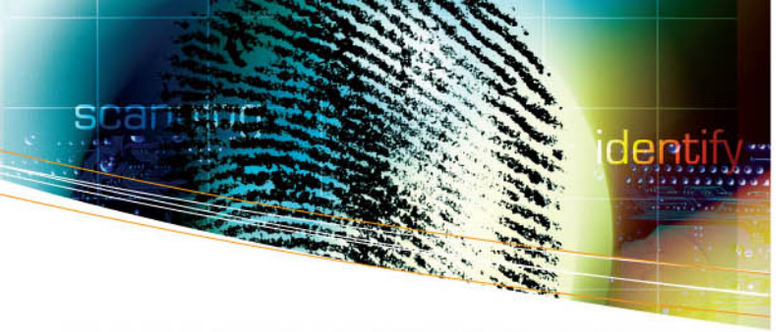

THE FOLLOWING ARE SOME TIPS FOR SAFER INTERNET SURFING AND EXPERIENCE:

- Be careful when giving out personal information through websites, email, instant messaging systems, chat rooms or on message boards, especially when you are not sure of the recipient or website owner. You have the right to ask how collected information will be used. Emails from unrecognised party are usually sent to convince you to provide your personal information, known as phishing emails. The information collected is usually used for fraudulent activities that can harm you financially or personally.
- Use anti-virus, anti-spyware and firewall software on your computers and servers. You must scan any email attachment, files and programs on CDROM, USB drives, external hard disk drives and those downloaded from any websites or computer network. It is recommended that "Auto Update" feature is enabled to ensure timely updates.
- Create strong password by combining characters made up of uppercase, lowercase, numeric and symbols with a minimum length of 8 characters. Also, ensure the password does not contain your username, real name or information that may reveal your personal information such as your spouse's name, pet's name, etc.
- Enable automatic updates for your operating system and application software and always use the latest version.
- Never provide confidential (e.g. personal, financial) information while replying email messages. Use encryption where possible. Ensure that Transport Layer Security (TLS) or Secure Sockets Layer (SSL) is used when performing online transactions.
- Regularly scan your computer for adware and spyware using security tools such as Ad-Aware (www.lavasoft.com) or Spybot (www.safer-networking.org). Be careful when clicking options appearing on "Pop up" windows or dialog boxes, it can send information from your computer to a third party. Unwanted applications or drive by download applications can be installed without your knowledge.
- Study and configure security features of your web browsers. Web browsers such as Internet Explorer 7.0 above and Mozilla Firefox comes with Phishing filter features and Pop-up blockers.
- Monitor Internet Access (e.g. Internet Explorer, Mozilla Firefox) Regularly check the history setting and use the content advisor in Internet Explorer. Firefox provides comprehensive content blocking features like Pop-up, scripts, images, etc.
- Never execute programs with automatic downloads.
- Refuse some or all cookies offered by websites.
- Always read the website's privacy policy on information handling before conducting transaction or providing information.
- Keep yourself updated with latest advisory and threats
  You can visit www.mycert.my to get latest advisory and threats and www.esecurity.org.my for internet safety tips and best practices.

INCIDENT REPORTING CHANNELS

Online Reporting
http://www.mycert.org.my/report_incidents/online_form.html

Telephone
Call Cyber999 Hotline number at 1-300-88-2999 or +603-8992 6969.
Office Hours only. Monday – Friday, 8:30am - 5:30pm, GMT+0800

Mobile Phone
Call +6019-266 5850 (24 x 7)

SMS
Send SMS to +6019-281 3801

Email
Send email to mycert@mycert.org.my

Fax
Download form at:
http://www.mycert.org.my/en/services/report_incidents/fax_details/main/detail/157/index.html and fax to +603-8945 3442

CyberSecurity Malaysia
Level 7, Sapura @ Mines, 7, Jalan Tasik
The Mines Resort City, 43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my

MOSTI
Ministry of Science, Technology and Innovation

Best Brand Internet Security

ISMS SIRIM

UKAS

INFORMATION SECURITY BEST PRACTICE SERIES:

SAFER INTERNET SURFING

CyberSecurity MALAYSIA
An agency under MOSTI

In today's world the internet has become part of everyone's life as vast amount of information and business transactions are conducted online and it has become highly accessible for many.

In today's world the internet has become part of everyone's life as vast amount of information and business transactions are conducted online and it has become highly accessible for many. Once connected to the internet, people can access various internet services such as web browsing, email, chat, newsgroups, online shopping, online auction, online banking, social networking, online gaming, file sharing, voice over IP and more. As internet technology progresses, new services are being introduced to cater for the needs of the people and businesses.

The threats on the Internet poses a broad range of risks to users and their computer which can lead to financial losses, identity theft, loss of confidential information/data, theft of network resources, damaged personal/business reputation, and loss of consumer confidence in online services such as online banking. This also includes businesses which offer online services and transactions.

The following are some of the main threats:

Threats	Definition	How it can affect you?
Virus	A piece of malicious computer code that attaches itself to a program or a file to cause damage.	It can spread from one computer to another via computer network, portable storage medias (CDROM, USB Flash drives), email attachments or downloaded files. These malicious codes will infect your hard disk or programs.
Worm	A malicious code / program that is able to replicate itself and spread over a computer network.	It can spread from one computer to another computer by making copies of itself and re-sending itself as an email attachment or become part of a network message without any user intervention.
Trojan Horse	A computer program that appears to be a useful program but performs malicious activity in stealth-mode to cause harm to your computer.	It infects when people open or install a computer program or file that appears to come from a legitimate source or appear to be useful.
Hoax	Hoaxes are misleading or false messages sent to computer users in order to convince them to respond so fraud or identity theft can be committed.	Hoaxes are usually sent via email with the intention to lure victims for fraudulent means. An example is a "chain letter" seeking computer users to forward to as many people they know. There also email messages that make false claim of virus alerts to mislead users to take action that could compromise their computer, e.g. update/download program from a fraudulent website.
Spam	Unsolicited bulk email messages from unknown party.	It is usually sent in bulk and to a large numbers of people to promote products or services. Spam can be annoying and confusing. Spammers obtain email addresses from chat rooms, websites, hackers, newsgroups and from use of malware to gather emails from address books.
Adware	Adware is any software application which downloads and displays advertising banners on your computer. Usually this happens after installation of a new software or while the software is being used.	Your personal information or information from your computer can be sent as the result of clicking some of the options or features in the "pop-up" window.
Spyware	Spyware is a malicious program installed stealthily that gathers information about a person or organisation without their knowledge.	It is often installed without user's consent, as a drive-by download, or as the result of clicking some option in a "pop-up" window.
Phishing scam	Legitimate-looking emails and websites designed to lure victims for fraudulent purposes.	Phishers send phishing emails and links to phishing websites in an effort to get personal or financial information from the recipient usually for financial gain or to commit fraud.