CyberSAFE

Security Awareness For Everyone

Vol. 6

Message from the CEO

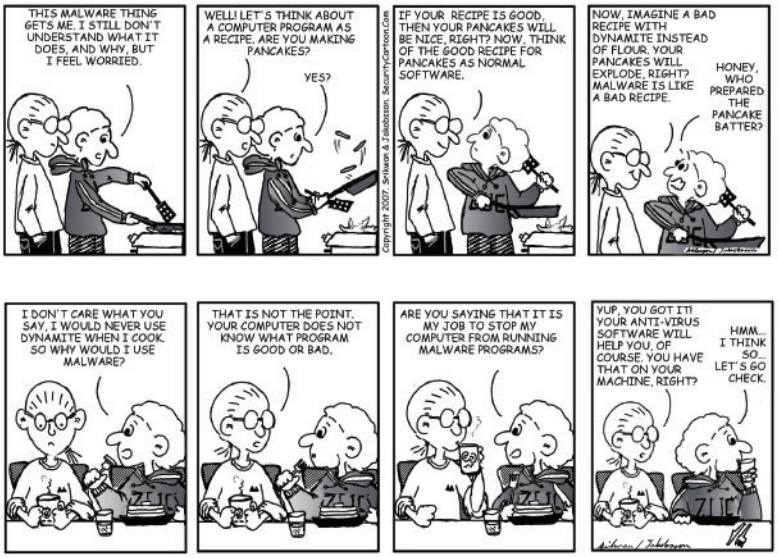
Welcome to our first issue for year 2009. Past couple of years of publishing CyberSAFE, we have learned a lot. As such, we will change slightly how CyberSAFE is put together. Previously, CyberSAFE only provide articles on tips and tricks of how to be safe while in the Net.

We also realize, we have a responsibility to promote the industry to the general public. From our experience, the public still don't know much on this industry called "Information Security". We will provide a "big picture" look of the various parts of this unique and exciting industry. The first is an Introduction on Cryptology, a subject very close to my heart. I came into the industry when I was in the Army and had the opportunity to take my Masters in Information Security. Of course we shall still keep you updated on the tips & tricks articles. Enjoy...

Best Regards,

Husin Jazri, CISSP

Cyber Cartoon



Cyber Jargons

Backdoor:
A back door is a means of access to a computer program that bypasses security mechanisms. Attackers often use back doors that they detect or install themselves, as part of an exploit. Some viruses and trojans install backdoors.

Keylogger:
A program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may saved to a file or even sent to another machine over a network or the Internet.

Identify Theft:
Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft.

Cyber Quote

"Computing is not about computers any more. It is about living"

Nicholas Negroponte

From the editor's desk

Year 2009, with the financial crisis hitting us hard, it is sad to hear many people losing jobs. As more people lose jobs, and less jobs available, there will be people becoming very desperate. Unfortunately, desperate people will use whatever necessary to cash in on other people. Internet is a cheap and easy tool for them to use to their advantage.

Thus it is more important for people like yourselves to be more careful and vigilant whenever you are in the internet and what you receive from the internet .

Do go to our website www.esecurity.org.my to get tips, trick and advises from past articles and any other updates we have put there.

Internet should be a place where we can do a lot of things like learning, banking, shopping, chatting with friends without fear of intrusion, harassment, or being cheated.

Like our mascots Nic & Pxl always say..."Be Smart. Be Safe"

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

CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

KDN License Number: PP15773/07/2009(022010) | Printed Quarterly

CyberSafety Tip

Kid Friendly Sites

By Rosnah Ab. Malek
Head, Knowledge Resource Centre, CyberSecurity Malaysia

Finding good Internet sites for your kids can be a challenge. There are lots of wonderful sites out there, but it can take hours of sorting through the junk to find the jewels.

You can find good sites and specific online content using kid-friendly search engines and directories on the Web. Search engines offer the widest choice of information; while directories focus more on specific topics.

A search engine, such as "Google," is a site on the Internet that searchers Web pages based on their titles, key words or full text. Directories, such as "Yahoo!" are similar to catalogues, where sites are reviewed, selected and then categorized by age and interests and usually provide a range of other services. Many search engines and directories focus on kid-friendly information or filter out sites that are inappropriate for kids.

Here is a list of some of the best 'Kid Friendly Sites' on the Web:

Great Web Sites for Kids

http://www.ala.org/gwstemplate.cfm?section=greatwebsites&template=/cfapps/gws/default.cfm&CFID=76395826&CFTOKEN=99671748

This American Library Association (ALA) directory includes links to online resources for fun and learning -- all reviewed and organized by children's librarians.

Ask Jeeves for kids

http://www.ajkids.com/

A unique commercial search engine that allows kids to search by using questions as well as key words.

Educational Software Directory

http://www.educational-software-directory.net/

In this directory, volunteers have reviewed and organized more than 23,000 sites into 14 categories.

Awesome Library

http://www.awesomelibrary.org/

This non-commercial directory included more than 20,000 sites reviewed by educators. It has a translation service that lets visitors browse in several different languages.

KidsClick!

http://www.kidsclick.org

This non commercial directory lists more than 5000 Web sites hand-picked by librarians.

Canadian Kids Page

http://www.canadiankids.net/ck/default.jsp

Through this directory users can search hundreds of sites - particularly Canadian ones - by age and topic.

Tips for using kid-friendly search engines and directories

Kid-friendly search engines and directories are not foolproof and offer no guarantee that inappropriate or offensive content will not crop up during a search. They are also not responsible for where your may end up once you leave their site and start moving through other Web pages.

If you use a directory, find out whom it was created by -- is it an established authoritative organization? Check the directory's criteria for choosing the sites in its index. If it is a commercial site, keep in mind that some sites may be included for marketing reasons.

Test several tools to find out which one works best for your family. Search sites offer different features, and each search tool offers a limited number of sites in its results, so use more that one search engine or directory.
Be Web Aware! Remember CyberSAFE!

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

Printed by:
MAX-PLUS BUSINESS CENTRE SDN. BHD. (439160-U)
TF 003 & 0004, 3rd Floor, BB Plaza,
Jalan Bukit Bintang,
55100 Kuala Lumpur,
Malaysia
Tel: +603.2148.4912
Fax: +603.2148.5376

Cyber Quiz

1. Which of the following is a good practice when participating in social networking site?

a. Only add the person if you know them in real life.
b. Add anyone you met online.
c. Add them if they show the same interest as you.

2. When you receive an email asking to update your information, this is known as_____.

a. Virus attack
b. Phishing scam
c. Malware

3. Which of the following programs is NOT necessary to be configured on your home computer?

a. Operating System Patching
b. Antivirus Program
c. Windows Media Player

4. Which of the following is a good practice to keep your computer safe from viruses?

a. Regularly update your antivirus program
b. Format your hard disk
c. Perform a computer scan when it is slow.

5. Which of the following is NOT a good practice when managing your passwords?

a. You should use different password for each account you access.
b. Password created should be easy to remember by you but difficult to guess by others.
c. Password should be written on somewhere on your computer

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

Cyber Article

An Overview of Cryptography

By Hazlin Abdul Rani & Mohamed Anfarri Kamarudin,
Cyber Technology Research Department, CyberSecurity Malaysia

With the advance in modern communications, technology has enabled businesses and individuals to transport information at a minimal cost via public networks such as the Internet. This development comes at the cost of potential exposing the data transmitted via this medium. Therefore, it has become imperative for businesses to make sure that sensitive data is transferred from one point to another in a secured manner over the public networks. Cryptography helps to achieve this goal by making messages unintelligible to all but the intended recipient.

In this article, we will explain the basic concept of cryptography, the history of cryptography and its applications in some circumstances.

What is Cryptography?

Definition: Cryptography *[krip-tog-ruh-fee]*
The science or study of the techniques of secret writing, especially code and cipher systems, methods, and the like.
http://dictionary.reference.com/browse/cryptography

Cryptography consists of an encryption; a process of converting normal or readable text (we called it plaintext) to an unreadable text or code (cipher), and a decryption; a reverse process, converting the cipher back to plaintext. These two processes will require a secret key. The key must only be known by the transmitter and the receiver. Figure 1 illustrates the basic process.

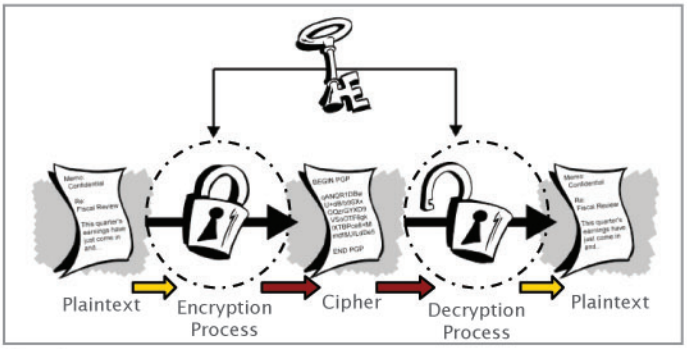


Figure 1

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

A brief history of Cryptography

Cryptography has existed since as early as 3500 BC during The Sumerians era, when humans are still illiterate. They used a 'word-picture' to represent objects or messages. However, the most significant usage of early cryptography was during the Ancient Greek era.

The Spartans claimed to be the first to use a **transposition** cipher (we rearrange each letter's position in the message; eg: "go south" become "gu otsho") while the Romans used **substitution** cipher (systematically replace each letters in the message; eg: "go south" become "jr vrxwk"). This is one of the simplest ways, which you can use to encrypt your message and exchange it with other people. However, bear in mind that this type of cipher alone is easily breakable.

Cryptography has evolved since then. Modern cryptography takes a lot more complicated mathematics calculations, computing power and science behind it to secure your data from prying eyes. Some of the publicly known cryptography systems are Data Encryption Standard (DES), Advance Encryption Standard (AES), RSA encryption (named after the creator – Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman) and ElGamal encryption.

Applications

Whether you are aware or not, cryptography is becoming part of our daily lives. Online banking is one of the best examples. You are required to enter your username and password in order to login to your account. If both your username and password are visible to other parties, it will become vulnerable as other people can access to your account by using your credentials and steal your money or view and modify your personal profile. Encryption will help to deal with this circumstance by encrypting your username and password, hence making them unintelligible to unauthorized party.

Another example is disk encryption. By applying cryptography, you can encrypt the content of your disk storage. In the event of your computer, notebook or external hard disk is lost or stolen, the contents of the disk is not accessible because it requires the key entered by user to decrypt the cipher and access it. The knowledge of the key is only with the authorized user.

Digital signature is another application of cryptography. It is used to verify that a particular email or computer program is written or developed by the authorized party. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior compared to a handwritten signature in such a way it is nearly impossible to counterfeit. Plus it attests to the content of the information as well as to the identity of the signer.

See page 04

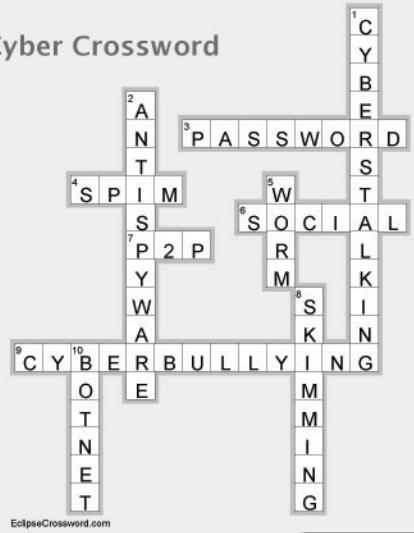
Answers:

The following are the answers to the activities in the last edition (Volume 5).

Cyber Quiz

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

Cyber Crossword



From page 03

Summary

Cryptography, over the ages, has been an art practiced by many who have devised ad hoc techniques to meet some of the information security requirements. The last forty years have been a period of transition as the discipline moved from an art to a science. There are now several international scientific conferences devoted exclusively to cryptography and also an international scientific organization, the International Association for Cryptologic Research (IACR), aimed at fostering research in the area.

Bear in mind that cryptography covers a bigger domain, and what we have told in this article is just a tiny piece of it. In the next issue, we will explore some other topics in cryptography such as research and development or how to possess a degree or higher certificates in cryptography. If you are interested to know more about cryptography, here are some documents and books that you may find helpful for beginners;

"Privacy on the Line," by Whitfield Diffie and Susan Eva Landau. MIT Press; this book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people, and contains information that even a lot of experts don't know.

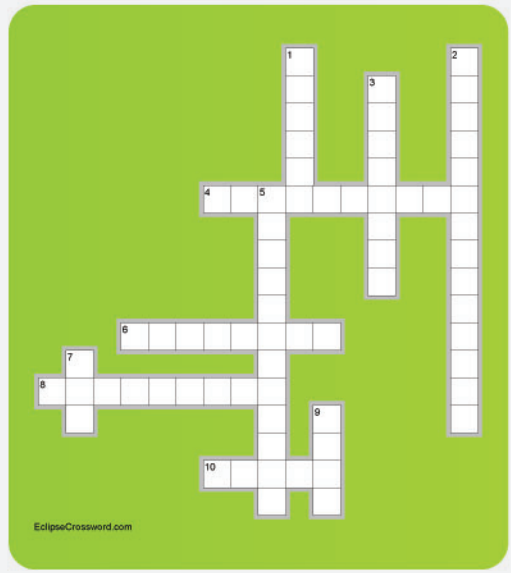
"The Codebreakers," by David Kahn. Scribner; this book is a history of codes and code breakers from the time of the Egyptians to the end of WWII. Kahn first wrote it in the sixties, and published a revised edition in 1996. This book won't teach you anything about how cryptography is accomplished, but it has been the inspiration of the whole modern generation of cryptographers.

"Cryptology Unlocked," by Reinhard Wobst; this book introduces cryptography in a unique and non-mathematical style and great for the beginners to understand the cryptography terminology.

Reference:

1. *http://en.wikipedia.org/wiki/Cryptography*
2. *Cryptology Unlocked by Reinhard Wobst*

Cyber Crossword



Across

4. A process to convert a normal text to a code text
6. Attackers accessed by bypassing security mechanisms
8. Monitoring user's input and keeping a log of all keys that are pressed.
10. One of the famous search engines

Down

1. Unreadable text
2. Layers of ..... is used to secure our online shopping activities and internet banking
3. Claimed to be the first to use transposition cipher
5. Study of techniques of secret writing
7. Advance encryption standard
9. Internet diary or journal

Note: The answers will be provided in the next issue

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, 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

Cyber Resources & Reporting

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.

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