# **En-têtes d'emails et d'enveloppes**

## Pourquoi analyser les en-têtes d'emails?

* 1. Interpréter les en-têtes d'emails est une compétence essentielle pour traiter des problèmes liés aux emails ou pour enquêter sur la source d'un message. Les en-têtes d'emails contiennent des informations précieuses sur le chemin emprunté par un email depuis l'expéditeur jusqu'au destinataire. Ils permettent de déboguer les problèmes d'emails tels que la non-livraison et de détecter les fraudes ou le phishing.

Dans cet article, nous allons apprendre à interpréter les données de base des en-têtes d'emails.

## Que sont les en-têtes d'emails?

Un email contient plus de contenu brut que ce que votre client de messagerie (Outlook, Gmail, Thunderbird ou votre interface de messagerie Web) vous montre. Les différents acteurs qui envoient, transportent et reçoivent votre email lui ajoutent du contenu tout au long de son parcours. Ces données sont contenues dans un ensemble de lignes en haut de l'email, au-dessus du contenu, appelées ***en-têtes*** (headers).

**Remarque:** la définition originale de l'en-tête de courrier électronique dans la RFC 822 appelle l'ensemble des en-têtes *l'en-tête*, composé de *champs*. La RFC 2076 plus récente appelle l'ensemble des en-têtes *titre (heading)* et chaque entrée distincte *un en-tête*. Dans le texte suivant, nous suivrons cette dernière convention.

Un en-tête est composé d'un *nom d'en-tête*, de *deux points (:)* et de *valeurs d'en-tête*.

## Un rappel sur SMTP

* 1. Dans un [article](https://blogfr.osix.be/smtp-comment-vos-emails-sont-transportes) précédent, nous avons expliqué le protocole SMTP.

Rappelez-vous: la transmission d'un email d'un agent utilisateur (MUA ou client de messagerie) à un relais de messagerie (MTA) se fait via les commandes suivantes:

* **HELO/EHLO**: utilisé par le client pour s'identifier;
* **MAIL FROM**: utilisé par le client pour identifier l'expéditeur;
* **RCPT TO**: utilisé par le client pour identifier le destinataire;
* **DATA**: introduit le contenu réel de l'email. La fin des données est marquée par une ligne contenant uniquement un point seul (".");
* **QUIT**: ferme la conversation.

## Enveloppe et email

Vous pouvez considérer que le contenu transmis par les différents composants manipulant votre email est divisé en deux parties.

### Partie 1: l'enveloppe

L' ***enveloppe*** montre les données nécessaires au transport de votre email. Dans le courrier traditionnel, c'est l'équivalent de ce qui est écrit à l'extérieur de l'enveloppe dans laquelle vous mettez votre lettre.

On y trouve:

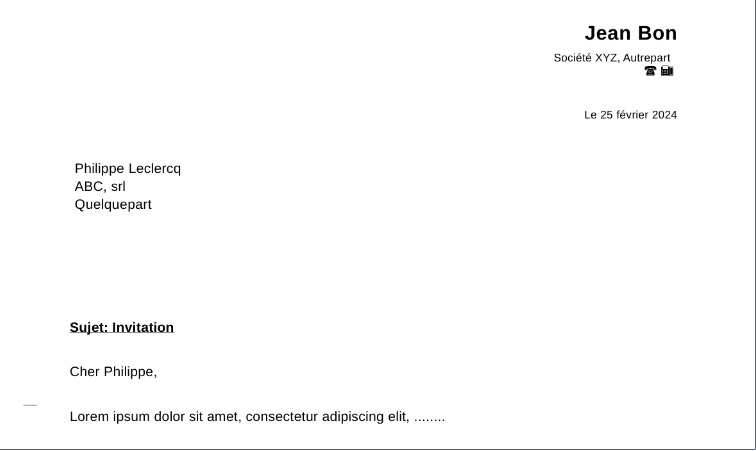
1. le nom et l'adresse postale du destinataire;
2. le nom et l'adresse postale de l'expéditeur, qui peuvent être utilisés par le service postal pour renvoyer le courrier s'il ne peut être délivré;
3. le cachet des services postaux qui ont transporté votre courrier. Chaque bureau de poste pourrait y ajouter son cachet.

Notez que le service postal n'ouvrira pas (normalement) l'enveloppe.

Les en-têtes ***HELO/EHLO***, ***MAIL FROM*** and ***RCPT TO*** sont les en-têtes ***enveloppe***, appartenant à la couche SMTP. Ils *peuvent* être modifiés pendant le trajet de l'email.

### Partie 2: l'email lui-m**ême**

À l'intérieur de l'enveloppe, il y a une lettre avec le contenu réel que vous souhaitez que votre destinataire lise.

La partie ***email*** est similaire, et apparaît après la balise ***DATA*** dans la conversation SMTP.

Un ensemble minimal d'en-têtes d'email contiendra:

* **From:** or **Reply-To:** l'adresse de l'expéditeur
* **To:** l'adresse email du destinataire;
* **Date:** quand il a été envoyé.

## Un exemple **minimal**

Nous allons envoyer un message très simple directement via telnet (sans client de messagerie) à un serveur de messagerie.

telnet mailserver 25

Trying 192.168.50.214...

Connected to mailserver.int.osix.be.

Escape character is '^]'.

220 mailserver ESMTP Postfix (Debian/GNU)

HELO gandalf

250 mailserver

MAIL FROM: Jean.Dupont@mydomain.com

250 2.1.0 Ok

RCPT TO: pleclercq@mydomain.com

250 2.1.5 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

Test.

.

250 2.0.0 Ok: queued as ADDF0224

QUIT

221 2.0.0 Bye

Connection closed by foreign host.

La source complète du message reçu est:

Return-Path: <Jean.Dupont@mydomain.com>

X-Original-To: pleclercq@mydomain.com

Delivered-To: pleclercq@mydomain.com

Received: from gandalf (unknown [192.168.50.31])

by mailserver (Postfix) with SMTP id ADDF0224

for <pleclercq@mydomain.com>; Sun, 16 feb 2025 18:20:04 +0100 (CET)

Test.

Les en-têtes d'enveloppe sont minimes:

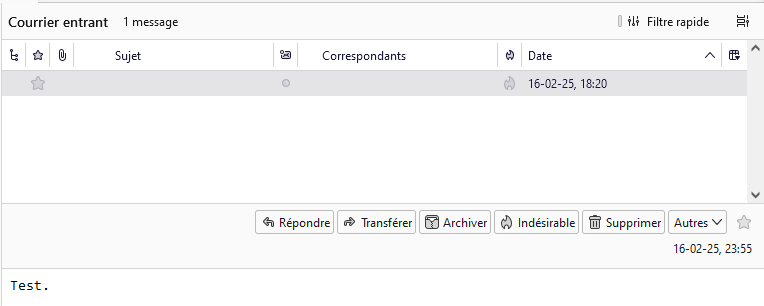
* La RFC 5321 impose que la valeur ***MAIL FROM*** soit copiée par le MTA final dans un en-tête, généralement ***Return-Path:***. C'est le cas ici.
* Le MTA final a également défini l'en-tête ***Delivered-To:*** avec l'adresse du destinataire.
* Un en-tête ***Received:***a été ajouté par le serveur de messagerie, contenant le nom et l'adresse IP de la machine émettrice(*gandalf, 192.168.50.31*), le nom de la machine réceptrice (*mailserver*), l'adresse du destinataire et un horodatage. S'il y a plusieurs étapes, chaque MTA ajoutera son propre en-tête *Received:* pour retracer le parcours du courrier électronique.

Comme expliqué précédemment, ces en-têtes d'enveloppe montrent la partie «transport» du protocole.

Il n'y a pas d'en-têtes d'email ***From:***, ***To:*** ou ***Subject:*** car ils n'étaient pas présents dans la partie *DATA*`

Les en-têtes X- sont des en-têtes propriétaires, non officiels utilisés par les logiciels clients et serveurs.

Voici comment le message s'affiche du côté du destinataire:

Il n'y a pas d'en-tête ***From:***, ***To:*** et ***Subject:*** dans la zone ***DATA***, donc le client de messagerie ne peut pas les copier dans les champs correspondants, et les laisse vides.

## **Un exemple plus complet**

Envoyons un courrier électronique plus complet avec les champs ***From:***, ***To:*** et ***Subject:*** dans la section ***DATA***.

telnet mailserver 25

Trying 192.168.50.214...

Connected to mailserver.int.osix.be.

Escape character is '^]'.

220 mailserver ESMTP Postfix (Debian/GNU)

HELO gandalf

250 mailserver

MAIL FROM: Jean.Dupont@mydomain.com

250 2.1.0 Ok

RCPT TO: pleclercq@mydomain.com

250 2.1.5 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

From: Jean.Dupont@mydomain.com

To: pleclercq@mydomain.com

Subject: Email de test

Deuxième test.

.

250 2.0.0 Ok: queued as B1F47569

QUIT

221 2.0.0 Bye

Connection closed by foreign host.

La source complète du message reçu est:

Return-Path: <Jean.Dupont@mydomain.com>

X-Original-To: pleclercq@mydomain.com

Delivered-To: pleclercq@mydomain.com

Received: from gandalf (unknown [192.168.50.31])

by mailserver (Postfix) with SMTP id B1F47569

for <pleclercq@mydomain.com>; Sun, 16 Feb 2025 18:42:35 +0100 (CET)

From: Jean.Dupont@mydomain.com

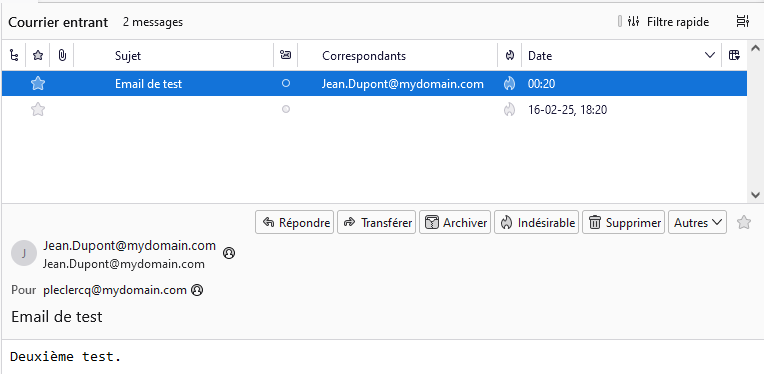
To: pleclercq@mydomain.com

Subject: Email de test

Deuxième test.

Les en-têtes d'email ***From:***, ***To:***et ***Subject:*** ont maintenant été remplis avec les champs correspondants de la partie ***DATA***.

Voici maintenant comment cela s'affiche du côté du destinataire:

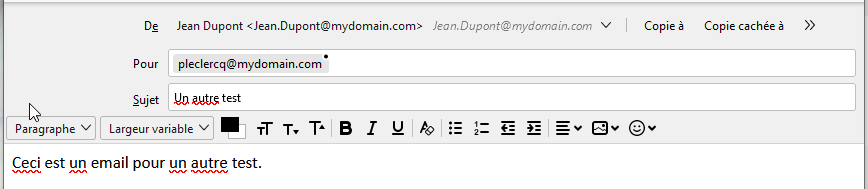
Les champs affichés dans le client de messagerie ont été extraits des en-têtes d'email.

## Un exemple avec un client de messagerie

Utilisons maintenant un client de messagerie classique pour envoyer un email.

Voici les paramètres du client de messagerie de l'expéditeur:

Voici l'email composé:

Et le contenu complet:

Return-Path: <Jean.Dupont@mydomain.com>

X-Original-To: pleclercq@mydomain.com

Delivered-To: pleclercq@mydomain.com

Received: from [192.168.50.215] (unknown) [192.168.50.215])

by mailserver (Postfix) with ESMTP ID 248261CD2

for <pleclercq@mydomain.com>; Mon, 17 Feb 2025 00:29:39 +0100 (CET)

Message-ID: <a84ab8f5-3f11-4d83-842e-959b9a18bdf@mydomain.com>

Date: Mon, 17 Feb 2025 00:29:40 +0100

MIME-Version: 1.0

User-Agent: Mozilla Thunderbird

Content-Language: fr-FR

To: pleclercq@mydomain.com

From: Jean Dupont <Jean.Dupont@mydomain.com>

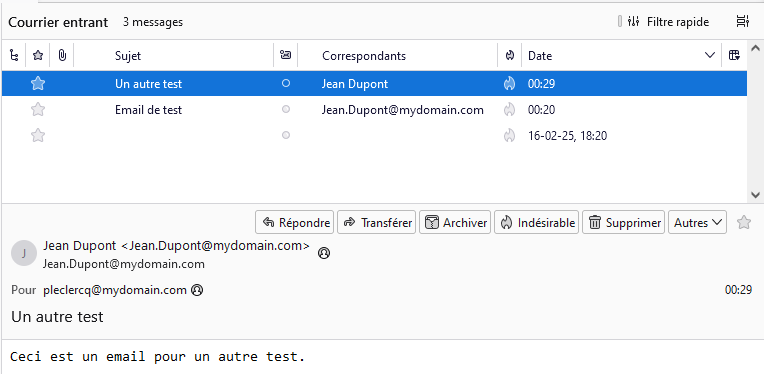
Subject: Un autre test

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 7bit

Ceci est un email pour un autre test.

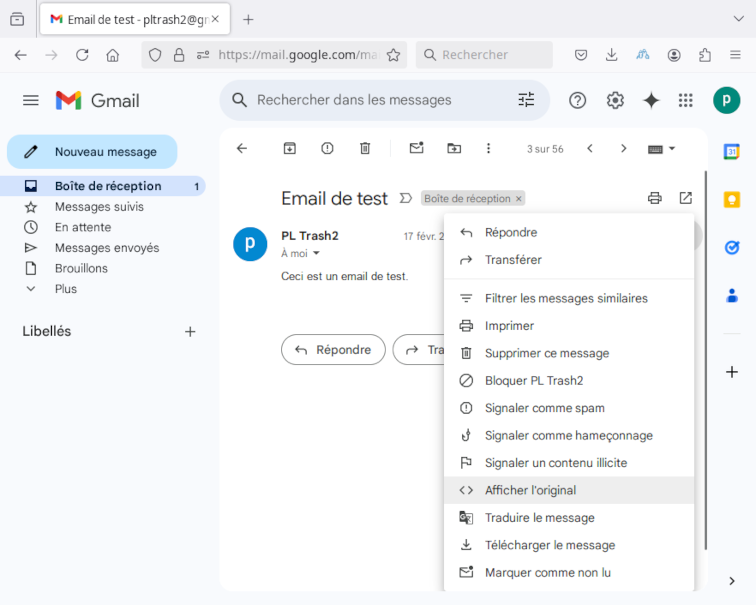
Voici comment il est reçu:

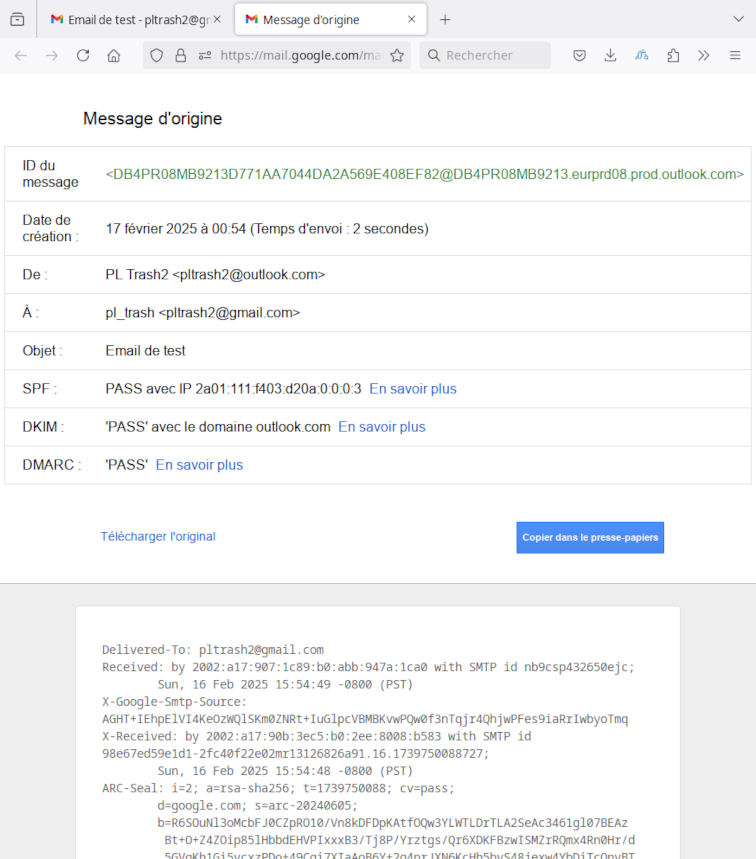
Encore une fois, les champs du client de messagerie ont été remplis à partir des en-têtes ***From:***, ***To:*** et ***Subject:***. Le champ ***De:*** *(Correspondants)* a un aspect plus complet, avec le nom d'affichage en premier et l'adresse entre crochets ensuite.

## Comment afficher les en-têtes

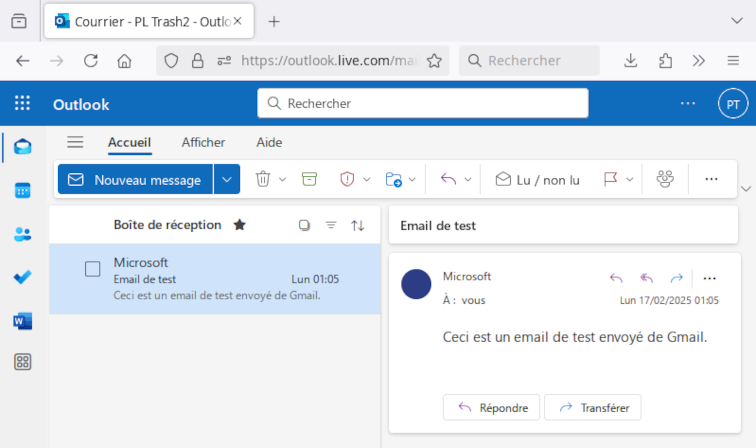
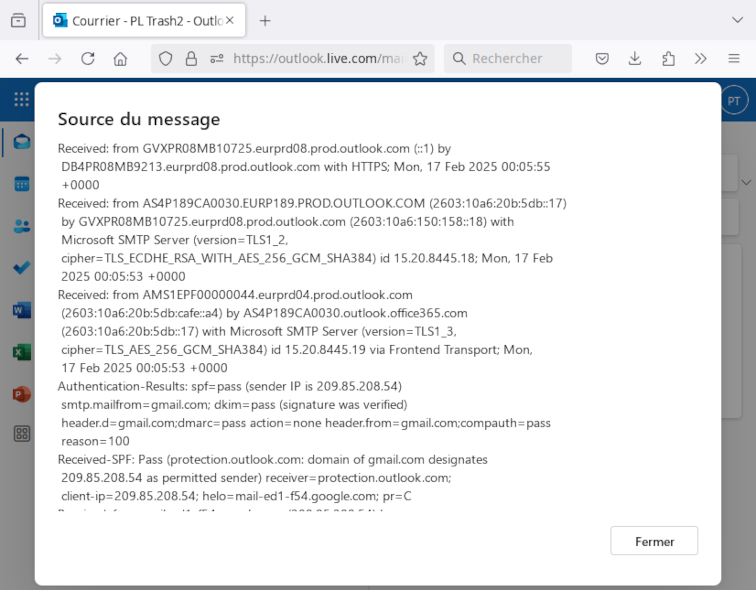
Comme indiqué au début de cet article, et comme indiqué dans les images du client de messagerie ci-dessus, le destinataire ne voit pas par défaut les en-têtes. Cependant, la plupart des clients de messagerie ou des interfaces de messagerie Web ont une option permettant d'afficher le contenu brut reçu, y compris les en-têtes.

### Gmail

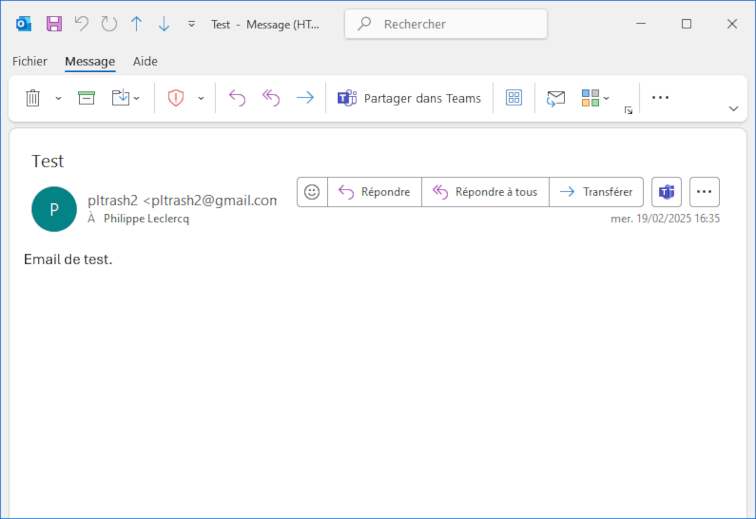
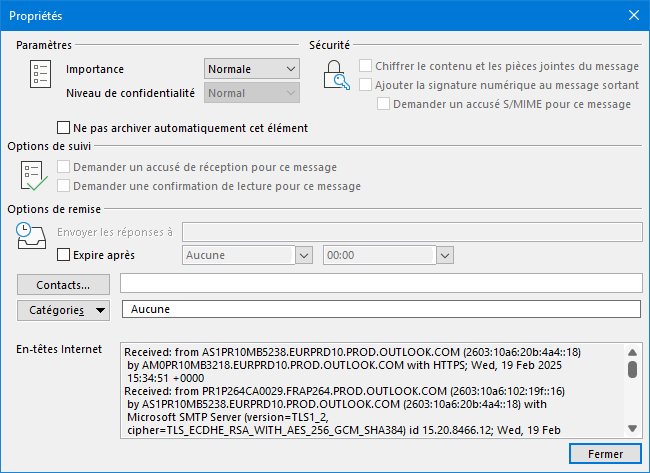
1. Cliquez sur l'email que vous souhaitez analyser, cliquez sur les trois points dans le coin supérieur droit et sélectionnez l'option ***Afficher l'original***.
2. Un nouvel onglet s'ouvre dans le navigateur, affichant l'intégralité du contenu brut de l'email. Vous pouvez le copier avec le bouton ***Copier dans le presse-papier***.



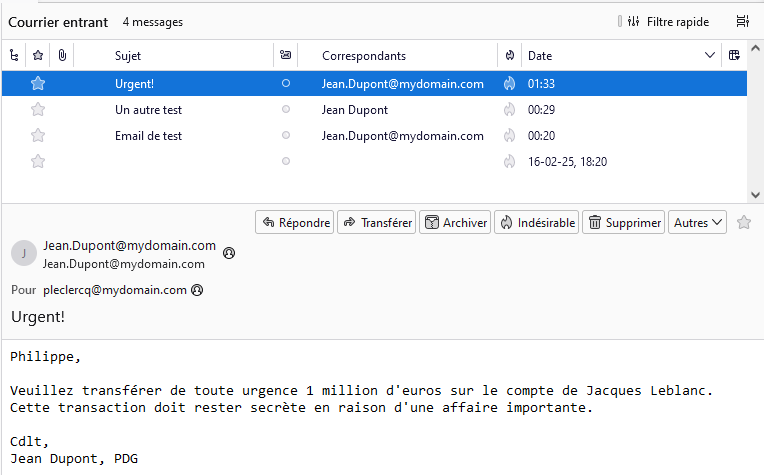
### Microsoft Office 365

1. Sélectionnez l'email que vous souhaitez analyser dans le volet de gauche.
2. Cliquez sur les trois points dans le coin supérieur droit et sélectionnez l'option ***Afficher -> Afficher la source du message***.
3. Une nouvelle fenêtre s'ouvre dans le navigateur, affichant l'intégralité du contenu brut de l'email.
4. Vous pouvez cliquer dans la fenêtre, sélectionner tout le texte avec <CTRL>-A, le copier avec <CTRL>-C et le coller dans une autre application (comme un éditeur de texte) avec <CTRL>-V.

### Outlook

1. Double-cliquez sur l'email que vous souhaitez analyser.
2. Cliquez sur ***Fichier -> Informations -> Propriétés***.
3. Une fenêtre de propriétés apparaîtra, affichant les en-têtes Internet dans la zone de texte inférieure.
4. Pour copier les en-têtes, cliquez dans la zone de texte, sélectionnez tout le texte avec <CTRL>-A, copiez-le avec <CTRL>-C et collez-le dans une autre application (comme un éditeur de texte) avec <CTRL>-V.

## Détection d'emails potentiellement frauduleux en analysant les en-têtes

Imaginez maintenant que vous receviez l'email suivant:

Il s'agit d'un processus inhabituel, vous êtes surpris. Vous essayez d'appeler Jean pour confirmation, mais il est à l'étranger et injoignable. Que faire ensuite?

Eh bien, regardons les en-têtes:

Return-Path: <attacker@evil.corp>

X-Original-To: pleclercq@mydomain.com

Delivered-To: pleclercq@mydomain.com

Received: from attacker?evil.corp (unknown [192.168.50.31])

by mailserver (Postfix) with SMTP id E03B81E92

for <pleclercq@mydomain.com>; Mon, 17 Feb 2025 01:29:40 +0100 (CET)

From: Jean.Dupont@mydomain.com

To: pleclercq@mydomain.com

Subject: Urgent!

Philippe,

Veuillez transférer de toute urgence 1 million d'euros sur le compte de Jacques Leblanc.

Cette transaction doit rester secrète en raison d'une affaire importante.

Cdlt,

Jean Dupont, PDG

Hmm. ***Return-Path: <attacker@evil.corp>***.

Ceci n'a **PAS** été envoyé depuis le compte de Jean, mais par un pirate usurpant son adresse. Pas de chance pour lui, vous l'avez repéré. **Bravo!**

(Au fait, il s'agit d'un exemple d'abus fréquent appelé fraude au président ou BEC - Business Email Compromise. Selon la Barclays Bank et le [Treasurer Magazine](https://www.treasurers.org/hub/treasurer-magazine/ceo-fraud-targeting-least-400-firms-day), la fraude au président cible plus de 400 entreprises par jour, dont 40 % sont des petites et moyennes entreprises, entraînant des pertes de plus de 3 milliards de dollars).