

INFOCOMM SECURITY



...is
incomplete
without
"U"



BE AWARE, RESPONSIBLE & SECURE!

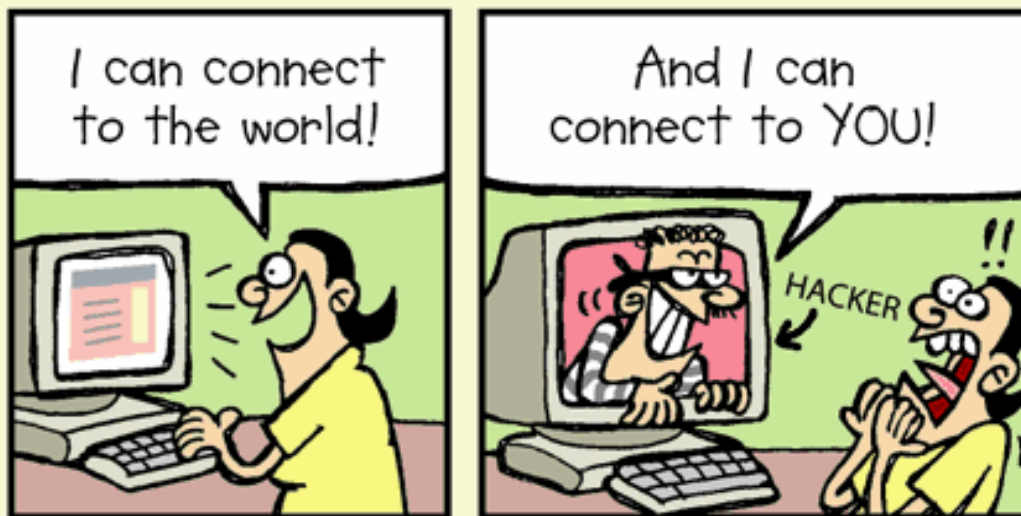


This publication is produced by the Infocomm Development Authority of Singapore (IDA) to promote security awareness amongst computer and Internet users.

IDA shall not be liable for any inaccuracy, error or omission in this publication or for any loss of income, loss of profit or damages, direct or indirect; arising or resulting from the contents of this publication or the use therefore for any purpose whatsoever.

Introduction

Information and communications (infocomm, in short) technologies have made our lives more enriching and convenient. The Internet provides us with online access to a wealth of information and services from all over the world.



However, there are potential security risks on the Internet that you should be aware of. Viruses and hackers may attack your computer and steal your personal information or use your computer to attack other computers on the Internet.

The best protection against viruses and hackers is your personal commitment to infocomm security. You should take the necessary precautions to protect your information and computer. We will like to share with you the good practices that you can take to protect your information and computer.

VIRUS ATTACK!

My computer just got infected by a virus! How is that possible when there is an anti-virus program in it all along?!?

Let me check...



Your anti-virus program was last updated 10 years ago!



Use an anti-virus software

- **Install an anti-virus software for your computer.**
- **Enable your anti-virus protection at all times.**
- **Keep your anti-virus software updated with the latest virus signature file.**
- **Perform a scan of your computer after each update of your anti-virus software.**

A virus is a program that can perform malicious activities on your computer, such as copying or deleting your files. Viruses can be transmitted via various ways such as emails, file downloads and diskettes.

An anti-virus software helps to detect and remove viruses and other malicious programs such as worms and trojans.

As new viruses are being introduced on the Internet almost every day, you should ensure that your anti-virus software is always updated with the latest virus signature file available from the software company. You can use the "live update" feature in your anti-virus software to automatically check for updates to the virus signature file.

FIRE POWER

I'd like to equip myself with fireballs to fight against any intruder to my computer.



It's called a 'fireWALL'.



Oh.

Use a personal firewall

- **Install a personal firewall for your computer.**
- **Configure your personal firewall to block other computers on the Internet from accessing your computer.**
- **Configure your personal firewall to block information in your computer from being sent out to the Internet without your approval.**
- **Perform a scan on your computer to check for security vulnerabilities.**

A personal firewall is a software or hardware designed to block hackers from accessing your computer.

A firewall monitors the communications between your computer and the network, and blocks unauthorised connections to your computer. A firewall can also block programs residing in your computer from sending out information to the Internet without your approval.

You can run scanning programs on your computer to check for security vulnerabilities that can be exploited by hackers.

PATCH IT UP

This is great - I need not worry about running out of storage any more: my harddisk space somehow gets bigger and bigger on its own!



That's because your operating system has a flaw that allows an attacker to hack into your computer and delete files!



Install software patches

- **Keep your computer software updated with the latest software patches.**
- **Use the automatic update or notification feature from the software company to keep abreast of software patches.**

When a vulnerability is discovered in a software, the software company will usually publish a software patch (update) to fix the vulnerability.

You should update your computer software, especially the operating system, Internet browser and email software, with the software patches once they are available.

Some software will automatically check for available updates, and many software companies offer automatic notification of updates via a mailing list. You can also check the software company's web site for the patches to your software.

POACHED!

Boss! Boss! I have come up with this new, innovative idea for the company!



No you didn't - that was your colleague's concept!

Stole his idea via file sharing over the network, then rushed it to the boss!



Disable file sharing

- **Disable file sharing if you do not need to share files on your computer with other network users.**
- **If you need to share files, protect the file share with a password.**

File sharing allows another computer user on the network to read, write or delete files on your computer. This ability to share files can allow someone on the Internet to access your files or infect your computer with a virus.

You should disable file sharing if you do not need to share files on your computer with other network users. You can disable the file and print sharing feature under Windows networking control panel if you do not need to share files or printer.

If you really need to share your files, you can protect the file share with a password so that only people who know the password can make use of the file share.

MAIL BOMBS



Do not open suspicious emails

- **Delete the email if the subject title is suspicious.**
- **If you do not know the person sending you the email, be very careful about acting on the email contents and opening any files attached to the email.**
- **Scan all email attachments for viruses before opening them.**
- **Do not open email attachments with the file extensions “.exe” and “.vbs”**

Emails are commonly used to propagate viruses, worms and trojans. You should exercise caution when opening emails and their attachments.

Delete the email if the subject title appears suspicious or strange, even if the email is from someone you know. The person may have unintentionally sent you a virus.

If you do not know the sender of the email, be careful about acting on the email contents. Such emails may be hoaxes or scams.

You should scan all email attachments for viruses before opening them. Do not open email attachments with the file extensions “.exe” and “.vbs” as such file attachments are often used to propagate viruses.

CARE & SHARE

Sayang, as husband and wife, we share everything with each other, right?

Certainly, dear.



Except my passwords.



Safeguard your password

- **Choose a password that is difficult for others to guess.**
- **Your password should comprise of at least 8 alphanumeric characters.**
- **Do not choose a dictionary word as your password.**
- **Do not reveal your password to anyone.**
- **Do not store your password on your computer.**

A password is commonly used by a computer system to verify your identity to determine if it should grant you access to the system. Someone can masquerade as you or access your personal information if the person knows your password.

You should choose a strong password that is easy for you to remember but difficult for others to guess. You can use a passphrase to help you choose a strong password. For example, the password "mla3ca7d" is derived from the first characters of the phrase "Mary looks after 3 cats and 7 dogs".

Beware of hackers who may try to trick you to reveal your password over the phone or email. Do not disclose your password to anyone. You should not store your password on your computer as your computer may be accessed by others.

CLONING

The virus has wiped out everything on your hard disk. Do you keep duplicates of your files?

Of course, I always backup my data.

That's very wise. Where are they?

In another folder... in that same hard disk!



Backup your important data

- **Keep a backup copy of your data on a separate media such as diskette or CD-ROM disk.**
- **Backup your data regularly.**
- **Do not backup your data on the same hard disk.**

If you lose your data on your computer, e.g. due to a hard disk failure or virus infection, you may not be able to recover the data unless you have a backup copy. You should backup your data on a separate media such as diskette or CD-ROM disk. Do not backup your data on the same hard disk as you may lose your backup data as well.

You should backup your data regularly (e.g. weekly), especially if there are frequent updates to your data. You can use backup software to help you schedule and automate the backup process.


JUNK MAIL

No more spam emails for me from now on, 'cos I have replied to every one of them, telling the senders that I want out!

That's even worse: now that you have made it known that your account is in use...

...they will send you even more!

**You have
168987 messages**



Fight spams

- **Be careful whom you give your email address to.**
- **Avoid publishing your email address on the Internet.**
- **Establish multiple email addresses for different purposes.**
- **Do not respond to a spam.**
- **Use anti-spam software or the spam filtering service of your email service provider.**

Email spam refers to unsolicited emails, often sent to large group of recipients.

Avoid providing your email address unless you are confident that it would not be used for spamming activities. Otherwise, having multiple e-mail addresses for different purposes allows you to use a “disposable” email address when you are at an unfamiliar web site or are posting to a newsgroup.

Do not reply to a spam, including asking the spammer to remove you from its mailing list. Your reply tells the spammer that your email address is active, and you may receive even more spam.

You can use an anti-spam software or the spam filtering service of your email service provider to help filter spam.

TOP SECRET


I disclosed my credit card details to a site; but it abused the info for unauthorised purchases!


You should report it to the police.


I can't...

...it's an illegal pay-per-view porn site!

Safe online shopping

- **Transact with e-merchants that you trust or are endorsed by accreditation bodies such as TrustSg.**
- **Ensure that your Internet browser displays both “https://...” and the unbroken padlock  when you transmit confidential data over the Internet.**
- **Clear the “cache” of your Internet browser to delete any confidential data stored on your computer after an online transaction.**

The TrustSg seal  is accredited to e-merchants that adopt sound e-business practices and value the importance of data protection and online security. These e-merchants undertake to adhere to the approved code of conduct for doing business over the Internet. You can refer to <http://www.trustsg.org.sg/> for more information on TrustSg.

When your Internet browser displays “https://...” and the unbroken padlock , it indicates that the information (e.g. your credit card details) that you are transmitting is encrypted. This protects your information from being read by unauthorised users on the Internet.

Clearing the “cache” of your Internet browser deletes any confidential data that may be stored on your computer after an online transaction. You can refer to the Help feature or the user documentation of your Internet browser on the steps to clear the “cache”.

NASTY INVADER

Oh no! My computer has been infected by a virus!
I must call for help immediately!

That's very wise of him
to call the Singapore
Computer Emergency
Response Team...

Hello, is this the Exorcist?



Take actions immediately if your computer is hacked or infected

- **Disconnect your computer from the Internet.**
- **Perform a virus scan of your entire computer.**
- **Contact SingCERT (Singapore Computer Emergency Response Team) to report the incident.**

If your computer behaves abnormally, such as if your hard disk starts up by itself when nothing is going on, or if your computer suddenly connects to the Internet, you should perform a thorough check of your computer to determine if it has been hacked or infected by a virus.

If your computer has been hacked or infected, you can contact SingCERT to report the incident and for further advice on what to do.

SingCERT's contact details:

Hotline: **(65) 6211 0911**

Email: **cert@singcert.org.sg**

Web site: **www.singcert.org.sg**

Operating Hours:

Mon-Fri 8:30am-6:00pm

Sat 8:30am-1:00pm

INFOCOMM SECURITY IS INCOMPLETE WITHOUT "U". BE AWARE, RESPONSIBLE & SECURE!

- Be aware of the potential security risks on the Internet.
- Be responsible and take the necessary precautions to protect your information and computer.
- Be a secure cyber citizen today!



iDA
SINGAPORE

Website: <http://www.ida.gov.sg>
Email: info@ida.gov.sg