CyberSAFE

Security Awareness For Everyone

Vol. 8

Message from the CEO

Welcome to another edition of our CyberSAFE Newsletter which coincides with the World Computer Security Day (WCSD) celebrated globally on the 30th November 2009 annually. This year CyberSecurity Malaysia is leading Malaysia's celebration of WCSD for the first time and we have planned a number of activities to mark this important date in Cyber Security. Among them are the FIRST Technical Colloquium, the launch of Malaysia's Malware Research Center and the 1st ASEAN Cyber Volunteers Development Course. Do check out our portal www.cybersafe.my <http://www.cybersafe.my> to find more information. As we are heading towards the end of 2009, we are intensifying our awareness activities and this will followed up by more exciting activities for 2010.

Realizing that we can't do this on our own, we are also looking at creating strategic partnerships with both organizations and individuals to help us spread CyberSAFE's Internet Safety message to a wider group of people. Therefore, we would like to encourage you to join us by registering your interest online via our portal.

And lastly, as this is the final edition of the newsletter for 2009, please allow me to wish you a meaningful and safe 2010 ahead.

Be Smart be Safe.....

Best Regards,

Husin Jazri, CISSP

CyberSafety Tips

The Guideline for Cyberspace Behaviour

Regardless of age, gender, ethnicity or country, people has an opportunity to access the internet everywhere, anywhere. The internet is a huge place for everyone to use. People has own individuals need while using the internet - retrieving information, chatting, gaming, online shopping etc.

Like in the physical worlds, cyberspace has their specific culture and behavioural patterns. In cyberspace, anybody can be 'anybody'. Some people behave differently while in the internet that can leads to misbehavioural patterns - cheating, bullying, stalking. It is due to the direct interaction is only between computer user - human and machine - computer. Therefore the core rules of cyberspace behaviour – netiquette are essential for behaving properly online.

1. There is a human being on the other side of computer
Always remember that your correspondent is a person with feelings more or less like your own. So respect other people's feeling for every action while connected to the internet.

2. Offline and Online - the behaviour should be the same
Some of people may think that they can do anything in the cyberspace since nobody could see them. Therefore they consider misbehavioural pattern is acceptable in the cyberspace.

3. Cyberspace is a huge place; there are many different cultures within it.
Different domain in cyberspace, different cultures. Please make sure to take a look around before participate. Observe and feel how the people who are already there behave.

4. Don't waste other people time's and bandwidth
Make sure any upload or post is beneficial to other people. It is your responsibility to ensure other people do not waste their time and network bandwidth to read your posting in the internet.

5. Always be good while online
Even though no one can see you, it is not make you invisible. People can judge you based on quality of your writing.

6. Cultivate knowledge sharing culture
The foundation of civilization is based on the quality of its citizen's knowledge. Don't hesitate to share your experience and knowledge to the public knowledge in the internet.

7. Do not ignite flame wars
Bare in mind that you need to very conscious that you must take care of other people's feeling in the internet. Hate speeches, inappropriate phrases will ignite flame war and could make unpleasant feeling to the other people.

8. Respect other people's privacy
You should not read, copy or distribute other people's privacy with/without their consent.

9. Do not abuse power
In cyberspace, some people have more power than others such as system administrator. Remember - it does not mean you can take advantage of them. Power comes with responsibility.

10. Everyone was a network newbie once- so be forgiving of other people's mistake
Be kind and forgive other for minor mistakes. Not everybody knows everything. Guide them.

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

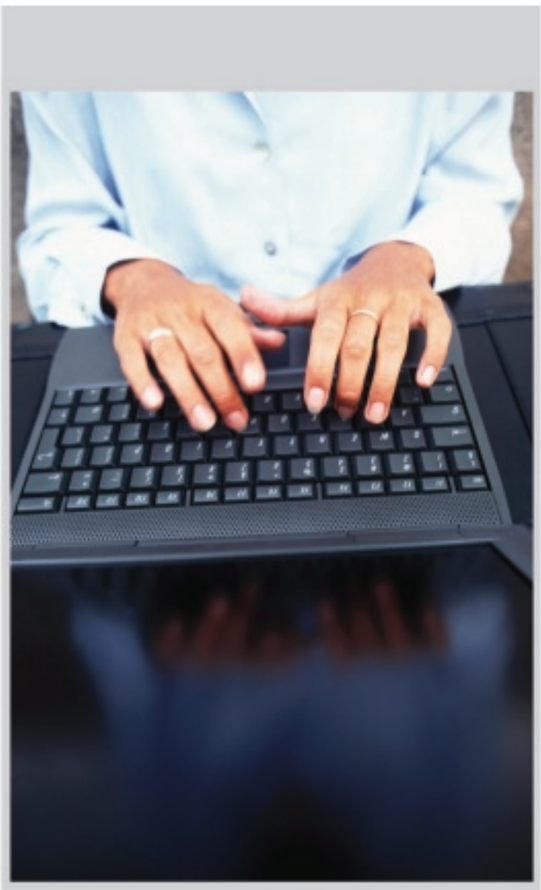
KDN License Number: PP15773/07/2009(022010) | Printed Quarterly

CyberGuideline

How can you participate in World Computer Security Day

Listed below are 50 ways on how we can participate in the World Computer Security Day.
Source by www.computersecurityday.org

1. Display computer security posters.
2. Present computer security briefings.
3. Change your password.
4. Check for computer viruses.
5. Show computer security videos, films or slides.
6. Protect against static electricity.
7. Modify the logon message on your computer system to notify users that Computer Security Day is November 30.
8. Vacuum your computer and the immediate area.
9. Clean the heads on your disk drives or other magnetic media drives.
10. Back-up your data. (after being certain that it is virus-free.)
11. Delete unneeded files.
12. Initiate a computer security poster design contest for next year.
13. Demonstrate computer security software.
14. Publicize existing computer security policy.
15. Issue new and improved computer security policy.
16. Declare an amnesty day for computer security violators who wish to reform.
17. Announce COMPUTER SECURITY DAY in your internal newsletter.
18. Examine the audit files on your computers.
19. Verify that the "Welcome" message that is normally used on your computer is appropriate for your organization.
20. Write-protect all diskettes that are not to be written to.
21. Take the write-protect rings out of the tapes in your library.
22. Verify your inventory of computer applications.
23. Verify your inventory of computer utilities and packaged software.
24. Verify your inventory of computer hardware.
25. Install and inspect power surge protection as appropriate.
26. Install fire/smoke detection and suppression equipment in computer areas.
27. Eliminate dust from computer areas, including chalk dust.
28. Provide dust and water covers for personal and larger computers.
29. Post "No Drinking" and "No Smoking" signs in computer areas.
30. Develop a recovery plan for all computer systems that require one.
31. Verify that passwords are not "Posted" and all other keys are secured.
32. Verify that backup power and air conditioning fit your needs.
33. Have a mini training session to provide all computer users with a basic understanding of computer security.
34. Verify that all source code is protected from unauthorized changes.
35. Verify that each computer has trouble log and that it is being used.
36. Verify that appropriate off site storage exists and is being used.
37. Remove all unnecessary items such as extra supplies, coat racks, and printouts from the computer room.
38. Select a computer system on which to perform a risk analysis.
39. Begin planning for next year's COMPUTER SECURITY DAY.
40. Change the FORMAT command in DOS to avoid accidentally FORMATing of disks.
41. Protect the computer on your store-and-forward phone message system.
42. Hold a discussion of ethics with computer users.
43. Volunteer to speak about computer security at a local computer club or school.
44. Collect Computer Security Day memorabilia to trade with others.
45. Register and pay for all commercial software that is used on your computer.
46. Register and pay for all shareware that you use regularly.
47. Install all security-related updates to your computer's operating system.
48. Help a computer novice backup their files.
49. Protect all cabin computers from floating droplets of liquid.
50. Plan to attend a computer security meeting or seminar.
51. Consider the privacy aspect of the data on your computer and protect it.
52. Update your anti-virus program



Cyber Article

Protect yourself in the Internet.

Introduction
Internet has been a norm for today's living. This has enabled the users to communicate without a boundary, leaving a mark in social media, transactions done with a click of a second and new set world of order waiting to be experienced and executed. Through the dominance and rise of Internet, it also paved for risk, threats and cyber crimes to take place. Most of us are aware the dangers that we are facing on the Internet. But some of them are uncertain on how to protect themselves from the dangers on the Internet. In this article we will be guided on the available techniques to protect from the Internet. The reminding tips that are suggested in this article may be a familiar one to you, but we should question oneself whether we follow the rules of protecting from the dangers of Internet.

Tip 1 – Look out for E-mail attachments and Internet download modules

The most common methods of transferring computer viruses is by embedding them in attachments that accompany e-mails or materials downloaded from attractive Web sites. Recently, attackers have engaged in capturing address books and embedding viruses via attachments that appear to come from people you know. Individuals share important information via e-mail, and attachments allow us to send reports, copies of files, spreadsheets, photos, cartoons, music, and the like. The easy to remember tips will help to be more alert on e-mail attachments and downloading modules from the Internet.

- Do not use the "preview" function for e-mail contents.
- Do not open an attachment that the anti-virus software has indicated is malicious
- Do not open e-mails (delete them instead) from some one you do not know, especially if the subject line:
  - Is blank or contains strings of letters and numbers that are nonsense
  - Tells you of winning a contest you never entered or money you should claim
  - Describes the details of a product that you might like
  - Notifies you of a problem with instructions to install software on your machine
  - Notifies you of a billing or account error for a service you do not use

- If you know the sender or decide to open the e-mail, check to make sure that the contents, along with the names of the attachments and the subject line, make sense.

Tip 2 – Use strong passwords and change them regularly.

Passwords are an easily implemented method of limiting access to your electronic work environment. Passwords that are hard to discover will discourage many kinds of intruders. Smaller businesses often have higher employee turnover rates, which increase the need to change passwords regularly. Since you may not know if a password has been guessed, change it at least every six months and preferably every three months, and do not allow the reuse of old passwords.

For each computer and service you use (e.g. online purchasing), you should have a unique password. By not reusing a password, a compromise in one area will not open access to other areas. You should not write down passwords or share them with anyone. But if you need to write them down, store the paper in a secure location such as a locked file cabinet (not under your keyboard where anyone can find them).

Every user of the computer system should have a unique account and be responsible for controlling his or her password. This provides a means of directly linking actions on the network to a specific individual.

To make a strong password, below are the tips that can be adhered.

- Use a combination of letters, both upper and lowercase, numbers, and punctuation marks. A password should be complicated so that it cannot be easily guessed. Do not use dictionary words, names, or minor variations of these. Lengths can vary (a minimum of six characters; longer is better). Construct the password using a pattern so that you can remember it whenever you need it without having to write it down to jog your memory.
- Educate employees to always change default passwords and initial access passwords as soon as possible. Policies should be established to require strong passwords and to mandate a frequency of change. Employees should be educated about the need for strong passwords as soon as they are hired and reminded to change them regularly.

See page 04

Greetings from the Editor's Desk!

Since the last edition the CyberSAFE has been working very hard to bring you more articles on internet safety. Though there are new threats popping up every day, the issues remain the same and boils down to educating and protecting oneself against these threats, including securing the device you use to connect to the internet. So in-conjunction of the World Computer Security Day 2009, we have include a list over 50 things that you can do individually or as a group to celebrate this event. However, we would like to encourage you to go further by practicing these tips throughout the year and promote it to people around you. Further to this, we would like to invite to attend any of the events where you can find out more about cyber security and how you can protect yourself. In this issue, you will also find some information on how to protect yourself in the internet and tips on protecting you computer.

We do hope you will enjoy reading this newsletter and before we sign off, the CyberSAFE team would like to wish all of you Happy 2010 and watch out for our next issue early next year.

Be Smart Be Safe.....

Produced, Design & Layout:
CyberSecurity Malaysia (726630-U)
Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.

Printed by:
Prima Lasindo Autoniaga Enterprise, No 75-1, Jalan 3-76D, Desa Pandan 55100 Kuala Lumpur.
Phone Tel/Fax: 0392815199

From page 03

Tip 3 – Install, Maintain and Apply Anti-Virus Program.

Anti-virus programs are a low-cost means of protecting your systems and information from external threats. Viruses (malicious code embedded in files) exploit vulnerabilities within the technology environment, and the number of identified vulnerabilities has doubled annually since reporting was initiated in 1988. Vulnerabilities exist in every aspect of the hardware and software available in today's marketplace. The most widely publicized viruses are transmitted via e-mail attachments, and infection is initiated when they are opened.

Viruses can infect a computer in many ways: through floppy disks, CDs, e-mails, Web sites, and downloaded files. When you insert a floppy disk, receive e-mail, or download a file, you need to check for viruses.

Anti-virus programs look at the contents of each file, searching for specific characters that match a profile or pattern-called a virus signature—known to be harmful.
For each file that matches a signature, an anti-virus program typically provides several options, such as removing the offending pattern or destroying the file or e-mail attachment that contains the virus.

Intruders have the most success attacking any computer when they use viruses as the means for gaining access. Installing an anti-virus program and keeping it up-to-date are among the best defenses. When a machine is infected, software can be disabled and data destroyed, and the affected machine will attempt to infect other machines, consuming available communication bandwidth, choking networks, and overloading servers. Protection is needed at each machine.

Here are the usual tips.

Install anti-virus software on every machine and keep the signature files current through automatic or manual updates at least weekly. Renew the automatic update capability annually as required to maintain a current virus signature file on every machine.

- DO NOT connect to the Internet without first activating an anti-virus program.

- Educate all computer users to remove or destroy infected files identified by the anti-virus software. Make sure that they know how to remove their machine from the network and who to call for help if they suspect an infection.

- Instruct all e-mail users not to open e-mail attachments from unexpected and unknown sources to avoid unleashing a new virus not yet blocked by the anti-virus program.

The 3 tips that are highlighted above will certainly help the users to protect themselves in the Internet. The formula to continuously stay smart and safe will be to have a balance and discipline to soundly practice the tips.

Reference

Common Sense Guide to CYBER SECURITY for Small Business by Internet Security Alliance.

Contact Cyber999
if you have problems online!

Cyber999 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/cyber999
Telephone	: (03) 8992 6969
Mobile Phone (24 hrs)	: (019) 266 5850
SMS	: (019) 281 3801
Email	: cyber999@cybersecurity.my
Fax	: (03) 8945 3442
Print online form	: www.mycert.org.my/report_incidents/online_form.html

Best Brand Internet Security

ISMS SIRIM

Cyber Resources & Reporting

CyberSAFE
Cyber Security Awareness For Everyone

Security Awareness Portal - www.cyberSAFE.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 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.
| Tel: (03) 8992 6888 | Fax: (03) 8945 3205 | www.cybersecurity.my |