# E-mail

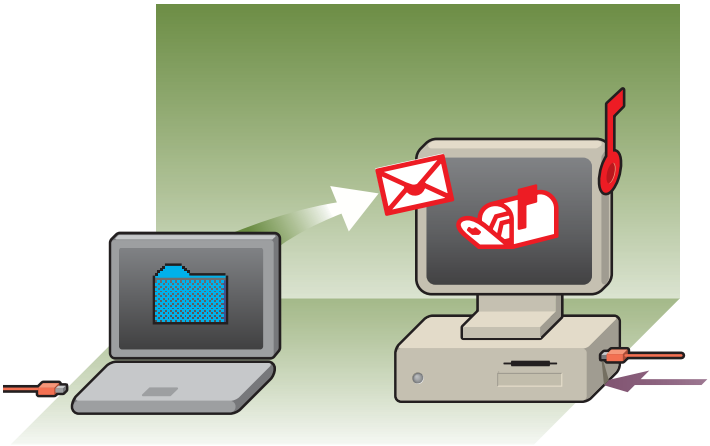
CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

## Résumé

L'utilisation accrue d'Internet comme moyen de communication tant privé que professionnel a pour conséquence l'émergence du courrier électronique comme moyen de communication universel. A l'heure actuelle, beaucoup de relations, commerciales, privées ou avec l'Etat sont largement facilitées par l'utilisation de ce moyen de communication. Le courrier électronique, également appelé e-mail ou courriel, est devenu un standard de facto de communication dans nos sociétés actuelles.
L'apparition d'accès à large bande (type DSL ou sur cable TV) accentue encore ce phénomène de généralisation de l'utilisation de l'e-mail. Grâce à ce gain de performance, les fichiers attachés peuvent aujourd'hui être des documents de plusieurs Mégabits et de toute nature (fichier texte, programme, fichiers musicaux...).

## Table des matières





## 1 Qu'est-ce qu'un courrier électronique ?

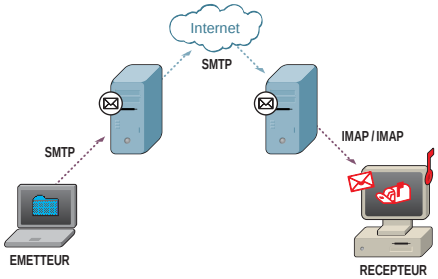
Un courrier électronique est un message transféré d'une boite électronique à une autre en transitant par des serveurs ou relais d'e-mail intermédiaires. Concrètement, l'e-mail est un flux de données structurées de manière à ce que les serveurs e-mails puissent les interpréter et les acheminer dans la boîte aux lettres du destinataire.

**Le courrier électronique est composé des éléments suivants :**

- De l'adresse électronique du ou des destinataires principaux.
- De l'adresse électronique de l'émetteur du message.
- D'un contenu (appelé aussi corps du message), qui contient le texte du message et souvent des fichiers attachés.
- À la différence du courrier postal, le courrier électronique comporte en plus un sujet permettant d'identifier le message.
- D'autres informations destinées à l'acheminement du message, équivalentes des tampons postaux (date, heure, liste des serveurs ayant relayé le message...).

## 2 Comment cela fonctionne-t-il ?

Comme évoqué précédemment, un courrier électronique est un flux de données transitant d'un émetteur à un récepteur en transitant par des serveurs ou relais e-mails intermédiaires. Le schéma suivant illustre ce mode de fonctionnement :




suite au verso

# E-mail



suite

Comme indiqué sur le schéma, plusieurs protocoles de communication sont utilisés lors des opérations d'envoi et de réception.

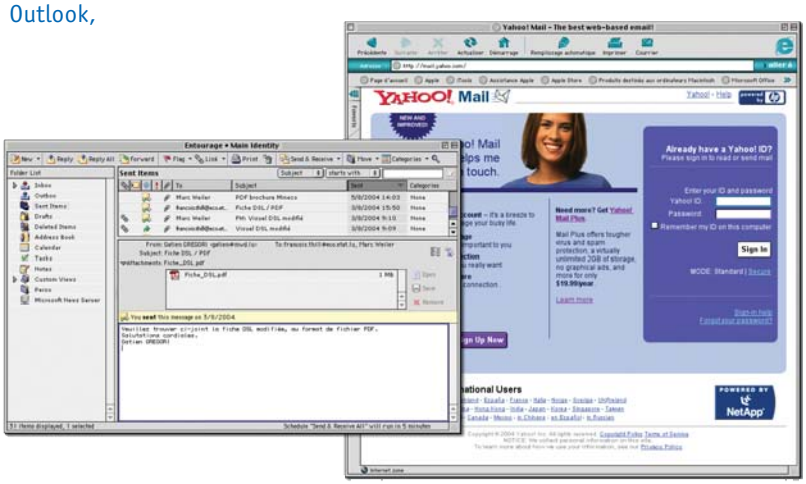
Pour rappel, un protocole est un mode de communication déterminé entre deux entités leur permettant d'échanger des informations. Il s'agit ni plus ni moins d'un langage commun que deux entités (généralement un client et un serveur) utiliseront pour pouvoir effectuer un travail donné, dans ce cas-ci envoyer un e-mail.

*(cf. fiche thématique Protocole)*

Le tableau ci-contre synthétise les différents protocoles utilisés dans le cadre de l'envoie et la réception de courriers électroniques.

| PROTOCOLE | DESCRIPTION |
|---|---|
| SMTP | SIMPLE MAIL TRANSFER PROTOCOL |
| | Envoi de l'e-mail de l'émetteur vers le serveur et transfert de serveur à serveur. |
| POP3 | POST OFFICE PROTOCOL |
| | Protocole de réception de courriers électroniques. Il s'agit du protocole de réception le plus ancien et également le plus utilisé. |
| IMAP4 | INTERNET MESSAGE ACCESS PROTOCOL |
| | Protocole de réception comparable à POP3. Il s'agit d'un protocole plus récent proposant de nouvelles fonctionnalités. Ces fonctionnalités ne sont pas d'une très grande utilité pour les utilisateurs, ce qui explique qu'IMAP4 ne soit pas très utilisé. |

Une autre méthode très populaire pour utiliser le courrier électronique est le webmail. Il s'agit en fait de remplacer le client e-mail par un simple navigateur internet (par exemple Opéra ou Internet Explorer). Dans ce cas, l'accès par le client au serveur d'e-mail se fait par l'intermédiaire d'un site web spécialement conçu à cet effet (par exemple **http://webmail.pt.lu** ou **http://mail.yahoo.com**).




## 3 Quels sont les risques liés à l'utilisation du courrier électronique ?

La nature même du courrier électronique présente un certain nombre de risques pour les utilisateurs et le rend vulnérable à de très nombreux abus. De par sa très large utilisation, ces risques sont donc très répandus et menacent presque tous les utilisateurs. Les risques principaux qui touchent les utilisateurs de courriers électroniques sont les suivants :

### Virus et vers (worm)

**Un virus** est un programme ou morceau de programme – également appelé code exécutable – qui, pour pouvoir se propager s'attache à tout type de fichier ou autre programme et qui a pour vocation d'infecter et de se propager d'un ordinateur à un autre à l'insu des utilisateurs. Le virus ne s'active que si un utilisateur exécute délibérément le code dans lequel il est intégré.

**Un ver** est un programme très similaire à un virus. Cependant et contrairement au virus, un ver n'a pas besoin d'intervention humaine pour infecter un ordinateur. Il dispose d'un moteur qui lui permet de délivrer automatiquement son code et par après, de chercher des nouvelles cibles à infecter.

*(cf. fiche thématique Vers et virus)*

Aujourd'hui, l'intégration de code actif directement dans certains clients e-mails ainsi que des nouvelles techniques de codage des virus permettent à ceux-ci de devenir actifs sans même qu'une pièce jointe soit ouverte.

# E-mail



suite

## Divulgation

Les concepteurs des protocoles de courrier électronique n'ont pas pris en compte le besoin de confidentialité et d'intégrité des données échangées : par défaut, tous les e-mails sont envoyés en clair sur Internet et toute personne pouvant avoir accès à l'e-mail sur son chemin vers le destinataire peut lire et copier son contenu. De plus l'intégrité du message n'est pas protégée et il ainsi facile d'envoyer un e-mail en indiquant une fausse adresse de l'émetteur (usurpation).

Les informations d'accès de l'utilisateur vers sa boite e-mail (username et mot de passe) sont également lisibles à toute personne pouvant les intercepter ou y accéder.

## Chevaux de Troie

**Un cheval de troie** est un programme ou morceau de programme (également appelé code exécutable) qui se présente comme programme anodin mais qui en réalité et de façon très similaire à un virus a pour vocation d'infecter un ordinateur à l'insu des utilisateurs.

A la différence d'un virus ou un ver, un cheval de troie ne se reproduit pas ni se propage mais peut cependant être aussi destructeur dans certains cas.

Le e-mail est un moyen privilégié pour activer et installer un cheval de Troie sur une machine cible.

*(cf. fiche thématique Chevaux de Troie)*

## Spyware

**Un spyware** est un logiciel qui transmet par le biais d'Internet des informations généralement à des annonceurs publicitaires sur l'utilisateur ou sur ses habitudes sans son autorisation. Les spywares se transmettent principalement par l'intermédiaire de sites web et parfois par e-mail.

EXEMPLE :

Le logiciel Keylogger qui garde une trace de toutes les frappes clavier sur un ordinateur.

## Usurpation et falsification

Les noms de comptes et d'utilisateurs nécessaires pour se connecter sur un serveur de e-mail sont envoyés en clair (sans chiffrement) sur le réseau. Une personne malintentionnée disposant de certaines connaissances et des outils adéquats peut écouter le trafic réseau, récupérer les identifiants et ensuite se connecter à un compte ne lui appartenant pas.

Il peut de cette manière envoyer et recevoir des courriers électroniques au nom de cette personne.

## Spam

**Le spam** est l'encombrement délibéré d'un compte e-mail par l'envoi de messages non sollicités, telles les annonces à caractère publicitaire. Il s'agit d'une technique d'envoi massif de courriers non-sollicités qui profite le plus souvent de la possibilité de falsifier l'adresse d'origine.

## Ingénierie sociale

**L'ingénierie sociale** est une technique de manipulation et d'agression non-technique qui consiste à utiliser la crédulité de la victime pour obtenir des informations personnelles ou confidentielles.

**Exemple 1 :**
Un attaquant se fera passer pour un employé de banque au téléphone et essayera d'une manière ou d'une autre d'obtenir un numéro de carte de crédit.

**Exemple 2 :**
Un attaquant se fera passer pour un administrateur réseau de la société voulant rectifier un problème logiciel et demandera le mot de passe personnel.

## Phishing (prononcer fishing)

**Le phishing** est l'association d'un e-mail non sollicité (spam) à un site Web illégal reproduisant le design d'un site commercial légitime et incitant l'internaute à y déposer ses coordonnées, en particulier bancaires.

Ces faux sites Web détournent majoritairement l'identité des grandes banques américaines. Mais pas seulement, car eBay devient aussi un alibi pour les bandits en ligne, avec 20% des détournements et 12% pour son système de paiement en ligne PayPal.

Le phishing est donc une combinaison d'ingénierie sociale et d'usurpation.

# E-mail



suite

## 4 Comment se protéger ?

### Virus, vers et chevaux de Troie

- Utilisation d'un logiciel anti-virus avec pare-feu (firewall) sur votre ordinateur.
- Eviter d'ouvrir des courriers électroniques (e-mails), logiciels, programmes ou tout autre fichier dont le sujet ou son contenu vous semble inhabituel voire anormal.
- Application des patches qui permettent également de protéger dans la majorité des cas contre une infection et propagation de vers.

*(cf. fiche thématique Vers et virus + fiche thématique Chevaux de Troie)*

### Divulgation

Si les données à transmettre par e-mail sont confidentielles, il faut utiliser un logiciel de chiffrement permettant de rendre les données uniquement lisibles par le destinataire. Ces logiciels permettent de crypter tout le contenu de l'e-mail ou sinon uniquement les fichiers attachés.

*(cf. fiche thématique Cryptographie)*

### Usurpation et falsification

La fonction de signature électronique permet de se protéger contre les risques d'usurpation et de falsification. En effet la signature électronique d'un e-mail permet de s'assurer de son intégrité (contre la falsification) et de l'émetteur (usurpation)

*(cf. fiche thématique Cryptographie)*

### Spam

Peu de protections efficaces existent pour se protéger contre le spam. Cependant les internautes peuvent s'assurer que leur fournisseur d'accès à Internet (FAI) filtre bien les spams connus. Il existe en effet des listes d'émetteurs de spam connus. Ces émetteurs sont placés sur des listes noires (appelée également blacklist) que les FAI peuvent utiliser afin d'empêcher tout serveur se trouvant sur cette liste d'envoyer des e-mails à un de ses clients.

### Phishing

Le seul moyen de se protéger contre le phishing et l'ingénierie sociale est de ne jamais envoyer d'information confidentielle (mot de passe, numéro de carte de crédit...) sans être sûr de l'identité de la personne qui le demande.