CyberSAFE

Security Awareness For Everyone

Let's Make The Internet A Safer Place

www.esecurity.org.my

CyberSecurity MALAYSIA

www.cybersecurity.org.my

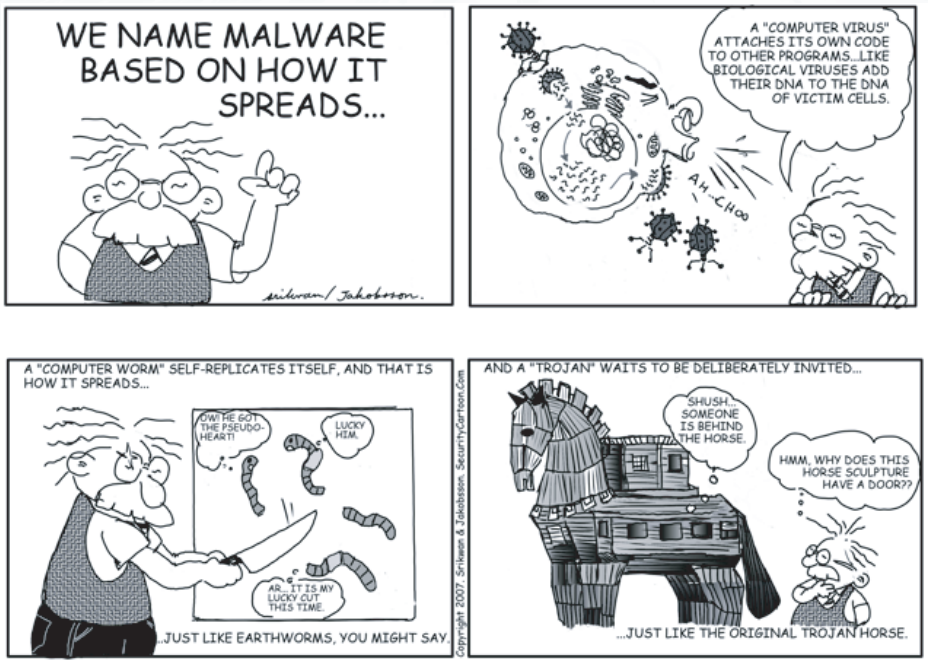
An agency under MOSTI

CyberQuote

Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.

Clifford Stoll

CyberCartoon



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

CyberSafety Tip – Don' t become a victim of Identity Theft

Identity theft occurs when someone uses your personal information, like your name, your birthday, telephone number, or credit card number without your knowledge, in order to commit fraud or related crime. It is important to take certain steps to minimize the potential threat from identity theft if your information is accidentally disclosed or deliberately stolen.

The following are some of the method used by thief you get hold of your information:

1. Dumpster Diving - Looking in rubbish bin for bills or other disposed documents with your personal information on it.
2. Skimming - Stealing credit/debit card numbers or information stored on them, by using a special device that can read your card.
3. Phishing - Someone pretending to be a financial institution or company and then sends spam or pop-up messages to get you to reveal your personal information.
4. Changing Your Address. - They divert your billing statements to another location by completing a change of address form. In this way, they will receive all your statements.
5. Pretexting - Someone pretending to be you and obtain your personal information from financial institutions, telephone companies and others.

Message from the CEO

I would like to take this opportunity to welcome you to the fourth edition of CyberSAFE awareness newsletter. Cyber attacks are becoming more sophisticated and it is coming largely from hackers around the world who hide themselves well. These attacks are crimes that can harm people, businesses, government and critical infrastructures. Today, cyber security issues such as security breaches, information theft, harassment and internet fraud is not something new and it is facing all internet users. As the internet is becoming more accessible to all walks of life, that include children, parents, senior citizens, organisations and government, it is vital for Internet users to be educated on Internet safety in order to protect themselves and learn to use it responsibly. Our security awareness portal (www.esecurity.org.my) is populated with many resources such as internet safety tips, posters, videos and more. We hope that you will find this edition to be fruitful and raises your current awareness to the next level!

Best Regards,
Husin Jazri, *CISSP*

From page 01

Some tips to safeguard your personal information from being stolen :

1. Be careful when giving out personal information in websites, emails, instant messaging systems, chat rooms or message boards, especially when you are not sure. You have the right to ask why it is needed and how the information is to be used.
2. Read privacy and policy information on the website before you send your personal information or conduct any transactions.
3. Close any compromised credit card/bank accounts immediately.
4. Monitor your credit card/bank account statements. This is good way to know if any fraudulent withdrawals or charges had taken place.
5. Consult with your financial institution about any unusual activities on your accounts.
6. Contact relevant authority to cancel and replace any stolen identification cards, including your driver's license.
7. Watch for signs of identity theft: late or missing bills, receiving offers/letters in your home mail box from people/companies you did not deal with, or getting contacted about purchases you didn't make.
8. Don't send or post a picture of yourself, your friends or family to someone you met or chat with online.
9. Memorize your password and if possible, do not write it down anywhere.
10. Report identity theft or any suspicious activity immediately to Cyber999 (Cyber999 is a service offered by MyCERT).

CyberJargons

Drive-by Download:

Software that installs on your computer without your knowledge when you visit certain websites. To avoid drive-by downloads, make sure to update your operating system and Web browser regularly.

Hidden Dialers:

Programs that you may unknowingly download that can use your computer to silently dial expensive phone calls which later show up on your phone bill.

Parental Controls:

Tools that allow parents to prevent their children from accessingcertain Internet content that they might find inappropriate.

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 and your mobile devices. 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 to download your copy. We hope that you find our newsletter to be resourceful and do share with your family members and friends.

Thank you.

Raj Kumar

Raj Kumar
Editor

CyberQuiz

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

1) Peer-to-Peer (P2P) or File sharing system allows you to:

a. Exchange files between two computers on the internet
b. Troubleshoot computers over the internet.
c. Encrypt files.

2) Which of the following is NOT a good practice for avoiding a virus infection:

a. Scan all attachments
b. Open files in a thumb drive without performing virus scan
c. Set your antivirus program to "Auto-Update" mode

3) If your credit card account has been comprised, what is the first thing you should do?

a. Inform the credit card company
b. Report to MyCERT
c. Cut the card

4) Which of the following is good practice when shopping online?

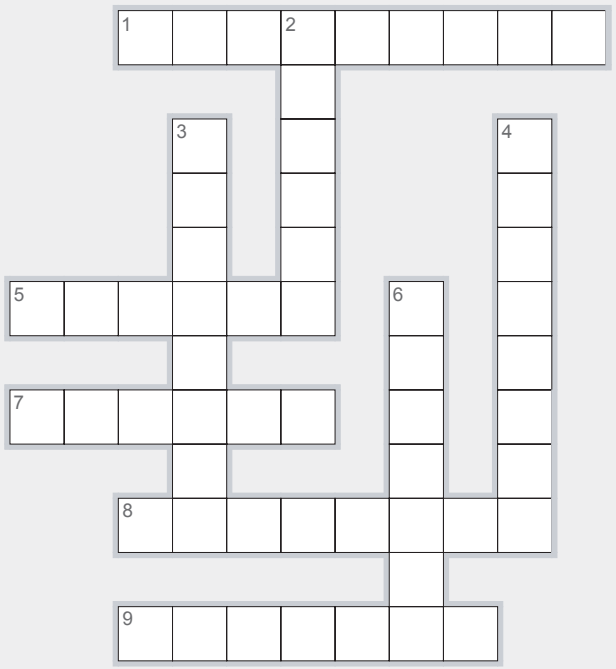
a. Read the refund policy and delivery information
b. Buy from the cheapest online store
c. Pay by sending cash to the merchant

5) Looking through a rubbish bin for documents that has personal informations known as:

a. Pretexting
b. Dumpster diving
c. Skimming

Crosswordpuzzle

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



Across

1. A term refered to when measuring Internet connection speed
5. Someone accessing your computer without your permission
7. .org, .com, .net are known as_____names
8. An act of stealing credit card information using a special data capture device
9. Someone who sends unsolicited email

Down

2. A program that dials phone numbers from your computer
3. A web browser feature used to save frequently visited websites
4. A scam where internet fraudsters send spam or pop up messages to get your personal information
6. Online_____ is where user's interest and preferences are recorded in order to create ads that are targeted at them

CyberArticle

Securing Our Mobile Devices

*By **Noor Aida Idris**, Security Management and Best Practices Department, CyberSecurity Malaysia*

Mobile device security is a critical issue that every one of us should be aware of immediately. Increasing usage of notebooks, PDAs, and other mobile devices, together with new technology such as wireless connectivity, has led to huge security risks from physical theft to malware infection. Even though the cost of replacing the stolen device may be relatively small, however lost photos, files and personal information can't be replaced.

Challenges in Mobile Device Protection

The main advantage of owning a mobile device is that they are small and compact, thus most of us find it is very convenient to carry them everywhere. Unfortunately, small mobile devices are more vulnerable to physical theft and damage. We use mobile devices in public places such as restaurants, hotels and airports and make connections over unsecured wireless network. This poses a security threat whereby dangerous malware can be downloaded to your portable device without your knowledge. Later, the same device when used in an organization's network can infect other computers and even other systems in the vicinity. Sometimes we tend to use our mobile device without considering the danger posed to the data it carries, e.g. USB thumb drives for storing sensitive company information including our private and personal data. The information regarding our company's trades and businesses are valuable and can be useful for our competitors, and they can use it to cause loss of revenue to our organization. Furthermore, our own and private data can be stolen to be used for performing online transactions, e.g. unauthorized users posing as yourself on the Internet and performing transactions using your credit card.

Steps to Mobile Devices Security

1. Lock, lock and always lock

Always lock your notebook using a notebook cable lock. Don't leave your handheld device or notebook backpack on a restaurant's table or in your car unattended. If possible, bring it with you everywhere and anywhere you go.

2. Limit confidential data

Be extra careful when saving or storing documents, either company or personal data in your mobile devices. If possible, save sensitive information in some other medium that is not prone to physical threat. This help to prevent or reduce leakage of your own as well as your company's private and confidential data.

Regularly create backups of your files and documents stored in your mobile devices. Make sure these backups are stored physically separated from your mobile device. Therefore if your mobile device is stolen, at least you still have your data and private files with you.

3. Encrypt files

For cases when you cannot avoid storing or saving confidential documents in your laptop, ensure that you encrypt these sensitive and highly classified files. Use an encryption tool such as Wi-fi Protected Access (WPA) for encrypting the documents in your wireless equipments e.g. PDA. For private files in your laptop, you can encrypt those EFS (Encrypting File System). EFS is a feature of Windows 2000, XP and Vista that allows you to store private information and sensitive files on your hard disk in an encrypted format. Consequently, if your laptop is stolen for the purpose of obtaining employee salary files for example, you can be sure that the file is at least protected and kept secret from malicious intention of an unauthorized person.

4. Use strong password

Always create strong password or PIN for all your mobile devices. Frequently change your password too; it is recommended that you renew it every 3 months. Following are step-by-step procedures to create a strong and easy-to-remember passwords:

(i) Use a long password, at least 6-8 characters long. Remember, if your password has only 3 letters, an attacker will only need 17,576 tries as compared to an unbelievable 208,827,064,576 tries for 8 letters password.

(ii) Mix numbers, symbols and upper case and lower case. Most attackers use dictionary attack method where a dictionary is used as base to speculate your password. By mixing your password with other symbols and numbers, it can eliminate your password to be listed in any dictionary.

(iii) Combine English and foreign word. Make a unique password which combines your own native language (Malay, Chinese, Tamil) and an English word. Examples are 'ulatbook' or 'kerusirock'.

(iv) Memorize your password. Adding or including information that is relevant to you only might help you to remember your password. For instance, you want to use 'I gave birth to Suraya in Subang Jaya' as your password. If you take the first letter of every word, your new password is now 'igbtsisj'. Now change to upper case; 'IgbtSiSJ'. Next replace 'S' with the symbol '$'; 'Igbt$i$J'. And finally add a numeric figure by switching 'I' with the number '1'. So your new password is now '1gbt$i$J'. From a simple yet long statement, your password is now a word that has jumbled letters, numbers and symbols.

References

1) *http://www.hardwarezone.com.sg/*
2) *http://www.privacyrights.org/*
3) *http://attrition.org/errata/laptops.html*
4) *http://www.absolute.com/resources/computer-theft-statistics.asp*
5) *http://www.fbi.gov/ucr/ucr.htm*
6) *www.ic3.gov/*

5. Install Personal Firewall and other security software

Protect your mobile devices by installing a personal firewall, anti virus and other security program and update them regularly. Security software can stop virus and malicious code from entering your organization's network.

6. Configure device correctly

Your mobile device is vulnerable to attack even when you are not connected to the network. For example, an active Wi-Fi (Wireless Fidelity) card in your notebook may connect automatically to a nearby public access point without your knowledge. It is best if you disable your Wi-Fi card when you are not connected to the Internet.

Follow these steps to disable the Wi-Fi connection in Windows XP:

1) Go to **Start** > **Control Panel**
2) Click **Network and Internet Connections**
3) Click **Network Connections**
4) Right-click your wireless connection icon
5) Select **Disable**
6) The connection will be disconnected, and the wireless connection icon will disappears from the system tray.

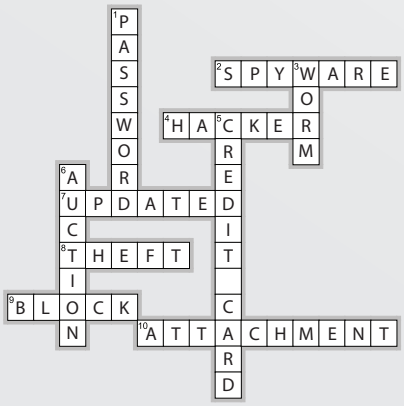
Always remember that risks that mobile devices pose, so that you are committed to fully protect them. PDAs and notebooks are attractive targets for criminals; not just for the devices themselves, but also for data stored in the devices. Ensure to implement these best practices everyday to help you to secure your mobile device.

Answers to activities from the previous edition:

CyberQuiz

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

CrosswordPuzzle



CyberResourcesand 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/
Mobile : phone (24 hrs) - 019-266 5850
SMS : 019-2813801
Email : mycert@mycert.org.my
Print online form and fax : (603) 8945 3442

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