like reading your face or remotely helping you to score better marks, and so forth Do not encourage such conversations.
5	Do not try to confide in a stranger rather than people you know personally. Remember that our problems can best be solved by you and people close to you, therefore do not let people make use of your distress at a situation, if any.
Identify Theft	
1	Do not write your password or any other confidential details on places like the last page of your notebook, mobile phone notepad, diaries and so forth. It is best to memorize it. If you must save it, write a hint instead of your actual password.
2	If you use your mobile phone to access emails or other applications, make sure you lock your mobile using a password or pin code to prevent leakage of information in case of mobile theft or if it gets misplaced.

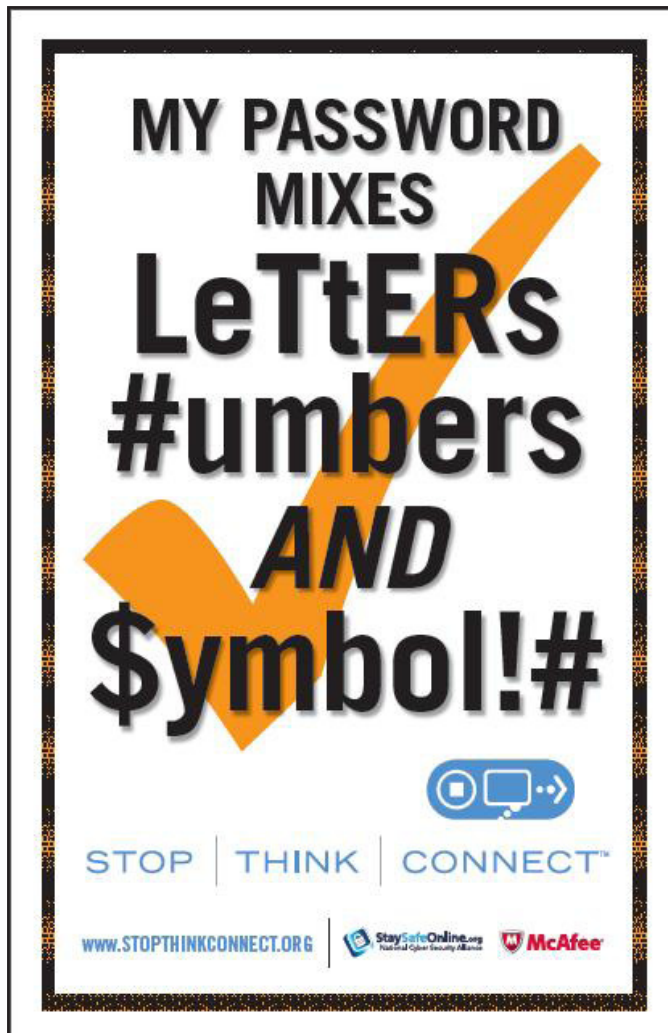
Appendix D

Protective Measures for Cyber Safety

3	Do not share your passwords with any friend even if you completely trust them. Remember they may not use your password for any purpose but they could become a source of your confidential information for others.
4	If you possess a personal computer, use a firewall software and anti-virus program to protect the information stored on your computer. Also, keep your computer password protected.
5	If you receive any such email that claims to provide any kind of lottery money or requests you to be a business partner and so forth, do not open it or download attachments from it. Do not provide any personal information at all.
Gaming Addiction	
1	Do not let computer games take away time from your friends, family or daily tasks. Create a daily activity schedule that balances online and offline activities.
2	Do not spend time playing computer/mobile games when you know some important task requires your attention such homework, dinner, helping to take care of siblings, household chores and so on.
3	If you think, you are getting addicted, make a decision to spend only a pre-fixed amount of time playing computer or mobile games and seek help from friends and family to remind you to stick to that time limit.
4	Gaming should only be a hobby not your main activity every day. You should spend most of your time playing outdoor games to keep your body and mind healthy.
5	Calculate the total number of hours per week that you spend on gaming. If you notice an increase in the time the last week, cut down time from the coming week and hence keep it in balance.
Malware	
1	Use an antivirus and update it often. Do not run your computer without an antivirus for a long period. Always, use the latest version of your browser. This increases the security on your machine as well.
2	If you see any pop up window which wants you to download a free anti spyware, do not accept it and use ATL + F4 to close the window if you cannot close it otherwise.
3	Do not disable your antivirus for a long period of time.
4	Do not run two anti-virus, anti-spyware programs on your computer at the same time.
5	Do not download an unknown file, link, music or video from an unknown source. It may have a virus.

Protective Measures for Cyber Safety

One of the most important protective measures is setting a strong password for any online account. Here is what you should keep in mind while creating a password:



Popular Social Media Sites and Apps

Appendix E- Popular Social Media Sites and Apps



Many parents believe social media sites are suggested for children over 13 years based on the network's content, like a PG-13 movie. However, this is NOT true. In the United States users of social media sites must be 13 years old by Federal law:

1. **A child under the age of 13 years (U13) is protected by the Children's Online Privacy Protection Act (COPPA).** Essentially, COPPA protects a child's personal information from being collected and shared. These legal protections include online data tracking, geolocation, photos, videos, and information available by 3rd party advertising networks. Creating an account for a child U13 (using a false date of birth) circumvents the Federal law intended to protect them, and consequently makes all of the information provided to these social networks entirely out of the parent's control.
2. **The contention is that children U13 do not yet have the intellectual or emotional maturity to handle many social media themes.** Pre-teens are just learning to handle real-life social interactions and challenges. It takes a level of maturity and reasoning to correctly respond to online social exchanges. Many younger kids become victims of online harassment, solicitation, and cyberbullying. In these uncharted digital waters, the long-term repercussions of a child's online profile are still the unknown.

Popular Social Media Sites and Apps

The fact of the matter is that millions of kids do use these social networking sites. What can YOU do to stop kids from getting into trouble on some of these troublesome applications and websites?

- It's a good idea to make sure they don't do it unsupervised.
- Remind kids that ANY TIME they post, send or forward an image, email or text... it is permanently OUT OF THEIR HANDS and entirely out of their own control.
- These sites typically collect personally identifiable information (PII) about their users and share it with third parties. Service agreements contain verbiage like the following:

You can remove Content that you posted by specifically deleting it. In certain instances, however, some Content (such as posts or comments you make) may not be completely removed and copies of your Content may continue to exist on the Service and/or elsewhere

The Tattoo Effect: Once you've created an account with one of the services listed below, unless you have taken the steps to delete and remove the account, the information you have uploaded is going to stay there for a long time.

- Activating parental controls on your kids' devices can keep them from installing apps without parental approval.
- Another method to safeguard what your child is doing is to make sure all app purchases go through the parent's account.

Even if your child is over 13 years of age, there are some risky applications and sites that parents should be aware of. Here is a list of some of the most popular apps today, with a general description and some of the things to look out for.



Ask.fm is a web site where users can ask other users anonymous questions.

- Unfortunately this is often used for cyberbullying and has been highlighted recently in the news due to bullying-related suicides.
- Teen Instagram users typically post a link to their Ask.fm profile on their Instagram bio.
- A person typically adds Ask.fm to their Instagram account in the 'About Me' section. This application is also a website – Ask.fm
- Another cause for concern is that Ask.fm is based in Latvia, and the company has not shown they have usable tracking data or monitoring of who asks the questions and other activity. According to research the headquarters for Ask.fm is based in Latvia, however the .fm part of the web address suggests it is hosted from Federated States of Micronesia.

Popular Social Media Sites and Apps

- The content you submit, post, or display will be viewable by others.
- Users must be 13+ to use this service.



Chatroulette is an online chat website that pairs random strangers from around the world together for webcam-based conversations. Visitors to the website begin an online chat (text, audio, and video) with another visitor.

- This site receives criticism particularly with respect to the offensive, obscene or pornographic material that some of its users exhibit.
- Psychiatrist Dr. Keith Ablow advises that “Parents should keep all children off the site because it’s much too dangerous ... It’s a predator’s paradise.”
- Lookalike services include Omegle, ChatRandom, or DirtyRoulette
- The age requirement is 18+ and it is not suitable for minors.



Facebook is a social application where users can share status updates, pictures, videos, and web content with their “friends”.

- Parents and teens are advised to set privacy controls and check them regularly. This is due to the fact that Facebook often updates its features, and users should check settings to confirm what information they’re sharing.
- Most recently, changes allow kids 13 to 17 to share timeline posts publicly rather than only with friends (or friends-of-friends).
- Users must be 13+ to use this site.



Flickr is a website where users store, manage and share digital photos and videos online.

- If a user’s account is set to public, anyone can view the images. This means that kids can also see offensive photos (including nudity, drugs and violence).
- A free membership includes a huge amount of storage.
- Registered users have the option to keep photos private for personal use and are free to delete photos at any time.
- Users must be 13+.

Popular Social Media Sites and Apps



Foursquare is a location-based social networking website and application for mobile devices such as smartphones.

- Parents need to know that this site essentially encourages members to meet in person. The service warns users to “friend” carefully and includes the option to post anonymously.
- This new breed of social networking that entails sharing where you are and inviting other members to drop by, lends itself to a host of obvious dangers.
- Photos of attractive young members are featured on the site with tie-ins to Facebook and Twitter, making it very tempting for some kids to attempt making new real-life friends with Foursquare.
- There are no age limits or predator filters.



GifBoom A photo and video sharing social networking application, where users upload silent animated GIFs to share with “followers” (GIF means Graphics Interchange Format)

- Users can also “reboom” GIFs that they’ve received and send them to other users, as well as follow and subscribe to other users.
- Users post content through the application at their own risk. GifBoom cannot control the actions of other users with whom you may choose to share your information. Therefore, they do not guarantee that user content posted with them will not be viewed by unauthorized persons.
- Members should be 13+.



Instagram is a popular social application for instantly enhancing photos and videos with cool effects, and then sharing them across a number of social media platforms.

- Parents should know that photos shared are public by default and may have location information embedded in them. Users can make posts private by adjusting settings.
- Users can ‘like’ or comment on images of other users they are following and vie for an opportunity to become ‘InstaFamous’ (which means you are famous because your image has been posted on the popular page with others that have the most “likes”).
- Users should be 13+ to use this site and should not post partially nude or sexually suggestive photos, but the site does not prohibit the portrayal of violence, swear words, or drugs.

Popular Social Media Sites and Apps



Kik is an alternative texting service that lets teens chat and swap pictures while bypassing their parent's wireless provider's SMS service.

- Using Kik is similar to making a phone call – there's a record of messages being sent and received, but the text of the messages isn't saved.
- Users commonly receive messages from other users they don't know, often times of inappropriate nature.
- Teens between 13 and 18 years old need to have permission from their parent or legal guardian before they create a Kik account. Children under the age of 13 are prohibited from using this application.



Keek is a social application that allows users to upload 36 second long videos and share them with "followers".

- The option for a private profile is not provided.
- Some dangers include the fact that adults can subscribe to a child's updates, view all their content, and comment on their videos.
- There are no privacy settings, restrictions to adult content, or parental controls.
- Used by many celebrities
- Keek does not actively regulate content unless specifically flagged as inappropriate.
- This app is for kids ages 17+. Children 13+ must have parental permission.



One True Media is a site where people can create their own personalized movie montages by uploading photos, videos, and adding music.

- Some of the user-created montages in the online gallery contain violent or sexual content, as well as issues with language, drinking, drugs, or smoking.
- Users must be 13+ to use this service.

Popular Social Media Sites and Apps



Pinterest is a free pin board style photo sharing application and website where users can create and manage theme-based image collections i.e. recipes, interests and hobbies.

- “Followers” can view these collections if they are not private.
- Users should also keep in mind that Pinterest stores actual copies (not just thumbnails and links) of the images being pinned.
- Parents need to know that to join, users must be invited by another Pinterest member -- or request an invitation through the site. When registering, you have to sign up using a Facebook or Twitter account.
- Users must be 13+ to use this service.



Pheed is a social networking application where users upload content such as texts, photos, video and audio to share with followers.

- Users can choose if they want to charge a fee to view their content by opening a channel and becoming a “pheeder”.
- Users must be 13+ to use this service.



Path is a social networking-enabled photo sharing and messaging service for mobile devices similar to Facebook.

- The service allows users to share with their close friends and family with a limit 150 contacts. The hope is that it will be the network people will use to speak to people that they actually like, due to the friend limit. They call this a person’s “Inner Circle”.
- The FTC fined Path in February 2013 for not spelling out their collection/use/disclosure policy for children’s personal information; not providing parents with direct notice of its collection; and not obtaining verifiable parental consent before collecting children’s personal information.
- Users must be 13+ to use this service.



SnapChat is a social application where users send pictures and videos (“snaps”) to other users, which then disappear from the recipient’s device after a specified amount of time.

- Users set a time limit for how long recipients can view their snaps. As of December 2013 the range is from 1 to 10 seconds. Once the specified time elapses the images will supposedly be hidden from the recipient’s device and deleted from SnapChat’s servers.

Popular Social Media Sites and Apps

- Parents should be aware that any snap can be saved by taking a simple screenshot of the image before it disappears, which clearly defeats the original purpose of the app itself.
- Messages sent via SnapChat do not appear on a phone bill, leaving parents without any visibility into who their child is sharing information with.
- SnapChat is known to be popular for sexting.
- Users must be 13+ to use this service.



Tango is a messaging app similar to Kik, but it is multi-platform which means that it can be used across all different kinds of devices.

- Tango also provides the ability for group chats and calls, a social feature teens are likely to enjoy.
- Part of the appeal is that during a video chat users can send cute animations, play games, and share music using [Spotify](http://www.bewebssmart.com/app-review/music-discovery-services/) (http://www.bewebssmart.com/app-review/music-discovery-services/) right within the app. There are even filters that enhance photos and add cool effects during a video chat.
- Tango profiles are public by default. There is a “find friends nearby” feature that uses location services to find other Tango users near you. Users can manually make an account private and turn off location services.
- There is a page called “Popular People” which gives you access to some user’s profiles.
- Users must be 13+ to use this service.



Tinder is a dating app that facilitates communication between users by notifying them when other ‘Tinder’ users are nearby. Users can then choose whether they are interested romantically in the other user or not.

- Hookup apps like Tinder let you scroll through images of other members and flag the ones you like. If they also like you, you’re both notified, and then you can contact each other.
- The users create their account through Facebook, and the app accesses the users Facebook “likes” and “friends” when selecting potential matches.
- The app gathers users’ basic information to match up potential candidates based on geographical location.
- The primary concern is that similar services require users to be 18 or older but Tinder’s minimum age is 13.

Popular Social Media Sites and Apps

- There are dozens of similar apps with names like Blendr, Grindr, Down, Skout, Swoon, and Pure.



Twitter is a free social application where users can post brief 140 character messages or “tweets” visible to their followers, and where they can follow “friends” activities through the Web, IM or cell phone.

- Tweets are public, but users can also send private messages directly by creating a private profile where only users you accept can view your tweets. We highly recommended this for teens.
- Twitter reserves the right to sell Personally Identifiable Information (PII)
- Twitter is often used as a promotional tool for products and celebrities.
- Users can opt to post their location along with each Tweet, raising privacy and safety concerns. Public tweets will turn up in Google searches, so if someone tweets your child’s name publicly, it will be surfaced in a Google search.
- Twitterers often engage in ugly public fights, or use the service to cyberbully.
- Users can search Twitter and find tweets (posts) with sexual and other inappropriate content.
- Users must be 13+ to use this service.



Tumblr is a microblogging platform and social networking website owned by Yahoo!

- Users post multimedia and other content to a short-form blog, and the site hosts more than 152.2 million blogs.
- Tumblr is noted by technology journalists as having a sizeable amount of pornographic content, depictions of violence and drug use, and offensive language.
- Upon creating a profile the site defaults to public and viewable by all. To obtain full privacy users must create a second profile which they can password protect.
- Users must be 13+ to use this service.

Popular Social Media Sites and Apps



Reddit is a social news and entertainment website where users submit content in the form of links or text posts, and where other users then vote on the posting thereby raising or lowering the ranking on the site's pages.

- The site features a collection of entries that are split into numerous sub-categories like educational, entertainment, humor, discussion, image sharing and more.
- Users can post comments on the submissions.
- Parents should know that this is a place for free speech and kids will see things that are both credible and factual, as well as offensive and inappropriate.
- The good news is that moderators watch posts for inappropriate behaviour, and if kids post something by mistake, they can delete it themselves.
- Users must be 13+ to use this service.



Wanelo is a social shopping community where users can post images of items that they like (such as clothing, cosmetics, and home furnishings) for their friends and followers to see. They can also browse others' items and make comments. The name Wanelo is a combination of the words want/need/love.

- When a user clicks on an image, they are taken directly to the place where it's available for sale and Wanelo gets a commission for the sale.
- Users must be 13+ to use this service.



WhatsApp is a cross-platform instant messaging subscription service for smartphones with Internet access.

- Teens can send text messages, videos, photos, and short audio messages to one or many people with no message limits or fees (after paying for the app). Messages can only be sent to other smartphone users who also have WhatsApp. Once you install the app, it checks your address book to see if anyone else you know is already using WhatsApp, and connects you automatically.
- Users must be 16+ to use this service.

Appendix E

Popular Social Media Sites and Apps



Whisper.sh is an application which allows users to send messages anonymously, and receive replies. The messages are displayed as text superimposed over an image.

- The site's concept is to promote online anonymity, and the tagline is: Share Secrets, Express Yourself, Meet New People
- The site contains a large amount of adult content.
- Users must confirm they are at least 18 years of age.



Vine is a social media application where users share 6 second long video clips with followers.

- The site serves up endless amounts of six-second looping cute and fun videos... unfortunately it also demonstrates just how much inappropriate content can be packed into six seconds (posting pornography is not against guidelines).
- Vine Labs has removed the ability to search for adult hashtags like #XXX or #NSFW, but the videos are still there.
- All profiles are public. There are no options for setting your Vine account to be private like you can on Instagram. That means that any "vine" you create and share could potentially be seen by anyone else using Vine.
- Users must be at least 17 years of age.



4Chan is an image based message board which does not have a registration system, and all users post anonymously with the most recent posts appearing above the rest.

- User registration is not required nor is it possible.
- Anonymity can sometimes create hostile online environments, so parents are encouraged to talk to teens about how to deal with virtual aggression.
- The most popular posts are on the site's "Random" message board known as /b/ pronounced "slash b" or "b" and features a no rules policy on posted content, except for bans on certain illegal content such as child pornography.

Popular Social Media Sites and Apps

SOCIAL NETWORKING TERMS:

Friend In social networking friends are individuals who have mutually agreed to allow access to each other's social profile.

Follower Someone who subscribes to the feed of another user.

Microblog Similar to a blog but smaller Microblogs consist of short sentences, individual images, or video links.

GIF Pronounced 'jiff', a GIF (Graphics Interchange Format) is an image that consists of multiple frames or photos that move like an animation.

Hashtag Is a word or phrase preceded by a hash or pound sign (#) and is used to identify messages on a specific topic.

Appendix F- Social Media Safety Tips

Read the social media safety tips provided to keep your social media profile safe from any online risks and harassment. Go through all these points to check if your profile is safe on social media sites. Make the required changes to your profile, if any, immediately. If you have a profile on Facebook, read the section under the heading 'Safety Tips for Facebook' carefully to modify your profile to be safer.

Social Media Safety Tips

1. Your profile should not have any contact details or personal information on it.
2. Avoid making any online friends who you do not know personally.
3. Avoid posting personal pictures of yourself or family members.
4. Do not update your location on your social media profile when you visit a place and guide your friends not to tag/include you in the same, if they update their location.
5. Use privacy settings on such social media sites to make personal information (such as friend list, relatives, specific details like address, phone number and so forth) is accessible only to you or a carefully chosen set of people.
6. Have a strong password for your account and keep different passwords for different websites. If you have more than one email account, keep a different password for all of them.
7. Any emails dropped into your SPAM folder must be deleted. You can read the subject line to identify if the email has not been transferred to spam by mistake.
8. If you are using Internet in a cyber café or using a public computer, remember to delete your user name and password, if saved. Also, go to History and delete recent history to remove your login details.
9. If you use a smart phone, do not let others use your mobile unless they require it to make calls only and disable GPS for social networking apps.
10. Keep '**Geotagging**' disabled to avoid revealing your location.

Appendix F

Social Media Safety Tips

What is **Geotagging**?



Many phones and cameras today have a feature that “geotags” photos. This means that the geographical coordinates (latitude and longitude) are actually embedded into the picture. This identifies the exact location of where the picture was taken.

If the geotagging feature is not disabled on your device, posting a picture allows anyone who sees it to figure out exactly where you were when you took the picture. This is dangerous—especially if the picture was taken at your home or at school.

Check your phone’s instruction manual and disable the geotag setting. But remember, even when geotagging is disabled on your device, be aware that your friends’ camera phone may be putting you at risk too.

Social Media Safety Tips

Facebook Safety Tips

Facebook is very widely used by Internet users. Read the tips given below carefully to ensure safety on Facebook.

1. Use a separate password for Facebook than the one for your email.
2. Do not post any personal information such as address, phone number, pictures, name of your school and so forth and keep all other information only visible to your close circle of friends and family.
3. If you use Facebook on mobile, keep GPS disabled when not in use. Do not update your location.
4. Friend requests from people you don't know should not be accepted.
5. Check your Facebook profile for its log in location details regularly, as follows: Settings > Security > Where You're logged In
6. Enable Login Notifications which informs you if there's a new log in location identified by Facebook: Settings > Security > Login Notifications > then check the required boxes.
7. If you receive any unpleasant message, from a stranger, do not reply to it.
8. If you are using someone else's computer or phone to check your profile, make sure you log out after you are done. Do the same if you visit a cyber café.
9. Do not use Facebook to access external applications.

Scenario-based Questions

Appendix G- Scenario-based Questions

Read each scenario, identify the issue and think of a suitable response.

SCENARIO #1 GAURAV

A friend sent Gaurav a message with a **link to a website** where you can post **anonymous comments and pictures** about your classmates.

Almost all of the postings and pictures are mean or embarrassing. Gaurav's friend wanted him to help start a rumor about another classmate that he did not like.

What are the issues here?

**SCENARIO #2 RADHA**

Radha receives some **cruel emails** and instant messages from a couple of other kids at school.

She is not sure what to do.

What is the issue here?



Scenario-based Questions

RESPONSE: GAURAV

Cyber ethics: Proper online behavior is everyone's responsibility. This is an act of **cyber bullying**. Saying mean things, starting rumors and posting embarrassing pictures about others is **never OK**.

Cyber security: A site like this could also potentially download harmful viruses and malware on to your computer.

Cyber safety: Cyber bullying is cruel and has real life consequences like depression, fear and anxiety.



RESPONSE: RADHA

Stop...Block...and Tell

These kids are **cyberbullying**

- **Stop:** Never respond to the **mean messages** – that will only make things worse.
- **Block:** Keep the bully from being able to communicate further by blocking their email or removing them from friends lists. Print out the messages for evidence.
- **Tell:** Let a trusted adult like a parent or teacher know what is going on. They can help!



Scenario-based Questions

SCENARIO #3 DIPAK

Dipak receives an email with a subject line that reads
“You have just won \$10,000!”

All he needs to do is open the email, click on the link
provided and enter the personal information requested.

He is not sure what to do.

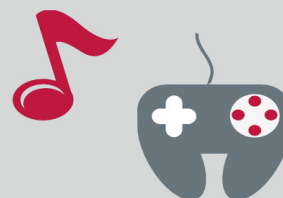
What is the issue here?

**SCENARIO #4 VINAY & SUDHA**

Vinay and Sudha have discovered a **file-sharing website**
that allows them to **share music and games** with their
friends.

They can get all the **latest music and coolest games for
free**. Should they use it?

What is the issue here?



Scenario-based Questions

RESPONSE: DIPAK

Cyber security:

This is a popular scam called 'phishing'.

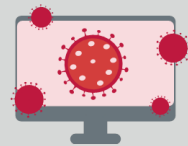
- Do **NOT** open the email! Tell your parents!
- Online criminals try to trick you into giving away your personal information so take your time and slow down. Don't just click, click, click...
- If it looks too good to be true, it probably is.



RESPONSE: VINAY & SUDHA

Cyber security:

File sharing sites, also known as peer-to-peer (P2P), like **BitTorrent, Limewire and Kazaa** can be dangerous! They are useful for sharing large files like music, games and software, but they also come with risks. They can expose your computer to **viruses**.



Cyber ethics:

It is illegal to download music, movies etc. that you haven't paid for. Additionally they often come at the cost of giving out personal information and can install a 'cookie' that tracks your Internet usage. In this instance **Vinay and Sudha would be stealing.**



Scenario-based Questions

SCENARIO : SANJAY

A friend sent **Sanjay** a message with a **link to a website** for downloading movies for free.

Most of the movies haven't been released on video yet. **Sanjay** isn't sure what to do?

What is the issue here?

**SCENARIO : LATA**

Lata just got a **skype** account.

Her best friend doesn't have one and wants to see how it works.

She asks **Lata** for her **username and password**.

Lata isn't sure **what to do?**

What is the issue here?



Scenario-based Questions

RESPONSE: SANJAY

Responsible Online Behaviour: He could be purchasing movies that have been illegally copied. **Sanjay** needs to do a little investigating before purchasing anything from this site.

Cyber security: A site like this could also potentially download harmful software (virus/malware) on his computer **Sanjay** needs to investigate before purchasing anything from this website. Everything points to these movies being illegally sold.



RESPONSE: LATA

Cyber security:

- User names and passwords are private information!
- The only people that should have access to your skype, facebook, email, instagram or other accounts are your parents and carers.

