

Un mail suspect

1- Ce que je ne dois pas faire

- Je ne répons pas
- Je ne clique pas
- Je ne scanne pas
- Je n'affiche pas les images

2- Je vérifie

La provenance du message, selon le logiciel de mail utilisé :

- Click droit, afficher la source du message
- Menu afficher la source
- Clique sur le nom de l'expéditeur pour lire l'adresse mail
- Regarde le menu pour trouver les fonctions afficher la source ou enregistrer le message
- Je trouve l'adresse mail de l'expéditeur et l'adresse mail de réponse de l'expéditeur
- Je trouve l'adresse IP de l'expéditeur
- Dans l'adresse email de l'expéditeur je trouve le nom de domaine

Pour trouver la source du message dans OUTLOOK, j'ouvre le message en double cliquant dessus

The screenshot shows an Outlook email window. The top ribbon has tabs for 'FICHIER' and 'MESSAGE'. The 'MESSAGE' tab is active, showing options like 'Ignorer', 'Courrier indésirable', 'Supprimer', 'Spam', and 'Pas Spam'. A yellow callout box points to the 'Spam' button with the text: 'Je peux designer le message comme un spam. Mon service informatique en centrale vérifiera'. Below the ribbon, the email header shows the sender 'Aurélien Lechevallier <aurelien.lechevalier1@gmail.com>' and the recipient 'À laurent.testard@diplomatie.gouv.fr'. A yellow callout box points to the sender's email address with the text: 'Je vérifie l'adresse mail de l'émetteur'. Below the header, there is a message attachment 'Message aurelien_lechevallier.vcf (265 o)'. A yellow callout box points to the attachment with the text: 'Je n'ouvre pas les pièces jointes'. The main body of the email contains the following text: 'Bonjour à l'ensemble de mes collaborateurs', 'Je vous prie de recevoir mes meilleurs vœux en cette nouvelle année 2022, à vous, ainsi qu'à vos proches', 'Vous retrouverez l'ensemble des informations concernant l'Ambassade en scannant le QR code disponible dans ma signature.', 'Encore un grand merci pour votre participation', 'Bien cordialement, Aurélien Lechevallier', and a blue link 'Retrouvez moi sur internet'. A large red 'X' is drawn over the link and the QR code below it. A yellow callout box points to the QR code with the text: 'Je ne clique pas sur le ou les liens' and 'Je ne scanne pas le QR code'.

Lorsque le mail est ouvert je clique dans **fichier et propriétés**

The screenshot shows the 'Informations' (Information) menu of an email client. The menu items are: Informations, Enregistrer, Enregistrer sous, Enregistrer les pièces jointes, Imprimer, Fermer, Compte Office, and Options. The 'Propriétés' (Properties) option is circled in red. The main content area shows the email title 'Séminaire de l'ambassade' and several actions: 'Définir les autorisations', 'Déplacer vers un dossier', 'Renvoyer le message et rappeler', and 'Propriétés'. The 'Propriétés' action is highlighted with a red circle.

J'aurai ainsi **accès à la source du mail** et je peux lire les éléments techniques réels. Je peux sélectionner le texte de la source et le copier dans un éditeur de texte comme Notepad. J'ai sauvegardé les preuves (CTRL A et CTRL C), je peux enregistrer le message ou l'envoyer en pièce jointe si besoin.

The screenshot shows the 'Propriétés' (Properties) dialog box. The 'Paramètres' (Parameters) section includes 'Importance' (Normale) and 'Niveau de confidentialité' (Normal). The 'Sécurité' (Security) section includes checkboxes for 'Chiffrer le contenu et les pièces jointes du message', 'Ajouter la signature numérique au message sortant', and 'Demander un accusé S/MIME pour ce message'. The 'Options de suivi' (Tracking Options) section includes checkboxes for 'Demander un accusé de réception pour ce message' and 'Demander une confirmation de lecture pour ce message'. The 'Options de remise' (Delivery Options) section includes 'Envoyer les réponses à' (aurelien.lechevallier@diplomatie.gouv.fr) and 'Expire après' (Aucune, 00:00). The 'En-têtes Internet' (Internet Headers) section is circled in red and contains the following text: Return-Path: <aurelien.lechevalier1@gmail.com>, X-Envelope-To: laurent.testard@PRY01EX00001.PRY01.diplomatie.gouv.fr, X-Spam-Status: No, hits=0.0 required=5.0 tests=TOTAL_SCORE: 0.000, X-Spam-Level: Received: from AZ011MX01C11.diplomatie.gouv.fr ([10.1.140.48]) by PRY01EX00001.diplomatie.gouv.fr (Kerio Connect 8.5.3 patch 1). The 'Fermer' (Close) button is visible at the bottom right.

Je dois vérifier le mail d'origine, tel que je l'ai reçu et pas dans un mail renvoyé ou forwardé, car je perdrais les éléments techniques de preuves.

- Je vérifie l'adresse IP de l'expéditeur et sa localisation, <https://iplookup.flagfox.net/>
- Je vérifie le nom de domaine figurant dans la ou les adresse mail de l'expéditeur, ce doit être DIPLOMATIE.GOUV.FR, la langue employée, la localisation, les dates de création, de renouvellement, le registrant et le registrar, <https://www.godaddy.com/en-za/whois>
- Je dois vérifier les url présentes dans le corps du message, sous la forme du lien que je peux copier, <https://mxtoolbox.com/MXLookup.aspx>
- ou sous la forme du QR code que je peux décoder en sauvegardant l'image du QR code, <https://4qrcode.com/scan-qr-code.php>

3- Je sauvegarde

- Je peux sauvegarder le mail en envoyant le message d'origine en pièce jointe, forward as attachment
- Je peux copier tout le texte de la source du message et coller ce texte dans un éditeur de texte, comme Notepad par exemple et enregistrer ce texte
- Je peux sauvegarder le message si le logiciel me le permet dans ses fonctionnalités
- Pour toutes les sauvegardes de message, l'extension EML doit être privilégiée.

4- J'avise, si je pense que le mail est frauduleux

- Mon service informatique, je place le mail en spam
- La personne victime, si je la connais
- Cybermalveillance sur le site <https://www.cybermalveillance.gouv.fr/>
- Le site web s'il s'est fait pirater