

Infocomm
Security is
incomplete
without

U

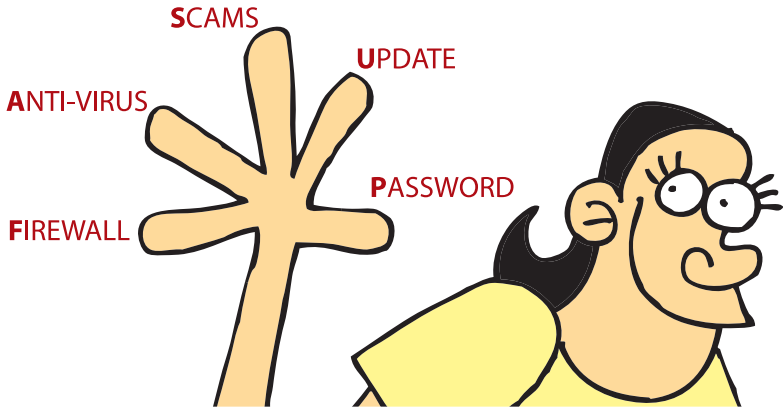


Be aware,
responsible
&
secure!



Smack that

What you can do with these
five online security measures...



FASTEN UP!

The world is highly connected through the widespread use of infocomm technology. To fully enjoy the experience and convenience of Internet, you should be aware of the potential security threats that might affect you. Be a responsible surfer and protect yourself when you surf the Internet.

FASTEN UP! is an acronym for a set of essential security practices. Follow them and protect yourself from hackers and viruses that can enter your computer to steal information or use it to attack other computers.

Firewall	Install a personal firewall and use it correctly
Anti-virus	Install anti-virus software and update its signature regularly
Scams & Spam	Beware of emails and websites with great offers that sound too good to be true
T E N	
Update	Update operating systems and application software regularly
Password	Create strong passwords and keep them safe

Remember to FASTEN UP! before you surf the Internet. More details regarding these tips can be found at **www.singcert.org.sg/awareness**

Get burnt

You lost your mobile phone? Does that mean all your contacts are gone too?

Nah, luckily I had the foresight of making a copy of my contacts in my computer. Let me show you.



You should have had the foresight of installing a firewall too - a hacker got to your computer and erased all your data...






Use A Personal Firewall

A personal firewall is a piece of software designed to block hackers from accessing your computer.

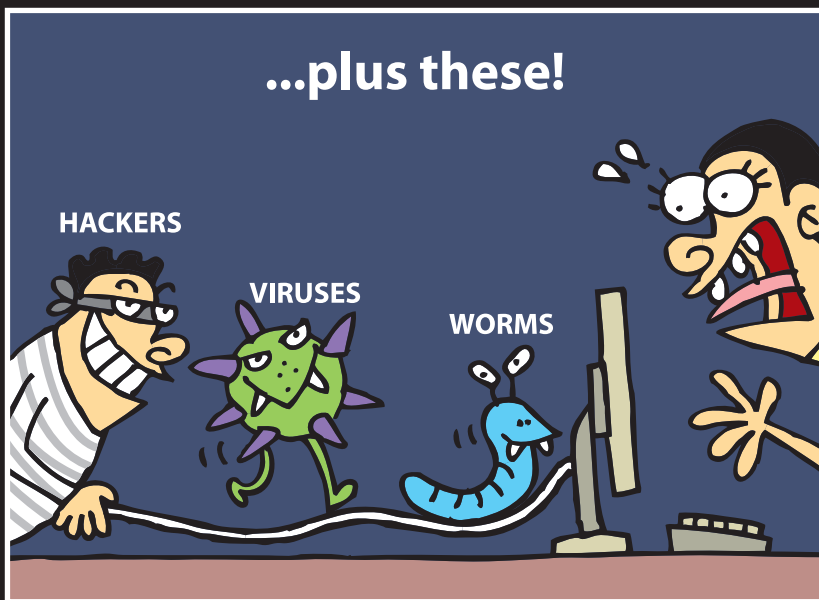
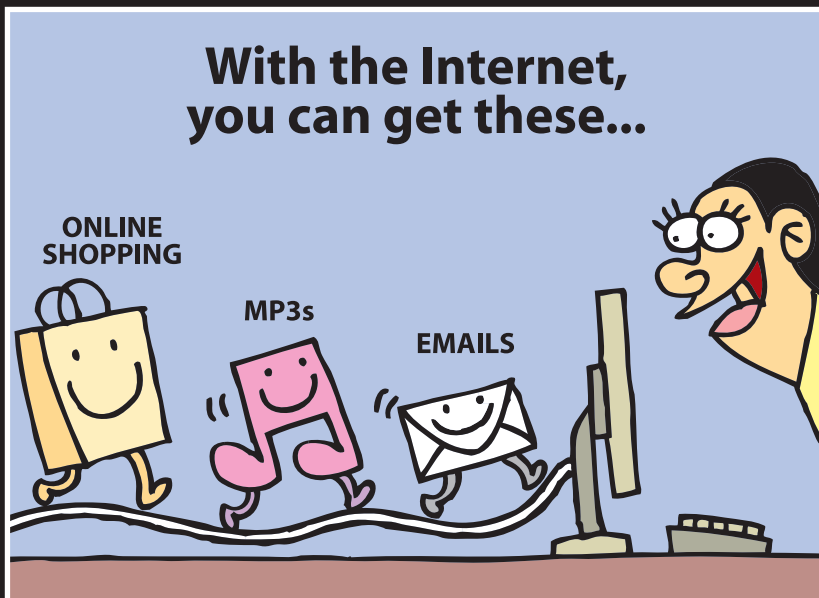
A firewall monitors the communications between your computer and the network, and allows you to block unauthorised connections to your computer.

A firewall can also block programs in your computer from sending out information to the Internet without your approval.

Security Tips

-  **Install a personal firewall on 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.**

You have company



Use An Anti-virus Software

An anti-virus software helps to detect and remove malicious software (e.g. virus, worm and Trojan) that can perform harmful activities such as copying and deleting your files without your permission.

An anti-virus software uses a virus signature file which contains the identities of all known viruses.

A virus-infected file is detected if it matches one of the patterns in the virus signature file.

The virus signature file has to be constantly updated in order to detect new viruses that have been discovered. Zero-day attacks are attacks by new viruses where their signatures have yet to be created to detect them.

Security Tips

- 👉 **Install an anti-virus software on your computer.**
- 👉 **Enable your anti-virus protection at all times.**
- 👉 **Use the auto-update feature to update your anti-virus software with the latest virus signature file.**
- 👉 **Perform a scan of your computer after each update of your anti-virus software.**

clickfest

I heard you have installed a freeware.
Did you read the license agreement
before doing so? Some freeware come with
spyware components...



Now you tell me! I have been closing
pop-up windows for the past three hours...
and there are many more still!!!



Use An Anti-spyware Software

Spyware is any software that is able to secretly gather information about users or organisations without their knowledge.

Typically, spywares will automatically install themselves when you visit websites run by hackers or click on the "OK" button from unsolicited pop-ups.

Make an informed decision when installing freeware or shareware, as some of their license agreements support auto-installation of spyware components.

An anti-spyware software helps to detect and remove spyware.

Security Tips

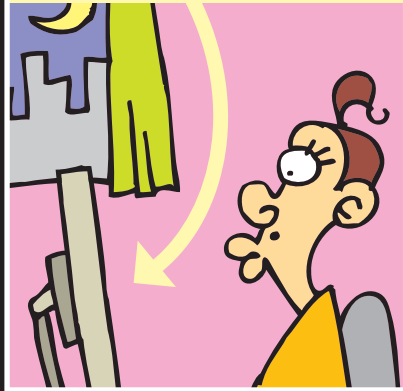
- **Install and update anti-spyware software regularly.**
- **Enable your anti-spyware protection at all times.**
- **Keep your anti-spyware software updated with the latest spyware signature file.**
- **When closing pop-ups, use < Alt > F4 > instead of clicking on the "X", "OK" or "Cancel" buttons.**
- **Read the license agreement or Terms & Conditions before installing freewares or sharewares.**
- **Do not allow the download and installation of dynamic or interactive content (Active Content) from unknown websites.**

♥ Irresistible

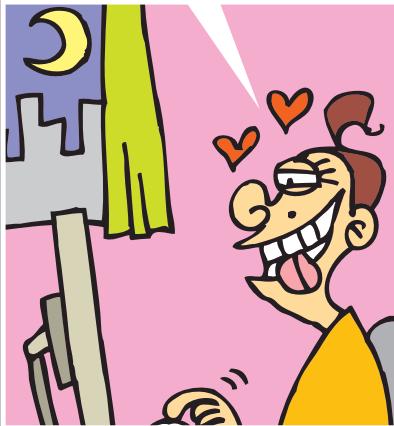
Ah, finally finished
my project!
Time to take a break.



♪ PING!
You have mail.
Attachment:
Sexy_Gigolo.exe



Ooo, just what
I need to unwind.
Must open...



Virus activated.
Erasing
entire hard disk.
Now.



Do Not Open Suspicious Emails

Emails are commonly used to propagate malicious software such as viruses and trojans. Your computer can be infected when you open infected email attachments or visit hackers' websites after clicking on links provided in suspicious emails.

A common sign of a suspicious email is a strange or enticing subject title such as "You have won a million dollars".

Unsolicited emails that appear to contain information about recent major events (e.g. earthquakes, terrorist attacks) may be used to trick you into clicking on the links provided or opening its attachment.

Email attachments that look normal may contain viruses. Common file types such as .exe, .vbs, .pif and .scr are often used to transmit viruses.

Security Tips

- **Delete the email if the subject title is suspicious.**
- **If you do not know the sender of the email, be careful about acting on the email contents and opening any files attached to the email.**
- **Scan all email attachments for viruses before opening them.**

\$\$\$ A windfall

I just received an email from my bank, asking for my credit card number.

Banks don't do that.
You didn't respond, did you?



Of course I did. How could I resist when it also offered to transfer US\$10,000 to my account via its branch in Nigeria?



Beware Of Phishing

Phishing is a common form of scam on the Internet.

Phishing attacks use fake emails and “look-alike” websites to deceive respondents into entering personal information. This information may include financial data such as credit card numbers, account user names and passwords.

Usually, the bogus e-mail looks as if it comes from a bank or payment service, requesting confidential account information for verification. Often, they may also threaten to discontinue service if the information is not provided.

Security Tips

👉 **Do not click on links provided in suspicious e-mails to access the website.**

👉 **Do not provide personal information to requests received via email.**

👉 **Look for tell-tale signs of a bogus website:**

- Suspicious website address.
- The address of the webpage where you submit information does not start with “https://” and the lock symbol is missing from the status bar.
- Asking for more information than required (e.g. Credit Card PIN number).
- Obvious spelling and grammatical errors.



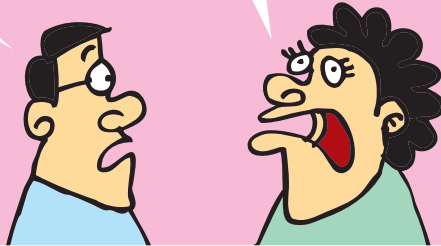


Missed opportunity

Why so glum?

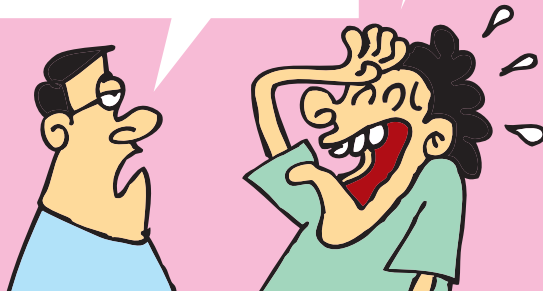
I found my dream job on the Internet and the company sent me an email for an interview.

And?



And I missed it because it was buried among the 2,000 spam messages I receive everyday!

You seriously need a spam control software...



Fight Spam





Spam refers to unsolicited commercial electronic messages, often sent in bulk to a large group of recipients. Electronic messages include both messages sent to mobile phone numbers and emails.

Spam may try to trick you into verifying that your email address is in use by asking you to unsubscribe from their mailing list.

A spam control software or the spam filtering service provided by your Internet Service Provider or email service provider can help filter spam.

Visit www.spamcontrol.org.sg for more information

Security Tips

-  **Be careful who you give your email address or mobile phone number to.**
-  **Establish multiple email addresses for different purposes.**
-  **Read the privacy policy that accompanies online registration forms and surveys to check if your contact information will be shared with others.**
-  **Use spam control software or spam filtering service provided by your email service provider.**

power down

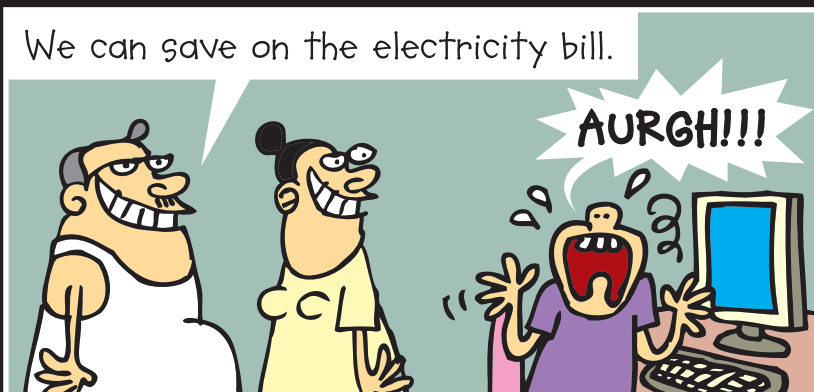
There are pros and cons when our son forgot to patch his computer's operating system.



The bad: a hacker made his computer crash and rendered it useless.



We can save on the electricity bill.



Install Software Updates

Software companies usually issue software patches (updates) to fix problems found in their software.

Software you recently purchased may also contain problems as the software could have been programmed some time ago.

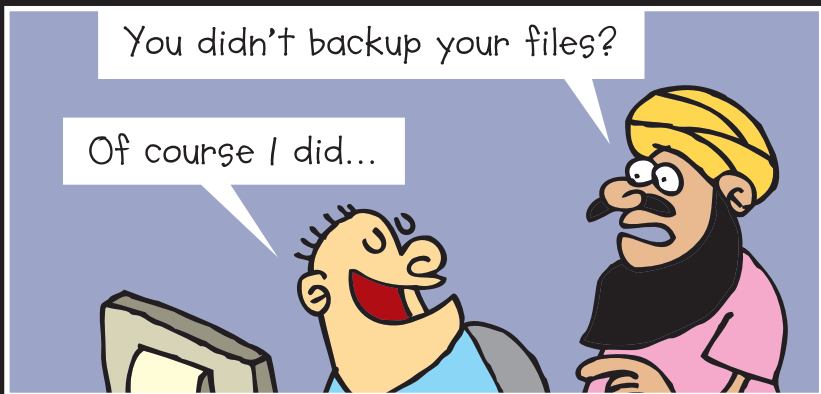
The automatic update feature that comes with your software allows you to install software patches as soon as the patches become available.

Software companies may also release information regarding the latest patches on their websites.

Security Tips

- **Keep your computer software updated with the latest software patches.**
- **Check and install available patches when you first install your newly purchased software.**
- **Use the automatic update or notification feature from the software company to keep abreast of software patches.**

Saved



Backup Important Data

Backing up your data allows you to recover the information if you lose your data on your computer e.g. due to a hard disk failure or virus infection.

Store a copy of your important data in a storage device other than your hard disk e.g. USB thumb drive, external hard disk or CD/DVD-RW disk.

Frequently updated information should be backed up regularly (e.g. weekly) to ensure that the latest information is saved.

Backup software can help you to automate the backup process.

Security Tips

- **Keep a backup copy of your data on a separate media such as USB thumb drive, external hard disk or CD/DVD-RW disk.**
- **Backup your data regularly.**



Ghost writer

You don't safeguard your email password?
That's risky!



Why should I keep it a secret? I don't send
or receive sensitive information.



Er, someone just used your account
and sent everyone an email entitled:
"OUR BOSS IS A SPINELESS SCUM"...



Safeguard Your Password

A password is commonly used by a computer system to verify your identity. Someone with your password can masquerade as you to access your personal information.

A password should be easy for you to remember but difficult for others to guess.

Use passphrases as a method to create strong passwords. For example, the password "Mla3ca7d" can be derived from the first characters of the phrase "Mary looks after 3 cats and 7 dogs".

By using the "log out" feature and clearing the Internet cache after you log out, you can prevent others from accessing your personal information.

Security Tips

- **Create a password that is difficult for others to guess.**
- **Your password should comprise at least 8 alphanumeric characters with a mix of upper and lower case letters.**
- **Do not choose a dictionary word as your password.**
- **Do not reveal your password to anyone.**
- **Do not store your passwords on your computer or write them down.**
- **Do not allow the browser to save or remember your password, especially if you are using a shared computer.**
- **Log out and clear the Internet cache after all transactions.**

((P)) Easy money

“Money doesn’t grow on trees” – that is so very true. But when some people do not use encryption when transmitting their bank details wirelessly...



...“Money DOES grow in the air”!



Surf Safely As You Go Wireless

The same wireless network that provides you convenient access to the Internet also makes your computer and information vulnerable to people with malicious intent.

A danger of using wireless is the possibility of losing personal and sensitive data to someone who is spying on the wireless network.

People with malicious intent may also set up an unauthorised wireless network to the Internet. Unsuspecting wireless users may connect to the unauthorised network and send their information to these un-trusted parties.

Security Tips

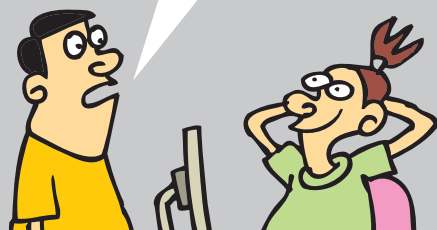
- **Practise the FASTEN UP! tips to secure your mobile devices (e.g. laptops, mobile phones and PDAs) before you surf wirelessly.**
- **Only connect to authorised wireless networks and disable the auto-connect feature in your wireless setting.**
- **Use passwords and encryption to protect your information before sending them over the wireless network.**

poison letter

So someone can piggyback on my unsecured wireless network – what's the big deal?



It is if that someone uses your account for malicious activities, such as sending emails...



...like this!

Please come to the station and assist us in investigating an email bomb threat.



Secure Your Wireless Network

An unsecured wireless network may be used for unauthorised activities such as hacking or stealing personal information.

The Access Point (AP) is a device which your mobile devices and desktop computers connect to via the wireless network. The AP can come in many forms; one of which is your wireless router at home.

Security controls should be put in place to “lock” the AP to minimise unauthorised access to your wireless network.

The procedures for securing your AP can be found in the manual that comes with your AP.

Security Tips

- **Change the default name or Service Set Identifier (SSID) of your wireless network and disable the broadcasting of the SSID.**
- **Change the default administrator username & password on your AP.**
- **Enable network encryption such as WPA or WEP.**
- **Allow only authorised users to access your wireless network.**
- **Turn off the AP when not in use.**
- **Turn off Remote Administration of your AP.**



Heart-stopper

Please send an ambulance over...
my husband's
computer
has been hacked.



Er, ma'am, you should
call the Singapore
Computer Emergency
Response Team
regarding the computer.



That I did. I'm now calling regarding
my husband: he has just lost a
20-page work report due tomorrow morning!



Report Virus Infections & Hacking Incidents

Your computer may behave abnormally when it has been infected by malicious software.

Computers that suddenly run at an exceptionally slow speed and unexpected connections by your computer to the Internet are some examples of abnormal behaviour.

Perform a thorough check of your computer when you suspect it has been infected.

If your computer has been hacked or infected, you should 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**

Website: **www.singcert.org.sg**

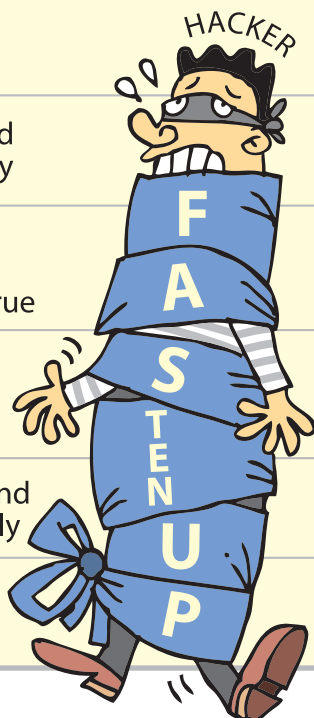
Operating Hours:

Mon – Thurs 8:30am – 6:00pm

Fri 8.30am – 5:30pm

FASTEN UP!

Firewall	Install a personal firewall and use it correctly
Anti-virus	Install anti-virus software and update its signature regularly
Scams & Spam	Beware of emails and websites with great offers that sound too good to be true
T E N	
Update	Update operating systems and application software regularly
Password	Create strong passwords and keep them safe



BE AWARE, RESPONSIBLE AND SECURE!



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

COPYRIGHT © March 2007 – Infocomm Development Authority of Singapore.
All rights reserved. Reproduction without permission is prohibited.