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

Message from the CEO

I would like to take this opportunity to welcome you to the third edition of CyberSAFE awareness newsletter. Internet users of today are made up of broad audience ranging from young children to senior citizens. As internet related issues are continually being reported in the media, it is vital that every internet user takes the little step in reading up on security tips and best practices. We at CyberSecurity Malaysia aim to ensure that everyone is educated on internet safety regardless of their computing experience and we sincerely hope that this new edition of CyberSAFE will help you to achieve just that.

Best Regards,
Husin Jazri, *CISSP*

CyberQuote

If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

White House Cybersecurity Advisor, Richard Clarke

CyberSafety Tip

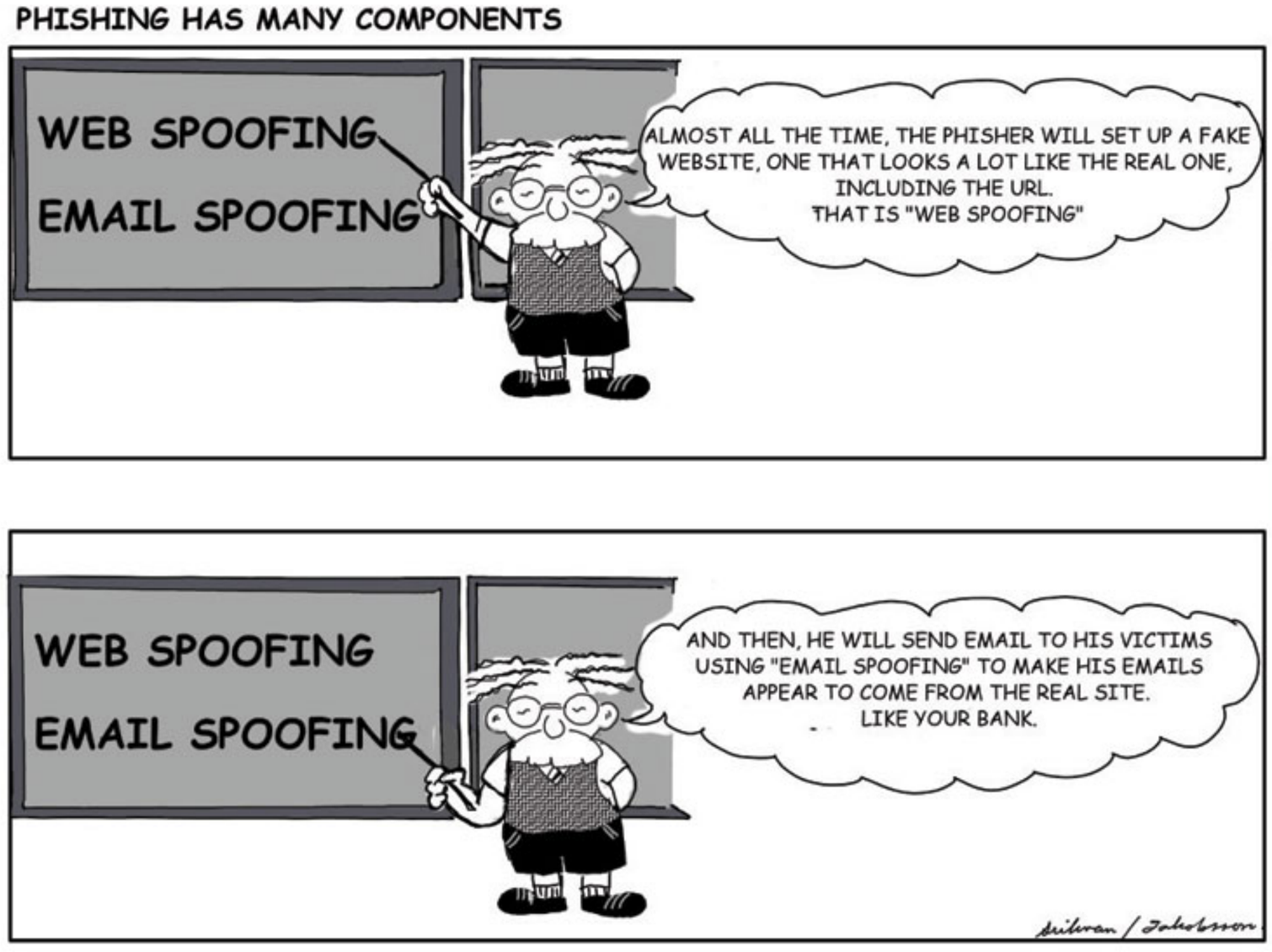
Cyberstalking and Harassment

We must be aware of the "dark side" of the Internet facing people. Cyberstalking and Harassment applies to just about anybody just like in real life.

If you get threatening emails at home or at school, or threatening text messages on your mobile phone, you must inform your parents or an adult that you trust, so such messages can be stopped.

See page 02

CyberCartoon



Editor's note

Welcome back and we are proud to bring to you next edition of the CyberSAFE newsletter with the aim of informing computer users on internet safety and best practices. This issue provides useful safety tips especially for those who have friends online and have met someone recently. You will also find the answers for the activities from the last issue and I hope you have done well. We hope that you find our newsletter to be resourceful and do share with your family and friends.

Thank you.

Raj Kumar

Raj Kumar
Editor

From page 01

The following are some tips for safer online experience:

- Don't respond to suspicious messages.
- Choose a genderless screen name when chatting.
- Don't flirt online, unless you're prepared for the consequences. This may create unwanted attention from unwanted suitors, just like in real life.
- Save offending messages and report them to Police or **MyCERT (www.mycert.org.my).**
- If someone makes threats in a chat room or on a message board, notify the **Police** or **MyCERT (www.mycert.org.my).**
- Don't confront the stalker/harasser, this might create more anger or emotional attacks.
- Don't give out any personal information about yourself or anyone else.
- Get out of a situation online that has become hostile, log off or surf elsewhere.
- Search yourself using a search engine to make sure no personal information is posted by others about you.

CyberJargons

Zombie Computer:
A computer attached to the Internet that has been compromised by a hacker, a computer virus or a Trojan horse.

Denial-of-Service attack (DoS attack):
The act of making a computer or internet service or application unavailable for its users.

SPIM:
A security protocol developed to fix flaws in WEP. Encrypts data sent to and from wireless devices within a network.

CyberQuiz

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

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

2. **_____occurs when someone uses your personal information without your permission to commit fraud or other crimes.**
   a. Identity theft
   b. Virus attack
   c. System attack

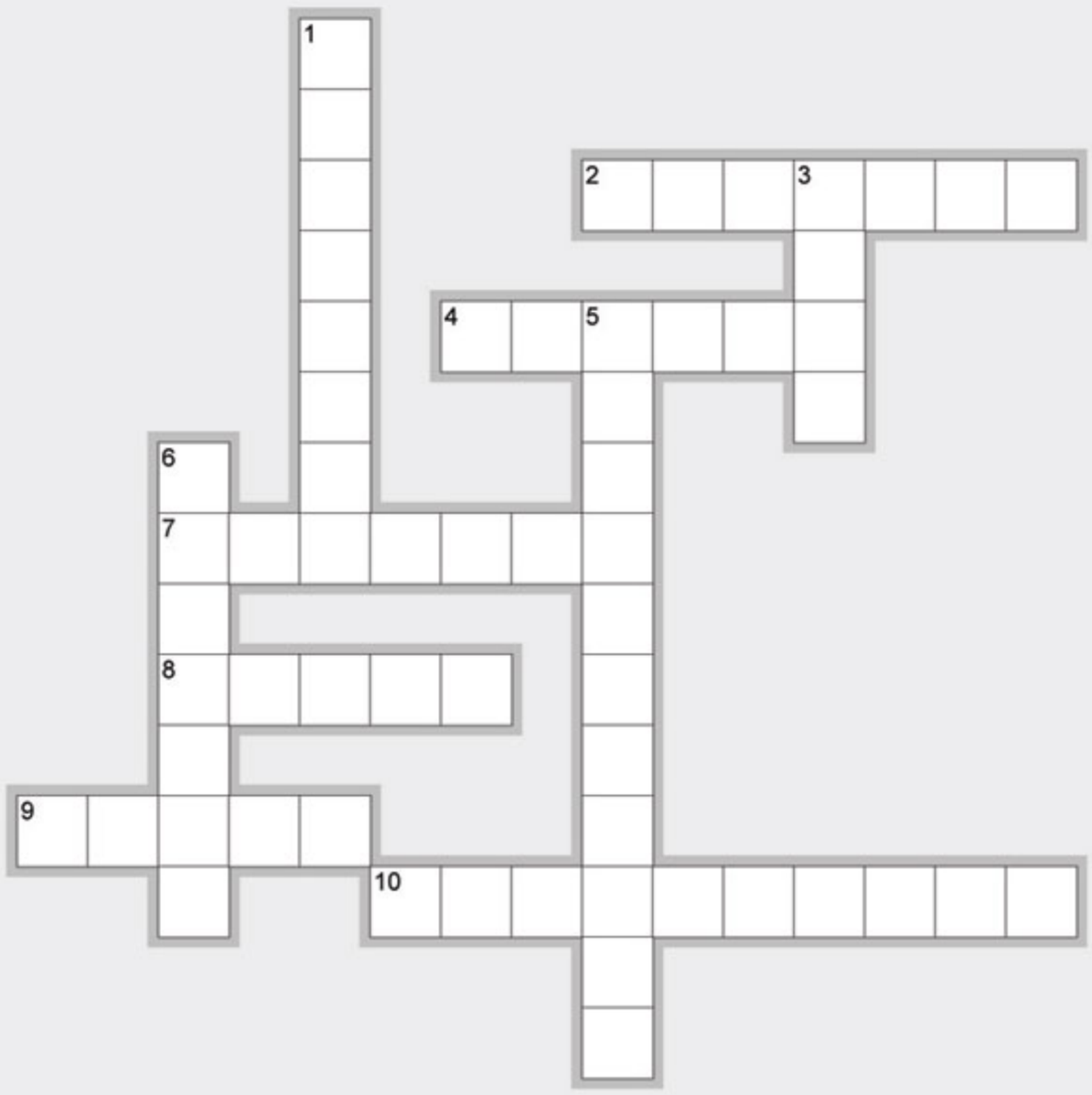
3. **File sharing programs or P2P systems used for downloading files can _____**
   a. Invite viruses to infect your computer system
   b. Install unknown programs onto your system
   c. All of the above

4. **Which of the following is good practice when shopping online?**
   a. Read the refund policy and delivery information
   b. Buy from the cheapest online store
   c. Pay by sending cash to the merchant

5. **Which of the following is not a computer security program?**
   a. Antivirus
   b. Antispyware
   c. Defragmenter

CyberCrossword

Note: The answers will be provided in the next issue



Across

2. Pop-up advertisement is a sign of _____
4. A word used to describe a person who breaks into computers
7. Your computer should be _____ regularly
8. Identity _____ is when your personal information is used by unknown person/party
9. You should_____ someone who makes you feel uncomfortable while chatting
10. You should not open email _____ from some one you don't know

Down

1. You should change this regularly
3. _____ is a form of Malware
5. Safer mode of paying for goods online
6. A website where you can bid for goods

CyberArticle

PC SECURITY: Threats and Countermeasures

By Sharifah Roziah Bt Mohd Kassim, MyCERT, CyberSecurity Malaysia

Cyber criminals on the Internet are well organized and tend to target PCs with combined threats. They are using various sophisticated and blended techniques to steal credit card numbers and credential information using malicious programs.

1) Malware – Bots, Botnets, Backdoor Trojans, Rootkits

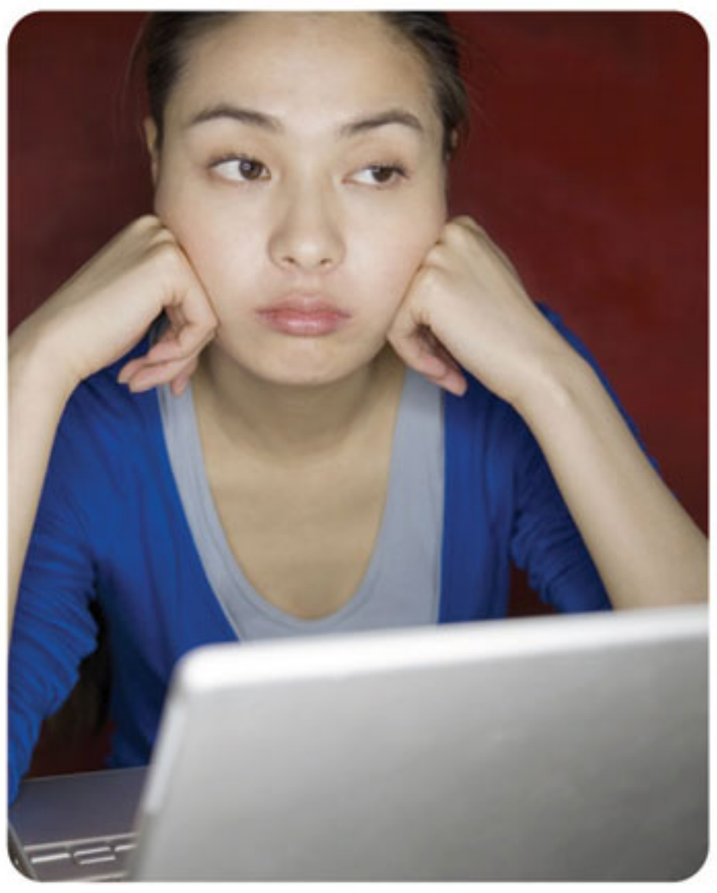
Some of the Malware that threatens PCs are bots, botnets, drones backdoor trojans and rootkits. Computers that are compromised by backdoor trojans , also known as a zombie PC, can be abused by their master for malicious activities in a network of bots, or "botnet". Normally, botnets can be rented out by their owner, this is known as bot herders, used to relay spam and to launch phishing scams to steal sensitive personal data for fraud.

2) Distributed Denial of Service (DDOS) Agent

Distributed denial of service has long become a threat to PCs. It is included in most of the bots deployed today. Botnets activities in compromised PCs are used as agents used to launch denial of service attack to targeted host.

3) Unsecured Windows File Sharing

With "File and Print Sharing" enabled or share level access, your PC is exposed to threats, commonly occurring in Windows operating systems. Unsecured windows shares can be exploited by intruders in an automated way to place tools on large numbers of Windows based computers attached to the Internet. Unsecured windows shares together with DOS tools can become a great opportunity for intruders to launch DOS attacks.



4) Potentially Unwanted Programs

Potentially Unwanted Programs, refers to adware and spyware as many people fall victim to such programs without knowing they are being installed in their computer.

5) Hidden File Extension

Malicious programs can exploit the default behavior of Windows operating systems which hides file extensions from the user and trick them to execute malicious code by making a file appear to be something normal.

6) Browser-based Attacks

The main browser based attacks are cross site scripting and active contents in Java, Java Script and Active X. A malicious web developer may embed a script to HTML codes. When the web site you are browsing from your home PC responds back to you, the malicious script embedded in it comes along into your browser. Browsing untrusted sites, opening email messages, or newsgroups postings and using interactive forms on an untrustworthy site can expose your web browser to malicious scripts.

1) Update your system with latest patches
2) Install a Personal Firewall
3) Update anti-virus software and malicious program detectors
4) Scan all email attachments
5) Do not open unknown programs
6) Disable hidden filename extensions – You will see all the known and unknown files in your system
7) Protect your "File Sharing" activities from attacks - Microsoft recommends that anyone with "File and Print" sharing enabled or use share level access on a Windows 9x or above PC, must install the patch available at Microsoft's website
8) Disable Java/JavaScript/ActiveX in your web browser - especially when you are browsing unfamiliar websites
9) Make regular backups

References

1) *http://www.pcworld.com/article/id,115939-page,1/article.html*
2) *http://www.cert.org/advisories/CA-2001-20.html*
3) *www.mycert.org.my*
4) *http://www.news.com/Microsoft-Zombies-most-prevalent-Windows-threat/2100-7349_3-6082615.html*
5) *www.sans.org*
6) *http://www.news.com/Alarm-growing-over-bot-software/2100-7349_3-5202236.html*

Answers:

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

CyberQuiz

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

CyberCrossword

CyberResources and Reporting

Security Awareness Portal - www.esecurity.org.my

www.esecurity.org.my is a portal developed by Cybersecurity Malaysia to inform and to educate computer users on various threats and to provide tips and best practices in order 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 for kids and teenagers, parents and adults, and organisations.

The website covers tips such as 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!

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

Cyber999 is a service offered by MyCERT (Malaysian Computer Emergency Response Team) to respond to security incidents faced by Internet users. 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) 8992 6969**
SMS: **(019) 281 3801**
Email: **mycert@mycert.org.my**
Mobile phone (24 hrs): **(019) 2665850**
Print online form and fax: **(03) 8945 3442**

CyberSecurity Malaysia
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