COMMENT EST PROTÉGÉE VOTRE BOÎTE ACADÉMIQUE CONTRE LE SPAM ET LES VIRUS ?

INTRODUCTION

La messagerie électronique est un support hélas privilégié pour la propagation de virus, de courriers publicitaires non désirés et de tentatives de fraude et d'escroquerie.
Comme tout fournisseur de service en matière de courrier électronique, l'Académie de Lille a mis en place des systèmes techniques de lutte pour limiter au maximum le transit des virus et des spams[1].

Cette fiche pratique vise à vous décrire brièvement les mesures prises en la matière par l'Académie, afin que vous sachiez comment sont traités les messages électroniques que vous envoyez et surtout que vous recevez.

LE FILTRE ANTIVIRUS

Un filtre antivirus est installé sur le réseau académique afin de lutter efficacement contre les infections virales et éviter de les propager. Toutes les pièces jointes aux messages reçus ou expédiés sont analysées automatiquement par le filtre antivirus.
Cette inspection est réalisée par un programme qui recherche les signatures virales sans en "visualiser" le contenu. Elle respecte les dispositions légales de confidentialité appliquées aux échanges de courriers électroniques.

Si le filtre détecte un virus :

- Un message signalant le virus est automatiquement envoyé à l'expéditeur, au destinataire et à l'administrateur de la messagerie (ingénieur DSIAL[2]).
- Si l'antidote est disponible, le virus est éradiqué avec mention au destinataire. Dans le cas contraire, la pièce jointe n'est pas remise au destinataire (elle est mise en quarantaine sur le serveur).

Attention ! Ce mécanisme assure une protection optimale contre les virus véhiculés par les messages électroniques mais ne vous protège pas contre les virus présents sur les supports externes (clés USB) ou contenus dans les fichiers que vous téléchargez à partir de sites web (hors académie).
La présence d'un **antivirus** avec des **mises à jour régulières** reste nécessaire **sur votre poste de travail**.

[1] Spam : néologisme désignant un message électronique non sollicité, aussi appelé « courrier indésirable » ou parfois « pourriel ».
[2] DSIAL : Direction des Services Informatiques de l'Académie de Lille

LE FILTRE ANTISPAM

Les spams sont des courriers envoyés à un grand nombre de destinataires dont les adresses ont été collectées souvent à leur insu (en scrutant les sites web sur lesquels ils ont laissé leur adresse, dans des carnets d'adresse volés par un programme viral, etc.). Le contenu d'un spam peut être relativement bénin, comme un simple message publicitaire ou la demande de participation à une chaîne de lettres. Mais il peut aussi être potentiellement plus dommageable, comme une tentative d'escroquerie (fausse loterie, appel à la charité) ou une tentative d'hameçonnage[3].

L'Académie de Lille a installé sur ses serveurs de messagerie un filtre antispam qui inspecte les courriers reçus selon des critères caractéristiques des spams. Si un message est détecté comme tel, il est intercepté et placé dans une zone de quarantaine. Il y reste pendant sept jours avant d'être définitivement supprimé.
Vous avez accès à cette zone de quarantaine et vous pouvez la configurer pour être averti lorsque des messages y sont dirigés. Reportez-vous à la fiche pratique « **Comment gérer votre filtre académique de courrier indésirable ?** » pour de plus amples informations.

LE QUOTA D'ENVOI DE MESSAGES

Il peut arriver que des ordinateurs du réseau Intranet dans l'Académie (Rectorat, DSDEN, IEN, EPLE...) soient infectés par un programme viral qui génère du spam vers l'extérieur. Afin de limiter les effets secondaires d'un tel phénomène, en particulier pour que des fournisseurs de messagerie tiers ne déclarent pas l'Académie de Lille sur leur liste noire, le nombre de messages électroniques qu'un même expéditeur peut émettre est limité.
Ce quota est de l'ordre de plusieurs milliers de messages si le client de messagerie est configuré pour utiliser le serveur de courrier sortant en mode authentifié, de plusieurs centaines s'il l'utilise de manière anonyme.

En conséquence, si vous procédez à un publipostage (mailing) en direction de plusieurs centaines de destinataires, pensez à configurer votre client de messagerie avec le serveur de courrier sortant en mode authentifié.
Reportez-vous à la fiche pratique « **Comme configurer votre client local de messagerie ?** ».

[3] Hameçonnage (phishing en anglais) : consiste à tromper le destinataire en simulant un courrier électronique d'une banque, d'une institution ou d'un fournisseur de service pour l'attirer sur un site factice, dans le but de récupérer des données confidentielles (notamment mot de passe et coordonnées bancaires).