



# Promoting a Culture of Cyber Security – Malaysia Case Study

**Philip Victor**

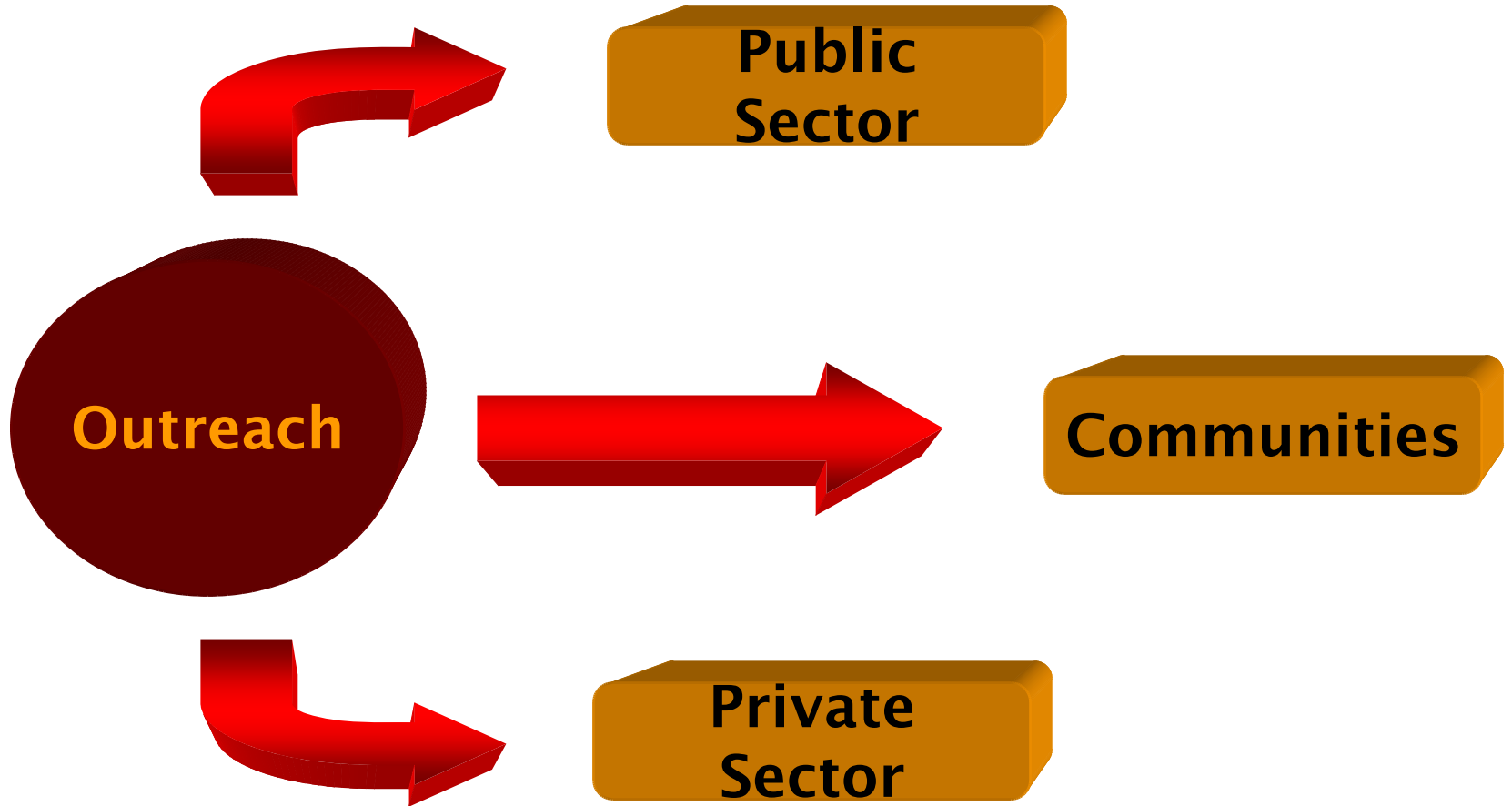
**vphilip[at]cybersecurity.my**  
**Head, Training & Outreach**  
**CyberSecurity Malaysia**

# Who Are We?

- Started in 1997 as Malaysian Computer Emergency Response Team (MyCERT)
- In 2001 assumed a larger role in protecting Malaysia's Cyber Space, known as National ICT Security & Emergency Response Centre (NISER)
- In 2005, Established as a Company Limited by Guarantee under the purview of the Ministry of Science, Technology & Innovation
- In 2006, assumed role as the national cyber security agency
- In 2007, given additional mandate and renamed as CyberSecurity Malaysia



# Everyone Matters



**Reaching out to all Internet users**



**To be aware of current online threats & dangers**



**Promote safe & responsible online behaviour**



**Promote best practices & positive use of the Internet**



# Co-operation & Collaboration

**Reaching out to all Internet users**



**Ministry of Education & other relevant ministries for schools**



**ISPs for home users**



**Public-Private co-operation for organisations (roadshow, portal, etc)**





# CyberSecurity Malaysia's Initiatives

Agenda



*Securing Our Cyberspace*

# The National Cyber Security Policy

## NATIONAL CYBER SECURITY POLICY



Designed to facilitate Malaysia's move towards a knowledge-based economy (K-Economy)

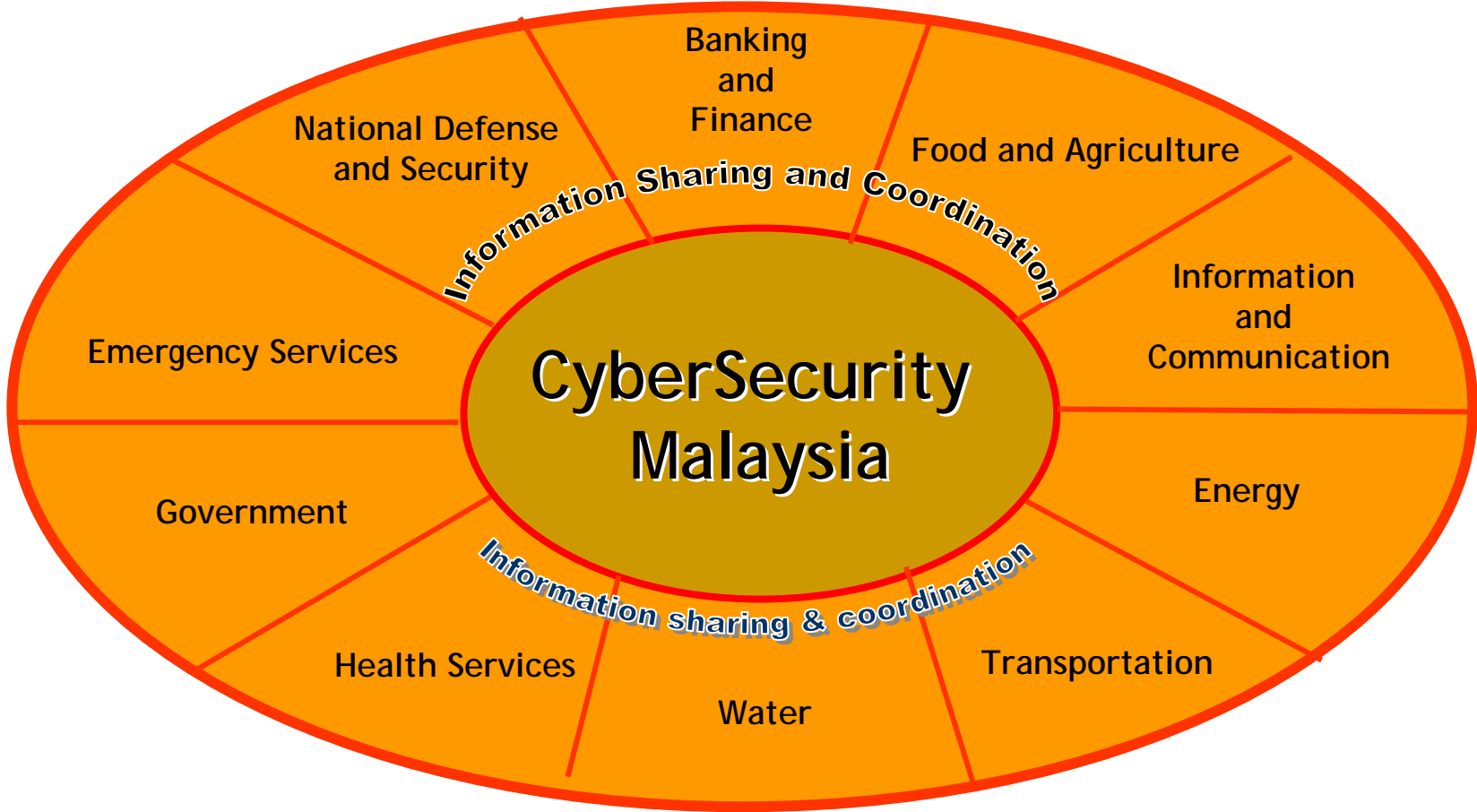


Formulated based on framework comprising:

- 1) Legislation and Regulatory
- 2) Technology
- 3) Public-Private Cooperation
- 4) Institutional
- 5) International



# Focus Area – 10 Critical National Information Infrastructure





# The 8 Policy Thrust



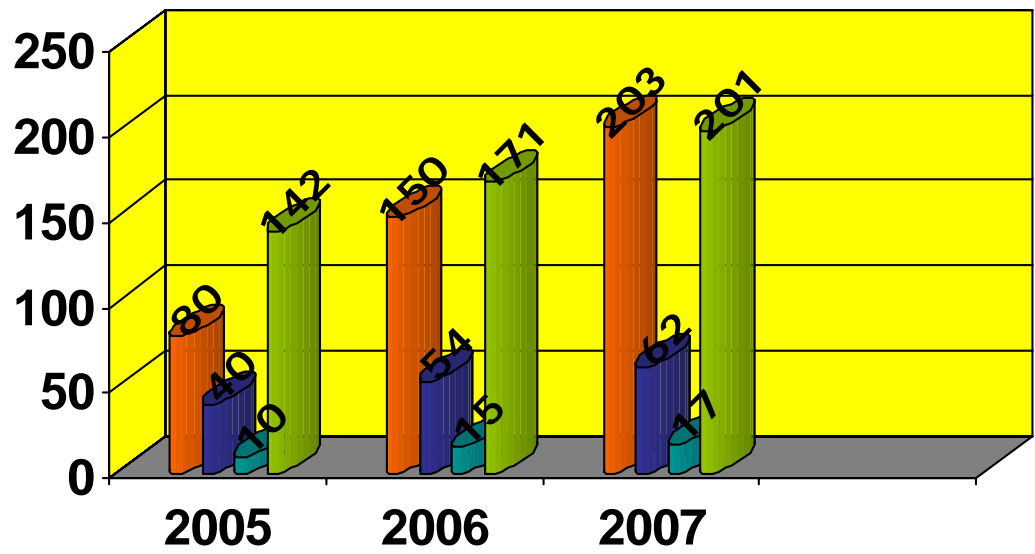


# Information Security Competency Development

To create knowledge workers through ***skill development programs*** and ***professional certification*** in Information Security

# Information Security Professional Certification

## Information Security Professionals in Malaysia



- (ISC)2
- SANS
- DRI/BCI
- ISACA



# Professional Development



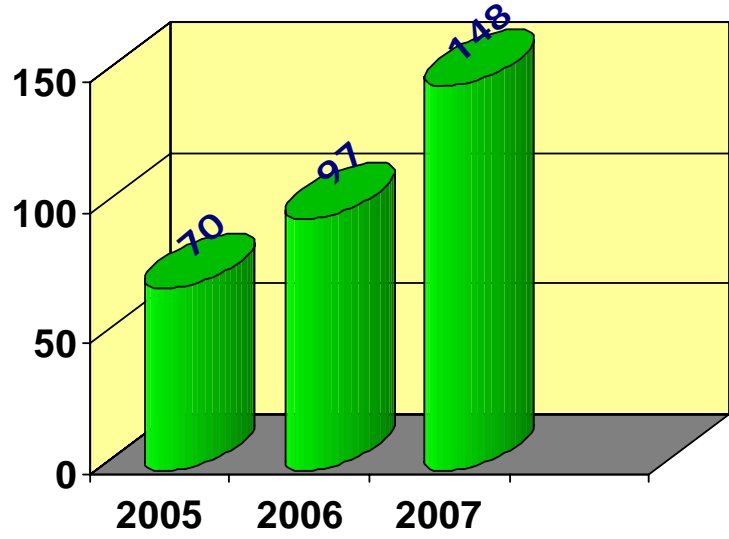
**BANK NEGARA MALAYSIA**  
CENTRAL BANK OF MALAYSIA



**PETRONAS**  
Petroleum National Berhad



## Skill Development for IT Professionals



■ Trained Professionals



*Securing Our Cyberspace*



# Other Initiatives

- Cyberlaw
  - Computer Crime Act 1997
  - Digital Signature Act 1997
  - Copyright Act 1997
  - Communications & Multimedia Act 1998
  - Telemedicine Act



# Standards

- Promotion of information security related standards to public & private sectors for greater adoption:
  - ISO27001/ISO17799
  - BCM Standard
  - Common Criteria



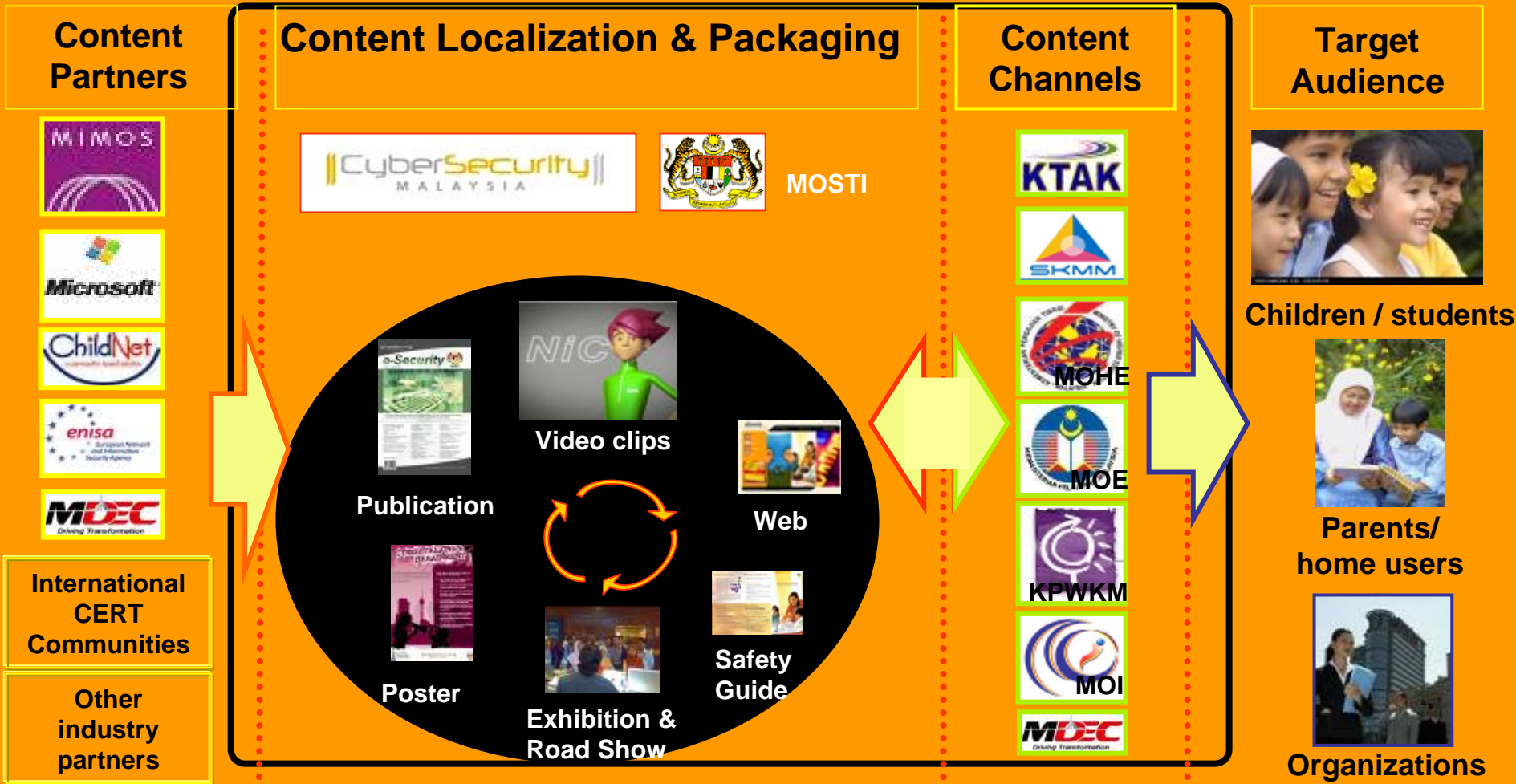
# CyberSecurity Malaysia Outreach Programs

To build a culture of security through ***awareness programs*** to target groups (kids/teenagers, parents/professionals & organisations)



# Outreach Program

## CYBER SECURITY AND INTERNET SAFETY AWARENESS CAMPAIGN





# Critical Information Infrastructure Protection Awareness Workshop



# INFOSEC.my Information Security Annual Conference



# INFOSEC.my Knowledge Sharing Session



# INFOSEC.my Knowledge Sharing Session



Reaching out to the schools & communities



## eSecurity

TOWARDS BUILDING A SECURITY CULTURE

KIDS/ TEENAGERS

PARENTS/ ADULTS

ORGANISATIONS



About Us



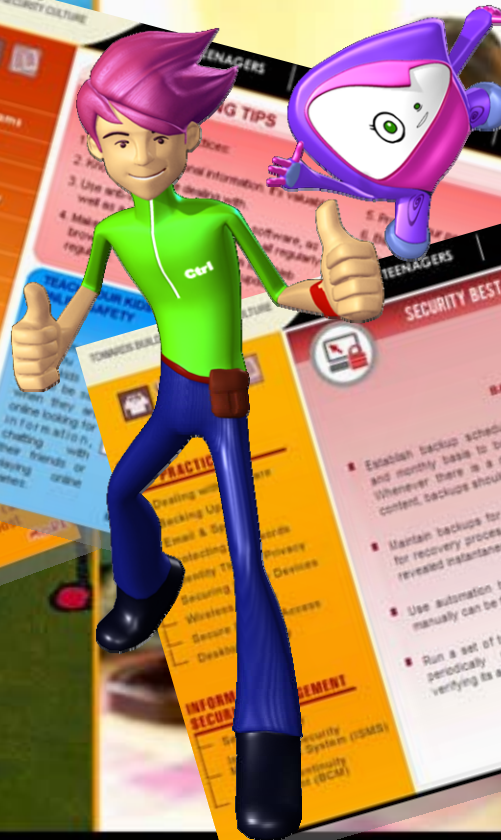
Video



Download



Download



### Information Protection

- When you are on the internet
- Don't give out information about yourself to someone you met online.
  - Don't send a picture of yourself to people you met online.
  - Be alert to what the people you met online said if it worries you, ask your parents.

### Virus & Worms

- When you are on the internet
- Protect your computer current with the automatic updates
  - Use an internet firewall
  - Subscribe to industry standard antivirus software and keep it current

### Mobile Device Safety

- Online Banking & Flashing Scams
- Online Auction
- Online Shopping
- P2P File Sharing
- Privacy & Identity Theft
- Safe Computing Tips
- Spyware Watch
- Wireless Access

### SECURITY BEST PRACTICES

- #### BACKING UP DATA
- Establish backup schedule on daily, weekly and monthly basis to backup all documents. Whenever there is a modification to original content, backups should be created instantly.
  - Maintain backups for a period of time to allow for recovery process or fixing issue that is not revealed instantaneously.
  - Use automation backups, as creating copies manually can be time consuming and tedious.
  - Run a set of tests on the backup process by periodically restoring the contents and verifying its accuracy.

### INFORMATION SECURITY MANAGEMENT

#### SECURITY POLICY

When employees have access to the internet at work, there are serious risks involved. They can download viruses, create legal liabilities, gain unauthorized access to critical information and potentially, leak it. Good technical security and staff training can help. Good staff/security policies are also important because they make it very clear what is acceptable and what is not.

- How to prepare and implement a policy
- Sample Security Policies



# Awareness Posters

(schools, public & organisations)



## IDENTITY THEFT

**HOW TO PROTECT YOURSELF!**

- Do not send personal information to unknown websites.
- Do not respond to unknown emails.
- If shopping online, know your sources.
- Read website's privacy statement carefully.
- Post your resumes only on prominent jobsites.
- Always LOG OFF your computer when not in use!

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## PHISHING SCAM

PHISHING SCAM is an act of getting someone into providing private information such as credit card numbers, bank account information, etc. through email, pop up messages and websites that appear to be legitimate.

**HOW TO PROTECT YOURSELF!**

- Don't reply to emails asking for personal or financial information.
- Use an antivirus and firewall software.
- Don't email personal or financial information.
- Be careful of downloading any attachments or files from emails.
- Don't follow links in emails.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## CYBERSTALKING & HARASSMENT

Some tips to avoid being stalked or harassed on the Internet:

- Don't respond to messages that asking for your information.
- Choose a gender/age/location screen name when chatting.
- Don't show your personal feeling or thoughts unless you're prepared to face the damage.
- Some blocking or blocking message and report them to the Malaysian Computer Emergency Response Team (M-CERT) at <http://www.mcert.org.my> (CyberTIT).
- Do a search on yourself by using a search engine to make sure no personal information is posted for others about you.
- If the situation becomes any disturbing, log off and seek assistance.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## PROTECT YOUR PASSWORD

- Never reveal your password to anyone.
- Never provide your password over phone or email.
- Change your password regularly.
- Create difficult to guess password.
- Mix uppercase and lowercase letters, symbols and numbers (e.g. a!c#790j)
- It should be more than 8 characters long.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## SHOP SAFELY ONLINE

- Shop with merchants that you know or trust.
- Check that the shopping website is secured.
- Be wary of unsolicited phone calls or emails from a merchant.
- Read merchant's refund and exchange policy before making purchase.
- Do not share your password.
- Always print and keep the order confirmation documents.
- Read the privacy statement.
- Use an anti-virus, anti-spyware and personal firewall and keep it updated.
- Never enter your personal information in a pop-up screen.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## BEWARE OF SPYWARE

SPYWARE refers to software that performs certain tasks on your computer without your consent. This may include giving you advertisements or collecting personal information about you. (It is also, like viruses, spyware, changes in your system, may include as your browser, uninstalled software)

**HOW TO PREVENT FROM SPYWARE!**

- Use a firewall.
- Adjust your security setting on your browser for the Internet zone to "Medium".
- Install and update your anti-spyware software.
- Download software from websites that you trust only.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## SAFETY ON INTERNET CHAT

- Use nicknames as ID instead of real names, e.g. Topkooke instead of Abdul Hamid.
- Never provide personal information that is sensitive.
- Do not meet a stranger that you met on Internet chat.
- Only open or download files from people you know.
- When using a public computer log in your ID and password manually.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## CHAT TOPIC (for your info)

Your name?  
Where do you live?  
Your parents' name?  
Where do you go to school?  
Your phone number?

## DON'T GIVE

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## YOUR COMPUTER SECURITY CHECKLIST

- Install and use a personal firewall.
- Update your software.
- Use an updated anti-virus software.
- Use an updated anti-spyware software.
- Scan all email attachments.
- Scan all your external drives (thumb drives, memory cards, hard disk).
- Back up your files on your computer.
- Create and use a strong password and change them regularly.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

## SAFE ONLINE BANKING

- Keep your passwords/PIN code safe and memorize them.
- Check that the Online Banking website is secured.
- Log out immediately after you have completed your online transaction.
- Use an anti-virus, anti-spyware and personal firewall and keep it updated.
- Do not copy or click on any links attached in emails.
- Do not respond to emails asking for personal information.
- Read privacy and policy information before conducting any transactions.
- Check your account statements to ensure that no unauthorized transaction has taken place.
- When visiting your online banking site, always check that the Date and Time, matches the date and time when you last signed in.

Let's Make The Internet A Safer Place  
CyberSecurity Malaysia  
MOSTI

# Information Security Newsletter (quarterly publication)

**CyberSAFE**  
Security Awareness For Everyone

**Editor's note**

Hi, and I am glad to announce that you are receiving an important new publication. It is something that is for people like us to help them learn from past techniques that are still used today, but we are adding new content to make sure you are up to date with the latest threats and the way we can protect ourselves. There are two main parts to this newsletter. The first part is the 'CyberSAFE Tip' which is a short, easy-to-read article that provides a quick tip on how to stay safe online. The second part is the 'CyberSAFE Tip' which is a short, easy-to-read article that provides a quick tip on how to stay safe online.

**CyberSafety Tip: Safe Internet Banking**

As more people use the convenience of conducting their banking transactions and paying their bills using the Internet, this has become a place for hackers to look for their victims to capture their information or even to use the Internet and through your email accounts.

**Comic Strip**

Thank you and I hope you find this issue to be helpful and the share it with your friends and family members.

*Raj Kumar*  
The Editor

**e-Security**  
Volume 12 (Q3/2007)

**MOSTI**

From the Editor's Desk

Greetings from the editor's desk. We have a new look for our newsletter and if you have any feedback on our new design, please do let us know. The new design includes a more vibrant and technological look and feel.

As what has happened in the second quarter? Well, the much-awaited International Conference and Exhibition took place very successfully from the 28th July - 29th July 2007. The event was opened by Y. Dato' Sri Dr. Jambak Marican, the Minister of Science, Technology & Innovation.

It was a great event with many great speakers from all over the world. We had the former President of MOSTI, the former Minister of the IIC President on Cyber Security and the former CEO of MAMPU & S&I. It was a privilege to have them all at the event and we had Steve Chikwa and Dr. Alan Bawa.

This issue will see a variety of articles from our contributors looking at many areas of information security. I do hope that you will find it useful and also to contribute with the newsletter if you need more information.

Our Cyber issues are ongoing and our last issue for 2007 is in August 2008 and expect to see more and more security professionals to contribute to our newsletter and website if you can help us out.

Philip Victor  
victor@cssec.org.my

**Reader Enquiry**

Training & Outreach Unit  
Malaysia Cyber Security Centre  
MAMPU Street (8th Floor)  
Telok Ayer Staircase  
50450 Kuala Lumpur, Malaysia  
Tel: 463 2857 7342 Fax: 463 2857 8227  
Email: training@cssec.org.my

**e-Security**  
Volume 7 (Q3/2004)

**MOSTI**

**Contributors**

1. Banking With Confidence From Within  
By Dr. Jambak & Lim Yuen  
jambak@cssec.org.my
2. Accreditation for Information Security  
Information@cssec.org.my
3. How To Develop A Security Policy  
By Dr. Jambak & Lim Yuen  
jambak@cssec.org.my
4. Introduction to Incident Management  
By Jambak & Lim Yuen  
jambak@cssec.org.my
5. Keeping Your Database Secure  
By Alan Bawa  
alan@cssec.org.my
6. News Analysis  
By Alan Bawa  
alan@cssec.org.my
7. Supporting Against DDoS!  
Protecting Your Assets  
By Jambak & Lim Yuen  
jambak@cssec.org.my
8. Reading and Not Getting  
Misleading Messages  
By Alan Bawa  
alan@cssec.org.my
9. Why Customers Must Take  
A Closer Look At Their  
Personal System  
By Alan Bawa  
alan@cssec.org.my
10. The New Version of Cookies  
By Alan Bawa  
alan@cssec.org.my



Securing Our Cyberspace



# Awareness Messages

**CyberSecurity MALAYSIA**
  
 MYCERT 24/7 call centre reporting: 019-2813801 / 019-2665850
   
 Email: [mycert@mycert.org.my](mailto:mycert@mycert.org.my)

### 10 TIPS FOR SAFER COMPUTING AND INTERNET EXPERIENCE

1. Protect your personal information and know who you are dealing with. Do not reveal information about yourself to people or websites you do not know on the Internet.
2. Create hard-to-guess passwords and keep them private.
3. Don't open emails from unknown sources.
4. Use anti-virus, anti-spyware and firewall, and keep them updated regularly.
5. Update your operating system and web browser regularly.
6. Know the dangers of using file sharing or Peer-to-peer (P2P) systems as it may contain spyware and viruses. It can also create legal and ethical issues regarding the unauthorized sharing of copyrighted materials.
7. Back up your important files regularly.
8. Don't leave your computer unattended and password protect it when not in use.
9. Never reveal your true identity in chat rooms.
10. Contact MyCERT if something goes wrong online.

**CyberSecurity MALAYSIA**

## 13 SECURITY TIPS TO SAFE INTERNET BANKING

1. Keep your password/PIN code safe and memorize them. Ensure you change them regularly (recommended every 3 months). If you conduct Internet transactions in a number of websites, use different passwords for each website. Create unique passwords that are difficult to guess, e.g. use a combination of letters and numbers.
2. How do you know the website is secured?
  - Look for https:// in the URL and not http:// when you log on
  - Look at the status bar of the security lock (locked padlock) when you visit the bank site. Double click on the padlock and ensure that it has a valid digital certificate.

WEB BROWSER	SECURED	NOT SECURED
Microsoft Windows Platform		
Internet Explorer		
Netscape Navigator		
Firefox		
Apple MAC Platform		
Apple Safari		
Firefox		

3. Log out immediately after completing your Internet transaction. Then, clear the browser cache, cookies and history later to your bank's website for online guidance. Ensure that you log out properly after every Internet banking session and not just close the browser.
4. Never leave your computer unattended when you are conducting your Internet transactions.
5. If you are unsure of the security of the computer, do not use it for Internet transactions.
6. Use an anti-virus, anti-spyware and personal firewall and keep it updated. Some of this software are freely available on the Internet.
7. Ensure that your PC and browser are updated with the latest patches/fixes. Use the Automated Update feature of your Operating System (e.g. Windows Update for Windows users).
8. Do not be influenced by appealing offers, especially from unknown parties. Do not click on any links attached in your emails. Do not copy and paste any website address (URL). Retype the website address to surf or use your Bookmark.
9. Do not respond to emails asking for personal information, login information or on changing password notification. Report to your bank or CyberSecurity Malaysia.
10. If you decide to go to other websites linked via your Internet banking website, read the privacy and policy information of that website first before conducting any Internet transactions.
11. Always check your account balance/statement to ensure that no unauthorized withdrawal has taken place.
12. When visiting your Internet banking site, always check that the Date and Time matches the date and time when you last signed in.
13. If your bank account has been compromised, act fast and inform the bank, or contact CyberSecurity Malaysia (<http://www.cybersecurity.org.my> or <http://www.mycert.org.my>)

Level 7, Sapura @ Mines No. 7,  
 Jalan Tekis, The Mines Resort City,  
 43300 Seri Kembangan,  
 Selangor Darul Ehsan.

• Tel No: 03-89926969      • Fax No: 03-89453442      • Q&A: 019-2613801  
 • MYCERT 24/7 call centre reporting: 019-2665850      • Email: [mycert@mycert.org.my](mailto:mycert@mycert.org.my)





# Information Security Brochures

## Parental Control Tools

Parental control tools can help you to monitor and restrict your children's online activity. It can be useful especially when you are not around or the computer is not located in the family room. There are many parental tools available in the market today which some are free and some you have to purchase. Please take note that each control tool determines whether materials are "inappropriate" or "safe for kids" differently. Shop around and go through each software to ensure it contains all the necessary features before purchasing it. No parental control tool is 100% reliable therefore parents would still need to monitor their child's online activities.

### Make your Computer Safe

One of the practical ways to help your children to stay safe online is to protect your computer.

**You can protect your computer by:**

- Installing internet filter software
  - To block out certain types of content on the Internet.
- Installing security software like antivirus, firewall and antispware.
- Using Spam filter to block junk emails.
- Using Parental monitoring software to monitor your children's activity online.
- Using Pop-up Blockers to stop "pop-up" windows.
- Enabling and change Internet browser security setting to "higher".
- Update your system software.

**For more information:**  
Visit our Security Awareness Portal at [www.esecurity.org.my](http://www.esecurity.org.my)

[www.esecurity.org.my](http://www.esecurity.org.my) is a portal developed by CyberSecurity Malaysia to inform and educate computer users on threats and offer safety tips for protecting their computer while online.

**To report incidents - contact Cyber999**

Cyber999 is a service offered by the Malaysian Computer Emergency Response Team (MyCERT) to handle incidents faced by computer/Internet user.

**You can report incidents via:**

Online - <http://www.mycert.org.my/>  
Tel: 03-89926969  
Mobile phone (24 hrs) : 019-2665850  
SMS: 019-2613801  
Email: [mycert@mycert.org.my](mailto:mycert@mycert.org.my)  
Print online form and fax - 603-89453442

**Internet Safety tools**

**Parental Control Tools**  
<http://www.tn.net.my> - (look for XFilter)  
<http://www.berster.com>  
<http://www.cyberpatrol.com>  
<http://www.netnanny.com>

**Children-friendly Search Engines**  
Yahoo Kids! - <http://www.yahoo!igans.com>  
Kids Click - <http://www.kidclick.org>  
Lycos Kids - <http://www.lycos.com/kids>  
Ask Jeeves For Kids - <http://www.ajkids.com>  
Safe Search - <http://www.google.com/help/customize.html>

## Surf with your Children

A Parent's Guide to Internet Safety

Now that I know all about Internet security, what's your opinion on that new laptop? No!

**I am chatting online with someone I don't know. What should I do?**

- Always keep your personal information private.
- Do not talk about anything that makes you feel uncomfortable.
- Do not pretend that you are someone you are not.
- Always tell an adult if someone is asking you personal questions.

**I want to keep my mobile number safe. What should I do?**

- THINK before you send. You cannot unsend a message or control where it ends up.
- Get your friends' permission before you send out pics of them.
- Only give your mobile number to people you know and trust.
- Never answer text messages from people you don't know (ignore them or better yet, delete them).

**Someone asks for my password. What should I do?**

- NEVER give your password away. If you do, change it immediately.
- Use numbers that represent letters and punctuation to mix up the password. e.g. My Big Cat Eats could be My3!C@t@z J. Nearly impossible to guess!
- A bank or Website will NEVER ask for confirmation of login details in an email or any other message.

**My parents don't get the net. What should I do?**

- Get them involved, teach them the tricks.
- Show them how to open and use an email account; and how IMs work.
- Do searches on their hobbies; show them how to Google.

Let's Make The Internet A Safer Place  
[www.esecurity.org.my](http://www.esecurity.org.my)

## ARE YOU DOWN WITH WHAT'S UP ON THE NET?

### Free Internet Safety Tools

Remove AdWare (removes AdWare and Rogue Cookies)  
Ad-Aware  
<http://www.removedware.com>

Anti SpyWare (finds malware other free ones don't)  
Spybot  
<http://www.wasfr-networking.org>

Firewall  
ZoneAlarm  
<http://www.zones.com/!preview/213160>

ZoneAlarm (easy-to-use teaching system)  
<http://www.zonelabs.com/store/content/home.jsp>

Anti-Virus  
Avast  
<http://www.avast.com>

AVG  
gr806

Anti Spam (for Outlook and Outlook Express)  
spamfighter  
<http://www.spamfighter.com/newsite/Features.asp>

Browser (Mozilla Firefox as the browser)  
<http://www.mozilla.com/firefox/central>

Mail (free spam / Phishing filters)  
Mozilla Thunderbird  
<http://www.mozilla.com>

Freeware (good source for information)  
<http://www.zones.com>

Downloads (good source for information)  
<http://www.zones.com>

Written by JRCY with support from Chikka.  
Written by JRCY with support from Chikka.

(ISC)<sup>2+</sup> [www.isc2.org](http://www.isc2.org) [www.childsafe.org](http://www.childsafe.org)

(ISC)<sup>2+</sup> [www.isc2.org](http://www.isc2.org) [www.childsafe.org](http://www.childsafe.org)

## Parent's Guide to Internet Safety

## Teenager Guide to Internet Safety



Securing Our Cyberspace



# Awareness Videos

## Email & Spam



## Safe Chatting



## Safe Internet Banking

## Cyber Stalking



# Exhibition & Road Show



- Information security strategies must cover all user groups
- Public-private co-operation is crucial in building a security culture
- Security is everyone's responsibility and starts at the top management
- Adoption of international standards and best practices is crucial in creating the competitive advantage (e.g. ISO 17799)
- Awareness & education must be deployed throughout the organisations and include all vendors & and alliances



# Thank You

Level 7, Sapura@MINES  
No. 7, Jalan Tasik, The Mines Resort City  
43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia  
Tel: +60 3 8992 6888 Fax: +60 3 8945 3205  
MyCERT: Tel: +60 3 8992 6969 / Fax: +60 3 8945 3442  
**[training\[at\]cybersecurity.org.my](mailto:training@cybersecurity.org.my)**



**Website: <http://www.cybersecurity.org.my>**  
**For General Inquiries: [info@cybersecurity.org.my](mailto:info@cybersecurity.org.my)**  
**E-security: <http://www.esecurity.org.my>**  
**MyCERT: <http://www.mycert.org.my>**