

THE NEED FOR INFORMATION TECHNOLOGY SECURITY

Information Technology has become an indispensable part of modern military operations. Many operations information are stored on computing devices and transmitted to other computing devices through a private network or the public Internet. The following are several reasons for Information Technology security.

Value of data – The data residing on computing devices or transmitting through the network can contain valuable information, for example, a classified operation message, system access identity codes and passwords.

No disruption to operations – Military operations are fast pace and the success of a mission depends on the decisions and actions based on timely and accurate operational information.

Software applications running on computers and networks are often without Information Technology security measures. This happens for several reasons:

Lack of education – Programmers lack knowledge about Information Technology security.

Low priority – Information Technology security only gained visibility in the last few years.

Hence, many software program developers of yesteryears chose to give less importance to Information Technology security even though they know about the issues.

Time and cost – Certain software program developers set aside Information Technology security measures due to constrains in time and cost.

Carelessness – Software programming errors were made during the development process and some of these errors make Information Technology security breaches possible.

Malicious – A number of software programs are intentionally written with codes that breach Information Technology security. These programs may be disguised as free software for download on the Internet.

Practising Information Technology Security

There are many software tools that implement information technology security measures. These software tools are either sold commercially or available as freeware.

Time management is required to implement and follow information technology security measures. You will need to install the appropriate software and perform regular updates.

05/08
/

The information technology security mindset requires vigilant action. Information technology security incidents result from individuals not acting in a cautious manner when handling information technology equipment.

Responsibility

It shall be the responsibility of the chiefs of offices that all computers and computer networks, referring to Local Area Network (LAN), Wide Area Network (WAN) and other wireless networks, are secured physically and electronically from unauthorized access.

Chiefs of offices shall designate a competent MIS Officer to ensure that all computers and computer-related networks are working properly, and ensure that all protective measures commensurate to the sensitivity of the stored data are undertaken to prevent unauthorized access from unscrupulous persons. The MIS Officer shall formulate office SOPs and operating procedures to ensure that all computers and computer-related networks are protected from unauthorized access.

It is also the responsibility of all personnel to ensure that no unauthorized person shall have access to their respective computer workstations. Any breach in access to office/unit computers and computer-related networks shall be reported immediately to the MIS Officer, who will inform the chiefs of offices on the nature of violation.

Computer Security

To keep the computer physically secure, reduce the risk of data loss and corruption of software program.

Physical Security

A computer is a valued item. It could be accessed without authorization for the purpose of obtaining stored data or insertion of malicious software program. The following paragraphs present several tips to ensure the physical security of your computer.

Computers should be kept in a secure location. It could be locked up in a room or watch over by colleagues. Computers should not be left unattended in public places. The same measures are applicable to removable storage media like flash drives and portable hard disks.

Most laptops have a connection point for a security lock and cable. This allows the laptop to be tied down at a location.

Configure computers with a login identity and strong password. Computers should have a password protected screen saver. These measures will reduce the risk of unauthorized access when the owner is away from the computer. *Passwords should be kept confidential and must not be written on a piece of paper and pasted on the computer or the surrounding work area.*

If using a shared computer, separate login accounts should be created. The accounts should be configured to restrict the user from accessing data belonging to other users.

Protecting Data and Software Program

Data and software programs can be corrupted or lost due to accidental action by user, malicious action by unauthorized user or software programs and hardware failures.

Backup of data and software programs should be done on a regular basis. Backup media should be stored at another place for safe keeping. In the event of a corruption or loss, the affected data or software program can be restored from the backups.

Anti-virus software must be installed on the computers. The anti-virus software must be configured to scan the computer for malicious software programs automatically and take immediate action to contain or eradicate any malicious software programs. *Always scan removable media using anti-virus software every time it is plugged into the computer.*

The number of malicious software program grows tremendously with each passing day. It is important to keep your anti-virus software updated with the latest signature. This action will reduce the risk of your anti-virus protected computer being infected by new malicious software programs.

The computer operating system and software programs must be updated regularly to address any newly discovered information technology security vulnerabilities. Unauthorized user or malicious software programs often exploit the computer operating system and software programs to carry out malevolent actions.

Do not install software programs of dubious origins onto computers. Malicious software codes can be embedded in software programs and are often introduced to the computer unknowingly by the owner when installing the software program.

Storage of Electronic/Digital Data:

All electronic and digital data shall be stored in an appropriate storage device such as the computer hard drive and other external storage devices available in the commercial market. However, the appropriate external storage device shall be encrypted using folder encryption software depending on the sensitivity of the stored information.

Storage of External Storage Devices

All digital and electronic storage devices such as diskettes, compact discs (CDs) universal serial bus (USB) mass storage and other storage devices, shall be stored in a secured container as prescribe for storage.

Ensure that no computer storage devices, to include computers, laptops, notebooks and other similar devices, shall be brought out of the office by any personnel unless on official activities.

Accounting of all External Storage Devices

Accounting of all computer-related external storage devices shall be in accordance with the provisions for storage.

Transmission of Electronic and Digital Data

The transmission of electronic or digital data is usually by means of e-mail utilizing internet, cellular phones and other devices of same capability; as such, all measures shall be undertaken to protect transmission from interception, traffic analysis and deception.

All classified documents for transmission via electronic mail (e-mail) or digital means shall be encrypted except as prescribed.

A suitable encryption software shall be prescribed to be used in sending classified information by e-mail or digital means.

Loss of Computer and Computer-related Devices

It is the responsibility of all individuals who have access to office computers and networks to prevent any loss of computer hardware, software and storage devices.

Any individual having knowledge or suspicion that computers and computer storage devices have been lost, compromised or have come to the knowledge of unauthorized persons shall immediately report the facts to the MIS Officer.

Destruction

Destruction of classified information stored in computer devices shall be by complete erasure of the classified data from the computer storage device. However, for storage device that cannot be deleted from the storage device such as compact discs, the method of destruction shall be as prescribed.

Network Security

Several software programs are used to provide communication functionalities such as: emails, file transfer, web browsing, instant messaging, voice-over-IP and video streaming.

Wire tapping, network intrusion, identity spoofing, spread of malicious software programs, denial of service and unauthorized modification of data in transit are common information technology security threats on network. The following paragraphs offer several means to protect the network and to carry out networked computer activities in a secure manner.

Email

Email contains text messages and could carry a file attachment. Email can also be formatted using encoding techniques to contain colourful fonts and pictures. Malicious software code can hide in the file attachment or the encoding. Malicious software codes can be downloaded to the email recipient's computer if the file attachment or the encoded email is opened.

Do not configure email programs to open file attachments automatically. Before opening an email attachment, look at the file name and verify that it is not an executable program. Good practise is to scan the attached file with an anti-virus software. Do not open an email attachment from unknown senders unless you are sure that the attachment does not contain malicious software code.

Email security can be further enhanced by configuring email programs to not allow automatic display of encoded email. This will reduce the risk of executing hidden malicious code.

Email sent over the Internet is not authenticated. This function is heavily exploited by spammers. Spammers send unsolicited emails in massive numbers. Some spam emails contains content that looks genuine and request personal information. An example is an email that claims that the recipient has won the lottery and requests personal information or even a credit card number. If the recipient replies, his credit card number can be stolen and misused.

Do not reply to spam email that request for your personal information. Most email programs can be configured to block out spam email.

World Wide Web

Web sites can contain executable programs that run on your computers. These programs can contain malicious software codes that infect your computer if executed.

Do not permit web sites to upload programs to computers unless the site is trustworthy. In general, scan the program with anti-virus software to make sure that it does not contain malicious software codes.

Pay attention to all website Uniform Resource Locator (URL). Sometimes a web site is redirected to an imitation website. This fake website will attempt to acquire sensitive information, such as username, password and credit card details. This is known as web phishing.

If entering any personal information on a web site, clear the computer memory cache. This measure is especially important if using a shared computer as personal information can be retained in the memory cache and accessible to other users.

Secure Socket Layer (SSL) is a popular mechanism to secure web access using encryption. SSL is commonly used in online email and banking. A key feature of SSL is the using of digital certificate to establish the trust of the web site. Check the information of the digital certificate to ensure it is indeed the intended web site.

Never surf the Web on a computer that contains highly sensitive information such as operational plans, orders, military personnel records, intelligence reports or critical financial information.

Ensure that the individual browser is kept up-to-date with the most current security patches.

Visit only known and trusted sites on the Web. Monitor the Universal Resource Locator (URL) or internet address shown in the box at the top of the browser screen. These addresses typically take the form of <http://www.sitename.com>. If one is unsure about the safety of the site, contact the network administrator or designated network support group.

Be aware that some websites automatically download small application programs, dialogue boxes or windows that may pop out on the monitor screen called applets that execute in ones workstation. What the applets appears to be doing on the screen, may not be all that is happening. Hostile applets can exploit security holes to gather information from the users computer, such as user password files and critical network information.

Always close the browser when one has finished surfing the web. Log off ones workstation when leaving work premises at all time.

File Sharing

File sharing can be done over the network using various methods. The common information technology security concerns include data theft or spread of malicious software codes.

Only enable the file sharing function when needed. Enable access control by implementing login and password. *Also limit the file access permission to a level sufficient for enabling work to be done.* For example, set “read-only” permission if there is no requirement to edit the file remotely.

Make sure other users who are sharing files take information technology security seriously.

Instant Messaging

Instant messaging is extremely useful for carrying out interactive conversation over the network. However, most instant messaging software does not keep the conversation content confidential over the network. *Hence, do not send sensitive information over instant messaging.* Consider using encryption tools to keep the content of the conversation confidential.

Wireless Transmission

Wireless technology is used to extend the reach of a network beyond physical cables. However, this means interception of the wireless transmission can be carried out in an easier manner compared to physical network cables.

A popular wireless technology is “WiFi”. Change the WiFi base station identity from the default name. *In addition, do not extend the WiFi connection to unknown personnel.* Configure the base station to not broadcast the base station identity. Only inform authorized personnel people about the base station identity.

To keep the wireless transmission confidential, configure the base station to use WiFi Protected Access (WPA) encryption. This is the latest encryption mechanism and it resolves problems faced by earlier encryption mechanism.

Virtual Private Network

Virtual Private Network (VPN) encapsulates data transfer between networked computers to keep the transferred data confidential from other computers. VPN makes use of encryption protocols to scramble the transmitted data and only the intended receiver can unscramble the transmitted data. A widely adopted encryption protocol is the Advanced Encryption Standard (AES).

VPN can provide data integrity by preventing the alteration of the data during transmission. As only the sender and receiver have the means to encrypt and decrypt the data, the message cannot be altered by anyone else.

User authentication can also be done by VPN to block identity spoofing. Common methods include passwords and digital certificates.

VPN security is also used to secure VOIP, video streaming, instant messaging and file sharing.

Firewall

A firewall is used in a network to keep out illegitimate access while permitting legitimate communications. A firewall can be a software program on a computer or a dedicated computer device.

Firewall inspects the network traffic passing through it and denies or allows passage based on a set of rules. It is usually placed between an internal network and an external network. This configuration is used to prevent unauthorized users from the external network from accessing the internal network.

Router

A router interconnects computer networks and interchanges data packets between them based on the routing table. Hence, the router should be configured with the correct settings so that the data packets can be delivered from the source to destination.

Access control list is usually implemented on the router to keep out unauthorized user from accessing the network. Certain routers have additional security features, for example, firewall, network intrusion detection, and these features can be turned on to enhance information technology security.