Antispam et antivirus de l'Université de Nantes

1) Qu'est ce que le Spam

On appelle spams les courriers électroniques non sollicités envoyés par millions servant le plus souvent des desseins illicites : ventes de produits contrefaits, manipulations boursières, vols de données bancaires ou personnelles, pornographie, etc.

Les spammeurs collectent les adresses de plusieurs façons : sur le web, sur les newsgroups, sur les PC contaminés par des virus de leur cru (en savoir plus)

Ne pas confondre le spam avec :

- La publicité électronique : le mail de publicité électronique (ou “prospection électronique”) est encadré par la loi. Il doit respecter certains critères :

1. l'expéditeur doit être clairement identifiable
2. le destinataire doit avoir accepté explicitement de recevoir ces offres
3. le destinataire doit pouvoir se désabonner de manière simple et définitive

Il est très fréquent lorsque vous vous inscrivez sur un site commercial (vente en ligne, clubs, site de rencontres, jeux, etc) que vous acceptiez de manière involontaire de recevoir de la prospection de l'entreprise derrière le site voire même parfois de ses partenaires.

Ainsi, les mails de publicité, bien qu'ils semblent parfois ne pas être sollicités, s'ils respectent les 3 règles précédentes, ne peuvent pas être assimilés à un spam. En revanche, s'il n'y a pas de lien de désabonnement ou si celui-ci ne fonctionne pas, alors ce mail est considéré comme un spam puisqu'il s'agit d'une prospection forcée.

- La lettres d'information ou “newsletter” : la lettre d'information est envoyée par un site auquel l'utilisateur est abonné. Il permet de maintenir l'utilisateur à jour avec l'évolution du site ou de ces produits/services. Le destinataire doit pouvoir se désabonner et ne plus recevoir ces courriers.

Exemple de sites envoyant régulièrement des courriers de publicité et/ou d'information : amazon.fr, discount.com, rue-du-commerce.fr, voyages-sncf.fr, dell.com, etc.

Pour en savoir plus : Dossier "spam" sur le site de la cnil

2) Solution antispam en place à l'université

Depuis juin 2025, Nantes Université utilise l'antispam de Renater. Cette solution permet une meilleure réactivité face au menaces envoyées par courrier électronique et de meilleurs moyens de détection.

L'antispam, de manière classique, marque les courriers indésirables avec l'étiquette [SPAM] en début de sujet afin de vous permettre de filtrer ces courriers dans un dossier séparé (cf ci-dessous) mais elle

détecte aussi, sans marquer le sujet, la publicité. Aussi, une publicité ne sera pas marquée spam mais elle fera l'objet d'un traitement spécifique (ajout d'entête).

2.1) Détection de la publicité et des réseaux sociaux

L'antispam détecte les courriers publicitaires et les classes en 3 catégories:

- PCE : Professionnal Commercial Emails, les courriers publicitaires provenant de sociétées reconnues et respectant les bonnes pratiques (origine du mail évidente, lien de désabonnement, etc.)
- MCE : Miscellaneous Commercial Emails, les courriers publicitaires divers provenant de régies connues
- DCE : Dirty Commercial Emails, les courriers publicitaires qui ne semblent pas respecter les bonnes pratiques

De même l'antispam détecte aussi les courriers provenant de réseaux sociaux.

Bien que l'antispam n'ajoute pas de marque dans le sujet pour les publicités et les réseaux sociaux, il ajoute toutefois des entêtes qui vous permettent de filtrer ces courriers en fonction de leur classification (PCE, MCE, DCE ou réseau sociaux).

2.3) Entêtes ajoutés par l'antispam

L'antispam ajoute un entête dans les courriers afin de simplifier la création de filtres pour désencombrer votre boîte de réception. Il s'agit de l'entête **X-Renater-SpamState** qui reflète la détection du courrier:

Valeur	Signification	Explication
0	LEGIT	Mails légitimes
1	SPAM	Mails non sollicités
2	VIRUS	bloqué
3	BOUNCE	
4	EXVIRUS	
6	Suspect	certains mots clés ont été repérés dans le contenu du mail
10	PCE	PUB : Professionnal commercial Emails (le B2B)
11	MCE	PUB : Miscelaneous Commercial Emails
12	DCE	PUB : Dirty Commercial Emails (les mass mailing non sollicités)
13	Social	réseaux sociaux, etc.
14	Transaction	Mails de boutiques en ligne
101	Phishing	Hammeçonnage. Bloqué
102	Scam	Arnaques. Bloqué

3) Corriger l'antispam

Quand le système antispam de l'université pense avoir à faire à un spam, il va modifier le sujet du

courrier en y rajoutant la chaîne de caractères **[SPAM]**

Vous avez reçu un message qui a mal été interprété par l'antispam :

- il a été marqué spam alors que ce n'est pas un courrier non sollicité.
- ce message est un spam et pourtant il n'a pas été marqué.

Dans ce cas il est éventuellement possible de corriger l'antispam pour ne plus faire cette erreur.

> Seul la détection des spams est corrigible. Il n'est pas possible de corriger la détection des publicités ou des réseaux sociaux

Pour être corrigible, le message doit remplir certaines conditions :

1. **le message doit être passé par l'antispam de l'université** : il s'agit d'une correction et pas d'un apprentissage, il faut donc impérativement que l'antispam ait déjà vu ce courrier.
2. **il ne doit être en aucun cas modifié, ni le corps, ni les entêtes**
3. **le message doit être correctement envoyé au système de correction**

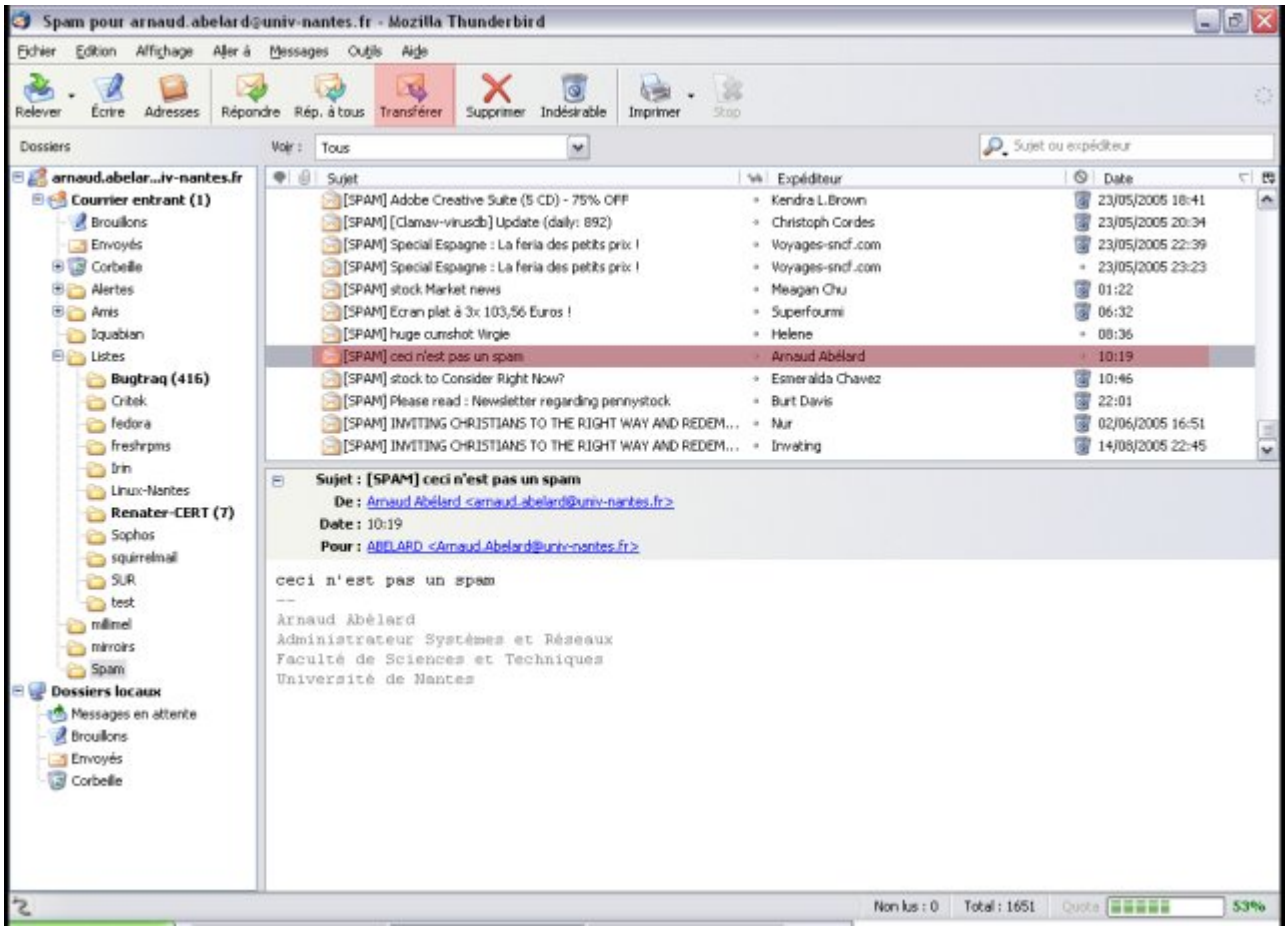
La correction se fait en 3 étapes :

1. Vous devez transférer le message original **en pièce attachée** à l'adresse **traitementspam@univ-nantes.fr**
2. Un “robot” va recevoir le courrier et l'analyser afin de déterminer si celui-ci peut être corrigé. Si ce n'est pas le cas, un message vous sera renvoyé vous expliquant le problème. Si le courrier n'est ni trop petit, ni trop gros, s'il est bien passé par le système de l'université, s'il n'a pas été modifié et s'il a bien été envoyé en pièce attachée alors il sera transmis aux administrateurs du système.
3. Les administrateurs vont vérifier qu'il s'agit bien d'une erreur puis faire la correction au besoin.

> Le message à corriger doit impérativement être envoyé à **traitementspam@univ-nantes.fr** en pièce attachée.

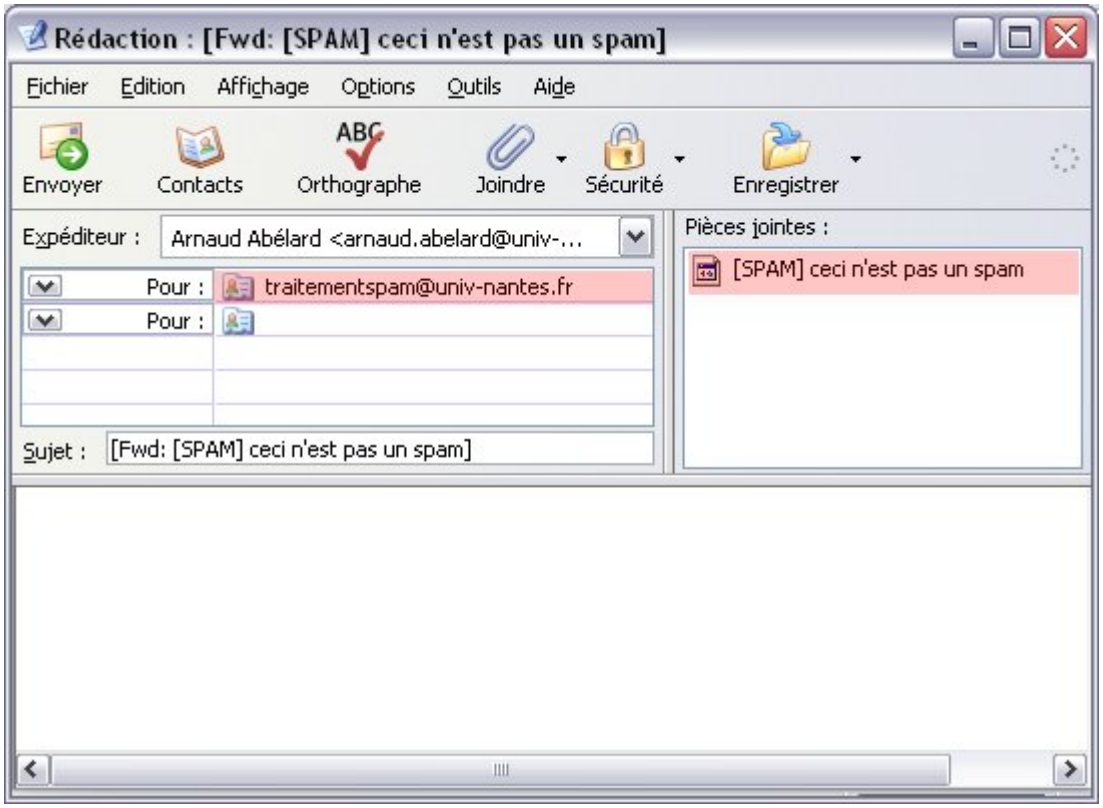
3.1) Avec Mozilla Thunderbird

- sélectionnez le message à corriger puis cliquez sur «Transférer» :



Il est possible que les versions récentes (2021) de Thunderbird dupliquent le contenu du message plutôt que de le mettre en pièce jointe. Pour convertir un message frauduleux en pièce jointe, le plus simple est de faire un clic droit sur le mail puis **Transférer au format > Pièce jointe** (faire glisser le mail vers la zone “pièces jointes” d'un mail en cours de rédaction ne fonctionne pas).

- vérifiez que le courrier à transférer est bien en pièce attachée et saisissez l'adresse du destinataire : **traitementspam@univ-nantes.fr** puis envoyez le courrier :



3.2) Avec le webmail

- Dans la fenêtre de lecture du courrier à corriger, cliquez sur le menu "**...**" puis "**Transférer comme pièce jointe**"

- Entrez l'adresse du destinataire **traitementspam@univ-nantes.fr** puis envoyez le courrier :

4) Protection antivirale des courriers

A l'université chaque courrier reçu ou envoyé est systématiquement testé par deux antivirus différents (clamav et McAfee uvscan). En plus de cette vérification nous filtrons les mails contenant des fichiers attachés potentiellement dangereux.

Liste des fichiers potentiellement dangereux

Il existe actuellement plusieurs dizaines de milliers de virus différents, infectant une multitude de types de fichiers. Bien souvent, le virus se fera passer pour quelqu'un d'autre et incitera l'utilisateur à cliquer sur le fichier attaché en espérant ainsi contaminer l'ordinateur. C'est pour cela que nous encourageons les utilisateurs à compresser au format .zip les fichiers potentiellement dangereux, ainsi le destinataire devra effectuer au moins deux manipulations volontaires, réduisant par la même occasion le risque d'une ouverture accidentelle des pièces jointes. Voici donc la liste des types de

fichiers que vous ne pourrez envoyer sans compression au format zip :

> Les extensions suivantes sont purement et simplement interdites en provenance de l'extérieur de l'université, même dans une archive zip. En interne celle-ci sont toujours autorisées une fois compressées pour imposer un minimum de 2 actions à l'utilisateur

extension du fichier	**description du type de fichier**
ade	Projets Access
adp	Projets Access
bas	Fichiers de script Basic
bat	fichiers batch DOS
chm	fichiers help de windows
cmd	fichiers batch XP/NT
com	executable
cpl	extensions du panneau de controle windows
crt	fichiers de certificats windows
exe	executables
hlp	fichiers help windows
hta	applications html windows
inf	fichiers setup (autoexecutables sous windows)
ins	fichiers setup (autoexecutables sous windows)
isp	fichiers de configuration internet windows (utilisé par les malware/payphones)
jar	archives java
js	javascript
jse	javascript
lnk	liens symbolique windows
mdb	access
mde	access
msc	fichiers de configuration de la console Windows
msi	fichiers d'installation automatique de windows
msp	patchs d'install windows
mst	Fichiers Visual Test Microsoft
one	Fichiers OneNote
pcd	Fichiers Visual Test
pif	fichiers executable dos
reg	fichiers base de registe
scr	economiseurs d'ecran
sct	composants Windows Script
shs	fichiers script windows
shb	raccourci windows
vb	scripts visual basic
vbe	script visual basic
vbs	scripts visual basic
wsc	composants windows script

extension du fichier	description du type de fichier
wsf	fichiers windows script
...	...

5) Lire également

* Le vol d'identité par des techniques de hameçonnage (ou phishing) par courriel.