SPAM, l'arme des cybercriminels mais pas que !

Bonsoir le Monde !

Mis à jour le 25 avril 2021 (Merci à Sergei)

Un **SPAM** c'est un message non-sollicité !

C'est juste au cas où vous ne le sauriez pas encore ! Rien que la taille de l'article Wikipédia ci-dessus en dit long sur cette sale bestiole !

Jusque là, ça n'a pas l'air bien grave mais en fait:

- Le trafic mail mondial est actuellement composé de plus de 90% de SPAMs et de moins de 10% de mails légitimes => la pollution causée par les mails ? Ce n'est pas à cause de vous !
- 90% des SPAMs sont arrêtés par les protections anti-spam de votre

fournisseur de messagerie électronique (GMX, Gmail, Hotmail/MSN/Outlook.com, Yahoo, Skynet, Voo ou autres)

- Dans les 10% restant qui arrivent dans votre boîte mail, il reste malheureusement encore des SPAMs
- Le **SPAM** ou sa pièce jointe est très (trop) souvent infecté par un **malware** qui peut passer inaperçu pendant très longtemps avant de s'activer et quand il s'active:
    - il peut s'agir de vol d'information personnelle (mot de passe, carte de crédit, téléphone, mails de vos contacts, …) – C'est du **phishing** ou **hameçonnage** !
    - il peut s'agir d'encrypter vos fichiers et de vous demander de payer pour les décrypter – C'est du **ransomware** ou **rançongiciel**
    - il peut s'agir de faire de votre PC un **zombie** aux ordres d'un hacker (ou plus souvent d'une organisation criminelle) et qui risque donc d'être utilisé pour d'autres attaques de plus grande ampleur

      En 2007, on considérait déjà qu'un PC sur cinq était un zombie ! À part parfois un ralentissement, vous ne savez pas que votre PC est un zombie.
    - il peut s'agir de "miner" (fabriquer) de **la crypto-monnaie** comme le Bitcoin. Dans ce cas le ralentissement du PC est souvent plus perceptible…
    - ici, il n'y a pas de limite à l'imagination des cybercriminels !

Le malware éventuellement contenu dans un SPAM ne peut généralement s'activer QUE SI VOUS OUVREZ LE MESSAGE (cliquer dessus sur Windows/MAC/Linux ou le toucher sur Smartphone/Tablette et écrans tactiles) !
Je dis "généralement" car si votre prévisualisation de mail est active, il peut parfois s'activer tout seul comme un grand !

Je dois aussi préciser qu'un malware peut infecter votre PC via d'autres moyens que le mail (nouveau programme, mise à jour, clé USB et disque externe infectés, script reçu en visitant un site web,…) mais le SPAM est de loin le plus courant.
Le futur verra probablement très vite les objets connectés s'ajouter à cette liste…

Si vous poursuivez la lecture, préparez-vous un plateau TV, mettez de la musique douce d'ambiance et accrochez-vous à vos chaussettes ! Ça va fumer !

[Update] Il faut savoir existe plusieurs prévisualisations dans vos interfaces mail !

- **La Prévisualisation des messages** affiche le contenu du message simplement sélectionné (simple-clic ou case à cocher); il ne faut donc pas "l'ouvrir" (double-clic). Cette prévisualisation devrait être désactivée.
- **La Prévisualisation des pièces jointes** affiche le contenu des pièces jointes après le contenu du message sans devoir cliquer sur chacune d'elle pour en voir le contenu. Cette prévisualisation devrait être désactivée.
- **La Prévisualisation des 2 ou 3 premières lignes du message** s'affiche sous le titre dans la liste des messages. C'est la moins risquée des visualisations mais très peu d'interfaces mail la permettent.
- **La visualisation des images externes** (pas en pièces jointes) n'est pas activée par défaut car c'est la plus risquée des fonctions d'affichage des contenus de vos messages. Une image externe peut en effet être infectée et n'est pas passée à travers toutes les protections mises en place par votre fournisseur de service mail. Cette visualisation devrait rester désactivée par défaut et activée seulement manuellement après avoir vérifié le message et pour autant que cet affichage apporte quelque chose à la compréhension du message. Ces images externes sont normalement utilisées à des fins statistiques et on les trouve en général dans les newsletter (celle du blog ne fait pas exception)

1er conseil: fermer/désactiver la prévisualisation des messages ! (cliquez ici pour voir comment faire)

[Update] 2e conseil: fermer/désactiver la prévisualisation des pièces jointes ! (cliquez ici pour les explications)

[Update] 3e conseil: désactiver l'affichage des images externes ! (suivez le guide)

[Update] 4e conseil: activer l'aperçu texte court des messages ! (on y va ?)

Il faut savoir que 98% des attaques informatiques sont causées par l'ouverture d'un mail contenant un malware ! Vous avez bien lu: 98% !

[Update] Les différentes prévisualisations doivent ouvrir le message et/ou les

pièces jointes pour vous en prévisualiser le contenu et il y a donc un risque de se faire infecter par un malware si vous les utilisez.

Il n'est pas toujours facile de savoir si un mail est un SPAM ou non et il faut bien dire que les interfaces d'accès à votre boîte aux lettres électronique ne vous facilitent pas la tâche que ce soit les interfaces Web que vous utilisez via votre navigateur Internet (Firefox, Chrome, Edge, Safari, Opera, Vivaldi, …) ou les interfaces de programmes de mail (Outlook, Thunderbird, Courrier, …)

Si vous avez le moindre doute, n'ouvrez pas le message et menez l'enquête ! J'essaye de vous aider dans cette tâche difficile un peu plus loin dans l'article…

Il y a vraiment TRÈS peu de chance qu'un illustre inconnu ou même une connaissance vous fasse gagner des millions via un mail !
Je sais bien que vous n'avez pas plus de chance de gagner à la loterie mais le ticket de loterie ne vous fera pas plus d'ennui que l'argent perdu pour l'acheter tandis que le mail … The Sky is Not The Limit But Just The Beginning !

Comment désactiver la prévisualisation des messages ?

La prévisualisation des messages peut aussi être appelée l'aperçu ou le volet de lecture ou je ne sais trop quoi d'autre pour désigner la même chose.
Le truc, c'est de désactiver cette trop dangereuse fonctionnalité même si c'est comme par hasard bien confortable [Update] et que les fournisseurs de service mail ont fait de très gros progrès dans la chasse aux cochonneries !

Je vous mets des liens qui expliquent ça pour les cas les plus courants pour ne pas que cet article fasse 200 pages.

Sur PC et tablette, il y a 2 situations (cliquer pour voir les instructions):

1. **Vous lisez vos mails depuis votre navigateur** internet (Firefox, Chrome, Edge, Safari, Opera, Vivaldi, …):
    - Gmail (volet d'aperçu)
    - Yahoo: Paramètres – Mise en page des messages – Liste
    - Hotmail/MSN/Live/Outlook.com: Paramètres – Volet de lecture – Masquer
    - GMX

- Cherchez dans l'aide en ligne pour les autres…

2. **Vous lisez vos mails avec un client de messagerie** (programme Windows, Linux, macOS, …):
    - Outlook (volet de lecture)
    - Windows 10 Mail (prévisualisation de message)
    - Thunderbird (panneau d'affichage des messages ou F8)
    - Mail (Mac 10.11): Cliquer sur la ligne séparant la liste des mails et le message prévisualisé et la tirer à fond vers la droite ou le bas (suivant la vue)
    - Cherchez dans l'aide du programme pour les autres…

Sur Smartphone (Android, IOS et autres), il n'y a pas de prévisualisation car l'écran est trop petit.

[Update] Comment désactiver la prévisualisation des pièces jointes ?

Cette fonctionnalité pourtant bien confortable également reste un risque non-négligeable de se faire infecter par un malware. La plupart des "visualiseurs" n'autorise pas l'exécution de code actif mais de nouvelles méthodes d'infection sont inventées tous les jours par ces emmerdeurs de "hackers black hat" !

1. **Vous lisez vos mails depuis votre navigateur** internet (Firefox, Chrome, Edge, Safari, Opera, Vivaldi, …):
    - **Gmail**: n'affiche qu'une vignette représentant la pièce jointe; il faut cliquer dessus pour l'ouvrir, on ne sait pas désactiver cela.
    - **Yahoo**: n'affiche qu'une vignette représentant la pièce jointe; il faut cliquer dessus pour l'ouvrir, on ne sait pas désactiver cela.
    - **GMX**: ne permet pas la prévisualisation des pièces jointes y compris sous forme de vignette.
    - **Hotmail/MSN/Live/Outlook.com**: n'affiche qu'une vignette représentant la pièce jointe; il faut cliquer dessus pour l'ouvrir, on ne sait pas désactiver cela.
    - **Infomaniak Mail**: n'affiche qu'une vignette représentant la pièce jointe; il faut cliquer dessus pour l'ouvrir, on ne sait pas désactiver cela.
2. **Vous lisez vos mails avec un client de messagerie** (programme

Windows, Linux, macOS, …):

- **Outlook**: menu “Fichiers – Options – Centre de gestion de la confidentialité – Paramètres du Centre de gestion de la confidentialité… – Gestion des pièces jointes – Désactiver l’aperçu des pièces jointes” ! Ouf !
- **Windows 10 Mail**: “Paramètres – Liste des messages – Afficher l’aperçu des images jointes”
- **Thunderbird**: menu “Affichage – Afficher les pièces jointes dans les messages”
- **macOS Mail**: je n’ai pas trouvé comment désactiver cela sur macOS Mail (10.11)

[Update] Comment désactiver l’affichage des images externes ?

La plupart du temps cet affichage est désactivé par défaut car le risque d’infection est plus élevé qu’avec les pièces jointes qui sont passées à la moulinette des protections en tout genre mises en place par votre fournisseur de service mail.

Je vous conseille de n’activer cet affichage qu’après avoir vérifié le message et si cela apporte quelque chose à la compréhension du message.

1. **Vous lisez vos mails depuis votre navigateur** internet (Firefox, Chrome, Edge, Safari, Opera, Vivaldi, …):
   - **Gmail**: “Paramètres – Voir tous les paramètres – Général – Images – Demander confirmation avant d’afficher des images externes”
   - **Yahoo**: “Paramètres – Autres paramètres – Affichage d’un mail – Afficher les images dans les messages – Demander avant d’afficher les images externes”
   - **GMX**: “Paramètres – Contenu Externe – Désactiver le contenu externe dans les e-mails – Sauvegarder”
   - **Hotmail/MSN/Live/Outlook.com**: je n’ai pas trouvé ce réglage.
   - **Infomaniak Mail**: “Paramètres – Réception – Images dans le contenu du message – Me demander”
2. **Vous lisez vos mails avec un client de messagerie** (programme Windows, Linux, macOS, …):

- **Outlook**: menu “Fichiers – Options – Centre de gestion de la confidentialité – Paramètres du Centre de gestion de la confidentialité… – Téléchargement automatique – Ne pas télécharger les images … (2 réglages)”
- **Windows 10 Mail**: “Paramètres – Volet de lecture – Télécharger automatiquement les images et formats de style externes…(2 réglages)”
- **Thunderbird**: menu “Outils – Options – Vie privée et sécurité – Contenu des messages”, décocher “Autoriser le contenu distant dans les messages”
- **macOS Mail**: menu “Mail – Préférences – Présentation”, décocher “Charger le contenu distant des messages”

[Update] Comment activer la prévisualisation des premières lignes du message ?

Cette prévisualisation est la moins risquée de toutes et permet un tant soit peu de vérifier un message avant de l’ouvrir. Il est dommage que toutes les interfaces mail ne possèdent pas ce réglage.

1. **Vous lisez vos mails depuis votre navigateur** internet (Firefox, Chrome, Edge, Safari, Opera, Vivaldi, …):
    - **Gmail**: “Paramètres – Général – Aperçus”; affiche les premiers mots suivant la largeur de l’écran.
    - **Yahoo**: “Paramètres – Autres paramètres – Personnaliser la boîte de réception – Aperçu des messages”; affiche les premiers mots suivant la largeur de l’écran.
    - **GMX**: ce réglage n’est pas présent.
    - **Hotmail/MSN/Live/Outlook.com**: “Paramètres – Afficher tous les paramètres d’Outlook – Courrier – Disposition – Texte d’aperçu des messages”; affiche les premiers mots suivant la largeur de l’écran.
    - **Infomaniak Mail**: ce réglage n’est pas présent.
2. **Vous lisez vos mails avec un client de messagerie** (programme Windows, Linux, macOS, …):
    - **Outlook**: menu “Affichage – Aperçu du message”, choix de 0 à 3

lignes

- **Windows 10 Mail**: “Paramètres – Liste des messages – Texte d’aperçu – Afficher l’aperçu du texte d’un message”; affiche les premiers mots suivant la largeur de l’écran.
- **Thunderbird**: ce réglage n’est pas présent.
- **macOS Mail**: menu “Mail – Préférences – Présentation – Aperçu en mode liste”, choix de 0 à 5 lignes.

Comment un SPAM est-il détecté ?

Votre fournisseur de mail (Gmail, GMX, Yahoo, Microsoft, Apple, Proximus et autres …) fait de son mieux pour éliminer un maximum de SPAM, chacun a sa petite recette et vous n’êtes donc pas tous égaux devant les SPAMs !
Tous les fournisseurs utilisent des anti-spam basés sur une détection automatique s’appuyant sur les SPAMs déjà connus (un peu à la manière des antivirus) mais aussi en évaluant les paramètres les plus courants que l’on trouve dans un SPAM comme le mail de réponse qui ne correspond pas à l’expéditeur (vous recevez un mail de “ami@gmail.com” et quand vous répondez le destinataire est jlkkhkhkj@gmail.com) , le domaine d’expédition ne correspondant pas à celui de l’expéditeur (votre correspondant semble être “ami@gmail.com” mail le mail a en fait été envoyé par un serveur s’appelant “saloperie.fauxdomaine.com” qui n’a rien à voir avec Gmail) et d’autres moins faciles à expliquer.

Cet exercice est très compliqué et délicat à effectuer et il arrive que certains messages légitimes soient déclarés SPAM alors qu’il n’en sont pas et inversement !

Certains services de mail comme Microsoft (Hotmail, MSN, Live, Outlook.com) choisissent la solution facile et déclarent d’office comme SPAM tout mail d’un nouveau correspondant qui ne soit pas un contact existant ! C’est un peu gênant car chaque fois qu’on communique avec un nouveau correspondant, ces mails sont déclarés comme SPAM et il faut penser à aller les rechercher dans le dossier des indésirables !
Si vous ne voulez pas que cela arrive, il faut créer le contact et/ou marquer le message comme acceptable **au niveau de l’interface Web de votre messagerie** (créer le contact dans Outlook 2013/2016/2019 ne suffit pas pour Microsoft; je n’ai pas testé avec Outlook 365).

Thunderbird fait son possible pour notifier votre fournisseur de mail quand vous marquez un message comme acceptable dans le programme vous épargnant la tâche de le faire dans l'interface web…
Thunderbird, encore lui, intègre un filtre anti-spam utilisant "SPAM Assassin" mais il n'est pas activé par défaut.

Chez Gmail et quelques autres, on mouille un peu plus sa chemise et on détermine un score de probabilité de SPAM basé sur l'analyse de l'en-tête du mail (combien de paramètres semblent indiquer qu'il s'agit d'un SPAM) sur base duquel le message vous est:

- soit transmis tel quel (considéré par l'analyse comme non-SPAM)
- soit transmis mais avec [SPAM] ajouté au sujet (l'outil n'est pas certain qu'il s'agisse bien d'un SPAM)
- soit versé au dossier des indésirables (considéré comme SPAM par l'analyse)

L'intelligence artificielle trouve ici un excellent terrain d'application en ajoutant des paramètres comportementaux au calcul du score (ex: l'utilisateur a-t-il déjà ouvert un mail similaire ?) …

Si vous êtes toujours là, bravo et respect ! Je vous offre un peu de détente avec Arobase et les Monty Python qui sont pour quelque chose dans le choix du mot SPAM !

Comment détecter un SPAM vous-même ?

Si vous voyez un mail d'un expéditeur inconnu et/ou avec un titre qui ne soit pas dans votre langue et/ou qui semble très suspect (même si il semble provenir de quelqu'un que vous connaissez), vous êtes très probablement en présence d'un SPAM et il vaut mieux l'effacer immédiatement. Il ne faut surtout pas le lire et encore moins ouvrir la moindre pièce jointe !!!

Si malgré les filtrages mis en place par votre fournisseur de service de messagerie électronique, vous suspectez un message dans votre boîte de réception d'être un SPAM, il faut essayer de mener l'enquête d'abords avec les informations directement visibles (expéditeur, titre, date, etc…) et d'en visualiser l'en-tête complète **AVANT de l'ouvrir** si il devait toujours y avoir un doute !

Visualiser l'en-tête complète d'un message (qui est toujours en anglais) n'est malheureusement pas toujours facile ni très compréhensible mais essayons d'expliquer ça quand même !

L'en-tête complète d'un mail contient toutes les information de routage du message depuis son envoi jusqu'à l'arrivée dans votre boîte de réception !
Tout est malheureusement en anglais mais il y a donc moyen de vérifier d'où il a été envoyé, de qui il vient dans une certaine mesure (jamais sûr à 100%), le timing des opérations et par quels serveurs intermédiaires il est passé…

Apprenez comment déchiffrer l'en-tête complète d'un mail sur Arobase.org: https://www.arobase.org/bases/entetes-detail.htm

La méthode pour afficher l'en-tête d'un mail diffère malheureusement pour chaque fournisseur et pour chaque programme de mail !
Encore un point ô combien dommageable où l'informatique n'est pas à la hauteur de ses promesses !

Essayons de documenter les plus courants (ne lisez que celui que vous employez pour éviter l'indigestion…):

- **Gmail** via navigateur Internet (Firefox, Chrome, Edge, Opera, Vivaldi, …):
  - **Mauvais point chez Gmail, impossible de voir l'en-tête sans ouvrir le message** ! Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
  - Suivez les instructions sur https://support.google.com/mail/answer/29436?hl=fr#zippy=%2Cgmail
  - Google fournit un outil d'analyse d'en-tête de mail sur https://toolbox.googleapps.com/apps/messageheader/ où il suffit de coller le texte de l'en-tête pour obtenir une explication un peu plus claire pour un néophyte.
  - Description de l'en-tête complète Gmail (en anglais) sur https://emailheaders.net/gmail.html
- **GMX** via navigateur Internet (Firefox, Chrome, Edge, Opera, Vivaldi, …):
  - **Mauvais point chez GMX**, idem que chez Gmail, **pas moyen de visualiser l'en-tête sans ouvrir d'abords le message** !

Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
    - Mode d'emploi sur https://support.gmx.fr/email/receiving-and-reading/header.html
    - Ouvrir le message puis cliquer sur le petit "i" à droite du titre et de la date du message
    - GMX fournit également un outil d'analyse (toujours en anglais) via copier/coller sur https://www.ip-adress.com/trace-email-address
    - Description de l'en-tête complète GMX (en anglais) sur https://emailheaders.net/gmx.html
- **Outlook.com, Hotmail, MSN, Live** (Microsoft) via navigateur Internet (Firefox, Chrome, Edge, Opera, Vivaldi, …):
    - **Mauvais point chez Microsoft**, idem que les deux précédents ! **Il faut ouvrir le message avant de pouvoir regarder l'en-tête complète ! Paaaas bon !** Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
    - Ouvrir le message puis cliquer sur les 3 points à droite (menu ellipsis) et choisir Afficher – Afficher la source du message
- **Yahoo** via navigateur Internet (Firefox, Chrome, Edge, Opera, Vivaldi, …):
    - **Bon point pour Yahoo, vous pouvez voir l'en-tête SANS d'abords ouvrir le message !**
    - Cocher la case devant le message pour le sélectionner
    - Cliquer sur le menu "Autres Options" (menu 3 points) et choisir "Afficher le message en texte brut"
    - Description de l'en-tête complète Yahoo (en anglais) sur https://emailheaders.net/yahoo.html
- **Outlook 2019 sur Windows**:
    - **Mauvais point pour Outlook car il faut d'abord ouvrir le message pour voir l'en-tête complète !** Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
    - Ouvrir le message
    - Menu Fichier – Propriétés
    - L'en-tête apparaît dans une toute petite fenêtre (En-têtes Internet) d'où on peut la copier.
- **Thunderbird sur Windows, Mac ou Linux**:

        - **Bon point pour Thunderbird ! Vous pouvez regarder l'en-tête complète d'un mail SANS devoir d'abords l'ouvrir** !
        - Sélectionner le mail (1 seul clic sur le message dans la liste)
        - Ctrl+U (Windows et Linux) ou Cmd+U (Mac) ou Menu "Affichage – Code source du message" (appuyer sur la touche Alt si le menu "Affichage" n'est pas visible)
        - L'en-tête apparaît dans une fenêtre séparée au format texte et peut être facilement sauvée, imprimée et copiée…
        - Description de l'en-tête complète Thunderbird (en anglais) sur https://emailheaders.net/thunderbird.html
- **Courrier** (Windows 10):
        - **Mauvais point pour Courrier ! Il est impossible d'afficher l'en-tête complète d'un mail !**
- **Mail** (macOs 10.11 El Capitan):
        - **Mauvais point pour Mail sur Mac ! Il faut ouvrir le message avant de pouvoir regarder l'en-tête complète ! Paaaas bon !** Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
        - Ouvrir le message
        - Alt + Cmd + U
        - L'en-tête apparaît dans une fenêtre séparée au format texte et peut être sauvée, imprimée et copiée…
- **Gmail** sur Android:
        - **Mauvais point pour Gmail, impossible d'afficher l'en-tête complète ! Risque de contamination par un malware !**
- **GMX** sur Android:
        - **Mauvais point pour GMX car il faut d'abord ouvrir le message pour voir l'en-tête complète !** Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
        - Toucher le message pour l'ouvrir
        - Ne touchez surtout pas "AFFICHER LES CONTENUS EXTERNES" ! (ceci risquerait encore plus de charger le malware)
        - Toucher "AFFICHER LES DÉTAILS" puis toucher "DÉTAIL DU MESSAGE"
- **Yahoo** sur Android:
        - **Mauvais point pour Yahoo Mail, impossible d'afficher l'en-**

tête complète ! Risque de contamination par un malware !

- **Outlook** sur Android:
  - **Mauvais point pour Outlook, impossible d'afficher l'en-tête complète ! Risque de contamination par un malware !**
- **K9 Mail** sur Android:
  - **Mauvais point pour K9 Mail car il faut d'abord ouvrir et télécharger le message complet pour voir l'en-tête complète !**Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !
- **FairEmail** sur Android:
  - **Mauvais point pour FairEmail car il faut d'abord ouvrir le message pour voir l'en-tête complète !**Dommage car si il devait contenir un malware, vous risquez d'être contaminé avant de pouvoir contrôler quoi que ce soit !

Donc pour la détection personnelle de SPAM, il n'y a QUE l'interface Web de Yahoo et le programme Thunderbird qui soient bons !!!!!! Situation gravissime !!!!!
AUCUN des 6 programmes testés sur Smartphone/Tablette Android n'est "safe" de ce point de vue !

Espérons que les développeurs de programmes et interfaces mail intégreront rapidement des outils simples à utiliser car les utilisateurs ne devraient pas être des geeks pour pouvoir vérifier leurs messages !
Lançons un nouveau complot: sont-ce les hackers qui font ces interfaces et programmes mail ?

5e conseil: utilisez Mozilla Thunderbird sur PC, Mac et Linux ! Vous pouvez le télécharger sur https://www.thunderbird.net/fr/ ! Gratuit, facile, sûr et Open Source !

Maintenant que vous avez peut-être réussi à afficher l'en-tête d'un mail, que faut-il regarder ?

Si vous ne savez pas afficher une en-tête de mail avec votre interface ou programme, vous pouvez télécharger et analyser les deux fichiers d'en-tête inoffensifs disponibles sous cet article qui me serviront de support pour les 2 prochains articles de cette série et déjà vous exercer !
Il n'y a aucun risque à ouvrir ces fichiers texte !

Les premiers trucs à regarder sont "**From**" (expéditeur), "**To**" (destinataire = normalement c'est vous), "**Reply-To**" et "**Return-Path**" qui doivent être cohérents !

Le problème est que le "From" qui apparaît tout en haut de l'en-tête n'est pas le bon ! Il faut en fait trouver le premier "From" qui apparaît en début de ligne en commençant pas la fin de l'en-tête !!!!
L'analyse de l'en-tête démarre avec ce "From" et se poursuit en continuant vers le haut du texte de l'en-tête du mail…

En règle générale, le "From", le "Reply-to" et le "Return-Path" doivent être identiques excepté pour une newsletter où le "Return-Path" est souvent une adresse cryptique utilisée comme adresse intermédiaire pour pouvoir faire des statistiques.

Pour les vrais geeks et les impatients, je propose de prolonger l'expérience sur
https://www.ionos.fr/digitalguide/email/aspects-techniques/les-en-tetes-de-mails-pour-demasquer-les-spams/

Pour tous les curieux, je vais continuer cette série prochainement en publiant un 2e article expliquant l'en-tête d'une de mes Newsletters qui est donc un mail légitime et ensuite, dans un 3e et dernier article, j'expliquerai un exemple d'en-tête d'un SPAM envoyé au nom de Colruyt.
Ces 2 futurs articles utiliseront les fichiers disponibles au téléchargement ci-dessous comme support (oui, je sais, je me répète…).

Li P'ti Fouineu vous salue bien !

PS: si vous en voulez encore, voyez toute l'histoire du SPAM chez Arobase.org.

PPS: https://www.safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux

Cliquer sur un des fichiers texte ci-dessous pour l’ouvrir dans un nouvel onglet et tester vous-même une analyse d’en-tête de mail:

Ouvrir En-tête Newsletter Li P’ti Fouineu Gmail dans un nouvel onglet
ou le télécharger

Télécharger
Ouvrir En-tête SPAM Colruyt reçu sur Gmail dans un nouvel onglet
ou le télécharger

Télécharger