CyberSAFE

Security Awareness For Everyone

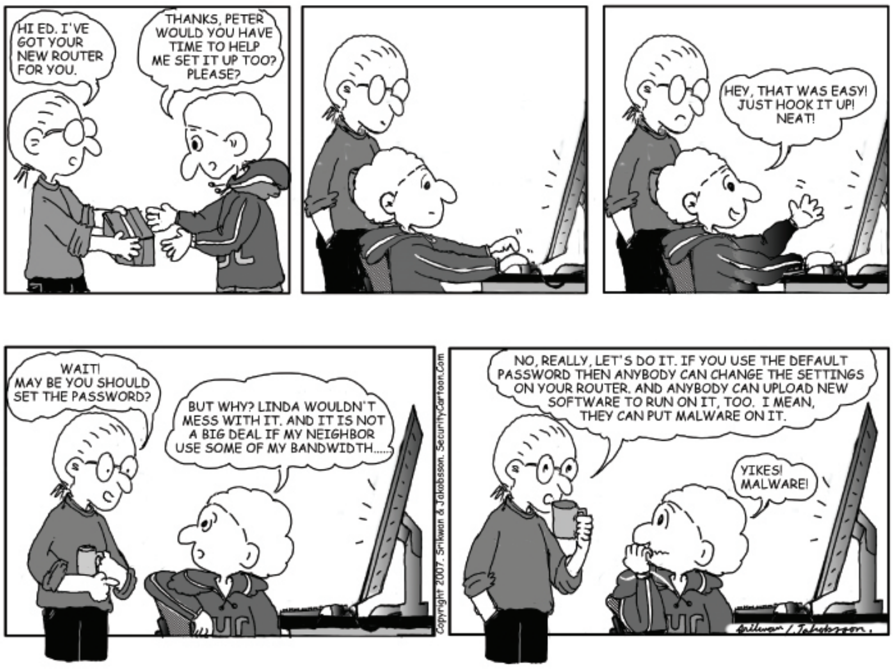
CYBERSAFE Vol.5 2008 | KDN License Number: PP15773/07/2009(022010)

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

CyberSecurity MALAYSIA

An agency under MOSTI

CyberCartoon


HI ED. I'VE GOT YOUR NEW ROUTER FOR YOU.
THANKS, PETER WOULD YOU HAVE TIME TO HELP ME SET IT UP TOO? PLEASE?
HEY, THAT WAS EASY! JUST HOOK IT UP! NEAT!
WAIT! MAY BE YOU SHOULD SET THE PASSWORD?
BUT WHY? LINDA WOULDN'T MESS WITH IT. AND IT IS NOT A BIG DEAL IF MY NEIGHBOR USE SOME OF MY BANDWIDTH.....
Copyright 2007. Srikwan & Jakobsson. SecurityCartoon.Com
NO, REALLY, LET'S DO IT. IF YOU USE THE DEFAULT PASSWORD THEN ANYBODY CAN CHANGE THE SETTINGS ON YOUR ROUTER. AND ANYBODY CAN UPLOAD NEW SOFTWARE TO RUN ON IT, TOO. I MEAN, THEY CAN PUT MALWARE ON IT.
YIKES! MALWARE!
Srikwan / Jakobsson.

Reproduced with permission. All material © 2008 Srikwan & Jakobsson. Please see www.SecurityCartoon.com for more material.

CyberSafety Tip - Safer Social Networking Experience

Social networking site allows you to express yourself and helps you to keep in touch with your friends. You can use this platform to exchange messages and post personal profiles to describe who you are and your interest, photos, creative writings, artwork, video and music.

The following are some tips for managing friends online:

- You should not post too much information on your personal profile and communicating with people you've only met recently online can put you in potential danger.
- Potential exploiters can use these profiles or your information to search for victims.
- Users can pretend to be someone else with a different age and background.
- Never post your personal information, such as your hand phone number,home address or the name of your school or workplace.
- Do not give your password to anyone.
- Add people as friends to your site if you know them in person.

See page 02

Message from the CEO

Welcome to the fifth edition of CyberSAFE awareness newsletter. As the internet has become is very much part of our life, therefore awareness on Internet safety and applying best practices is a must for every Internet user. This issue of CyberSAFE focuses on tips for social networking and an article on safer web browsing. For more tips, you can visit our security awarenessportal (www.esecurity.org.my). This portal is populated with many resources such as internet safety tips, posters, videos and more, in order to promote awareness. CyberSAFE is also designed to do the same and we hope that you will find this edition to be informative and helps you to pick up some tips for a safer online experience.

Best Regards,
Husin Jazri, *CISSP*

CyberQuote

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

Editor's note

Welcome back! We are proud to bring to you next edition of the CyberSAFE with the aim of sharing internet safety tips and best practices. This issue focuses on tips to protect your personal information when participating in social networking sites. You will also find new set of CyberQuiz and CyberCrossword to challenge your knowledge in information security, and also you will find the answers for the activities from the last issue. For those who missed out on the last issue, please visit www.esecurity.org.my and download a copy. We hope that you find our newsletter to be resourceful and do share with your family and friends.

Raj Kumar

Raj Kumar
Editor

Produced by:
CyberSecurity Malaysia (726630-U)
Level 7, SAPURA @ MINES,
7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan,
Malaysia.

Design & Layout:
Ilham Design (001690307-U)
7302 Jalan 18/11,
Taman Sri Serdang,
43300 Sri Kembangan,
Selangor Darul Ehsan,
Malaysia.
Tel: (03) 8948 2843
Fax: (03) 8948 2843

Printed by:
Arena Press Corporation Sdn Bhd
2, Jalan Lingkongan Brunei,
Off Jalan Pudu,
55100 Kuala Lumpur,
Malaysia.
Tel: (03) 2144 5668
Fax: (03) 2145 6078

From page 01

The following are some tips for safer online experience:

- Do not meet in person anyone you first "met" on a social networking site. Some people may not be who they say they are.
- Think before posting your photos. Personal photos should not have revealing information, such as school/workplace names or locations.
- Do not respond to any harassing comments posted on your profile.
- Delete messages of those who leave inappropriate comments.
- Check the privacy settings of the social networking sites that you use. You can set the privacy setting for your profile and items such as photos to either "Private" or "Public".
- Set privacy so that people can only be added as your friend if you approve it.
- Don't give out any personal information about yourself or anyone else.
- Set privacy so that people can only view your profile if you have approved them as a friend.
- Do not post information about your friends as you could put them at risk.
- Do remember what you post online are not private. Parents, teachers, and employers, may go online and find out things about you.

CyberJargons

VoIP

VoIP is a way to make and receive phone calls using a broadband internet connection instead of a traditional phone line.

The "Nigerian" Email Scam

Con artists claim to be officials, businesspeople, or the surviving spouses of former government official in Nigeria or another country whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or "taxes" to help them access their money.

Banner Ad

Also known as ad banner or online ad, is a graphical Web advertising image usually placed at the top of content pages that links to the advertiser's content page.

CyberQuiz

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

1. You can control access to your personal profile/information in social networking sites by using the privacy control features:

a. Yes
b. No
c. Not sure

2. Which of the following is a NOT good practice when you meet a stranger online:

a. Meet them in person
b. Do not share your personal information
c. Ask your parents or teacher if not sure about this person you met

3. Which of the following is sign of malware being present in your computer?

a. "Pop-ups" appear for no reason
b. Your system is unusually slow
c. All of the above

4. What you should NOT do when you receive an email attachment with .exe extension?

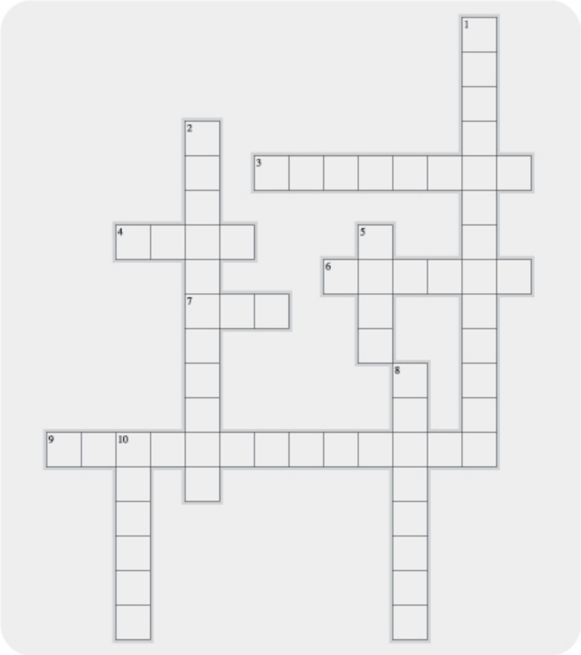
a. Scan for virus
b. Click and install the program
c. Delete the file

5. What should you do when you receive a hate speech via SMS (mobile phone) or Instant Messaging Systems?

a. Save it and report to MyCERT or Police
b. Delete it
c. Reply with another hate speech

CyberCrossword

Note: The answers will be provided in the next issue



Across

3. A ________should be changed often
4. A message spam that comes through Instant Messaging System
6. ______networking sites are where people can make new friends and share information
7. A short term used to describe a file-sharing systems between two people
9. The act of bullying someone using a mobile phone or computer

Down

1. The act of threatening someone online
2. A security program that detects spyware on your computer
5. ____is a form of Malware
8. The act of stealing credit card information using a special device
10. A network of malware-infected computers controlling other computers to do the same

CyberArticle

Guide to Safe Web Browsing

By Sharifah Roziah Bt Mohd Kassim (roziah@cybersecurity.my),
MyCERT Department, CyberSecurity Malaysia

Introduction

Security threats are not only being targeted at systems and networks but also web browsers. Malicious hackers and virus writers can take advantage of low security settings or vulnerabilities in your web browser to attack your computer. One of the ways they can do this is by convincing you to visit a malicious website and download a malicious code into your web browser without your knowledge.

Threats & consequences related to Web Browsing

- **Unauthenticated/fake sites**

Phishing scam is an example of how users can be duped into browsing an unauthenticated and fake websites. Phishing scam is an activity where an attacker spoofs the original email or website, mainly targeting financial institutions, and tries to convince customers to provide personal data such as credit card numbers, username and passwords, social security numbers, etc to be used to commit fraud.

- **Browser exploit/malicious code**

Lack of proper use of software engineering techniques and code checking can create software bugs. If a software bug is found and it is not rectified, the software bug can become the channel for malicious code to penetrate into software to create further damage or software errors.

- **Explicit Content**

Web platform allows for creative, independent, interactive exchange of information than the traditional media. Since content posted or created is often not filtered or moderated, it can be comprised of negative or menacing nature.

- **Man in the middle attack**

This type of attack is known as eavesdropping attack, where conversations between two parties are intercepted to gather information. Say person A talks to person B, and person C act as an eavesdropper, so he or she can hear what ever being talked about by person A and B. Electronic eavesdropping can be done via a network device such as network interface cards (NIC). The NIC is a device that delivers data from sender to the intended receiver.

Countermeasures to These Threats

- **Regularly update your web browser**

Web browsers must be patched and regularly updated to counter latest threats. When a threat is found, the web browser company will release a patch/update to protect your web browser and your computer. You should refer to the related vendor of your web browser for updates.

The following are the websites where you can find information in regards to current threats and vulnerabilities :

i) http://www.us-cert.gov/
ii) http://www.microsoft.com/security/default.mspx
iii) http://www.mycert.org.my
iv) http://www.incidents.org
v) http://www.securityfocus.com/
vi) http://update.microsoft.com

- **Verify that the sites you're browsing is "valid" site**

When you visit a website, sometimes it is hard to tell whether the site is a valid or hosted by the company "they say they are". Since there are many techniques that are used to spoof a website, a certificate is introduced. By default, the browser will always ask the user whether to accept or not to accept connection from the website. But in most cases, people will click OK and proceed to view the site of the URL that they have typed in.

- **Verify that a Website is secured**

Before you browse a website especially if you need to make a purchase or share sensitive personal information, you need to ensure that the website is using an encryption technique to secure the information that you are submitting. Look for the following security measures:

- Make sure you see https:// in the web address (URL) of the website.
- Look for a padlock icon (example: 🔒) in the lower right hand corner of your web browser, indicating that the web page is using a security certificate to encrypt the information that you submit.
- Click the padlock icon in the browser, or the "security certificate information" link, usually displayed on secured websites. The link will verify the identity, validity and security of the site, as well as provide the status of the security certificate.

• Configure browser to High Security

Most of the current security breaches came from ActiveX, Java and scripting. By default all these scripting is being accepted by browser. But due to high risk of security came from certain sites. It's a good thing to customize again the security level of your browser. Even though, customizing this security level doesn't fully secure you from the threat from the net. But it could somehow provide mitigation against it. And be sure to enable other security mechanism such as antivirus, firewall and intrusion detection system.

• Use SSL for secure transaction

Internet users are vulnerable to sniffing attack, since protocol such as HTTP, IMAP, and POP conduct transactions in clear text. The use of encryption technology can help to mitigate the effort of data being sniffed on the network. SSL or Secure socket Layer, a technology that adopts the advantage of encryption. SSL provides a mechanism for encrypting all kinds of network traffic - LDAP, POP, IMAP and most importantly HTTP.

• Download security tools that block "pop-up" windows

Pop-ups can also be considered as an unsafe feature that is usually used to advertise products and services. Pop-ups can also download malicious programs or scripts when a user clicks on it.

There many security software that can block pop-up ads. For example:

1. Pop-up stopper by Panicware
2. Earthlink toolbar
3. Noadware by Noadware.net
4. Google toolbar

• Use plain text to read emails

Email is one of the common channels an attacker use to spread malicious scripts and programs. The motive is to make the user to execute the code that they have sent. Therefore, it is easy spread via HTML-based email messages or systems. If you are using text-based email like Pine, this threat is lesser of a concern. It is recommended that the HTML feature to be disabled.

Answers:

The following are the answers to the activities in the last edition.

CyberQuiz

1. a
2. b
3. c
4. a
5. b

CyberCrossword

		1 B	A	N	2 D	W	I	D	T	H
					I					
			3 B		A				4 P	
			O		L				H	
			O		E				I	
5 H	A	C	K	E	R		6 P		S	
			M				R		H	
7 D	O	M	A	I	N		O		I	
			R				F		N	
		8 S	K	I	M	M	I	N	G	
							L			
		9 S	P	A	M	M	E	R		

References :

1) *http://www.mycert.org.my/data/content_files/11/78.pdf*
2) *http://www.microsoft.com*
3) *http://www.cert.org/advisories/CA-2002-04.html*
4) *http://communities.microsoft.com/newsgroups/default.asp?icp=xpsp2&slcid=us*

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 educate computer users on various cyber threats and to provide tips and best practices for them to be safer online.

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

Contact Cyber999 if you have problems online!

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

If someone makes you feel uncomfortable (harass or make threatening comments) or if you face some issues (identity theft, Internet scam) while online, seek assistance from Cyber999.

Cyber999 is a service offered by MyCERT (Malaysian Computer Emergency Response Team) to handle security incidents faced by Internet users. This service is provided free and your information submitted will be treated with strict confidentiality.

Cyber999 Contact Details:

Online	: **http://www.mycert.org.my/**
Telephone	: **(03) 8992 6969**
Mobile Phone (24 hrs)	: **(019) 266 5850**
SMS	: **(019) 281 3801**
Email	: **mycert@mycert.org.my**
Fax	: **(03) 8945 3442**

Print online form:
www.mycert.org.my/report_incidents/online_form.html

CyberSecurity Malaysia
Level 7, Sapura@MINES, No.7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan. | Tel: (03) 8992 6888 | Fax: (03) 8945 3205
www.cybersecurity.my