ICTA

Be Safe in Cyberspace

Know your Rights
Know your Responsibilities

Staying safe online

The Internet and World Wide Web have revolutionized the way people live around the world giving unprecedented access to a world of knowledge and immense opportunities to interact and communicate across geographical boundaries. Not surprisingly, the Internet has become very popular with the young people of today. The Internet provides avenues for you to learn, discover the world, create content, interact and have fun.

And online access can now be obtained not just through PCs but also via mobile handsets, game consoles, android and other devices. This is our virtual world.

But are you aware that the Internet can also pose many dangers to children and young people? This is because there are many people who knowingly use the Internet to conduct illegal activities and cause harm to others. This can be harm caused while the victim is online or worse still the victim may be lured to meet the criminal offline. So it can be very difficult to stop someone victimizing you if you do not know who they really are or where they are physically in the real world.

The ICT Authority's initiative to organise this talk by Justice Tandon is both timely and warranted given that many people, especially the young fall prey to cyber criminals. Many people may, without realizing it, misuse the Internet not considering the harm they may be causing others or worse still they may be committing crimes punishable by law.

In cyberspace, you could be exposed to cyber crime wherever and whenever you are on line. I hope this guide gives you a glimpse of the pitfalls in order to help Mauritian youth make the most of this astounding technology that the Internet is and will doubtless continue to be.

Trilock Dwarka, Chairman
Information and Communication Technologies Authority &
National Cybercrime Prevention Committee

Some typical dangers and how to avoid them

Malicious software: Malware, botnets, Trojans and computer viruses are all tools used by offenders to gain unauthorised access to a computer system or network. If the virus was sent to you via an infected email from someone you know, then you should let them know their computer is probably also infected. If you cannot solve the problem yourself, get help from an IT professional.

Internet Banking or Financial Fraud: Cyber criminals will also use technology to illegally remove money from or transfer it to a different bank account. The criminal will use spam e-mails to obtain information about the customer's internet banking details. Millions of such e-mails are sent and some innocent people do get caught. Internet banking fraud is fraud or theft committed using online technology to illegally remove money from, or transfer it to, a different bank account.

Phishing: Phishing is an activity that criminals online use to commit Internet banking fraud. The term 'phishing' refers to the use of spam e-mails as if they are being sent from a bank; in this way criminals 'fish' for bank customer's logon information.

Scams: Criminals will also ask victims to provide bank account or personal details in order to receive a windfall. The windfall could be "lottery win" or other fictitious promise.

Identity theft :Criminals can use personal details to steal your identity to get money from you or your friends . This is online identity theft -- that is the criminals will use the details to pretend to be you and commit fraud. So don't reveal too much in early emails and online conversations. Questions you are being asked may be used as security passwords to get access to your online accounts.

Impersonation: Impersonation is when the actions or behaviour of someone is copied for illegal purposes. Very often the intention behind this is identity theft in order to commit fraud to obtain confidential information or property.

Defamation: involves the publication of material that tends to injure the personal, professional, and trade or business reputation of an individual or a company; defamation can expose people to ridicule and should be reported to the police.

Grooming or child solicitation: this is when ill meaning adults encourage young people to make friends with them to obtain personal information with a view to exploiting the child or young person usually via sexual abuse. Such predators may also exploit lonely or deprived children by offering them false emotional support or bribing them with gifts. Take care when choosing screen names and email addresses. Do not choose anything that reveals gender, location, age or is suggestive or attractive. Terms such as 'Young boy', 'Sweet girl' or 'Innocent' can attract child sex offenders. Exposure to problematic or illegal materials: a child or young person can without expecting it come across disturbing material online like violence, pornography or racism. This can be traumatic or encourage the young person to partake in similar behaviour.

Cyberbullying: this can be someone sending text messages that threaten or posting unpleasant information about someone or use hurtful words which can cause distress. Ignore bad behaviour. If you must react tell a responsible adult whom you trust. Trust your feelings. If you feel uncomfortable about any online activity, report it.

Harassment: this is a crime and public safety issue. Any case of harassment should be reported to the police, particularly if you are concerned for your physical safety. Avoid using websites where you think you will be harassed.

Social Networking: Social networking allows you to make friends across the world and develop many skills such as communication but many people have fallen prey to over exposing themselves on social network sites. Beware of putting too much personal information like telephone numbers, pictures which can later be manipulated and distorted by ill meaning people. The victim can lose all privacy. Don't be tempted to meet people whom you get to know online. If you must, make sure you are accompanied by a trusted adult.

Spam: this is unsolicited messages sent via email, SMS, MMS and other, similar electronic messaging media. If you receive a suspect email, the best course of action is to delete it immediately. Do not follow any links, or reply to the sender.

Make the Internet your friend, not your foe

- Make the Internet your friend and not your foe
- Protect yourself and others more vulnerable than you.
- Remember you need to keep learning how to use the Internet wisely to benefit from its full potential.
- Set your boundaries - keep yourself safe. Just do as you would do in real life. Ask yourself would you give out your personal details or about your parents to people you meet the first time?
- Help to protect those younger than yourself from the above dangers.
- Respect the intellectual property and creative work of others. Don't copy material that is copyrighted.
- Keep an open mind but don't believe every thing and anything you see or hear or watch online.
- Keep your password only for yourself. Change it as often as you can.

Become a responsible digital citizen.

Information & Communication Technologies Authority of Mauritius (ICT Authority)