Information Security Awareness for Student

Internet safety is every ones responsibility. It's all about being able to have fun online – to be able to chat with your friends, to post a video that you've made or a song that you've written, to be free to find out more about information you're interested in and check out the latest trends - without being bullied, annoyed or scammed, or having your ideas stolen including identity theft.

Internet safety is a lot more than just about ensuring that your computer has the latest anti-virus and firewall software installed. It's about being smart about how you handle yourself online and savvy about how you deal with other people (especially strangers who you meet online), and not falling prey to an online scam artist who takes advantage of your ignorance

Why is it important to stay safe online?

Most of us are 'connected' via our laptops, mobile phones, tablets or personal computer. The potential for the internet to be a valuable and a fun resource for entertainment, making friends, keeping in touch and learning is huge. But if you use the internet without safety awareness, you could be at risk of illegal activity or abuse - be it bullying, fraud or something more serious. Unlike seeing someone face to face, on the net, people aren't always what they first seen.

In the same way you learn about safety when you leave the house, it is important to learn how to stay safe online. These are skills that will stay with you for life time.

Some Golden Rules to follow when you're online

- Don't give out personal information such as your address or phone number.
- Don't send pictures of yourself to anyone, especially indecent pictures.
- Don't open emails or attachments from people you don't know.
- Don't become online 'friends' with people you don't know.
- Never arrange to meet someone in person whom you've met online.
- If anything you see or read online worries you, tell someone/inform your parents about it.

ISEA-Awareness Program will always gives you tips and suggestions for the teenagers/students for online safety. Do follow these guidelines/ steps before using the internet.

Using a Web Browser

The internet is a way to stay connected with friend so a way to stay current on news, research informatio ooks, online applications etc.,. The Internet has also bec ying bills and completing and submitting applications an

Using the Web browser is easy, to do things online, but there can be some hidden dangers to you and your computer. These risks can include exposure of sensitive personal information

and infection by malware, which includes viruses, spyware, and adware. Safe browsing means being aware of these online threats and taking the necessary precautions to avoid them.

It only takes a little bit of effort, a few tools, and some basic information to be safe as you browse the Internet. Follow these guidelines to protect your personal information and your computer online.

- Install and maintain up to date anti-virus software on your computer or device.
- Keep your internet browser up-to-date
- Be alert to unusual computer activity or problems.
- Install and maintain a firewall on your computer.
- Use a modern browser with features such as a pop-up blocker.
- Avoid storing sensitive material indefinitely on your computer.
- Change your passwords often.
- Beware of links sent via instant messaging and e-mail attachments.

Making ‘friends’

We all know it's not healthy to spend hours and hours in front of a computer screen. But another problem with social networking is the pressure you can feel to make sure you have lots of ‘friends’. But here are some things to remember:

- Friendships made online are made by clicking a button rather than talking to people and sharing experiences.
- Being online ‘friends’ with someone is much less meaningful than face to face friendship.
- You can easily fall out with an online ‘friend’ because of a misunderstood comment.
- It is far easier, and healthier, to sort out arguments and problems when you can talk to someone face to face

So although you might know someone who likes to boast about how many ‘friends’ they've got on their social networking site, remember that real friendships aren't made by computers.

What should parents know about Instagram?

- Kids and teens love using the photo-sharing app Instagram because it lets them apply cool effects and captions to photos and videos and easily share them across a number of social media platforms. The ability to quickly change the look of their pics makes their lives look a little more awesome.
- Collecting a large number of followers -- and flattering comments -- is a badge of honour for diehards. On the other hand, negative comments can be really hurtful. If your kid uses Instagram, make sure he/she knows how to comment respectfully and deal with haters.
- Photos shared on Instagram are public and may have location information unless privacy settings are adjusted. Tagging a location when posting will show where the photo or video was captured including

private vicinities. Explaining to your child the consequences of this is advisable.So it's important for kids to use privacy settings to limit their audience. There are various steps you can take to make sure your child's profile and experience are both as safe as possible starting with the option of a Public or Private Profile: Private Profile This ensures only followers that your child knows and approves personally can see their posts. Public Profile All posts and activity can be seen by everyone who uses the app and web version of Instagram.

- By default, all profiles are Public, a Private Profile can be activated by selecting the gear icon in the top right of the profile view followed by Private Profile. The sharing and posting of content Public The most relaxed profile setting. All photos and videos are searchable and can be viewed and commented on by all users. Private Videos and photos are only seen by 'approved followers. All followers must be approved by your child

Tips to stay safe on social networking sites

- Make sure you're old enough to join
- Maybe use a made up name or nickname on your profile.
- Do not make friends you don't already know personally.
- Maybe use an email address that does not include your name.
- Use the strongest privacy setting when you set up your profile. This means that only your friends will be able to view your information.
- Pictures and Videos can be shared very careful when uploading-even if you only share it with friends, it can easily be spread much further
- Be very careful about sharing content online - especially if it isn't yours to share .Illegal downloads definitely should be avoided.

What risk does it pose?

- Device loss or theft. Losing a device to mishap or theft can cause lost productivity, data loss, and potential liability under data-protection laws.
- Loss of sensitive data. Many mobile devices may contain sensitive or confidential information, for example, personal photographs and videos, email messages, text messages and files.
- Unauthorised network penetration. Because many mobile devices provide a variety of network connectivity options, they could potentially be used to attack protected corporate systems.
- Intercepted or corrupted data. With so many business transactions taking place over mobile devices, there is always a concern that critical data could be intercepted via tapped phone lines or intercepted microwave transmissions.
- Malicious software. Viruses, Trojan Horses, and Worms are familiar threats to mobile devices it has become a significant target.

How can I avoid it from happening?

- When choosing a mobile device, consider its security features and ensure they are enabled.
- Install and maintain an Anti-Virus application on your smart device.
- Do not follow links sent in suspicious email or text messages.
- Carefully consider what information you want stored on the device
- Be cautious when selecting and installing applications
- Avoid joining unknown Wi-Fi networks and using unsecured Wi-Fi hotspots.
- Disable interfaces that are not in use, such as Bluetooth, infrared, or Wi-Fi.
- Delete all information stored in a device prior to discarding it.

Role of parents

- Talking to your child – openly, and regularly – is the best way to help keep them safe online. Tell your child that if they're in any doubt they should talk to you first.
- Talk to your child about what 'personal information' is - such as email address, full name, phone number, address and school name - and why it's important.
- Explain simple ways to protect privacy. For example, avoiding usernames like birthdates or locations that give away too much information.
- Discuss images and photos, and what might be appropriate. Help your child understand how photographs can give people a sense of your personality