CyberSAFE

Security Awareness For Everyone

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA
www.cybersecurity.org.my

An agency under
MOSTI

Editor's note

Hi and I am glad to announce that you are holding an inaugural issue of CyberSAFE newsletter that is for people like us to learn tips and techniques for us to be safe when we are online. The online world is a place where we communicate, entertain and do our work today and it has become very much part of our life now. Gone are the days where the computer system is for the computer geeks or those who study computing. Now it's everybody's tool and one that people can't do without. So why is there a need for security awareness? Just like in the real life, we are bound to face hurdles and dangers in our daily life. Therefore, we need to be aware of the dangers and learn to be safe when chatting or banking online.

This newsletter is fun-filled with activities, articles and safety tips for you to get to know the cyber world better. This newsletter is produced quarterly and is made available to everyone. Your feedback is most welcomed for us to improve further.

Thank you and I hope you find this issue to be fruitful and do share it with your friends and family members.

Raj Kumar

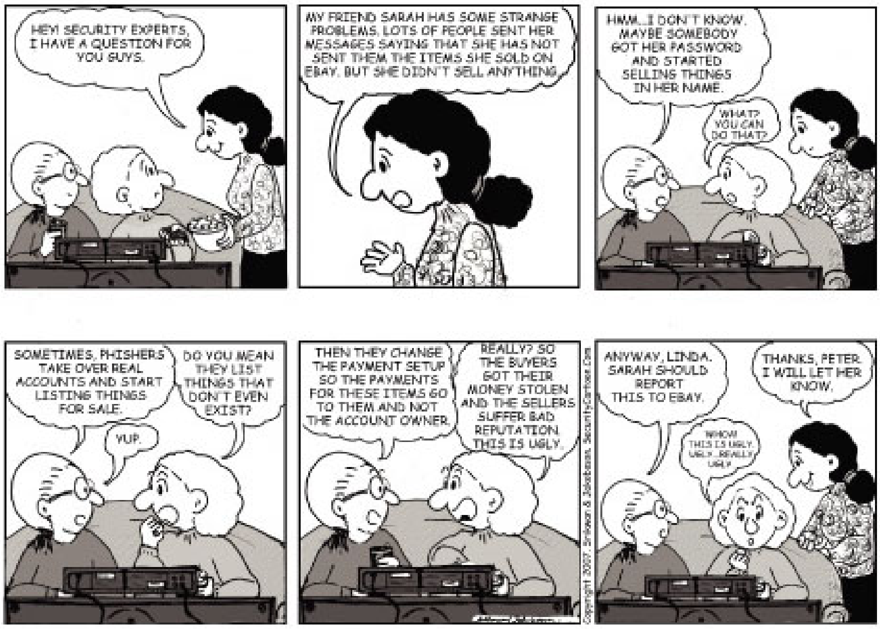
Raj Kumar
Editor

> **Just as drivers who share the road must also share responsibility for safety, we all now share the same global network, and thus must regard computer security as a necessary social responsibility. To me, anyone unwilling to take simple security precautions is a major, active part of the problem.**
>
> *Fred Langa*

CyberSafety Tip:
Safe Internet Banking

As more people see the convenience of conducting their banking transactions and paying their bills using the Internet, this has become a place for fraudsters to look for their victims. It is not difficult for fraudster to capture your information or user ID over the Internet and through your email messages.

See page 02


HEY! SECURITY EXPERTS, I HAVE A QUESTION FOR YOU GUYS.
MY FRIEND SARAH HAS SOME STRANGE PROBLEMS. LOTS OF PEOPLE SENT HER MESSAGES SAYING THAT SHE HAS NOT SENT THEM THE ITEMS SHE SOLD ON EBAY. BUT SHE DIDN'T SELL ANYTHING.
HMM...I DON'T KNOW. MAYBE SOMEBODY GOT HER PASSWORD AND STARTED SELLING THINGS IN HER NAME.
WHAT? YOU CAN DO THAT?
SOMETIMES, PHISHERS TAKE OVER REAL ACCOUNTS AND START LISTING THINGS FOR SALE.
DO YOU MEAN THEY LIST THINGS THAT DON'T EVEN EXIST?
YUP.
THEN THEY CHANGE THE PAYMENT SETUP SO THE PAYMENTS FOR THESE ITEMS GO TO THEM AND NOT THE ACCOUNT OWNER.
REALLY? SO THE BUYERS GOT THEIR MONEY STOLEN AND THE SELLERS SUFFER BAD REPUTATION. THIS IS UGLY.
Copyright 2007, Srikwan & Jakobsson, SecurityCartoon.Com
ANYWAY, LINDA, SARAH SHOULD REPORT THIS TO EBAY.
WHOA! THIS IS UGLY. UGLY...REALLY UGLY.
THANKS, PETER. I WILL LET HER KNOW.

Reproduced with permission. All material © 2007 Srikwan & Jakobsson

Volume 1 – 2007 | Printed Quarterly

CyberJargons

- **Cyberbullying** - is when a person, usually a child or teenager, is threatened, harassed, humiliated or embarrassed by another child or teenager using the Internet. If an adult is involved then it is often referred to as Cyberstalking.
- **Cyberstalking** - its use on the Internet means to stalk someone. Stalking is referred to as the conduct of harassing or threatening behavior repeatedly. Such action can be in the form of making threatening comments using chat rooms or mobile phones, following someone, damaging items or property that belong to you. This term is also often referred as online harassment and abuse.
- **Botnets** - is a network of computers that are infected with Malware (virus, worm, Trojans) that are used to send spam emails to other computers and can be used to shut down web sites. The computer owners are usually unaware that their computers have been compromised and used to carry out such malicious activity.

What you need to know:

1. Banks don't send emails asking users to update their account details.
2. Be alert of suspicious email that looks real.
3. Check for the security certificates issued for the website and to verify the website address.
4. Password and ID can be stolen using Malware and / or insecure browser settings.

What you should do to protect yourself and your account:

1. Use your own computer only, don't use public computers.
2. Besides updating your system and antivirus, update your desktop applications as well.
3. Ensure you secure your browser, use anti-phishing tool.
4. Keep your password safe and memorize it. Don't write it down.
5. Avoid clicking on links in email that appears from the bank.
6. Check your account balance regularly.
7. Ensure that the website is secured (padlock icon) and verify the website address.

CyberQuiz

Note: The answers will be provided in the next issue.

1. When you meet a stranger while you are chatting, you should:
   a. Give your personal details
   b. Be careful not to give your personal information
   c. Introduce them to your friends

2. Which of the following is the strongest password, yet easy to remember?
   a. Tom123
   b. Am2pm
   c. Wdywtd@5t? (What do you want to do at 5 today?)

3. Anti-phishing toolbar___________
   a. traps suspicious URLs
   b. indicates a secured website
   c. is a Malware

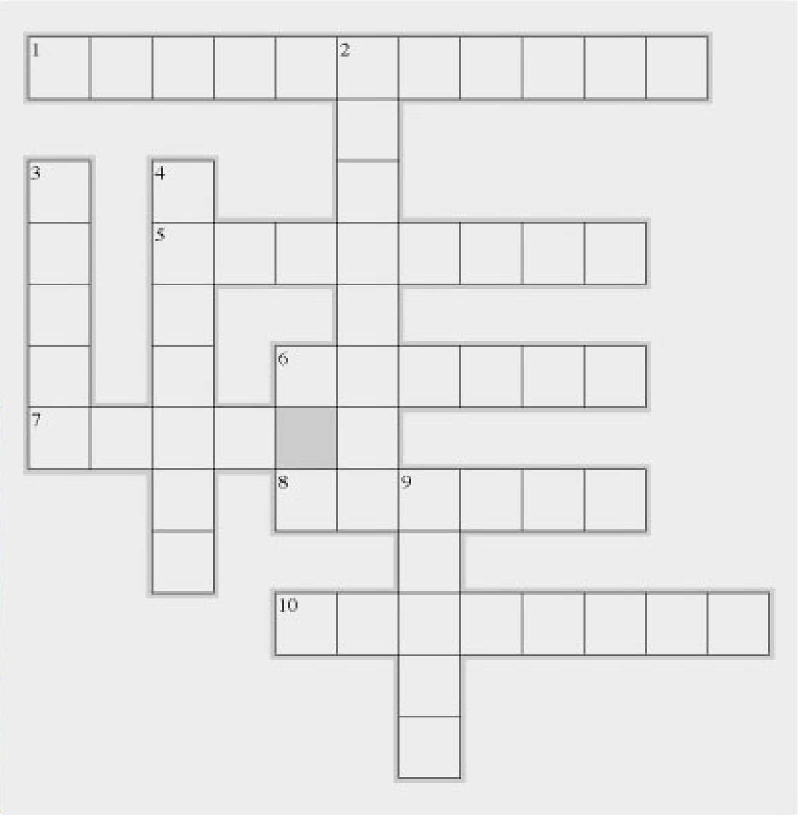
4. Trojans, worms and virus are also known as:
   a. Malware
   b. Adware
   c. Spyware

5. _______ is a program that hides programs or processes running in a computer

   a. Root kit
   b. Antivirus
   c. Firewall

CyberCrossword

Note: The answers will be provided in the next issue



Across

1. A program that finds spyware
5. An act of sending fake information
6. A file on your computer that enables websites to remember your details
7. Unwanted email
8. A program or script that displays advertisements on your computer
10. Acts as barrier between networks and blocks malicious traffic

Down

2. Secret word used for access
3. A harmful program or script
4. A program that collect information from your computer without your knowledge
9. A program or script that create copies of themselve and spread over the Internet

CyberArticle

Internet Safety for Children by their Parents

By Noor Aida and Raj Kumar, CyberSecurity Malaysia

Today, a computer system is affordable and the Internet is highly accessible for anyone at home. Parents usually make the decision of buying a computer and connecting it to the Internet for their children. Parents believe that the Internet has much to offer to cultivate their children's knowledge from informative websites and also to be used as tool for communication among their peers.

Lately, there have been many reported cases around the world relating to Cyberstalking and Cyberbullying targeted at children. Many of these cases can be avoided if the children are made aware of the workings of such activities and how best it can be prevented, e.g. safe chat, meeting strangers, etc. Parents need to be involved and teach their children on Internet safety and preventive tips. They also need to monitor their children's behavior when using the Internet. By teaching children Internet safety, they will be better aware of the dangers and more responsible when going online. It is crucial that parents get involved and advise their children to share their Internet experience.

Some tips for parents to educate their children on Internet safety:

1. Keep the computer in a public area of the house instead of the children's bedroom as it is more difficult to supervise them. Ensure that the computer screen is not hidden and can be easily seen. Once in a while, observe the website they are visiting.

2. Set reasonable rules and guidelines on computer and Internet usage for your children at home. You may set the time to be spent, allowable websites, etc. Discuss these with them so that they understand the reason why.

3. Study and monitor the time and pattern your children spend on the Internet regularly. You are not violating their privacy. This is part of your responsibilities as a parent to prevent and protect them from Internet threats.

4. Talk and educate your children on Internet safety frequently. Share with them any new tips or best practices you just learnt yourself.

5. Maintain all Internet and email accounts in your name, and not on their name. In addition, be in charge of all passwords especially the email and chat program. Regularly view your email sent box and chat history to ensure that they are not violating any of your Internet rules.

6. Get to know your children's online friends or chat buddies just like in real life. If possible, check and verify them. Block unknown buddies who try to make contact and make sure only you who can approve the person.

7. Learn what your children's favorite websites or online activities. Keep a list of safe websites and bookmark them so that you and your child will not mistype them. You can check in the browser's history to learn new websites they have visited.

8. Ensure that you create strong password for your computer and personal files to prevent unauthorised access. A good password consists of upper and lower case letter, numbers and symbols and must be changed every 6 months. Easy-to-remember yet good password can be created by taking the first letter of every word in a phrase, e.g. 'My three daughters stays at home with Fiona' will be 'M3ds@hwF'.

You should tell your children to:

1. Never give out personal information such as home address, phone number or school name without your permission, and to never share their photos with their online friends. Educate them on what information can and cannot be shared online with anyone.

2. Never respond to online friend's request to meet them without your consent. If you agree, you must accompany your child to the meeting and ask to meet in public places.

3. Never open email attachment from people whom they do not know. Educate them about danger of virus spread through email attachments and how it can harm their computer.

4. Seek for your help when they are unsure or upset over certain stuff in the Internet. You should be positive and don't overreact when they are telling the truth. Try not to give harsh punishment as this will make them unlikely to approach you in the future.

5. Remember that friends they met online may not be who they seem, and things they were told or what they read online may not be true.

6. Guard their passwords carefully. Do not share it with other people, even their best friends.

Parents need to get involved in their children's Internet exposure and activity, it would better enable them to be safer online and this would eventually create a safer society for all. Children seem to be the weakest link when it comes to communicating over the web and they can easily become a victim for harassment and stalking. There are many resources available online that focuses on this issue and what is more important is the proactive approach to be taken by all parents to educate their children.

Reference: U.S Dept of Justice - Federal Bureau of Investigation, 2007, A Parent's guide to Internet safety (http://www.fbi.gov/publications/pguide/pguidee.htm) [Cited 27th September 2007]

CyberResources and Reporting

Security Awareness Information, Videos and Posters for
Kids, Parents and Organisations
www.esecurity.org.my

Security Awareness Portal - www.esecurity.org.my

www.esecurity.org.my is a portal developed by CyberSecurity Malaysia to inform and educate computer users on threats and offer safety tips for protecting their computer while online. Contents of this portal is also contributed by local and international organisations and security experts. The website is targeted at three target audiences, namely, kids and teenagers, parents and adults, and organisations.

The website covers tips ranging from creating strong passwords, safe chatting, handling spam emails, safe online banking and more. The website is populated with awareness materials and information such as video, posters newsletters and more. The website is regularly updated with new content and safety tips for computer users and organisations.

Who to call when you have problems online?

Contact Cyber999!

CYBER999
REPORTING INCIDENTS & ALERTS
MyCERT
Malaysian Computer Emergency Response Team
www.mycert.org.my

If someone makes you feel uncomfortable (make harassing or threatening comments) or you face some issues (ID theft, Internet scam) while online, you can report to Cyber999. Cyber999 is a service offered by the Malaysian Computer Emergency Response Team (MyCERT) to respond to security issues or incidents faced by Internet users while online. This service is provided free and every reported case is treated with strict confidentiality.

To report incidents:
Online - **http://www.mycert.org.my/**
Tel - 03-89926969
Mobile phone (24 hrs) - **019-2665850**
SMS - **019-2813801**
Email - **mycert@mycert.org.my**
Print online form and fax - **603-89453442**

CyberSecurity Malaysia (formerly known as NISER)
Level 7, Sapura@MINES, No.7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan. | Tel: 03-89926888 | Fax: 03-89453205
www.cybersecurity.org.my