AITI

Authority for
Info-communications
Technology
Industry of Brunei Darussalam

CYBER SAFETY TIPS

Be Aware
Secure &
Vigilant

CONTENTS

AKNOWLEDGEMENT

> INFORMATION TECHNOLOGY PROTECTIVE SECURITY SERVICES PTE LTD (ITPSS)
> INTERNATIONAL TELECOMMUNICATION UNION (ITU)
> INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE (IDA)

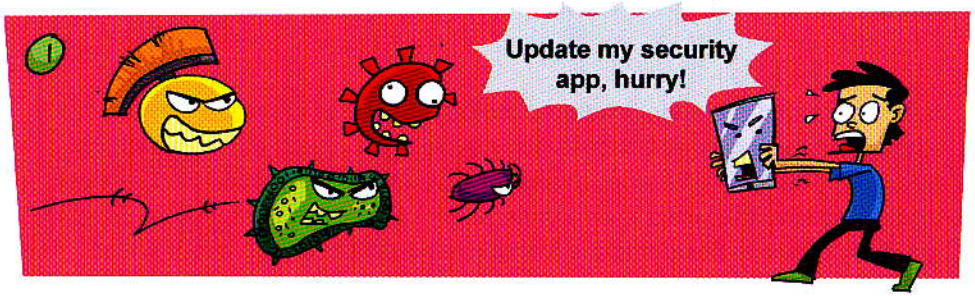
INTRODUCTION

Information and communication technology (ICT) has changed tremendously throughout the years and is constantly evolving to enrich our lives with its potential. The Internet makes available a wealth of information and services from all around the world to everyone at the click of a button. However, every good thing has its flaws and the Internet is no different. The exponential growth in Internet use exposes users to potential threats such as computer viruses and hackers that can mine personal information such as bank accounts details, access private emails and commit other cyber crimes such as the exploitation of children. One way of fighting off these dangers is by committing to cyber safety and security. We would like to share some of the ways to protect yourself and family when going online.

Disclaimer:

The information contained in this document is provided by AITI for general information purposes only. AITI makes no representations or warranties of any kind, expressed or implied, about the completeness, accuracy, reliability, suitability or availability of the information, products, services, or related graphics contained herein for any purpose. Any reliance you place on such information is strictly at your own risk. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this document.

ANTI-VIRUS SOFTWARE



Computer virus is a computer programme that can copy itself and infect a computer without permission or knowledge of the computer owner or user. It can spread from one computer to another through emails, USB device or through a network file system which perform malicious activities.

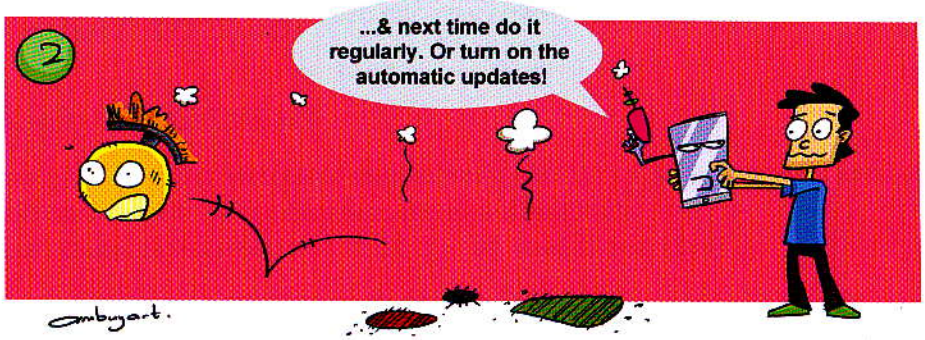
Always Remember To:

1. Install anti-virus software in your computer. Anti-virus software helps to detect and remove computer viruses and other malicious programmes such as worms and trojans.

2. Enable your anti-virus protection.

3. Update your anti-virus software regularly. Set the update to automatic so that when you are online, you will be prompted to download any latest update.

4. Scan your computer regularly after updating your anti-virus programme.



PERSONAL FIREWALL

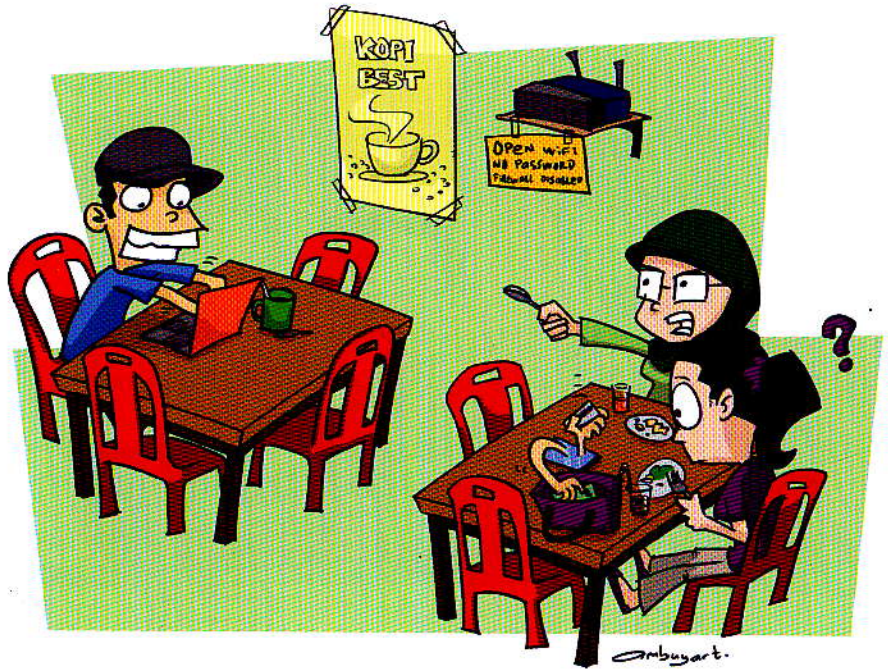
A **firewall** is a software or hardware designed to block hackers from accessing your computer. It monitors the communications between your computer and the network, and blocks unauthorized connections to your computer. A firewall can also block programmes residing in your computer from sending out information to the internet without your approval.

Always Remember To:

1. Install a firewall on your computer or home network.

2. Configure your firewall to prevent or block other computers on the Internet from accessing your computer.

3. Configure your firewall to stop information in your computer being sent out to the Internet without your approval.

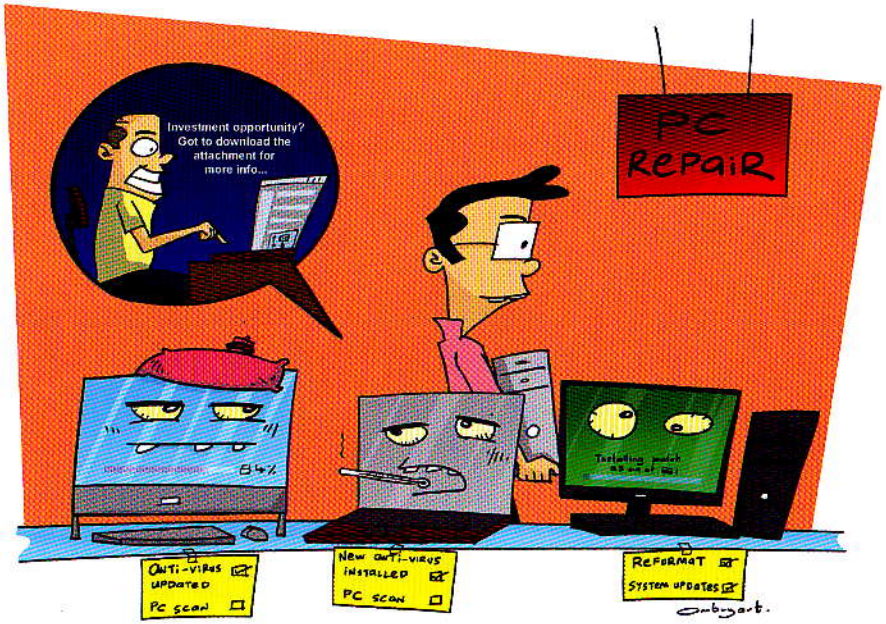


SUSPICIOUS EMAILS

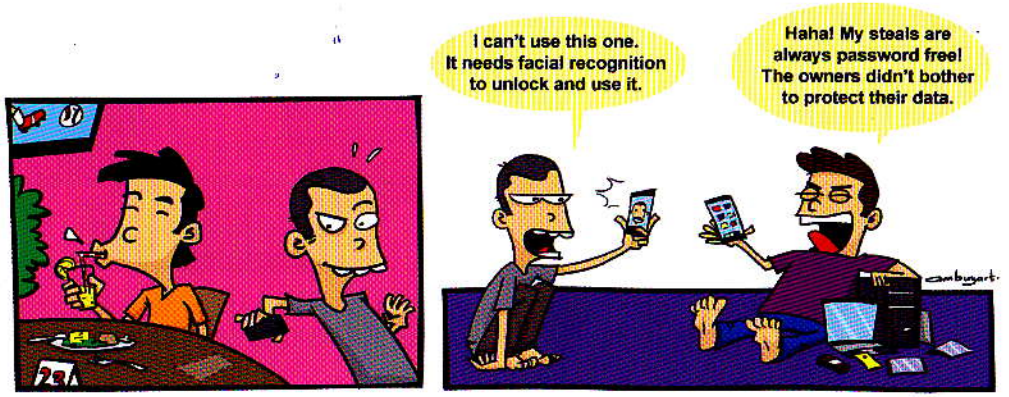
Never open an **email** which has a suspicious title especially when you do not know the sender. Emails are commonly used to disseminate viruses, worms and Trojans. Be very careful of acting on the contents of the email and opening files from an unknown sender. Such emails may be frauds or scams.

Always Remember To:

1. Scan all email attachments for viruses before opening them.
2. Delete the email if the subject title appears suspicious or strange, even if the email is from someone you know. The person may have sent you a virus unintentionally.
3. Never open attachments with the file extensions ".exe" and ".vbs" as they are often used to spread viruses.



SAFEGUARD YOUR PASSWORD



A **password** is commonly used to access a computer system. A password is like your house keys. Most people would not leave the house keys hanging on their front door and so you should safeguard your password.

You should choose a strong password that is easy to remember but difficult to guess. You can use a paraphrase to create a strong password.

For example, the password "Ah2r3da1c" is derived from the first characters from the phase "Abu has 2 rabbits, 3 ducks and 1 cat".

Always Remember:

1. Your password should consist of at least 8 alphanumeric characters.
2. Never share your password with others. Be very wary of people who may try to trick you to reveal your password over the phone or email.
3. Never share your password in your computer as anyone can access it or write it down.

WIRELESS NETWORK

A **wireless network** refers to wireless LANs (Local Area Networks). It can be used by more than one person within range to access the Internet. This means any neighbour or passer-by in the street with a wireless laptop can find and access your home network.

Always Remember To:

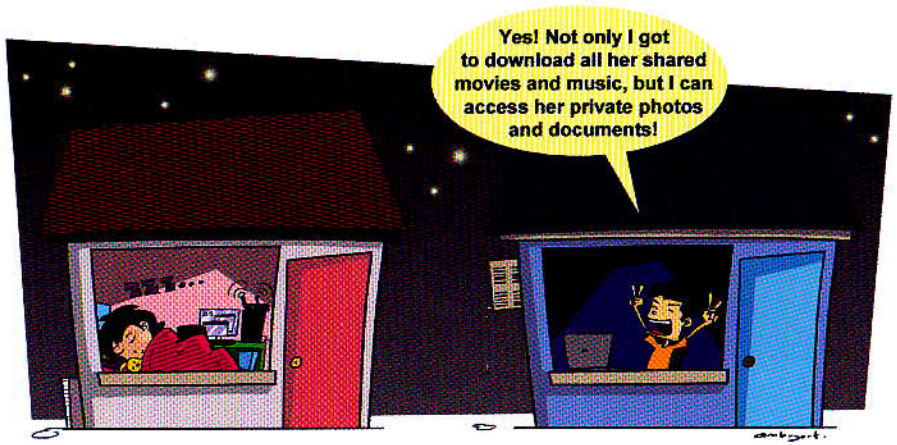
1. Secure your wireless network with a password. An unsecured network makes it easier for hackers to access your computer.

2. Change the Service Set Identifier (SSID).
   Your router will have its own default name (SSID). Hackers know default manufacturer's settings so you need to change the SSID to prevent them gaining access.

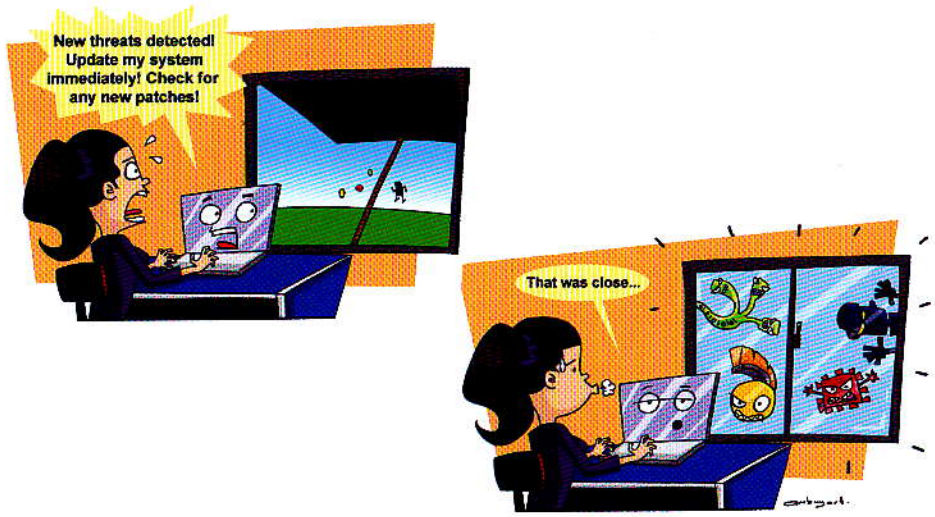
3. Disable the SSID Broadcast.
   An SSID broadcast sends a signal to nearby computers to tell them you have a wireless network, so it is important to switch it off to keep your network hidden.

4. Change Your Router's User Name and Password periodically.

5. Enable WEP Security.
   WEP stands for Wired Equivalent Privacy and you can ask your computer to automatically turn it on. It encrypts your wireless broadband signal to prevent anyone snooping on it.



SOFTWARE UPDATE



Software patch (update) is designed to fix small bugs, glitches, or address software-to-hardware or operating system compatibility issues. It removes programming flaws and vulnerabilities in computer software that can be exploited by hackers and malware.

Some software patches require a reboot to take effect. Save your work and reboot at the earliest opportunity when prompted by the system.

Always Remember To:

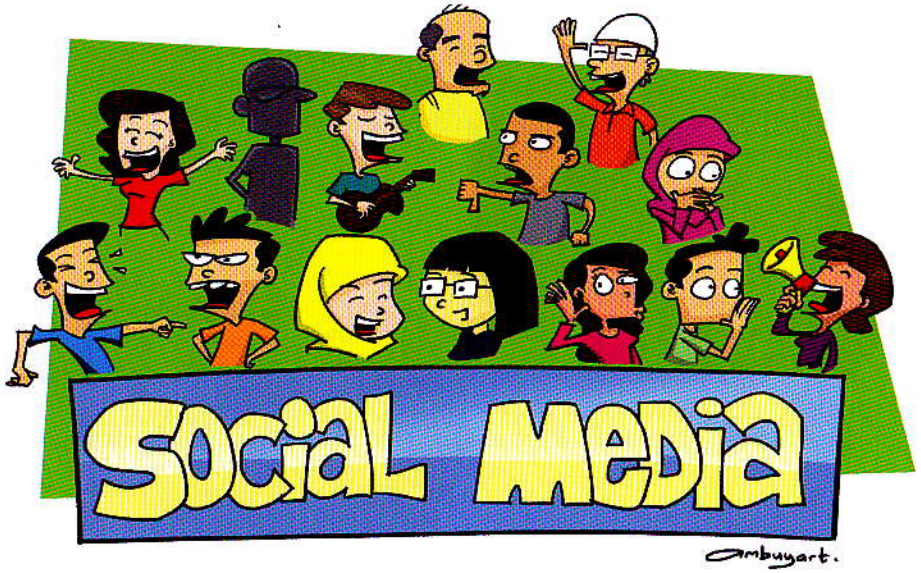
1. Keep your operating system and software up-to-date and turn on automatic updates.

2. Never allow the download and installation of dynamic or interactive content (active content) from any suspicious websites.

3. Check authenticity of contents, attachments and links with the sender when in doubt even when it appears to be from someone you know.

4. Scan your computer often with an anti-virus software.

SOCIAL NETWORKING



Social networking websites like Facebook, Twitter and Instagram are services people can use to connect with others to share information like photos, videos, and personal messages.

Once information is posted and uploaded to a social networking site, it is permanent and becomes public information. The more information you post, the more vulnerable you may become. Hackers, spammers, virus writers, identity thieves, and other cyber criminals constantly follow the Internet traffic.

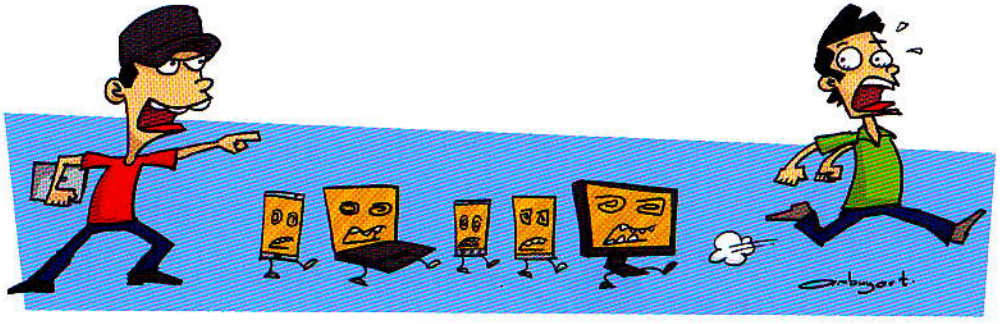
Always Remember To:

1. Learn and use the privacy and security settings on social networks. They can help you control and restrict who sees what you post and manage your online experience in a positive way.
2. Be cautious about how much personal information you provide. Avoid revealing your personal information such as addresses, contact numbers and credit card numbers.
3. Make passwords long, strong and unique.
4. Know and manage your friends.
5. Avoid meeting people you know online.

BOTNET

A **botnet** is a group of computers that have been infected with malicious software (also known as zombie), allowing the attacker to remotely control the systems. Victims are usually not aware that they are infected or their system is being controlled remotely by a botnet administrator.

Botnets can be used to send spam or viruses or perform Distributed Denial-of-Service (DDoS) attack against governments or private organizations, bringing down their online services (e.g. Government websites, Internet banking and media websites). This is accomplished by directing the vast number of zombies to simultaneously make request to a particular online service, thereby crippling its ability to handle legitimate requests. The service then becomes inaccessible.



Always Remember To:

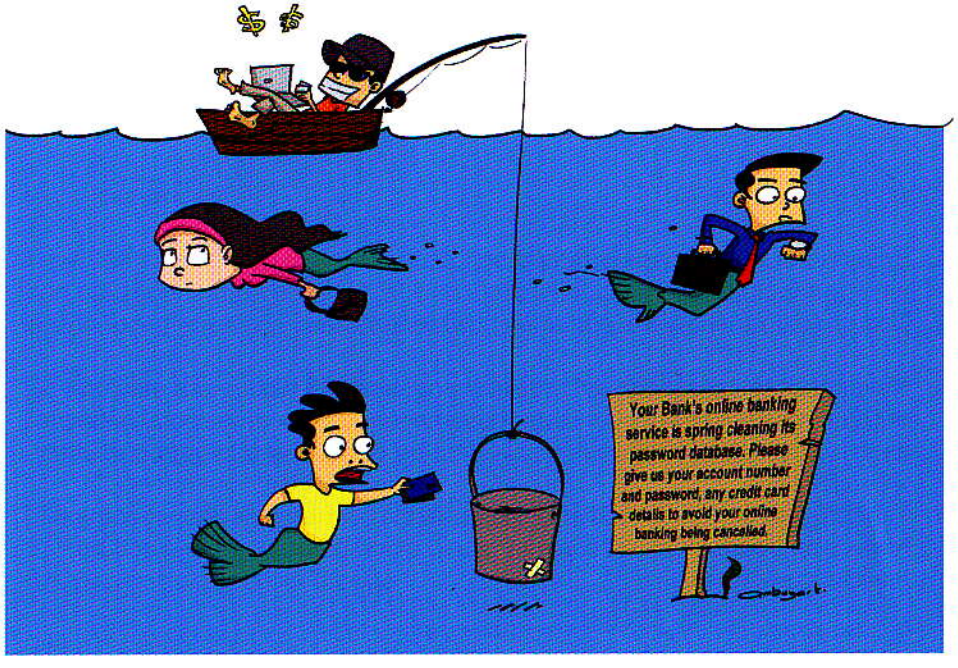
1. Ensure that your firewall is turned on.
2. Use up to date anti-virus and anti-spyware software.
3. Never click on links or downloads that you think are pictures or movies, or links you click in email or instant messages (IM), or on a social network as they may cause malicious software to be downloaded to your computer.
4. Turn off your computer and internet connection when you are not using it. Always on internet connection can cause a computer to get infected by malicious software.

PHISHING

Phishing is a criminal activity carried out by fraudsters attempting to obtain sensitive information, and informing the recipient that some type of problem has affected his account and directing him to follow a provided hyperlink to clear up the problem such as passwords, credit card details and PINs.

Always Remember To:

1. Never click on the link in an unexpected or suspicious message you receive.
2. Be more cautious as your email accounts may be used to conduct fraud or other illegal activities.
3. Never click on pop-ups or ads.
4. Log-off when connecting to secure web sites. If you do not, the next user of the computer may have access to your data.



BACK-UP DATA

System back-ups are very crucial but it is often overlooked. If you store original data on local drives or laptops, you are personally responsible for the backup and secure storage of data.

Backup original data files and software programs with hard drive or CDs. The frequency of the backup cycle should be consistent with the frequency with which you modify the information.

Always remember to:

1. Perform your data backups regularly.
2. Ensure that your backup software (agent and server) are properly patched.
3. Store back-up disks at a geographically separate and secure location.
4. Choose backup which save your data in encrypted format.

AUTHORIZED HARDWARE AND SOFTWARE

The **end-users should only use software and hardware that are authorized or licensed**. This is to ensure that end users do not introduce unlicensed software or malware to their computer.

This includes all software application installed on your office computer as well as the storage media that you plug into your computer.

Always remember to:

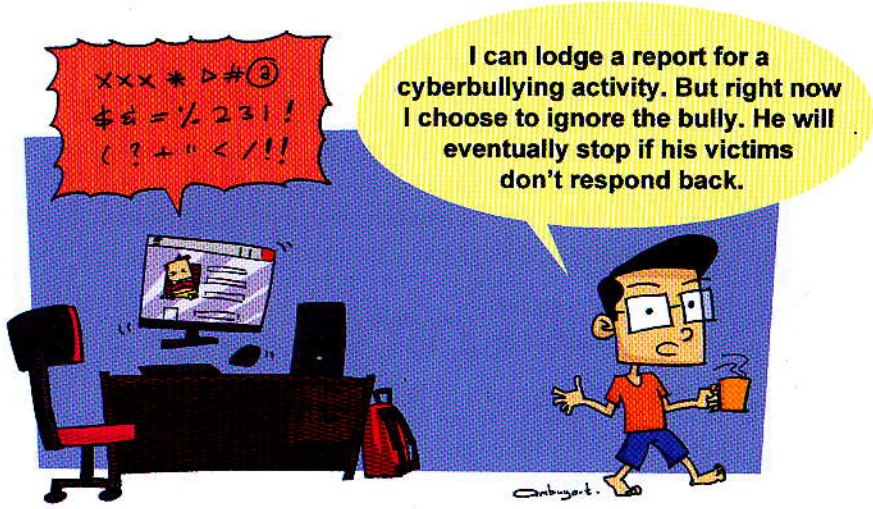
1. Use licensed software to ensure that you can receive regular patches to fix vulnerable in the software.
2. Never download unauthorized software to your computer.
3. Never access to unauthorized websites.
4. Reduce the risk of infection by disabling the autorun feature. Click on files and installers manually to launch them.

CYBER BULLYING

Cyber bullying refers to a situation when someone is repeatedly and intentionally humiliated, threatened, harassed and embarrassed by another person using email, instant messaging, text messaging, chat rooms, cell phones, website posts, social networking sites and other forms of information technology.

Always remember to:

1. Restrict excess visibility. You must be very careful while providing your personal information online and limit the number of the people who can see your details. Different access options are provided in almost every online community. This actively will discourage cyber bullying and protect you from becoming the victim of cyber bullying.
2. Keep records of the data, websites and pages that you have visited along with the exact time and date. Documenting your activities will make it easier for you to know the cyber bullies.
3. Seek the help of people who are in a position to assist you such as your parents /guardians, supervisors or the authorities.
4. Provide good security facilities to your computer. To remain safe from cyber bullies, restrict unauthenticated websites and use efficient and effective anti-virus which has the ability to respond any interruption in work.



14

MY COMPUTER IS UNDER ATTACK - WHAT DO I DO?

1. Disconnect your computer from the Internet immediately.
2. Perform an overall virus scan on your computer.
3. Contact BruCERT (Brunei Darussalam Computer Emergency Response Team) to report the incident and get further advice on what to do.

WHAT IS BruCERT?

Brunei National Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

BruCERT will coordinate with local and international Computer Security Incident Response Teams (CSIRTs), network service providers, security vendors, government agencies, as well as other related organisations to facilitate the detection, analysis and prevention of security incidents on the Internet.

In its capacity as BruCERT, Information Technology Protective Security Services Pte Ltd (ITPSS) is affiliated with Asia-Pacific CERT (APCERT), which acts as a platform to share and gather information related to cyber security with other CERTS worldwide. Its membership makes ITPSS a window to security related activities in other parts of the world.

BruCERT's contact details:

Hotline:	+6732458001
Email:	cert@brucert.org.bn
Website:	www.brucert.org.bn

Operating Hours:
Mon-Fri 8.30 am – 5.00 pm