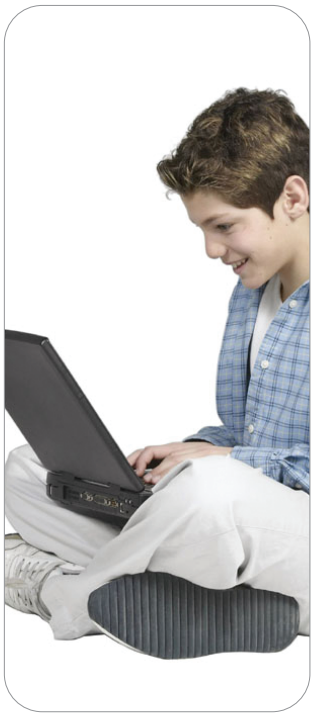
CyberSAFE

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



Cyber Safety Tip

Social Networking: Helping Kids to Socialize Safely Online

Social networking sites have become a popular communication channel for teenagers and adults. These sites enable people to exchange information, share pictures and videos and send private messages to friends and others who share similar interests. It is important for everyone, especially kids, to be aware of the possible dangers. Parents need to teach their kids the ways to stay safe while they socialize online.

The following are some tips for safe social networking:

- Advise your kids on information such as their name, home address, school name, phone number, names of family members to be kept private and why it should be kept private.
- Teach your child on the use of privacy settings found on social networking sites and restrict who can view their online profile and who can access and post on your child's website.

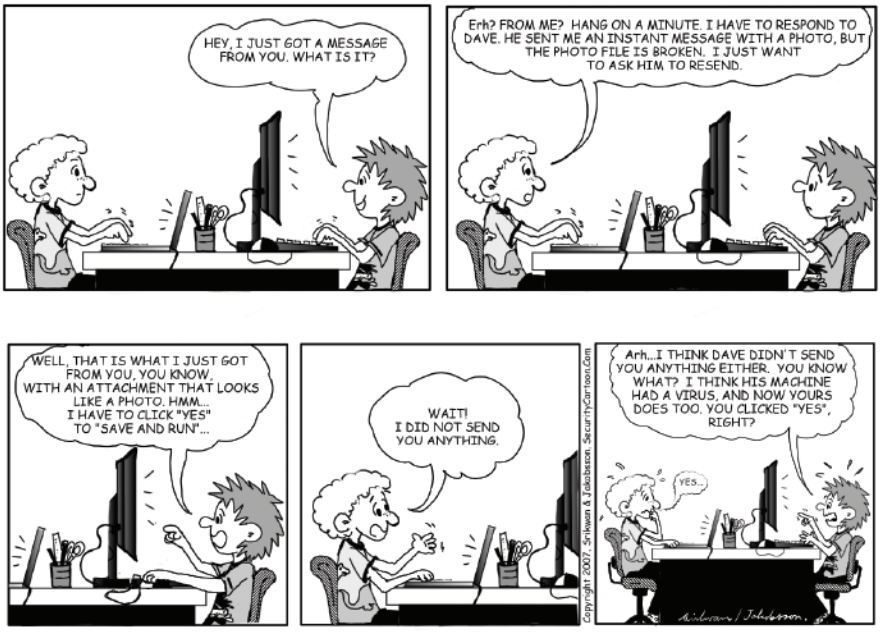
See page 02

Message from the CEO

I would like to take this opportunity to welcome you to the second edition of CyberSAFE awareness newsletter. The Internet has made possible high level of usability and access for social and business interaction. As number of cyber threats and attacks are being reported around the world, we in Malaysia are not left alone. We at CyberSecurity Malaysia have taken the initiative to develop many resources to better inform and educate Internet users both at home and at work. The Internet users of today are made up of young children, teenagers, parents and senior citizens, whom may not be well informed of issues on the internet. Our aim is to ensure that everyone is made aware and educated on internet security and safety regardless of their computing experience and we hope that this edition of CyberSAFE will heightened your awareness level in most fun and interesting way.

Best Regards,
Husin Jazri, CISSP

Cyber Cartoon



Reproduced with permission. All material © 2007 Srikwan & Jakobsson

Cyber Quote

The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.

Kevin Mitnick

From page 01

- Explain to your kids that they should post only information that you and they are comfortable with others seeing. Encourage your child to think before posting pictures and videos.
- Remind your kids that once they post information online, they can't remove it.
- Talk to your kids about Cyberbullying, which can take place in the form of by spreading rumours, posting and forwarding of messages without their permission.
- Inform your kids to talk to you if they feel uncomfortable with someone or threatened by someone online. You can report abusive, suspicious, or inappropriate online behavior to Cyber999 ***(http://www.mycert.org.my)***, a service brought to you by CyberSecurity Malaysia.
- Talk to your kids to avoid strangers who talk about sexual matters or sensitive issues.
- If you suspect that your child is engaging in some risky online behavior, you can perform a search on blog sites by using their name, nickname, school, hobbies or area where you live.
- Read site's privacy policies and parental controls, to understand the features and privacy controls and also your right as a parent, especially concerning young kids.
- Keep the computer in the living room of your home, so your child's online activities can be easily monitored.

Cyber Jargons

Wireless Network (WiFi):
A method of connecting a computer to other computers or to the Internet without linking them by cables.

Wired Equivalent Privacy (WEP):
A security protocol that encrypts data sent to and from wireless devices within a network. Not as strong as WPA encryption.

Wi-Fi Protected Access (WPA):
A security protocol developed to fix flaws in WEP. Encrypts data sent to and from wireless devices within a network.

Cyber Quiz

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

1. **When you receive an email with a link to update your bank account, you should:**
   a. click on the link and update your account
   b. report to the bank and delete the email
   c. scan the email for virus
   d. perform a system virus scan

2. **If someone threatens you in a chat room or message board, you should:**
   a. report to Cyber999
   b. confront the person
   c. tell your parents
   d. don't tell anyone

3. **Which of the following indicates a possible spyware being present in your system?**
   a. Pop-up advertisements appear when you are not connected to the web
   b. A new toolbar installed in your browser
   c. Your system crashes or hangs for no reason
   d. All of the above

4. **Which of the follow is the common message used in phishing emails?**
   a. "Verify your account"
   b. "Click the link below to update your account information"
   c. "You have won…"
   d. All of the above

5. **A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information such as credit card numbers, bank account information, passwords or other sensitive information from unsuspecting victims.**
   a. Malicious code
   b. Phishing
   c. Spammer
   d. Trojan

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 involved in social networking sites and for those accessing internet using wireless connection. 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.

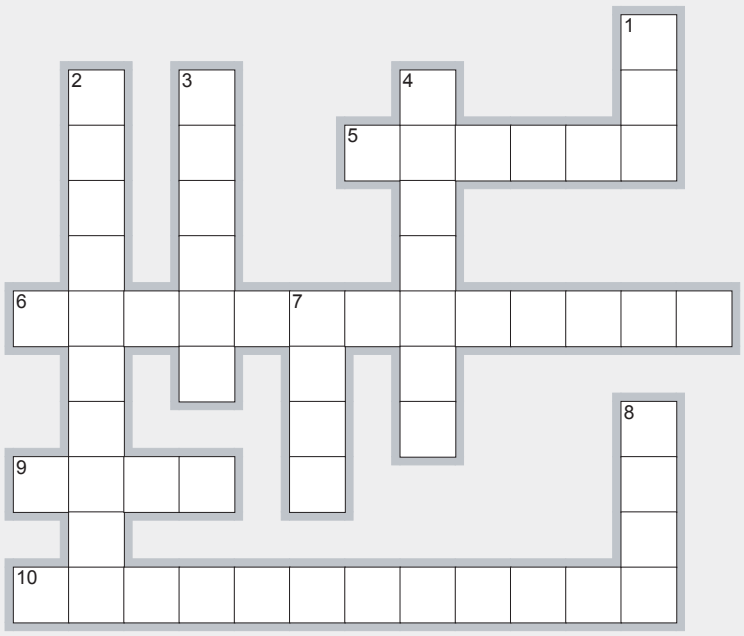
Thank you.

Raj Kumar

Raj Kumar
Editor

Cyber Crossword

Note: The answers will be provided in the next issue



Across

5. Act of saving and storing important files remotely
6. Act of harassing or threatening someone continuously online
9. Short term used commonly to describe wireless network
10. Type of toolbar used to trap suspicious URLs

Down

1. An informal network that allows people to share files (music, games, software) with other users
2. Scrambling of data into a secret code
3. A network of infected computers used to send spam emails
4. Trojan is a form of _____
7. Unwanted emails sent by unknown person or company
8. A web application where people post their thoughts and share their interest online

Cyber Article

Why Worry About Securing your Wi-Fi?

By Mohamad Nizam Kassim, CyberSecurity Malaysia

Wi-Fi networks offers great convenience and flexibility for computer users to be connected to the Internet in anywhere, everywhere mode where a wireless access point is provided. For home users, the ability to network computers anywhere around the house without having to figure out how to run cable all over is very appealing. WiFi access points are becoming common and are widely implemented at coffee shops and college campuses to cater for the growing needs of internet users.

Lately, the security concerns of Wi-Fi networks have been haunting wireless users with series of questions such as, how do I ensure that my confidential information is not being disclosed, how do I protect myself from wireless attackers and how do I ensure that wireless communication is secured. This article will offers basic guidelines on how to overcome the security concerns so that WiFi users are able to access WiFi network in secured manner.

What Should You Know?

To protect yourself from wireless attackers, you should be aware of the common mistakes that usually made by wireless users.

The common mistakes are:

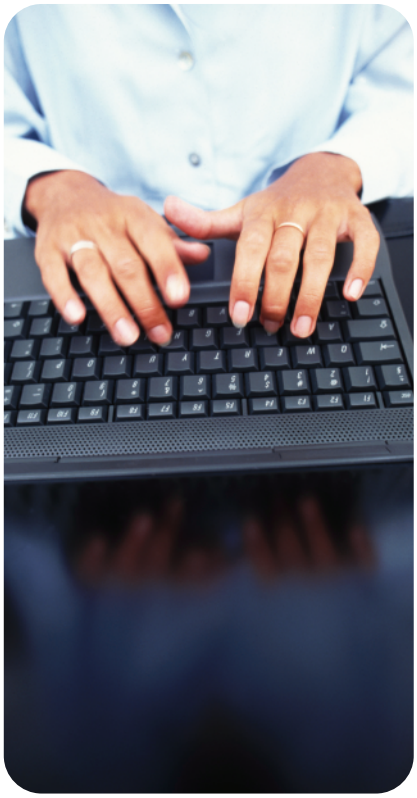
1. Tendency to connect to any free available Wi-Fi networks. Usually this type of services is less secured due to encryption not being enabled or where a shared password is used.

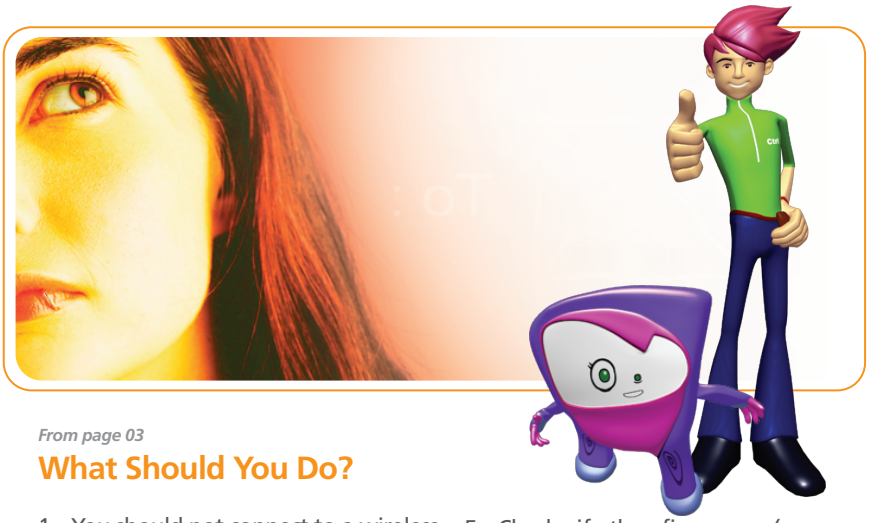
2. Tendency to connect to WEP-enabled Wi-Fi networks. WEP can be easily cracked.

3. "Always-On" wireless connection. Most laptops search for Wi-Fi signals automatically and the connection stays open even if you don't open your Web or email application. If your laptop automatically connects to a Wi-Fi network run by attackers, they might be able to search your computer for sensitive data and information that would allow access to your company's network.

4. Neglecting to find out which wireless access point you are connected to. Wireless users are usually more eager to surf internet as long as they are stay connected without considering which access points that they are being connected to.

5. Conducting financial or transactions at any available Wi-Fi network. Wireless users are not aware of the capabilities of wireless frame being viewed over air ithout proper wireless access point encryption protocol.





From page 03

What Should You Do?

1. You should not connect to a wireless network without encryption enabled or WEP-enabled.
2. You should connect to access point with a strong encryption protocol such as WPA or WPA2 with mutual authenti cation 802.1 x protocols.
3. You should stop wireless connectivity when not in use or while you are connecting to the wired network.
4. Implement Personal Firewalls. Even if an attacker is able to associate with an access point, the personal firewall will prevent them from accessing files on your laptop on the same WLAN (Wireless Local Area Network).
5. Check if the firmware (program embedded in hardware) for your Wireless Adapter is up to date and update if required. It is a good practice to check for new updates. **(Right hand click to My Computer > Properties > Device Manager > Network Adapter > Right hand click to Wireless Driver > Update Driver)**
6. Encrypt wireless traffic using a VPN (Virtual Private Network), e.g. using IPSEC or other VPN solutions.
7. Disconnect immediately when connecting to the unknown wireless access point.
8. Manage your directory or file sharing properly before turning on wireless connectivity.

References
[1] Wireless LAN Security, 802.11/Wireless LAN Wardriving & Warchalking (http://www.wardrive.net/, 11/02/2008)
[2] Flickenger, Roger Weeks. Wireless Hacks, 2nd Edition, O'Reilly, 2005.
[3] Moerschel, Dreger, Tom Carpenter. CWSP Certified Wireless Security Professional, 2nd Edition, Grant McGraw Hill, 2006.
[4] Glenn, Josh. WLAN Security Challenges, 08/03/2005, http://www.securitydocs.com/library/3534, 11/02/2008

Answers:

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

CyberQuiz

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

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 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.

Contact Cyber999 if you have problems online!

If someone makes you feel uncomfortable (make harassing or threatening comments) or 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 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 : **(603) 8992 6969**
SMS : **(019) 281 3801**
Email : **mycert@mycert.org.my**
Mobile phone (24 hrs) : **(019) 266 5850**
Print online form and fax : **(603) 8945 3442**

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: (603) 8992 6888 | Fax: (603) 8945 3205
www.cybersecurity.org.my