CHAPTER 10
MALWARE PROTECTION

10.1 Protection against Malware by Schools

10.1.1 Schools should ensure servers, workstations and mobile devices are installed with malware detection and recovery protection measures.

10.1.2 Schools should configure the malware definition updates as automatic and the update frequency should be at least on daily basis. If automatic update is not possible, manual update should be performed at least once a week and whenever necessary.

10.1.3 Schools are recommended to acquire security software, e.g. malware detection, for centralised management, i.e. using a dedicated server / workstation to manage all agents of the security software in schools. It usually provides features like remote update, policy enforcement, status query, report generation and security functions, etc. It can save deployment time of policy / signatures / updates, enforce a standardised organisational security policy, assist in compliance assessment and save efforts of the technical support staff.

10.1.4 Schools should enable anti-malware protection on all local area network servers, personal computers, mobile devices and computers connecting to the school internal network via a remote access channel.

10.1.5 Schools should enable anti-malware protection to scan all incoming traffic from the Internet. The gateway should be configured to stop traffic with malicious contents, quarantine / drop them and create audit logs for future reference.

10.1.6 Schools should be aware that if the machines should be booted from removable media like USB flash drives or hard drives, optical disks, etc. The removable media must be scanned for malware before use. This can eliminate boot sector viruses from infecting the server.

10.1.7 Schools should consider using webpage content filtering software to prevent staff from abusing resources, e.g. downloading files in bulk from the Internet or browsing harmful websites. These activities not only consume bandwidth and waste resources, but also increase the risk of malware infection.

10.1.8 The technical support staff and IT Heads should subscribe to notifications / advisories so that they can receive critical malware alerts at the earliest possible moment. IT Heads should disseminate promptly the security alert to all end users and take necessary actions.

10.1.9 Schools should educate users to understand the impact of massive malware attacks, recognise ways of infecting with malware. For example, educate users that senders of electronic message containing malware can be forged as friends or colleagues, in order to prevent malware infection.

10.2 Protection against Malware by Users

10.2.1 Users should regularly update malware definitions and detection and repair engines. Updates should be configured as automatic and update frequency should be at least on daily basis. If automatic updates are not possible, e.g. mobile devices not often attached to networks, updates should be done manually at least once a week.

10.2.2 Users should enable real-time detection to scan malware for active processes, executable and document files that are being processed. They can also schedule full-system scan to run regularly based on operational needs.

10.2.3 Users should avoid opening suspicious electronic messages and should not follow URL links from un-trusted sources to avoid being re-directed to malicious websites. In particular, users should exercise extra care for attachments and downloads with filename extension of "exe", "bat", "cmd", "jar", "lnk", "msi", "inf", "scf", "scr", "pif", "com" and "vbs". They should be checked against malware before use.

10.2.4 User should check any files on storage media, and files received over networks against malware before use. They should not use storage media and files from unknown source or origin unless the storage media and files have been checked and cleaned for malware.

10.3 Malware Incident Handling and Recovery

10.3.1 If a computer is suspected to be infected with malware, users should disconnect the network cable of the computer to avoid affecting network drives and other computers, and stop all activities because continually using the infected computer may help spreading the malware further.

10.3.2 Users should report any suspected malware incident to the technical support staff / IT Head immediately.

10.3.3 The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) Helpdesk (hkcert@hkcert.org) can provide technical assistance for schools in handling malware incidents.

10.3.4 With the assistance or advice from technical support staff, users may also use anti-malware software available in the market to clear the malware on their own.

10.3.5 Removing malware does not necessarily imply that contaminated or deleted files can be recovered or retrieved. The most effective way for recovering corrupted files is to replace them with the original copies. Therefore, regular backups should be done and sufficient backup copies should be kept to facilitate file recovery whenever necessary. The backups should be offline to ensure that they will not be infected by malware.

10.3.6 After removing malware from a computer, users should perform a complete scan on the computer and other storage media to ensure that it is free of malware. Failure to rescan a computer for malware may lead to the resurrection of the malware.

10.4 Protection against Ransomware

10.4.1 Ransomware is a malicious software that cyber criminals used to lock the files stored on the infected computer devices. These locked files are like hostage and the victims are required to follow the instructions of this malicious software and pay a ransom to unlock them.

10.4.2 Users should be aware that opening suspicious emails, or attachments and hyperlinks inside, visiting websites embedded with malicious programs, downloading and installing software or mobile apps that are embedded with ransomware may cause inflection.

10.4.3 Do not open any suspicious emails or instant messages, as well as the attachments such as compressed files (zip) or executable files (exe) and hyperlinks inside them.

10.4.4 Users should refrain from visiting suspicious websites or downloading any files from them.

10.4.5 The technical Support Staff should install the latest patches for software in use. They should check and make sure the anti-malware program and signatures are up-to-date. Besides, they should schedule a regular full scan to detect and guard against malware attacks.

10.4.6 Schools should disable or restrict all unnecessary services and functions in computer systems.

10.4.7 The technical support staff should perform regular backups on important data and keep the backup copies disconnected from the computer.

10.5 Ransomware Incident Handling and Recovery

10.5.1 To handle infection cases, the technical support staff should:

(a) Disconnect the network cable of the computer to avoid affecting network drives and other computers.

(b) Power off the computer to stop the ransomware encrypting more files.

(c) Jot down what have been accessed (such as programs, files, emails and websites) before discovering the issue.

(d) Report to the HKCERT and Hong Kong Police Force (HKPF) the criminal offence if necessary.

(e) Recover the data from backup to a clean computing device.