Network and Communication Security (II)

Wireless Network Security

Wireless (Wi-Fi) network transmits information via the airwaves. Anyone may pick up the signals emitted from a wireless network. Intruders can make use of this opportunity to intercept the information. Therefore, organisations or individuals should protect their wireless network facility and the transmitted information in order to prevent data theft.

Organisations should execute stricter physical security control and user authentication, control the range of wireless signal propagation, limit access to authorised users only, and prevent unauthorised connection to its wireless network.

All information transmitted through wireless network should be encrypted to ensure its confidentiality. Organisations should use a stronger wireless security protocol and encryption algorithm such as WPA or WPA2 with encryption standard AES (Advanced Encryption Standard).

Preventive Measures of Network Communication

In addition to stealing sensitive information through a communication network, intruders can exploit security loopholes of the network to intrude the information system. To protect the computer network, it is necessary to adopt effective security measures such as regular check-up for security loopholes, installing the latest software security patches, etc.

Under certain circumstances, users might need to connect to the organisation's internal network and system through a computer network provided by the organisation. The organisation must implement appropriate security measures on the computer network, such as user identity authentication, access control, etc.

Users should avoid connecting to the organisation's internal system using computers in Internet cafés or any other public Internet facilities. It is because malicious codes such as keylogger might have been implanted in public computers by other users. A user's personal information may be recorded or stolen in this way.

If there is a real need to connect to the organisation's internal network through the Internet, proper security measures must be taken. For example, use the Virtual Private Network (VPN), Secure Sockets Layer (SSL), etc to protect transmitted information.

Virtual Private Network (VPN) is a technology called "encrypted tunnel", through which information transmitted between the sender and the receiver is encrypted. This establishes a safe connection on the network.

Secure Sockets Layer (SSL) is a security protocol which is mainly used to protect the data transmitted over the Internet. Nowadays, Internet browsers generally support SSL technology to provide protection on transmission of sensitive data.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk