FACILE MOYEN DIFFICILE EXPERT

par Maya, 15 ans
(membre du club informatique du Lycée Blaise Pascal à Orsay)

# Le mail, ça s'apprend!

# Les intrus du mail : comment gérer ta messagerie en toute sécurité

**Imagine qu'à ta soirée s'incrustent des personnes que tu n'as pas invitées, ayant malencontreusement trouvé ton adresse sur les réseaux sociaux. Comment réagirais-tu ? Un spam est comme cet invité indésirable, c'est un message que tu reçois sans que tu le veuilles.**

Un grand nombre de spams sont détectés et bloqués avant qu'ils ne polluent ta messagerie. Mais **certains messages passent au travers des mailles du filet** et arrivent dans ta boite aux lettres. Sache qu'il existe trois différents types de messages indésirables plus ou moins embêtants !

## 1

### Newsletters ou messages commerciaux envoyés par des sites connus

Tu as peut-être déjà visité un site marchand ou tu t'es abonné à une newsletter sur un sujet qui t'intéresse. Les services que tu utilises t'envoient des emails régulièrement pour maintenir ton attention. Normalement, **tu peux te désabonner** de ces mails si tu le veux en cliquant sur un lien prévu à cet effet, souvent situé en bas du message.


## 2

### Publicités qui sont diffusées en masse

Il est très difficile de se prémunir contre ces messages, car **les expéditeurs utilisent des adresses différentes pour chaque envoi**, comme s'ils postaient des lettres à chaque fois d'une ville différente. Ils contournent ainsi les dispositifs antispam mis en place par les serveurs et les utilisateurs.


N'HÉSITE PAS À DÉCOUPER TES FICHES POUR LES CLASSER ET LES CONSULTER PLUS FACILEMENT

3

## Messages malveillants envoyés par des pirates

**Ces messages sont les plus dangereux** et il est important de les reconnaitre pour se protéger. Envoyés par des personnes mal intentionnées cherchant à nous escroquer, ils prennent souvent l'identité d'expéditeurs connus, par exemple un opérateur internet, une messagerie, ou un organisme financier.

Souvent, ces mails te font croire que tu as gagné quelque chose, comme de l'argent, un voyage ou un smartphone, mais tu ne pourras le recevoir qu'en indiquant beaucoup d'informations confidentielles sur toi et ta famille ou en envoyant des codes soi-disant gratuits. Évidemment, c'est faux et tu pourras te retrouver à payer sans le savoir. Cette opération d'escroquerie s'appelle le *phishing* (hameçonnage en français), cela fonctionne comme un hameçon pour t'attirer vers le piège.

## Le récap' des bonnes pratiques

1. **Ne jamais envoyer un mot de passe à qui que ce soit par email.**
2. **Ne clique sur aucun des liens contenus dans un message qui te parait suspect.**
3. **Supprime le message suspect en utilisant le bouton « Ceci est du spam » de ta messagerie.**
4. **Organise le filtrage de tes messages. La solution *Mailo* offre par exemple un filtre antispam qui ne fait passer que les messages que tu veux bien recevoir en les classant automatiquement dans les dossiers que tu auras configurés.**



N'HÉSITE PAS À DÉCOUPER TES FICHES POUR LES CLASSER ET LES CONSULTER PLUS FACILEMENT