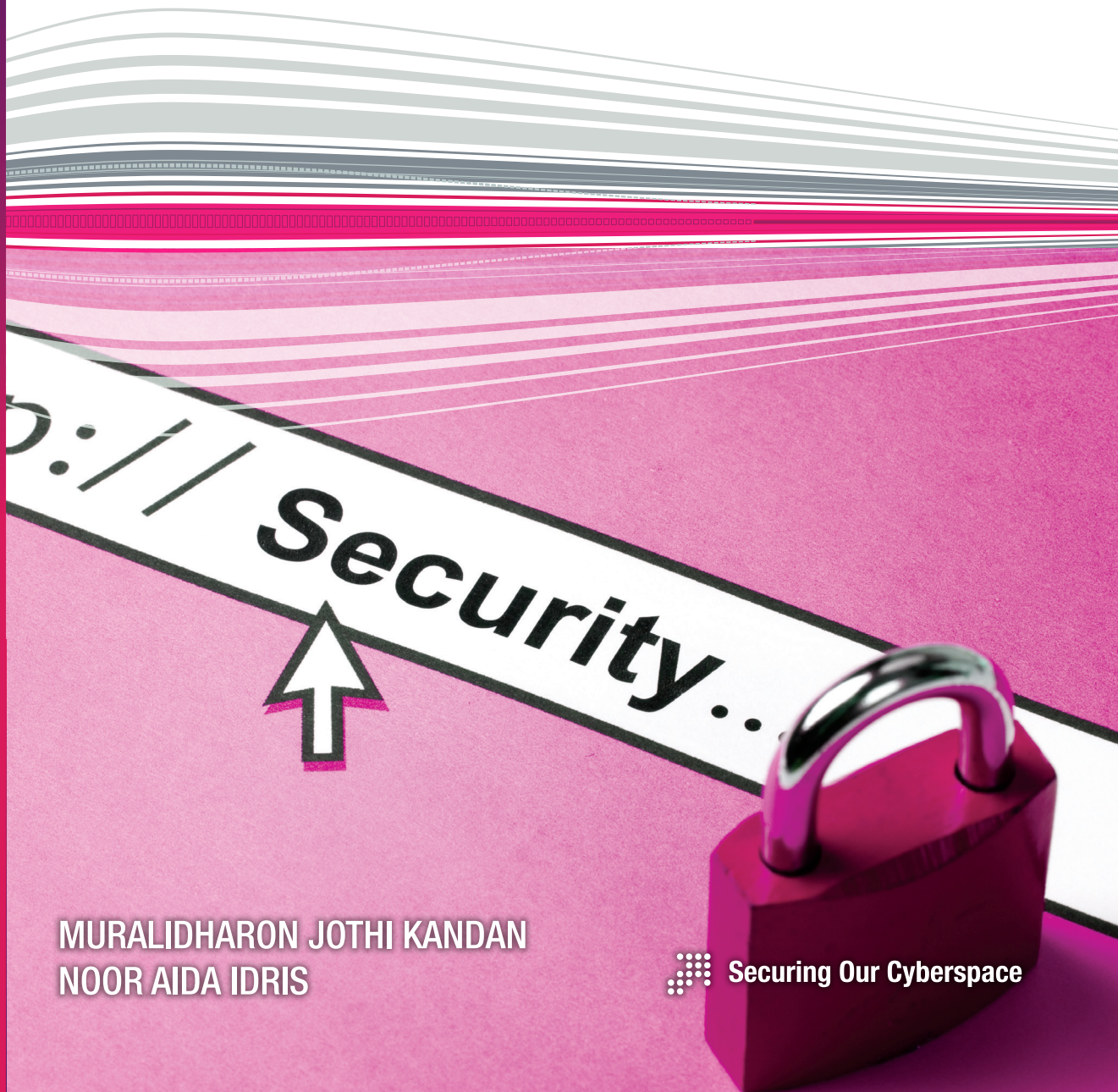
CyberSecurity MALAYSIA
An agency under MOSTI

Guidelines on Computer Security



MURALIDHARON JOTHI KANDAN
NOOR AIDA IDRIS

Securing Our Cyberspace

CyberSecurity MALAYSIA

An agency under MOSTI

Guidelines on Computer Security

MURALIDHARON JOTHI KANDAN
NOOR AIDA IDRIS

COPYRIGHT

NO ENDORSEMENT
Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only, and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

TRADEMARKS
All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

WARNING AND DISCLAIMER
Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained in this document.

REGISTERED OFFICE:
CyberSecurity Malaysia
Level 8, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor.
Phone: +603 – 89460999
Fax: +603 – 8946 0888
http://www.cybersecurity.my

Printed in Malaysia

Acknowledgement

CyberSecurity Malaysia wishes to thank the panel of reviewers (Internal & External) who reviewed drafts of this guideline.

Internal Reviewers

Adli Abd Wahid **(Digital Forensic)**

Ida Rajmee Ramlee **(Security Management & Best Practices)**

Mahmud Abdul Rahman **(Digital Forensic)**

Maslina Binti Daud **(Security Management & Best Practices)**

Noraini Abdul Rahman **(Security Assurance)**

Razana Md Salleh **(Digital Forensic)**

Rosly Yahil **(Cyber Consulting Group)**

Sabariah Binti Ahmad **(Security Management & Best Practices)**

Yati Mohammad Yassin **(Cyber Media Research)**

External Reviewers

Wan Roshaimi Wan Abdullah **(Sapura Secured Technologies)**

Table of Contents

Abstract

Your home computer is a popular target for intruders. Why? Because intruders want what you've stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money to buy themselves goods and services.

But it's not just your finances they're after. Intruders also want your computer's resources, your hard disk space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet. In fact, the more computers an intruder uses, the harder it is for law enforcement to figure out where the attack is really coming from. If intruders can't be found, they can't be stopped, and they can't be prosecuted.

How do intruders break into your computer? In some cases, they send you an email with a virus. Reading that email activates the virus, creating an opening that intruders use to enter or access your computer. In other cases, they take advantage of a flaw or weakness in one of your computer programs. Once they're in your computer, they often install new programs that allow them to continue using your computer even after you plug the holes they originally used to get onto your computer. These backdoors are usually cleverly disguised so that they blend in with other programs running on your computer.

This guideline provides directions for tasks performed on a Microsoft Windows system. Please note that your computer may vary from the example used. If so, you will still be able to perform the task, but it might take some effort to get your version of Windows to do the same thing.

Before diving into the security of your home computer, let's first relate the problem to something you are already familiar with; thus, you can apply your experience to this new area. Think of your computer as you would your house, apartment or condo. What do you know about how that living space works, what do you routinely do to keep it secure, and what have you installed to improve its security? (We'll use this "computer-is-like-a-house-and-the-things-in-it" analogy throughout, departing only a few times to make a point.)

For example, you know that if you have a loud conversation, folks outside your space can probably hear you. You also routinely lock the doors and close the windows when you leave, and you don't give the keys to just anyone. Some of you may install a security system to complement your practices. All of these are part of living in your home.

Let's now apply similar thinking to your home computer. Email, instant messaging, and most web traffic cross the Internet; that is, anyone capturing that information can read it. These are things you need to know. You should always select and use strong passwords and exercise due care when reading all emails, especially unsolicited ones. These are things you need to do. Finally, add a firewall, an anti-virus program and patches to improve the level of security on your home computer.

The rest of this guideline describes the things you need to know and do, and best practices to improve the security of your home computer. Whether your computer runs on Microsoft® Windows®, Apple's Mac OS, LINUX, or on another operating system, the issues are the same and will remain so as new versions of your system are released. The key is to understand the security-related problems that you need to think about and solve.

Introduction

Everyone from children to senior citizens enjoy the convenience of owning and using a computer at home nowadays. A home computer is a popular target for attackers. Why? Because there are no proper security measures implemented on home computers. Even if they exist, they are either poorly implemented or not properly enforced. As such, attackers find it is easy to break into home computers. The level of awareness among home users is very much lower compared to organisations.

Attackers love to access home computers to look for personal information such as passwords for online banking, or financial information such as credit card numbers and bank account numbers. By stealing the information, attackers can fake their online identity and use computer resources (e.g. hard disk space, Internet connection) as a launching pad to attack other computers.

There are many ways for attackers to access home computers unknowingly. One of them is through email attachments that contain malicious codes such as viruses; this can provide a platform to plant a backdoor access for the attacker. Another way is via a downloaded file from an unreliable website that also contains malicious codes. Yet another possible way is to exploit vulnerabilities in the computer's programs that are not updated or patched. In addition, they can easily take advantage of home users' inability or ignorance in securing the computer.

This 'Computer Security Guideline' is a guide for home users to secure home computers. Home users should understand and apply the steps to use their computers safely and securely, especially when browsing the Internet (e.g. reading, downloading, accessing, etc.), conducting online transactions (e.g. online banking, online shopping, etc.), and/or using web-based applications (e.g. email).

1

Chapter Contents

1.1 Scope

The scope of this 'Computer Security Guideline' focuses on ten computer security basics. They are:

- Protecting the computer's operating system (OS)
- Creating a strong password
- Installing and updating personal firewalls
- Installing and updating anti-virus software
- Installing and updating anti-spyware software
- Performing backups of computer data
- Applying patches and updates to software residing in the computer (e.g. email application)
- Best practices when opening email attachments
- Best practices on Internet surfing
- Configuring wireless networks

1.2 Target Audience

This Guideline is targeted to all home users including teenagers, parents, adults and senior citizens. They must have some formal training in computer and Internet security. These fundamental steps will help prevent home computers from computer threats and vulnerabilities. This Guideline does not guarantee that home computers will not be attacked by attackers after these basic measures are implemented. This is because there are many other security measures that can and should be taken to secure a home computer. Some examples include usage of technical mechanisms (e.g. software) or physical hardware (e.g. notebook cable lock). This Guideline is intended to provide basic technical know-how that also requires some basic IT knowledge for a better understanding.

Terms & Definitions

A glossary of terms is usually located at the back of a book and referred to only as required. However, the terms and definitions for this Guideline are placed here for easy reference. It is recommended that the reader spends a few minutes to familiarise him/herself with these computer and technical jargons.

2.1 Antispyware

Software used to prevent and detect unwanted spyware program installations and to remove those programs if installed[1].

2.2 Anti-virus

Software used to identify and remove computer viruses, as well as other viruses that are harmful to computers.

2.3 Application

An application, or “application program”, is a software program that runs on computers[2]. Examples are web browsers, email programs, word processors, games, and utilities.

2.4 Compact disk read-only memory (CD-ROM)

Compact disk (CD) that can be read by a computer with an optical drive[3].

2.5 Compact disk read-only memory (CD-ROM)

Compact disk (CD) that can be read by a computer with an optical drive[3].

1 http://whatis.techtarget.com/definition/0,,sid9_gci1245580,00.html
2 http://www.techterms.com/definition/application
3 http://www.techterms.com/definition/cdrom

2

2.6 Email

An application program used to communicate virtually with other users on the Internet, usually by sending and receiving virtual messages from one device to another, e.g. notebooks, personal computers, mobile devices.

2.7 Hard-disk

Spindle of magnetic disks, called platters, that record and store data or programs on a computer[4]. Also known as hard disk drive (HDD), hard drive, or fixed disk drive.

2.8 Hardware

Physical parts of a computer and its related devices. Internal hardware devices include motherboards, hard drives, and random-access memory (RAM). External hardware devices include monitors, keyboards, the mouse, printers, and scanners[5].

2.9 Internet

A global network that consists of countless interconnected computers that allow millions of people to share information[6].

2.10 Login/logon

The process of signing in and gaining access to computers, systems, networks, or other computer system[7]. Usually consists of a username and password.

2.11 Malicious code

Includes all programs (even macros and scripts) that are deliberately coded to cause an unexpected (and usually unwanted) event on a user's PC[8].

2.12 Malware

A software program designed to damage or perform unwanted actions on computers. Malware is short for "malicious software"[9]. Common examples of malware include viruses, worms, Trojan horses and spyware.

2.13 Operating system

Software that communicates with computer hardware on the most basic level[10]. Without an operating system, no software programs can run. The OS is what allocates memory, processes tasks, accesses disks and peripherials, and serves as the user interface. Also referred to as "OS".

4 http://www.techterms.com/definition/harddisk
5 http://www.techterms.com/definition/hardware
6 http://www.techterms.com/definition/internet
7 http://www.pcmag.com/encyclopedia_term/0,2542,t=login&i=46302,00.asp
8 http://www.yourwindow.to/information-security/gl_maliciouscode.htm
9 http://www.techterms.com/definition/malware
10 http://www.techterms.com/definition/operatingsystem

2.14 Password

A word or string of characters (usually between 4 and 16 characters) that is keyed-in to enter or access a computer, system or network[11] – this is usually part of the login process.

2.15 Patch

A piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs and improving the usability or performance.

2.16 Personal computer (PC)

A programmable machine that can execute a programmed list of instructions and respond to new instructions. It is built around a microprocessor and is used by an individual[12].

2.17 Risk

Combination of the probability of an event and its consequences[13].

2.18 Service Set Identifier (SSID)

A unique ID that consists of 32 characters and is used for naming wireless networks[14]. All wireless devices on a wireless network must employ the same SSID in order to communicate with each other.

2.19 Software

Consists of all programs and applications that run on computers. They provide instructions for computers to perform tasks[15].

2.20 Threat

Probable impending danger, or warning of impending danger where vulnerability may be exploited to cause harm to computers.

2.21 Thumb drive

Removable and rewritable data storage device that plugs into a PC's Universal Serial Bus (USB) port; it allows data to be easily transferred from one PC to another. Also known as a "flash drive", "pen drive", or "USB drive".

2.22 Username

A unique name which provides identification of a user to computers, systems or networks – this is usually part of the login process.

11 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213800,00.html
12 http://www.techterms.com/definition/computer
13 ISO/IEC 27002:2005 Code of Practice for Information Security Management
14 http://www.techterms.com/definition/ssid
15 http://www.techterms.com/definition/software

2.23
Vulnerability

Weaknesses that allow an attacker to violate the integrity of a computer.

2.24
Web browser

An application program used to access the World Wide Web (WWW). It interprets HTML codes including text, images, hypertext links, Javascript, and Java applets[16]. Often just called a “browser”.

2.25
Web application

Applications that are accessed via web browsers over a network (i.e. Internet or intranet). Examples are Internet Banking and Internet Shopping.

16 http://www.techterms.com/definition/browser

Overview of Computer Security

Computer security issues for home users are just as real as computer security issues for an organisation's users. In fact, home users may face far more serious issues because they do not have company policies to comply to or technical resources to ensure adequate computer security implementation.

Home users use computers for everything from online banking to shopping, and also to communicate with others via email and chat rooms. Thus, their computers usually contain sensitive and private information such as online banking statements and passwords that need to be protected. Computer security is the process of protecting computers from unauthorised access, use, modification, deletion or disruption. It includes not just data in the computer, but also the application, resource, and even hard disk space of the computer.

3.1 Importance of Protecting Computers

It is important for home users to protect their computers from threats such as viruses and attack. Attackers may not care about the computers they attack; they usually do not target any particular computer. They just scan the network, and will attack vulnerable computers (i.e. computers with inadequate security measures such as weak passwords or no anti-virus software). Often, the reason they attack computers is merely for fun. They may want to test out their hacking skills or impress their friends. Now however, many of them have changed their motive to financial gain.

There are new vulnerabilities found every day in computer software (e.g. software bugs/errors or computer viruses), which can be easily exploited by these attackers. When vulnerabilities are discovered, computer vendors will usually develop patches and security fixes to address these problems. However, it is up to the user to obtain and install the latest patch. Most reports of computer break-ins can be prevented if computers were updated with the latest patches and security fixes.

Regularly install new critical security patches for operating system vulnerabilities. Patches come out on a weekly basis. The infamous **Windows Update** needs to be run regularly to ensure the latest round of worms, viruses and other vulnerabilities have been patched and your computer is no longer vulnerable. To update patches, please visit any of the relevant vendors based on the operating system.

3

Chapter Contents

In most cases, it takes time to determine the type of security threat. To effectively protect computers at home, please follow the steps provided in *Section 4: Computer Security Basics, and Section 5: Computer Security Incidents and Procedures.*

3.2 Handling Computer Security Incidents

A computer security incident needs to be handled appropriately. Examples of these incidents include a computer being accessed without proper authorisation or being infected with malware, and an email program bombarded with unnecessary or unsolicited emails. Please refer to *Section 6: Reporting Computer Security Incidents* to find out how, where and to whom we should report such incidents in Malaysia.

Computer Security Basics

The good news is that most home computers can be protected by following these simple yet effective recommendations. These recommendations provide the basic protection in securing home computers.

Take note however that there are other security measures and steps that should be taken to mitigate certain security risks or threats in computers. (Please refer to *Appendix A* which provides a checklist on preventive steps that can be performed to mitigate computer security threats).

4.1 Update Operating System

An operating system (OS) provides a software platform on which other programs, called application programs, can run. An OS is the most important program that runs on computers. For a home computer, the most popular operating system is Windows, but others are available, such as Linux and Mac OS X. For security reasons, home users should use a supported version of an OS, and periodically update the OS with the most recent updates and/or patches. They should check the appropriate website regularly for upgrades or patches that can protect their computers.

The following are the recommended actions for updating an OS:

- Enable automatic updates so that the program is launched automatically when new upgrades or patches are available. For steps on how to perform an automatic update, please refer to section 4.2.
- Ensure that existing applications in a computer are compatible with new upgrades or patches. Please visit www.softwarepatch.com.
- Ensure all important data is backed up before updating the OS.
- Another helpful tool is the **Personal Software Inspector** from security vendor **Secunia**. It is a free program designed to inform users of when their application needs patching, and it periodically checks if new updates have been issued for several thousand other applications. To download this application, please visit https://psi.secunia.com.

Note: Not all software companies release patches for downloading, so it may be worthwhile contacting the software vendor or registering your product if you are unable to find what you need.

4

Chapter Contents

4.2 Turn on and Use Automatic Updates

Turn on Automatic Updates. To do this, follow these steps:

1. Click **Start**, type or click **Run** on the search panel, type control and scroll to the **control panel** icon and double click or press enter.
2. In Control Panel, scroll to **Windows Update** icon and double click.
3. Click the **available options** and click to select one of the following options. We recommend that you select the **Automatic update** (recommended) **Automatically download recommended updates for my computer and install them** option. Choose the appropriate date and time for automatic updates.
4. For more information on updating your computer for Windows OS, kindly visit the following URL http://windows.microsoft.com/en-us/windows7/Updating-your-computer.

4.3 Have Windows Remind You about Pending Updates

When you configure Automatic Updates to notify you before you download or install updates, Windows notifies you by displaying an icon and message in the notification area of your taskbar.

If you do not want to download or install the update immediately, click the **Automatic Updates** icon or message in the notification area of your taskbar, and then click **Remind Me Later** in the **Automatic Updates** dialog box. In the **Reminder** dialog box, you can specify the duration that Windows should wait before reminding you of the application that is ready for downloading. Windows reminds you only when you are connected to the Internet. If the reminder is for installing, Windows reminds you according to the schedule that you specify.

Note: The above method applies for the Windows operating system. If it is not a Windows OS, please refer to respective vendors for more details on Automatic Updates.

4.4 Create a Strong Password

A password is needed, along with a username, for login to computers, email applications or web applications (e.g. Internet-banking account). Its main purpose is to tell the system that you are an authorised user. Therefore, it is important for home users to learn how to create strong passwords.

The following are recommended actions for creating a strong password:

- Create a password that contains at least eight characters which include a combination of letters (upper and lower case), numbers and symbols.
- Avoid common words or terms in a dictionary. There are programs that can try to guess a password using every word in the dictionary (also known as a dictionary attack).
- Never use personal information or any related words or terms (e.g. name, birthday, address).
- Change passwords regularly. It is highly recommended that a user changes a password every 6 months; however, change the password immediately if it has been disclosed or if your computer has been infected by a virus or malware.
- Create a different password for each computer or application (e.g. email application, Internet-banking account).
- One way of creating a strong password is to get a phrase that can easily be remembered, taking the first letter of each word as the password and converting it to a phrase. For example, “Everyone knows the sun sets at dusk” would become “e1ktss@D”.
- Do not share passwords on the Internet, or via email or phone. No one should ask for a password to be revealed to them. Be careful if someone does.

Please refer to www.cybersafe.my for more information on creating a strong password.

4.5 The Importance of Installing a Personal Firewall

Personal firewall software is installed in computers by home users to protect against unwanted intrusion and attacks from the Internet by filtering incoming and outgoing traffic to and from the Internet. It helps allow communication from only trusted networks while blocking any unauthorised communication or communication that is not trustworthy. Firewalls are filters that filter any information passing from and into your computer when you are surfing the Internet. It is up to you to set a filtration level that determines what information gets in and what gets out. Many people believe that firewalls are the first level of security, and they are not far from the truth. There are many benefits of using firewalls.

The following are recommended actions for installing a personal firewall:

- Choose and install firewall software by following instructions provided by the software vendor. (Note: A new PC is most likely pre-installed with default firewall software. You just need to enable the default software by following instructions provided by the software vendor.)
- Connect to the Internet and test the firewall software with the instructions provided from the vendor.
- If the test fails, disconnect the Internet connection before taking any corrective action.
- Do not forget to regularly test the firewall and keep it updated with any patches provided by the vendor.
- There are many free Firewall software available online. One of them is ZoneAlarm. You can download the software for free at www.zonealarm.com/zonealarm-pc-security-free-firewall.htm For more information on Free Personal Firewall software, kindly access the following URL www.filehippo.com

4.6 Types of Firewall

Firewalls are offered in two forms: hardware (external) and software (internal). While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use.

- **Hardware**
  Typically called network firewalls, these external devices are positioned between your computer or network and your cable or DSL modem. Many vendors and some Internet service providers (ISPs) offer devices called “routers” that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers but also offer a high degree of protection for a single computer. If you have only one computer behind the firewall, or if you are certain that all of the other computers on the network are up to date on patches and are free from viruses, worms, or other malicious codes, you may not need the extra protection of a software firewall. Hardware based firewalls have the advantage of being separate devices running their own operating systems, so they provide an additional line of defence against attacks.

- **Software**
  Some operating systems include a built-in firewall; if yours does, consider enabling it to add another layer of protection even if you have an external firewall. If you don’t have a built-in firewall, you can obtain a software firewall for relatively little or no cost via online, software vendors, or ISP. Because of the risks associated with downloading software from the Internet onto an unprotected computer, it is best to install the firewall from a CD or DVD. If you do download software from the Internet, make sure it is from a reputable and secure source.

4.6.1 How do You Know What Configuration Settings to Apply

Most commercially available firewall products, both hardware- and software-based, come configured in a manner that is acceptably secure for most users. Since each firewall is different, you’ll need to read and understand the documentation that comes with it to determine whether or not the default settings on your firewall are sufficient for your needs. Additional assistance may be available from

your firewall vendor or ISP (either from tech support or a website). Also, be alert to current viruses or worms, information of which can be found on most security websites (such as MY-CERT Cyber Security Alerts at www.mycert.org.my).

Unfortunately, while properly configured firewalls may be effective at blocking some attacks, don't be lulled into a false sense of security. Although they do offer a certain amount of protection, firewalls do not guarantee that your computer will not be attacked. In particular, a firewall offers little to no protection against viruses that work by having you run the infected program on your computer, as many email-borne viruses do. However, using a firewall in conjunction with other protective measures (such as anti-virus software and "safe" computing practices) will strengthen your resistance to attacks.

Note: There are many types of free firewall. Kindly visit the following URL http://www.firewallguide.com/ for a list of firewalls.

4.7 Install Anti-virus Software

Anti-virus software is installed in computers by home users to detect, prevent and disinfect viruses from spreading in computers.

The following are recommended actions for installing anti-virus software:

- Choose and install anti-virus software by following the instructions provided by the software vendor (Note: A new PC is most likely pre-installed with anti-virus software. You just need to enable the default software by following instructions provided by the software vendor.)
- If you become confused or unsure, abort or cancel the installation process immediately.
- Ensure you enable the option to update signatures (reference files) automatically. (Note: Signature files can be updated through the Internet. Connect to the Internet first to automatically get the updated file. Alternatively, you can download them manually from the vendor's website.)
- Run a thorough scan of your PC with the new anti-virus software. It is recommended that you run a full scan on a weekly basis, or as frequently as you can.
- There are many free anti-virus software available online. One free available anti-virus is the AVG Anti-virus. Download this software for free at http://www.avg.com/my-en/homepage.

Note: Kindly visit the following URL for a list of free anti-virus software: http://www.downloadsquad.com/2009/02/23/9-free-anti-virus-programs-for-windows/

4.8 How Does Anti-virus Function

Anti-virus software is used to prevent, detect and remove malware, including computer viruses, worms and Trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

A variety of strategies are typically employed. Signature-based detection involves searching for known malicious patterns in executable codes. However, it is possible for a user to be infected with new malware for which no signature yet exists. To counter such so-called zero-day threats, heuristics can be used. One type of heuristic approach, generic signatures, can identify new viruses, or variants of existing viruses, by looking for known malicious codes (or slight variations of such codes) in files. Certain anti-virus software can also predict what a file will do if opened/run by emulating it in a sandbox and analysing what it does, to see if it performs any malicious actions. If it does, this could mean the file is malicious.

4.9 Virus Dictionary Approach

Most commercial anti-virus software use both of these approaches, with emphasis on the virus dictionary approach. In the virus dictionary approach, when the anti-virus software examines a file,

it refers to a dictionary of known viruses that have been identified by the author of the anti-virus software. If a piece of code in the file matches any virus identified in the dictionary, the anti-virus software can either delete the file, quarantine it so that the file is inaccessible to other programs and is unable to spread, or attempt to repair the file by removing the virus from the file.

To be successful in the medium and long term, the virus dictionary approach requires periodic online downloads of updated virus dictionary entries. As new viruses are identified "in the wild", civic-minded and technically inclined users can send their infected files to the authors of the anti-virus software, who then include information about the new viruses in their dictionaries.

Dictionary-based anti-virus software typically examines files when the computer's operating system creates, opens, and closes them, and when the files are e-mailed. In this way, a known virus can be detected immediately upon receipt. The software can also typically be scheduled to examine all files on the user's hard disk on a regular basis.

4.10 Anti-spyware Guide

Spyware is a software program used for advertising, collecting personal information for marketing purposes, or changing configurations in computers without their owners consent.

Spyware symptoms are as follows:

- You may see pop-up advertisements that are not related to the website you are browsing. If you see pop up ads as soon as you turn on your computer or when you are not even browsing the Internet, you might have spyware or other unwanted software on your computer.
- Some settings have changed and cannot be changed back to the original setting. Unwanted software can change a web browser's home page or search page settings. Even if these settings are changed to the original setting, they might revert back every time you restart your computer.
- The browser contains additional components without your consent. Spyware and other unwanted software can add toolbars to your web browser that you don't want or need. Even if these toolbars are removed, they might return each time you restart your computer.
- Some other types of spyware use rootkit-like techniques to prevent detection.

The following are recommended actions for installing anti-spyware software:

- Choose the right anti-spyware software to be installed in your PC. Free software is available in the market. One free anti-spyware software is ***lavasoft's ad-aware se personal edition*** and the URL is www.lavasoft.com/.
- Install the anti-spyware software by following instructions provided by the software vendor.
- Complete the installation by running a thorough scan of the PC with the new software. It is recommended that you run a full scan on a weekly basis or as frequently as you can.

Note: Check with different anti-spyware vendors and decide on the best there is through the amount of star ratings given by users. If necessary, multiple anti-spyware software can be installed. For more information on Free Anti Spyware software, kindly access the following URL www.filehippo.com

4.10.1 Features of Anti-spyware

- Adware detection and removal
- Suggests ways to remove spyware
- Auto-updating or auto-scheduling facility, which will ensure you keep upgrading your anti-spyware programs for the latest spyware threats on the Internet

4.10.2 How to Avoid Spyware

Always run an anti-spyware application. Perform on-demand scans regularly to root out spyware that

slips through the cracks. Many users don't really understand the need for software updates After all, when you buy an appliance, such as a washing machine or a TV, it doesn't need updating.

Unfortunately, modern computer software is a lot more complex, and the Internet is often a hostile environment. Therefore, quite frequently, security holes in a popular piece of software are discovered, and must be fixed by the software developer through updates.

The most important example is the operating system itself. It is vital that you keep it updated, since most attacks take advantage of social engineering attacks i.e. drive by download. In fact, that is how the spyware installs itself into the system. The easiest method is simply to have automatic updates enabled. This way, any OS periodically "communicates" with their respective vendors, and automatically installs new updates as they become available.

4.11 Backup Regularly

Computer data needs to be backed-up regularly, since malicious codes or hard disk corruption can cause loss of data. There are also many other reasons why computer data is lost, and they are not all related to security issues, e.g. power blackouts, hardware failures, and human errors.

The following are recommended actions in performing a backup:

- Select data and the type of storage device (e.g. USB thumb drive, external hard drive, CD-ROM) for backup.
- Carry-out backups regularly (recommendation is on a daily basis or before any new application is installed onto the computer).
- Store the backup storage device at a safe place (e.g. secure cabinet).

4.12 Update Software Regularly

Any software running on computers can be a source of security problems (e.g. infected with viruses if not updated regularly. Software that has been used for a long period of time will usually have some problems with regards to functionality, compatibility or security. Usually, with each new version of software, updates and/or patches will be created to fix each problem, and the new version may include additional security measures as well.

The following are recommended actions in updating software running on computers:

- Enable the 'automatic update' option to ensure that software is up-to-date. **(Please refer to section 4.2)**
- Browse the software manufacturer's website to know when the latest update is available.

4.13 Best Practices in Dealing with Email

It is advisable not to open email attachments from an unknown sender (someone you do not know In fact, even if the sender is known, do not open the attachment if you do not expect to receive any attachments from the sender. This is because viruses are easily and widely distributed via email attachments, with no user intervention at all.

The followings are recommended actions when opening email attachments

- Only open email attachments from a trusted sender, or when the attachment is sent by the sender intentionally (check with the sender first if in doubt).
- Perform a manual scan by clicking on the scan option (with anti-virus software) of the email attachment to determine if it is safe to open.
- Enable 'Spam/Junk Email' and 'Add to Junk/Spam Senders List' options in the email application. This can block unsolicited emails (although some may still go through).

4.14 Best Practices for Browsing the Internet

Ideally, computer users should evaluate the risks from the software they use. Many computers are sold with existing software. Whether installed by a computer manufacturer, operating system manufacturer, Internet Service Provider, or by a retail store, the first step in assessing the vulnerability of your computer is to find out what software is installed and how one program will interact with another. Unfortunately, it is not practical for most people, especially home users, to perform this level of analysis.

The following are recommended actions when browsing the Internet:

- Never click on pop-up windows that appear while browsing, and never click on any advertising pop ups that appear out of the blue – these may direct you to a malicious website. Do not click on the links even if they promise cash rewards. It is best to manually block pop-up windows.
- Be careful when downloading files from the Internet, especially from unreliable websites. These files may contain malicious codes that can infect computers. Carefully check and verify websites at http://www.urlvoid.com/ before downloading any files from a site. Depending on the file type, most files can be viewed prior to downloading them. Alternatively, always save them first and scan them with anti-virus software before opening them, or scan files online at www.virustotal.com.
- Be EXTRA careful of files with suspicious extensions such ***.exe, .com, .bat,*** and ***.vbs***. They may contain malicious codes, which are harmful, and can cause computers to hang or even crash totally. While there is no guarantee that any type of file is perfectly safe, pictures, music, and text files with names ending in .jpg, .gif, .mp3, or .txt are less likely to be harmful to computers.
- Always type the URL of the web application you want to access; **never click any URL link**, especially the ones sent via unsolicited email. The URLs may direct you to a **bogus** website.
- Always use the latest version of your web browser. Most popular web browser applications have an 'automatic update' option that can be enabled to receive automatic updates.
- Refuse some or all cookies offered by website applications. This may vary from one browser to another. The recommended advice is to visit the respective vendor sites for more information on how to enable or disable cookies.
- Always read the website's policies on the protection of personal information before providing your own personal information.
- Disable the Internet connection when you are not using the Internet.

4.15 Best Practices for Home Wireless

Home users have come a long way, from no Internet access to 9600 kbps dial-up Internet access, now moving on to wireless connections. Home wireless networks are most susceptible to potential wireless threats because home users usually implement wireless networks without considering security aspects.

The following are recommended actions when configuring and securing a wireless network at home[17]:

- Change the default username and password of access points (APs) immediately. Regularly change passwords (recommended every 6 months).
- Use the highest encryption level (e.g. WPA/WPA2 to secure communication between computers and wireless APs. (Note: Some PCs and APs may not support WPA/WPA2 for some reason; consider replacing those PCs and APs.)
- Change the default Service Set Identifier (SSID) immediately and do not broadcast the SSID.
- Configure wireless APs to accept only Media Address Control (MAC) addresses of identified and trusted wireless devices and equipments.
- Do not automatically connect to an open wireless network, such as a free wireless hotspot or your neighbour's network, as these open networks may be exposed to security risks.
- Turn off the wireless network when not in use.

17 http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

Computer Security Incidents and Procedures

A computer security incident is any real or suspected event that potentially threatens the security of your computer. Examples of incidents include activities such as:

- Attempts (either failed or successful) to gain unauthorised access to computers
- Unwanted disruption or Denial-of-Service (i.e. connection to the Internet is slow or refused)
- Unauthorised use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without your knowledge, instruction, or consent (you can view the computer's log files to learn about these changes)

5.1 What to Look for in an Infected Computer

It is not always easy to tell if your computer has been compromised. More than ever before, the authors of viruses, worms, Trojans and spyware will go to great lengths to hide their codes and conceal what their programs are doing on an infected computer. That is why it is essential to follow the advice given in this guide, in particular, when you install Internet security software – make sure you apply security patches to your operating system and applications, and backup your data regularly. It is very difficult to provide a list of characteristics or symptoms of a compromised computer because the same symptoms can also be caused by hardware and/or software problems.

Here are just a few examples of an infected personal computer:

- Your computer behaves strangely, i.e. in a way you haven't come across
- You see unexpected messages or images
- Programs start unexpectedly
- Your personal firewall tells you that an application has tried to connect to the Internet (and it's not a program that you ran)
- Your friends tell you that they have received e-mail messages from your address and you haven't sent them anything
- Your computer 'freezes' frequently, or programs start running slowly
- You get lots of system error messages
- The operating system will not load when you start your computer

5

Chapter Contents

- You notice that files or folders have been deleted or changed
- Your web browser behaves erratically, e.g. you can't close a browser window

Note: The above example could vary from one user's experience to another. The examples provided give you a hint of possible symptoms that could occur.

5.2 What Can be Done to Secure your Personal Computer

Don't panic if you experience any of the above. You may have a hardware or software problem, rather than a virus, worm or Trojan. Here's what to do:

- Disconnect your computer from the Internet.
- If your operating system will not load, start the computer in Safe Mode (when you switch on the computer, press and hold F8 as soon it begins, then choose 'Safe Mode' from the menu that appears), or boot from a rescue CD.
- Make sure your anti-virus signatures are up-to-date. If possible, do not download updates using the computer you think is compromised, but use another computer (e.g. a friend's computer). This is important: if your computer is infected and you connect to the Internet, a malicious program may send important information to a remote hacker, or send itself to people whose e-mail addresses are stored on your computer.
- If you have any problems removing malicious programs, check your Internet security vendor's website for information on any dedicated utilities that may be needed to remove a particular malicious program.
- If your computer is connected to a local area network, disconnect it from the network.
- Scan the whole computer.
- If a malicious program is found, follow the guidelines provided by your Internet security vendor i.e antivirus software good security programs provided the option to disinfect infected objects, quarantine objects that may be infected, and delete.

5.3 Actions Home Users Can Take to Protect their Computer Systems

1. Use virus protection software

Use anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available.

2. Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it is not sufficient to install a firewall but ignore all other security measures.

3. Don't open unknown email attachments

Before opening any email attachments, be sure you know the source of each attachment. It is not enough that the mail originated from an address you recognise. The Melissa virus spread precisely because it originated from a familiar address. Malicious codes might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedures:

- Be sure your virus definitions are up-to-date (refer to section 4.7)
- Save the file to your hard disk

- Scan the file using your anti-virus software
- Open the file

Another helpful tool for PDF documents is as follows

Gallus is a web-based malware detection service specifically to extract and analyze suspected malicious PDF documents. It is a free service designed to help security researchers and public to detect exploits and other useful information contained in PDF documents. Kindly access the following URL https://blog.honeynet.org.my/gallus/

For additional protection, you can disconnect your computer's network connection before openingthe file. Following these steps will reduce, but not wholly eliminate, the chance that any malicious codes contained in the attachment might spread from your computer to others.

4. **Don't run programs of unknown origin**
   Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or co-workers simply because they are amusing -- they might contain a Trojan horse program.

5. **Keep all applications, including your operating system, patched**
   Vendors will usually release patches for their software when vulnerability is discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's website. Read the manuals or browse the vendor's website for more information.

   Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look for information about automatic notification on your vendor's website. If no mailing list or other automated notification mechanism is offered, you may need to check periodically for updates. Please visit www.softwarepatch.com for more information.

6. **Turn off your computer or disconnect from the network when not in use**
   Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

7. **Make regular backups of critical data**
   Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store backup disks somewhere away from the computer.

8. **Make a boot disk in case your computer is compromised or damaged**
   To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help in the recovery of a computer after such an event has occurred. Remember, however, that you must create this disk **before** you have a security incident.

   Note: Read about Microsoft's security tips for home computer users. This site provides practical security tips for you and your family, the URL of which is as follows: http://www.microsoft.com/protect/resources/newsletter.aspx.

Reporting Computer Security Incidents

Security incidents (depending on the type of incident) can be reported to government agencies, Internet Service Providers, banking institutions and law enforcement agencies (please refer to Appendix B for more information).

It is important to stay calm and follow logical procedures when dealing with computer security incidents. First, report the incident immediately to CyberSecurity Malaysia (MyCERT). Please refer to Appendix C for more information.

6.1 Internet Service Provider

An Internet Service Provider (ISP) is a company that offers users access to the Internet. The ISP connects its users using data transmission technology appropriate for delivering Internet Protocol datagram, such as dial-up, DSL, cable modem, or broadband[18].

Contact the local ISP to report the following incidents:

(a) Spam
(b) Denial-of-Service
(c) Hacking attempts

If unsure, contact the local ISP's customer service centre for further information. A list of local ISPs and their contact information are listed in Appendix C.

18 http://searchwindevelopment.techtarget.com/sDefinition/0,,sid8_gci214028,00.html

6

Chapter Contents

6.2 Malaysian Communications and Multimedia Commission

The Malaysian Communications and Multimedia Commission (MCMC) is the regulator for the converging communications and multimedia industry. Its key role is to regulate the communications and multimedia industry based on the power provided under the Communications and Multimedia Act, 1998 (CMA). Other roles include implementing and promoting the government's national policy objectives for the communication and multimedia sector.

Examples of security incidents that you can report to MCMC are:
(a) Spam
(b) Fraud
(c) Network abuse

Incidents can be reported to MCMC via the following methods[19]:

Methods	Details
Address	Biro Aduan Pengguna, Suruhanjaya Komunikasi & Multimedia Malaysia, Off Persiaran Multimedia, 63000 Cyberjaya, Selangor.
Complaint hotline	1-800-888-030
SMS	SKMM ADUAN [Complaint Details] SMS to 15888
Fax	(03) 8688 1880
Email	aduanskmm@cmc.gov.my

6.3 Royal Malaysian Police

The Royal Malaysian Police (RMP) is the main law enforcement body in Malaysia. In line with emerging technological issues and the rise of crimes related to computers, the Internet and the converging globe of cyberspace, a special unit called the Computer Crimes Unit (CCU) was formed to enable specially-skilled police officers, together with the Attorney-General's Chambers (AGC), to investigate and prosecute computer crimes, which include crimes committed with the aid of a computer. The investigation and prosecution of a cybercrime is carried out by the CCU under the purview of Jabatan Siasatan Jenayah Komersil (Commercial Crimes Investigation Department).

Examples of security incidents that can be reported to RMP are:
(a) Cybercrimes (e.g. cyber stalking, child pornography)
(b) Fraud
(c) Harassment

19 http://www.mcmc.gov.my

6.4 Banking Institutions

Internet Banking is now very popular, and provides the convenience to manage your bank account without having to leave the comfort of your home or office. You can transfer money to another account, pay bills and check your account balance online. Usually, Internet Banking accounts can be accessed via a web browser, with a username and password. Contact your banking institution immediately if you know your password to your Internet Banking account has been compromised.

Examples of security incidents that can be reported to banking institutions are:

(a) Online banking fraud
(b) Credit card fraud
(c) Password/Identity theft
(d) Phishing

Note: For credit card fraud, please contact your respective credit card company and RMP for further action.

It is also important to understand the legal rights pertaining to computer security incidents. Please refer to *Appendix D: Malaysian Laws* to understand more on existing Malaysian Laws on Internet Security.

Appendix A : Checklist to Prevent Computer Threats

This section provides a checklist on preventive steps that can be taken to mitigate computer threats.

However, please remember that the steps provided here are in addition to the ones described in *Section 4: Computer Security Basics*. It is important that you have completed all recommended steps in Section 4: Computer Security Basics. As explained earlier, *Section 4: Computer Security Basics* provides the most simple and effective actions for protecting computers against threats.

Note: These are some ways to prevent computer threats:

Threat	Malicious codes (virus, worm, Trojan Horse)	
What is it?	Unwanted programs that can harm your computer by cloning itself, or providing a 'back door' access to your computer. Examples are viruses, worms and Trojan horses.	
Why is it dangerous?	Spreading of malicious codes through the Internet or email may cause inconvenience, damage or harm to your computer as well as to data stored on it. Trojan horse programs are 'back door' programs that allow unauthorised users easy access to your computer without your knowledge.	
Preventive steps on malicious codes (virus, worm, Trojan Horse)	Have you installed a personal firewall?	☐
	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you run a thorough scan of your computer (if possible, via alternative online virus scans)?	☐
	Have you updated your email application and/or other software applications with the latest patches/updates?	☐
	Have you stopped opening email attachments from someone you do not know?	☐
	Have you reported any incident to MyCERT?	☐

Appendixes

Chapter Contents

Threat	Denial-of-Service (DoS) attack	
What is it?	Denial-of-service attack occurs when your computer is being denied an authorised access to another computer, network (such as the Internet), or system. The following symptoms could indicate a DoS attack (Note: These are examples of symptoms only - other symptoms can exist during a DoS attack): • unusually slow network performance (opening files or accessing websites) • unavailability of a particular website • inability to access any website • dramatic increase in the amount of spam you receive in your account	
Preventive steps	Have you installed a personal firewall?	☐
	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you updated your email and/or software applications with the latest patch/update?	☐
	Have you reported the incident to MyCERT and your ISP?	☐

Threat	Hacking	
What is it?	The act of intruding or gaining unauthorised access into your computer.	
Why is it dangerous?	A hacker can steal your data or launch a DoS attack from your computer without your knowledge.	
Preventive steps	Have you installed a personal firewall?	☐
	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you updated your email application and/or other software applications with the latest patch/update?	☐
	Have you reported the incident to MyCERT?	☐

Threat	Phishing	
What is it?	Phishing is one of the more popular internet scams where attackers attempt to trick you into providing valuable and personal information. Phishing methods usually involve an email or a website parading as a legitimate organisation or financial institution.	
Why is it dangerous?	It tricks you into providing personal and valuable information such as your Internet Banking username and password.	
Preventive steps	Have you typed the URL of your Internet Banking or Online Shopping website (instead of clicking the link from an unsolicited email)?	☐
	Have you checked the lower right-hand corner of the browser for a lock icon? (This lock icon will appear when the site is using a secure HTTP and is verified to be legitimate. You can double-click the lock icon to verify the website.)	☐
	Have you installed an anti-phishing toolbar? (These toolbars are freely available to help combat phishing scams. These tools usually come in the form of web browser extensions. Some examples are Mozilla Firefox 2, Internet Explorer 7, and Netcraft.)	☐

continue

Threat	Phishing	
Preventive steps	Have you installed anti-virus software and enabled the 'automatic update' option?`	☐
	Have you reported the incident to MyCERT and the respective banking institution/online shopping website?	☐

Threat	Spam	
What is it?	Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.	
Why is it dangerous?	Spam can spread malicious codes and cause your computer to hang.	
Preventive steps	Have you stopped responding to any spam email or stopped clicking any link in the email? (You should never respond to unsolicited email as this will encourage spammers to send more spam.)	☐
	Have you immediately deleted spam email without opening them?	☐
	Have you ignored chain letters or other spam that encourage you to send or forward chain emails to others?	☐
	Have you enabled the 'spam/junk filtering' option that immediately blocks spam emails?	☐
	Have you followed good security practices when distributing your email address?	☐
	Have you updated your email and/or software application with the latest patch/update?	☐
	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you reported the incident to MyCERT, MCMC, and your ISP?	☐

Threat	Botnet	
What is it?	A botnet, also known as a "zombie army," is usually made up of tens or hundreds of thousands of computers which have been compromised.	
Why is it dangerous?	The main problem with botnet is that they are hidden. A botnet herder, without your knowledge, can instruct a botnet (i.e. your computer), to launch a DoS on another system, to access and modify personal information, and commit other crimes, all while remaining undetected. It also takes up computer resources.	
Preventive steps	Have you installed a personal firewall?	☐
	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you updated your software application with the latest patch/update?	☐
	Have you reported the incident to MyCERT?	☐

Threat	Identity Theft	
What is it?	Identity theft is when your online identification has been exploited for an unlawful purpose.	
Why is it dangerous?	Somebody can pose as 'you' on the Internet and perform online shopping using your credit cards, or perform valid transactions and even hack into other systems. In the end, the 'identity' is traced back to you and you will be accountable for any problem caused by the stolen identity.	
Preventive steps	Have you installed anti-virus software and enabled the 'automatic update' option?	☐
	Have you stopped posting your personal information (e.g. address, phone number) on the Internet? (Immediately remove your personal information from any site on the Internet as it may be used by somebody to pose as you).	☐
	Did you change your password immediately after noticing that your online identity has been compromised?	☐
	Have you stopped providing personal information via email or phone? (Do not provide personal information to just anybody; ask for verification first).	☐
	Have you watched out for signs of identity theft (e.g. late or missing bills, receiving credit cards that you didn't apply for, or getting contacted by debt collectors or others about purchases you did not make)?	☐
	Have you reported the incident to MyCERT and RMP?	☐

Threat	Cyber stalking	
What is it?	Stalking an individual via the Internet by sending messages that can be threatening, or sexually or emotionally harassing, with the intention of bullying, or for other ulterior motives.	
Why is it dangerous?	Cyber stalking may lead to more serious physical crime.	
Preventive steps	Have you ignored any unwanted communications in your chat program or email?	☐
	Have you saved all your communications for evidence?	☐
	Have you stopped exchanging photos with an online friend? (Do not provide personal information and photos to online friends).	☐
	Have you changed your online identity? Have you changed your username to a less provocative name (e.g. from 'sexygirl' to 'bubble')?	☐
	Have you stopped posting your personal information (e.g. address, phone number) on the Internet? (Immediately remove your personal information as it may be used by somebody to pose as you).	☐
	Have you brought somebody along when meeting an online friend? (Never meet an online friend alone; if possible bring another friend and ensure the meeting place is public).	☐
	Have you reported the incident to MyCERT and RMP?	☐

Appendix B : List of Computer Threats and Definitions

This section introduces the most common computer and Internet threats and their definitions. As there are new threats emerging everyday, it is impossible to list them all; please visit www.esecurity.org.my and www.mycert.org.my for updates on latest threats.

Computer Threats	Definitions
Intrusion	Refers to the successful unauthorised or illegal access to a system or network. This could be the act of root compromise, web defacements, or installation of malicious programs, i.e. backdoor or Trojan horses[20].
Denial-of-Service	Refers to the illegal act of bringing a particular system down or causing the system to malfunction. There are various types of DOS attacks i.e. ping flood attacks, smurf attacks, and syn attacks[21].
Hacking attempts	Refers to illegal and unauthorised hack attempts on a system or network with the malicious intention of compromising a vulnerable system, such as illegal port scannings and probes[22].
Harassment	A malicious act of annoying and threatening someone through various means, i.e via emails or letters, with personal motives and reasons. Harassment usually comes from someone close to the victim, but can also come from an unknown person[23].
Fraud	A computer system is instrumental to this crime, for example, its processing capability is used to divert funds illicitly, such as in email forgery (user impersonation), and e-commerce (payment anonymity)[24].
Spam	Refers to emails that you do not wish to receive and is irrelevant to you. These mails usually have business motives for marketing purposes and are sent by individuals with personal goals, or by marketing agents to sell their products[25].
Virus	A malicious code of programming, which survives and replicates in a computer system and attacks silently without the realisation of the user. Once in the system, they replicate and infect other files, changing them in the process. They are mainly found in software, programs, screen savers and data files. A virus might carry a “payload’’ which it releases when triggered, and it also determines the extent of the damage caused[26].
Worm	A self-contained program that is able to spread functional copies of itself, without any external help, to other computers via a network[27].
Mailbomb	The act of sending large quantities of email to a single user or system which could flood his/her mailbox and crash the system. A mailbomb is considered serious as it can disrupt mail traffic and in some cases, lead to denial of service to the network[28].
Trojan horse	A native of ancient Troy. A program that appears desirable but actually contains something harmful; the contents of a Trojan can be a virus or a worm, for example, “when he downloaded the free game it turned out to be a Trojan horse.”

20 http://www.mycert.org.my/
21 http://www.mycert.org.my/
22 http://www.mycert.org.my/
23 http://www.mycert.org.my/
24 http://www.mycert.org.my/
25 http://www.mycert.org.my/
26 http://www.mycert.org.my/
27 http://www.mycert.org.my/
28 http://www.mycert.org.my/

Appendix C : Reporting Channels and Contact Information

This section provides contact information for local government agencies, local banking institutions and law enforcement.

Malaysian Computer Emergency Response Team
Contact information for MyCERT[29]:

Address	Malaysian Computer Emergency Response Team (MyCERT) CyberSecurity Malaysia Level 7, SAPURA@MINES 7, Jalan Tasik, The Mines Resort City 43300 Seri Kembangan Selangor.
Phone	(03) – 89926969
Cyber999 Hotline	1 300 88 2999
Cyber 999 H/P	019-266 5850 (24x7 call incident reporting)
Fax	(03) – 89453442 (monitored during business hours)
Email	cyber999@cybersecurity.my
Website	http://www.mycert.org.my

Malaysian Communications and Multimedia Commission
Contact information for MCMC[30]:

Address	Suruhanjaya Komunikasi dan Multimedia Malaysia, Malaysian Communications and Multimedia Commission, 63000 Cyberjaya Selangor.
Phone	(03) 8688 8000
Fax	(03) 8688 1000
Email	ccd@cmc.gov.my
Website	www.skmm.gov.my

29 http://www.mycert.org.my
30 http://www.mcmc.gov.my

Royal Malaysian Police
Contact information for RMP[31]:

Address (Headquarters)	Royal Malaysian Police Ibu Pejabat Polis Diraja Malaysia, 50560 Bukit Aman, Kuala Lumpur
Phone	(03) 2262 6222
Fax	(03) 2070 7500
Email	rmp@rmp.gov.my
Website	www.rmp.gov.my

TMnet Streamyx
Contact information for TMnet Streamyx[32]:

Address (Headquarters)	House of Internet, Kelana Park View Tower, 1 Jalan SS6/2, 47301 Petaling Jaya
Phone	1 300 88 9515 (Support) (03) 7804 7086 (03) 7804 2000
Fax	(03) 7804 5910
Website	isp.tm.net.my/streamyx/

Jaring
Contact information for Jaring[33]:

Address (Headquarters)	Mimos Berhad, Taman Teknologi Malaysia TPM, 57000 Kuala Lumpur
Phone	(03) 8996 1900
Fax	(03) 8996 1898
Website	www.jaring.my

Contact Information for Local Banking Institutions - for complete **'Listing of Licensed Banking Institutions'** in Malaysia, please visit Bank Negara Malaysia's website (www.bnm.gov.my).

Banking Institutions	URL
Affin Bank Berhad	www.affinbank.com.my
AmBank (M) Berhad	www.ambg.com.my
CIMB Bank	www.cimb.com
EON Bank Berhad	www.eonbank.com.my
Hong Leong Bank Berhad	www.hlb.com.my
Malayan Banking Berhad (Maybank)	www.maybank2u.com.my
Public Bank	www.publicbank.com.my

For other useful information on banking institutions in Malaysia, please visit the BankingInfo website (www.bankinginfo.com.my).

31 http://www.rmp.gov.my
32 http://isp.tm.net.my/streamyx/
33 http://www.jaring.my/

Appendix D : Malaysian Legislation

When a computer security incident occurs, it is important to know your legal rights and the appropriate actions you can take. Among existing Malaysian legislation related to computer and Internet security are Computer Crimes Act 1997, Communications and Multimedia Act 1998, Copyright (Amendment) Act 1997, and E-commerce Act 2006.

(Note: The text of the legislation contained herein is not the official text, and is provided for information purposes only. For the official and updated version of Malaysian legislation, please refer to www.lawnet.com.my).

Computer Crimes Act 1997

The Computer Crimes Act 1997 aims to provide for offences relating to the misuse of computers such as hacking and cracking, theft of data, and the spreading of malicious codes. It deals with unauthorised access to computer material, unauthorised access with intent to commit other offences, and unauthorised modification of computer contents. It also makes provisions to facilitate investigations for the enforcement of the Act.

An abstract of the offences and punishment under the Act are listed below[32]:

List of Offences		List of Punishments		
Section	**Offences**	**Imprisonment**	**Fine**	**Or both**
3	Unauthorised access to computer material	Not more than 5 years	Not more than RM50,000.00	✓
4	Unauthorised access with intent to commit or facilitate commission of further offence	Not more than 10 years	Not more than RM 150,000.00	✓
5	Unauthorised modification of the contents of any computer	Not more than 7 years; if causing injury, not more than 10 years	Not more than RM100,000.00; if causing injury, not more than RM150,000.00	✓
6	Wrongful communication	Not more than 3 years	Not more than RM25,000.00	✓
7	Abetments and attempts punishable as offences	Not more than 1/2 of maximum term	Same amount as offences abetted	✓
11	Obstruction of search	Not more than 3 years	Not more than RM25,000.00	✓

Communications and Multimedia Act, 1998

There are specific provisions under this Act that deal with network-related crimes such as unauthorised interception of communication, telecoms fraud, transmission of obscene communications, theft of service, criminal damage or sabotage of networking infrastructure, and sale of counterfeit access devices.

The following are offences under the Act:

List of Offences		List of Punishments		
Section	**Offences**	**Imprisonment**	**Fine**	**Or both**
231	Use apparatus or device with intent to obtain information regarding the contents, sender or addressee of any communication without authority	Not more than 2 years	Not more than RM50,000.00	✓
232	Offences of fraudulent use of network facilities or services, etc.	Not more than 3 years	Not more than RM300,000.00	✓
233(2)	Offences of improper use of network facilities or services, etc.	Not more than 1 year	Not more than RM50,000.00; shall also be liable to a further fine of RM1,000.00 for every day during which the offence is continued after conviction.	✓
234	Offences of interception and disclosure of communications prohibited	Not more than 1 year	Not more than RM50,000.00	✓
235	Offences of damage to network facilities, etc.	Not more than 3 years	Not more than RM300,000.00	✓
236	Offences of fraud and related activity in connection with access devices, etc.	Not more than 5 years	Not more than RM500,000.00	✓

Copyright (Amendment) Act, 1997

In Malaysia, copyright protection is governed by the Copyright Act 1987 which provides comprehensive protection for copyrightable works. The Act outlines the nature of work eligible for copyright (including computer software), the scope of protection, and the manner in which that protection is accorded. This Act also enhances copyright protection by taking into account latest developments in information technology related to copyright under the World Intellectual Property Ownership (WIPO) Copyright Treaty 1996.

The following are offences under the Act:

List of Offences		List of Punishments		
Section	**Offences**	**Imprisonment**	**Fine**	**Or both**
41(1)(h)	Circumvents or causes the circumvention of any effective technological measures referred to in S.36(3)	Not more than 3 years Subsequent offence not more that 5 years	Not more than RM250,000.00 Subsequent offence not more than RM500,000.00	✓
41(1)(i)	Removes or alters any electronic rights management information without authority	Not more than 3 years Subsequent offence not more that 5 years	Not more than RM250,000.00 Subsequent offence not more than RM500,000.00	✓
41(1)(j)	Distributes, imports for distribution, or communicates to the public, without authority, works or copies of works where electronic rights management information have been removed or altered without authority	Not more than 3 years Subsequent offence not more that 5 years	Not more than RM250,000.00 Subsequent offence not more than RM500,000.00	✓

Electronic Commerce Act 2006

The Electronic Commerce Act (ECA) 2006 (Act 658) provides for legal recognition of electronic messages in commercial transactions, the use of electronic messages to fulfill legal requirements, and to enable and facilitate commercial transactions through the use of electronic means and other related matters. The Act applies to any commercial transaction conducted through electronic means including commercial transactions by the Federal and State Governments. Nevertheless, the use of such means is not made mandatory.

Appendix E : References

[1] MAMPU, “Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)”, Version 2, 15 Jan 2002. Retrieved from http://www.mampu.gov.my on 30 Jan 2009.

[2] National Institute of Standards and Technology Special Publication (NIST SP) 800-12, “An Introduction to Computer Security: The NIST Handbook”. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf on 30 Jan 2009.

[3] Carnegie Mellon University, “CERT: Home Computer Security (FedCIRC)”, 2002. Retrieved from http://www.cert.org/homeusers/HomeComputerSecurity on 30 Jan 2009.

[4] West-Brown, MJ., et al. “Handbook for Computer Security Incident Response Teams (CSIRTs)”, 2nd Edition, April 2003. Retrieved from www.cert.org/archive/pdf/csirt-handbook.pdf on 30 Jan 2009.

[5] Willert, J., Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters, October 22 2001. Retrieved from http://www.sans.org/reading_room/whitepapers/hsoffice/best_computer_security_practices_for_home_home_office_small_business_and_telecommuters on 30 Jan 2009.

[6] http://www.cybersafe.my

[7] http://www.mycert.org.my

[8] http://www.staysafeonline.info

[9] http://www.microsoft.com/protect/default.mspx

[10] http://www.onguardonline.gov/topics/computer-security.aspx

[11] http://www.buzzle.com/articles/top-5-best-free-anti-spyware-software.html

[12] http://sites.dehumanizer.com/spyware/en/details2.php

[13] http://www.bullguard.com

[14] http://www.isoftwarereviews.com/professional-anti-virus-vs-free-anti-virus-software/

Notes

Notes

Guidelines on Computer Security

This highly anticipated book fully introduces the guideline and best practices of computer Security. It is a comprehensive text, explaining the most fundamental and pervasive. aspects of the field, and a detailed reference filled with valuable information for home users. Home users should understand and apply the steps to use their computers safely and securely, especially when browsing the Internet (e.g. reading, downloading, accessing, etc.), conducting online transactions (e.g. online banking, online shopping, etc.), and/or using web-based applications (e.g. email). These fundamental steps will help prevent home computers from computer threats and vulnerabilities. This guideline is intended to provide basic technical know-how which also requires some basic IT knowledge for a better understanding.

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Business Park
No. 3, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my

Best Brand Internet Security

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

MS ISO/IEC GUIDE 52:1999
QS 02121999 CB 01

Status Company

ISBN 978-967-0118-01-7