# ELECTRONIC MAIL

Electronic mail or e-mail makes it possible to exchange messages through a local or worldwide communication network such as Internet. Computers are generally used as terminals, but electronic agendas, cell phones, data communication terminals or other data exchange equipment can also be used. The best known and most widely used network is Internet. Most e-mail software and services allow for the attachment of files containing text, documents, sound, pictures, and even computer programs.

There are two main types of e-mail. The first enables subscribers of a network provider to send and receive messages with e-mail software. Messages are processed on the sender's terminal. The second type, Web mail, is accessible through navigation software that enables a computer connected to Internet to send and receive mail, without the services of a network provider. If such service were offered in Québec, only data essential to the object of the file could be retrieved.

## CONFIDENTIALITY?

E-mail is a very convenient tool. However, it does not guarantee the confidentiality and integrity of messages, nor does it ensure the authenticity of their source and their author's identity. Specific steps must be taken to protect the information that is transmitted. It is fairly easy to access a message during transmission and read or modify it. *E-mail offers about the same degree of confidentiality as a postcard.*

Messages sent through Internet do not go directly to the recipient; they transit through a more or less large number of computers before reaching their destination. This path varies from one time to another depending on many factors, notably the state of the network and how busy it is.

Network providers must inform customers of their policy for the management of electronic mail and the protection of personal information. Messages sent and received by their subscribers go through their systems or reside in them for a more or less long period.

## PROTECTION MEASURES

### Apply patches proposed by software developers

Software developers constantly propose modifications to correct glitches in their programs. They offer patches and updates to improve e-mail security.

### Use up-to-date anti-virus software

A terminal can be contaminated by the introduction of a virus. Some of these viruses are harmless. But others can destroy the contents of a terminal or make possible illegal intrusions. Up-to-date anti-virus software can detect and eliminate most viruses.

Use encryption software

To protect a message's confidential data, the use of encryption software is recommended. This kind of software encodes the contents of the message, making it illegible and difficult to decipher. This has both a protective and deterrent effect.

Encryption software is available on the market and can be downloaded for free on Internet.

Manage your password

E-mail boxes are protected by a password. This password should be frequently modified to avoid being known by too many people who could access a user's mailbox without authorization. Changing your password regularly gives you better control of your mailbox. It is also advisable not to activate the password recording or memorizing function to better control access to the mailbox.

## ACCESS AND CORRECTION RIGHTS

Electronic messages and files circulating in public and private organizations are subject to provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information* and the *Act respecting theprotection of personal information in the private sector.*

Access and correction rights recognized to citizens by these two laws must be respected.

## CONSERVATION AND DESTRUCTION OF MESSAGES

E-mail system administrators must set time limits for the conservation of messages. In public bodies, these time limits must be recorded in a calendar approved by the National Archives. Private organizations would be well-advised to adopt the same policy. They could thus enforce more effectively access and correction rights citizens are entitled to.

## POLICY ON THE USE OF E-MAIL IN THE ENTERPRISE

Rules for the management and use of e-mail within a company must be clear and known to all users. They should know who can access mailboxes (system administrator, manager, auditor) and in which circumstances such access is authorized (redirecting undelivered messages, serious suspicions of fraud).

In the workplace, it is reasonable to expect employers to control the use of their own communication means. However, employees are entitled to the respect of their privacy in this process. Employees should be informed of the reasons for control, and the means of control they can be subjected to. They must be clearly informed of their rights and obligations.

## ELEMENTARY PRECAUTIONS

In addition to the measures already mentioned, other precautions should be taken.

- To each mailbox should be attached a password known and managed only by the employee authorized to access it.
- In case of a common mailbox, only employees authorized to access it should know the password.
- The organization’s computer system should require users to change their passwords regularly, say every month, and discard those previously used. Since network providers do not usually require users to modify their passwords, company policy on the use of e-mail should remedy the matter.
- No personal data should be transmitted, unless encrypted. If encryption software is used, the encryption keys should be carefully managed.