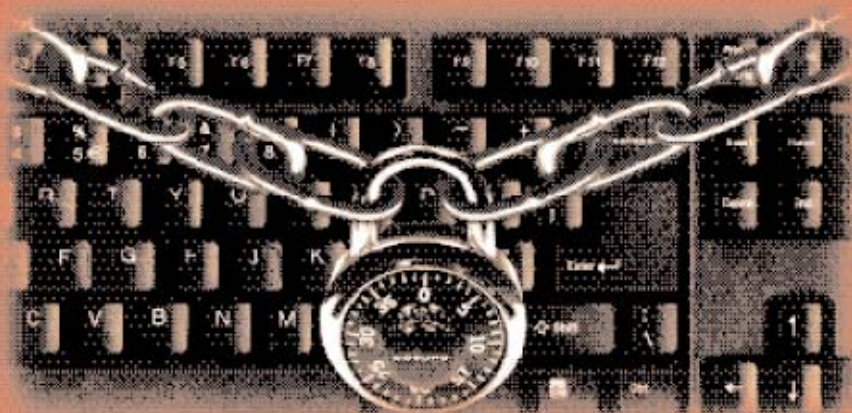


Information Security Guidelines



National Computer Board

Every one of us is responsible for protecting our systems and data. Below are some measures that can be implemented for improving computer security:

- ▶ Restrict access to important data and equipment.

- ▶ Use virus protection software and a firewall.

- ▶ Delete e-mail from unknown sources.

- ▶ Scan attachments with antivirus software.

- ▶ Do not leave systems unattended and accessible.

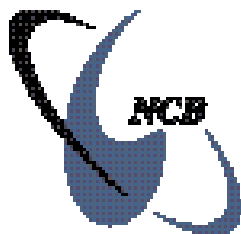
- ▶ Use not-easily-guessable passwords that include numbers and special characters.

- ▶ Do not tell anyone your passwords and do not leave them written where others can find them.

- ▶ Back up and test critical data regularly.



INFORMATION SECURITY GUIDELINES



National Computer Board



Table of Contents

1.	Introduction	1
2.	What is Information Security?	2
3.	Security Risks and Guidelines	2
	3.1. <i>Passwords</i>	3
	3.2. <i>Physical Security</i>	4
	3.3. <i>Social Engineering</i>	4
	3.4. <i>Email Security</i>	6
	3.5. <i>Phishing</i>	7
	3.6. <i>Viruses and Other Malwares</i>	8
4.	Guidelines for Securing Desktops	12



1. Introduction

The purpose of this document is to recommend guidelines for computer users in order to protect their information assets from threats, whether internal or external, deliberate or accidental.

It allows end users to have an understanding of the value of information security and be more responsible towards the protection of organisation's assets.

Also, it enables them to identify common security risks and threats for computer users in the workplace as well as be aware of measures and techniques that can be implemented in order to ensure business continuity and prevent breaches of security.

The information in this guide is based on RFC 2504 – User's Security Handbook.

2. What is Information Security?

Information security is the protection of information systems and data from unauthorized (accidental or intentional) modification, destruction, or disclosure. This protection also includes the confidentiality, integrity, and availability of these systems and data.

With new information technology systems, more information is readily available to more people. Information security has always been a concern. The aim of information security is to create the appropriate balance between ease of use and security. The appropriate balance depends upon the need for confidentiality, integrity and availability.

- Confidentiality has been defined by the International Standards Organization (ISO) as “ensuring that information is accessible only to those authorized to have access” and is one of the cornerstones of information security. It is important to protect information so that unauthorized persons cannot access it.
- Data Integrity is ensuring that data is unchanged from its source and has not been accidentally or

maliciously modified, altered, or destroyed.

- Availability refers to easy access of information systems by authorized users whenever needed.

3. Security Risks and Guidelines

The following section provides guidelines to users with regards to the six most common security threats facing computer users.

- Passwords
- Physical Security
- Social Engineering
- Email Security
- Phishing
- Malware

3.1. Passwords

A password is a combination of codes that a user inputs into a system which once validated and approved, grants him access to the computer system. If a password is easy to remember, it is easy to guess and if it is written down then you don't even need to guess. And if it is not changed regularly then the probability of being attacked is more likely to occur.



Passwords are used to grant access to approved parties. It is used as the first line of defense against unauthorized access to computer systems.

When submitting username and passwords on the Internet, users should ensure that the information is encrypted because otherwise, it can be intercepted and read by others.

■ **Password Tips**

The following are ten tips to help you select a password that is more secure and easy to remember.

- 1 Use a minimum of 8 characters.
- 2 Use a combination of numbers (1-9), alphanumeric characters (A-Z) and special characters (!, @, #, \$, %, ^, &, *, +, =).
- 3 Don't pick a password that someone can easily guess.
- 4 Use a phrase (e.g. title of the song "I Left My Dreams In San Francisco" – password: EYELMDISF).
- 5 Use a separate password for different accounts.
- 6 Do not write down your password and leave it in an easy view to spot.
- 7 Change your password regularly.
- 8 Do not give other people your password, intentionally or unintentionally.
- 9 Use the timeout feature to lock your

computer account when you are away from your desk so as to prevent any unauthorized user from gaining access to the computer.

- 10 Report any suspicious or abnormal circumstances to your system administrator as soon as you notice it.

■ **Examples of Weak Passwords**

- 1 Do not pick a password, which can easily be guessed. For example:-
 - Your login name in any form (as-is, reversed, capitalized, doubled, etc.).
 - Your forename or surname name in any form.
 - Your spouse's or child's name.
- 2 Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- 3 Do not use a password of all same digits, or which consists of the same letter. This significantly decreases the search time for a cracker.
- 4 Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.

3.2. Physical Security

Physical security is the lowest level of security measures which can be implemented to control physical access to a computer system.

Without physical security control, a thief can steal your hard drive, memory, CPU and other components. And in this situation, even the use of a password on the computer system would be of no protection against computer/data theft.

■ Physical Security Tips

- 1 Locking up the facility when it is not being attended
- 2 Not leaving resources unattended during the workday
- 3 Knowing whose responsibility it is to lock up
- 4 Not granting unauthorized people access to equipment
- 5 In an open area, request for a security cable for your equipment
- 6 If using a laptop, keep it close by all the time

3.3. Social Engineering

Many people do not realize it, but social engineering is a tool which many intruders use to gain access to computer systems.

Social engineering may be defined as the act of gaining the trust of legitimate computer users to the point where they reveal system secrets or help someone, unintentionally, to gain unauthorized access to their system(s).

The aim of social engineering is to trick people into revealing:

- Passwords or other information that compromises a target's system security,
- Credit card numbers or other personal information that compromises the individual, or
- To gain access to unauthorized areas where equipment are stored.

The 4 most common tactics used include:

- Telephone – most common means as it is easy, quick and fairly cheap.
- Internet – email & hacking
- Postal Mail – effective for the person trying to get information as it is cheap & people tends to trust written words.
- In person – people tend to trust people whom they can see. It is much easier to build a sense of trust in a person via faceless communications.



■ ***Here are a few examples of social engineering ploys.***

- A hacker may pretend to be a legitimate end-user who is new to the system or is simply not very good with computers. The hacker may approach systems administrators and other end-users for help. This "user" may have lost his password, or simply can't get logged into the system and needs to access the system urgently.
- Hackers have also been known to identify themselves as some VIP in the company, screaming at administrators to get what they want. In such cases, the administrator (or it could be an end-user) may feel threatened by the caller's authority and give in to the demands.
- Hackers who operate via telephone calls may never even have seen the screen display on your system before. In such cases, the trick hackers use is to make details vague, and get the user to reveal more information on the system. The hacker may sound really lost so as to make the user feel that he is helping a damsel in distress. Often, this makes people go out their way to help. The user may then reveal secrets when he is off-guard.

- A hacker may also take advantage of system problems that have come to his attention. Offering help to a user is an effective way to gain the user's trust. A user who is frustrated with problems he is facing will be more than happy when someone comes to offer some help. The hacker may come disguised as the systems administrator or maintenance technician. This hacker will often gain valuable information because the user thinks that it is alright to reveal secrets to technicians. Site visits may pose a greater risk to the hacker as he may not be able to make an easy and quick get-away, but the risk may bring fruitful returns if the hacker is allowed direct access to the system by the naive user.

■ ***Tips in order not to fall victim to Social Engineering***

1. Realize that computer security is a part of everyone's job.
2. Keep your personal account's password secret and known to you only. System administrators need not ask you for your password.
3. Ensure users are aware about social engineering and its associated threats and ploys;



4. Do not give out confidential information without verification; e.g.
 - Verify that the person is s/he says s/he is... on the phone and in person
 - Verify that the business that the person says s/he is from, is a real company
 - Verify that the person works at that company
 - Verify that the URL matches the one you are familiar with
 - Verify that the person is supposed to be working on the equipment.
5. Do not put confidential information in the trash without shredding it first; and
6. Report any suspicious behaviour to the system administrator or information security officer immediately.

3.4. Email Security

What is it about email that makes it in secure?

- Privacy – when you send an email, it passes through various networks as it travels to its final destination and as the email passes from one network to the next, there is no standard that regulates the level of security required in the network. Note that Email sent or received at work may not be private. Check

with your employer, as employers may (in some instances) legally both read your Email and make use of it.

- Spam – this is the Internet version of junk mail. A spam email is generally defined as an unsolicited mailing, usually to many people.
- Hoaxes – an email hoax is a specific type of chain letter that deceives you in order to prompt you to pass it along. Frequently email hoaxes pose an alert and use technical jargon so as to confuse readers and to make them feel as if they are doing a service by passing the hoax email along.
- Rebuttals – the rebuttal is a disguised attempt to combat chain letters, but in fact is a chain letter itself. A clever way to people who appeal to those who have grown very tired of chain mail.
- Information Leak – sending out confidential information of any kind on email can be harmful.
- Tampering – in addition to intercepting email for purposes of accessing confidential information, sometimes the underlying motive is to gain or harm by actually tampering the message.



- Offensive contents – proprietary or confidential information is not the only kind of content that you should be concerned when it comes to email. Offensive material (sexual comments or images, racial slurs, gender-specific comments) can be equally troublesome.
- Viruses – It is widely known that email is used to spread viruses. The effect of a virus passed via email can range from simple annoyance to serious destruction.

■ **E-mail Security Tips**

- 1 Minimize the use of attachments.
- 2 Questions unsolicited documents.
- 3 Never respond to spam email.
- 4 Never respond to spam email instructions to reply with the word remove.
- 5 Never sign up with sites that promise to remove your name from spam lists.
- 6 Do not include confidential information in email.
- 7 Do not include offensive materials in email.
- 8 Executable programs (.exe) received via email should be handled with caution. Do not run

the program until you have verified where it comes from.

- 9 Disable macros in your machine.
- 10 Make sure that file extensions are viewable. E-mails with attachments of extensions .exe, .vbs, or .shs should not be opened.
- 11 Notify the person you received an infected email from.

3.5. Phishing

Phishing refers to the sending of emails with spoofed addresses, i.e pretending to be from a well-known source organisation asking to confirm personal information on the Internet in an attempt to trick people into disclosing confidential information at a bogus (spoofed) website operated by fraudsters.

Phishers are usually after your personal information such as Password or PIN, Credit Card Number, Bank Account number and Social Security Number. They even fake the URL that appears in the address field at the top of the browser window and the padlock that appears in the lower right corner.

You are usually contacted through emails asking you to “update” or “verify” your

customer account information by clicking on a link from the email which takes you to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes. Financial institutions, such as banks and auctions sites are particularly vulnerable to these types of activity.

It is worth noting that even if you do not provide the information that is being requested, simply clicking on the link in the e-mail could subject you to background installations of Keylogging software or viruses.

■ *Tips To Prevent Phishing*

- 1 Do not respond to or click on any links within an email without first verifying its authenticity.
- 2 Contact the organisation it purports to come from to ascertain its authenticity.
- 3 Install a firewall, anti-virus and anti-spyware software.

3.6. Viruses and Other Malwares

Malware is a generic term used to describe malicious software such as: viruses, trojan horses, malicious active content, etc.

Malware exist under different forms. Some of the most common are listed below:-

1. Viruses

A computer virus is a program that has ability to replicate like biological viruses, computers viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of executable file and are spread as files that are copied and sent from individual to individual. Some viruses are intentionally destructive. E.g. Love Bug Virus.

2. Armored virus

This virus uses different methods to make tracing, reassembling and reverse engineering of its code more difficult. E.g. Whale virus.

3. Master boot sector virus

Master boot viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disk. The virus stays in memory, waiting for the DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses.



4. Resident virus

A resident virus loads into memory and remains inactive until a trigger event. When the event occurs the virus activates, either infecting a file or a disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

5. Self-garbling virus

A self-garbling virus attempts to hide from anti-virus software from garbling its own code. When these virus spread, they change the way their code is encoded so anti-virus software cannot find them.

6. Logic bomb or time bomb

A logic bomb is a type of virus that executes itself under specific conditions. Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, at a specific time or date. E.g. 'Time bomb' in "Microsoft's Visual Studio.Net Beta 2" causes the product to expire July 31, 2001.

7. Malicious code

A piece of code designed to damage the system or the data it contains, or to prevent the system from being used in its normal manner.

8. Worm

A computer worm is a self-replicating computer program, similar to a computer virus. Unlike viruses, however, worms self-propagate and so do not require other programs or documents to spread. Worms typically spread through email or other file transmission capabilities found on networked computers. E.g. Nachi (alias Welch, Welchia or MSblast.D).

9. Spyware

A program which is either installed on your computer while surfing the Internet or when you install free software downloaded on the Internet. It records and sends your personal information – includes marketing info (visited sites, list of your software, your interests, etc...) – without your knowledge to a remote recipient.

10. Keylogger or Keylogging Software

This is another method used to capture your personal information. The software can be installed in the background without you being aware, when you click on a link to a website or open an attachment in an e-mail. Once installed, it records everything you type including user ids, passwords and personal information such as Credit Card Numbers.

The information is then sent back to the site from where the software was downloaded. This is a very real risk when using public or shared computers such as those in Internet Cafés.

11. Trojan Horse

A non-replicating malicious program designed to appear harmless or even useful to the user, but, when executed, harms the user's system. Some software bundles containing malicious forms of spyware or other potentially unwanted software are considered to be Trojans, e.g. Trojan.Downloader.Inor

■ *Tips To Prevent Malware*

- 1 Install a Firewall – A firewall is a hardware and/or software that is designed to be your first line of defence against unauthorized users accessing your system.
- 2 Install an Anti-virus and Anti-spyware software – AntiVirus software is designed in such a way they detect and remove harmful viruses before they can do any harm to your data and the computer.
- 3 Updated & Patched OS – Install periodic and critical updates to protect your PC against the latest

known vulnerabilities, which could be exploited by viruses and other malwares.

- 4 Perform regular backup of your data and programs so that you can restore them in case of theft or if your computer crashes.
- 5 Secure your Browser (Internet Explorer) – There are many disadvantages to using Internet Explorer as your primary web browser, mostly security related (Active X and Active Scripting makes it relatively easy to install Malware on your computer without you knowing about it and the numerous issues/vulnerabilities that existed and still exist) and incomplete and incorrectly implemented core standards used for web authoring. Alternate browsers like Mozilla, Firefox and Opera are a lot more secure and are much more resistant to Malware installation attempts.
- 6 Secure your Email Client (Outlook Express) – Securing your email client is just one of the necessary steps to secure your system against Malware. In its default installation, Outlook Express does not offer adequate protection against viruses and other malwares.



- 7 Do not install peer to peer (P2P) software - P2P software allows users to locate, share and distribute information among workstations without connecting to a Central Server. Some common P2P softwares are Napster, Kazaa, Freenet and Gnutella. P2P software poses the following threats: bandwidth consumption, infringing of copyright, undermining of security policies, Trojan horse and virus distribution and disclosure of IP addresses.
- 8 Activate Real-time Spyware protection – Almost all Anti-Spyware programs offer real-time protection. With real-time protection enabled many known Malware programs can be blocked and eliminated before they are installed, helping to stop potential security leaks before a program can run.
- 9 Use ActiveX blocking software – SpywareBlaster is a prevention software that protects against ActiveX based Malware installation. It also protects against known tracking cookies being installed in Internet Explorer, Mozilla Firefox and adds thousands of known Malware installing sites to the restricted sites zone of Internet Explorer.
- 10 Use Malware blocker (Internet Explorer) - It uses a block list in the form of a Windows Registry file to add thousands of known unwanted sites to Internet Explorer's Restricted Sites security zone. This ensures the Websites on the block list are blocked from running ActiveX controls, Java applets, Active scripts or even set cookies or use pop-ups when you surf the net.
- 11 Use a HOSTS file – A custom made HOSTS file containing thousands of dubious URLs can be used to block all kinds of ads, Web bugs, cookies,etc., by stopping your computer from communicating with the ad servers. This way you may only block sites that serve unwanted content or any other site that you choose to block.

4. Guidelines for Securing Desktops

Security of a desktop workstation is ultimately the responsibility of the users. Users at work usually requires that protected information resources be accessed, manipulated, modified and transmitted across networks.

If users do not understand their security responsibilities and the organisation's expectations, then the technological measures to enforce security may be ineffective. Below are some general guidelines for users to implement in order to improve the security at the level of their desktops.

◆ Step 1: Activate a Password Protected Screensaver

Using a screensaver that requires a password can prevent someone from quickly accessing your computer and its resources. A person that has access to your computer can assume your identity: sending malicious emails from your account or worse, collect additional information that may be used to access more sensitive accounts or files.

◆ Step 2: Use Strong Passwords for All of Your Accounts

Hackers use special programs that attempt to find your password by running through all

words in a dictionary (programs have dictionaries in most languages), every common proper name, every sequence of 1-12 numbers, and various combinations of these. Once they have your password, they control your computer.

Your user ID and password identify you (authenticate who you are) and your access rights (authorization-what you have permission to see and do) to data on a server. If someone stole your password, that person could pretend to be you (identity theft) while doing unauthorized and/or illegal activities online.

Guidelines on what to avoid:

- 1 Avoid using a word contained in any dictionary, spelling list, or other word list in any language.
- 2 Avoid using personal information. For example: your name, your user ID, the name of a spouse, child, friend, or pet.
- 3 Avoid using personal information that may be easily obtained, such as license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.



- 4 Avoid using simple transformations of a word such as reversing the spelling, changing uppercase to lower-case or vice versa, or using all capitalization.
- 5 Avoid using a password shorter than six characters. This increases the number of possible password combinations a hacker would have to guess.
- 6 Watch out for anyone trying to shoulder surf e.g when someone watches you type in your password so that they can use it later.
- 7 Never type a password, such as a bank account pin, into a non-encrypted page.
- 8 Do not install peer to peer (P2P) or unlicensed software on your PC.

◆ **Step 3: Automatically Receive Critical Updates**

Hackers can get into your computer through unpatched holes and take control of it, using it as a launch pad for world wide spam, denial of service attacks, and the distribution of illegal material, some of which could get you in trouble if it is found on your machine. They can also use your computer to bring down the computer network, interfering with everyone's ability to do their job.

◆ **Step 4: Verify Antivirus Software is Configured Properly**

If your anti-virus protection is not up to date, new viruses can infect your computer. These viruses can wipe out your hard drive. They can also spread on the network, infecting other computers and degrading network performance.

◆ **Step 5: Use Anti-Spyware Software**

This software protects you from viruses and worms that are downloaded without your knowledge from web sites you visit. Sometimes these bad web sites install keystroke-logging programs on computers. Such programs capture your keystrokes; they are looking for passwords you enter in order to access sensitive data on other systems. They then steal your password and use it to get data out of these other systems (e.g. your bank account data.)

◆ **Step 6: Unique Passwords for all User Accounts**

When users share an ID and password, it is impossible to trace which user did what to cause the computer to fail. If your office setup requires that two or more people share the same computer, each should be



assigned a unique user ID and instructed to create a hard to guess password. Only one person should have the administrator password. This is the password that allows changes to be made in the operating system. If someone with ill intent getshold of this password, they control your computer and all the files on it.

◆ Step 7: Back Up Files Regularly

Despite all of your precautions, your files and even your entire hard drive can get corrupted. Protect yourself by backing up! Doing weekly back-ups requires a little planning and set-up. First, you should keep all of your documents in one folder on your main hard drive. Second, you should acquire either a USB flash drive or have a computer equipped with a DVD/CD burner.

If you have these things set up, you can then just copy your documents folder to either your USB drive or a DVD (USB drives are widely available in capacities up to 2GB, and DVDs can hold about 4+GB.) Don't forget that any device containing sensitive data should be password-protected, encrypted, and physically secure. Small portable devices are easily lost.

◆ Step 8: Never Open Suspicious E-mails or Attachments

You may recognize the name of the person who sent you an e-mail, but that is not

enough to protect you. There are many ways a hacker can seize control of someone's e-mail address and then send you malicious e-mail that will cause you problems.

Remember, e-mail is still the number one favourite method for distributing malicious code to your computer. Malicious code can come in the form of a virus, worm, trojan, spam, spyware, or phishing e-mail. If in doubt about an email, delete it and notify the sender.

◆ Step 9: Limit the use of Internet Explorer

Internet Explorer is deeply integrated with the Windows Operating System. While some web applications use this integration to support a positive computer experience others take advantage of it to install unwanted programs in your computer. Netscape and Firefox are web browser programs, not deeply integrated with Windows, so there is very little opportunity to go deeper into the computer from the outside. This feature keeps you safer on unknown websites.

Download and install an alternative browser such as Netscape or Firefox. Use the alternative browser to surf the Internet, especially to sites you are not familiar with or do not trust. Limit the use of Internet Explorer to websites that you know you can trust or specifically request its use.



National Computer Board

7th Floor, Stratton Court, La Poudrière Street, Fort-Louis

Tel: 210 5530 - Fax : 212 4340

Email: contact@ncb.rn

Website: www.ncb.rn