COMPUTER SECURITY

Although you may not consider your communications as top secret, you probably do not want strangers reading your email, using your computer to attack other systems, sending fake email from your computer, or examining personal information stored in your computer.

Hackers want to gain control of your computer so that they can use it together with other computers under their control to launch attacks on other computer systems. Having control of your computer will enable them to hide their true location as they launch the attacks, often against high-profile computer systems such as government or financial systems.

GUIDELINES TO SECURING YOUR COMPUTER

Delete unknown e-mails. Never download or open suspicious attachments.
Turn on or install a firewall to prevent hackers from gaining access to your computer.
Avoid disreputable websites. You are most likely going to get some virus or spyware if you browse disreputable website such as porn sites or your computer.
Minimize the storage on your computer. Don't keep all sensitive information on your mobile devices unless they are properly protected.
Don't click on unknown or unfamiliar advertisements.
Keep your computer updated. Run antivirus scans regularly and ensure all software and security updates are properly installed.
Beware of external devices such as USB flash drives or external storage devices as they may release a computer virus to your system.
Secure your wireless network from being "piggybacked" by hackers.
Be alert to your surrounding before leaving your computer unattended.
Use a memorable but strong password for all your accounts.
Shut down or lock your computer when it's not in use. Ensure that a secure password is required to start-up the system.
Avoid peer-2-peer file sharing software.

SIGNS OF AN INFECTED COMPUTER

Pop-ups and messages that indicate your computer is infected with a virus and needs protection. Don't click on the pop-up alerts or the cross to close the alert as this may result in more pop-ups. Instead, hit CONTROL + ALT + DELETE buttons to view a list of programs currently running and delete the alert from the list.

Your computer or internet browser is running extremely slow, or it is unable to connect to the Internet.

Once connected to the Internet, all types of windows would open on their own or the browser displays sites that have not been permitted or requested.

Missing files and disabled computer security systems.

The computer is speaking a strange language. The language of certain applications changes, the screen appears back-to-front, or strange insects start 'eating' the desktop.

Applications on the desktop or start menu don't launch or a different program might launch instead.

Running out of hard drive space.

Browser homepage changed, unwanted toolbars installed, and unrequested websites open up.

The computer starts acting on its own or shuts down without reasons.

The computer program or system crashes constantly, or the Blue Screen of Death appears regularly.

REDUCING CYBER RISKS FOR ORGANIZATIONS

It is not easy to be one step ahead of the attackers since cyber threats increase in their complexity, sophistication, and variation by the minute. Organizations may have access to best-of-class technical tools, highly skilled IT professionals, and effective monitoring of cyber-attacks. However, the human factor remains the weakest link in the chain. It is best for businesses to build up their capabilities in prevention, detection and responses to computer security.

Organizations can reduce the risks to their business by building up capabilities in prevention, detection, and response.

Keep all software up-to-date
Most organisations use legacy or older version software that has critical vulnerabilities which attackers can use to access into the systems.

Develop incident response strategies
Having incident response strategies in place would greatly reduce your response time and costs in the long run.

Monitor privileged users
Solutions to control and monitor actions of privileged users should be employed in order to ensure the company is protected from this most trusted, yet most risky group.

Maintain effective security policy
Security policy is the backbone of any organisations' security program that establishes and formalises security procedures in the organisation. Enforcement needs to start with upper management and move downward, ensuring that every employee is aware of the policy.

Raise employees' awareness about cyber security and its policy
Disable access to company data on termination of former employees.

Manage third-party vendors
Manage and establish strong security policies with third-party vendors and subcontractors.

Bring Your Own Device (BYOD)
Most organisations allow their employees to use their personal devices at work and some allow connection to the corporate network. It's important for organisations to cover BYOD in their security policy.