Un mail suspect

1- Ce que je ne dois pas faire

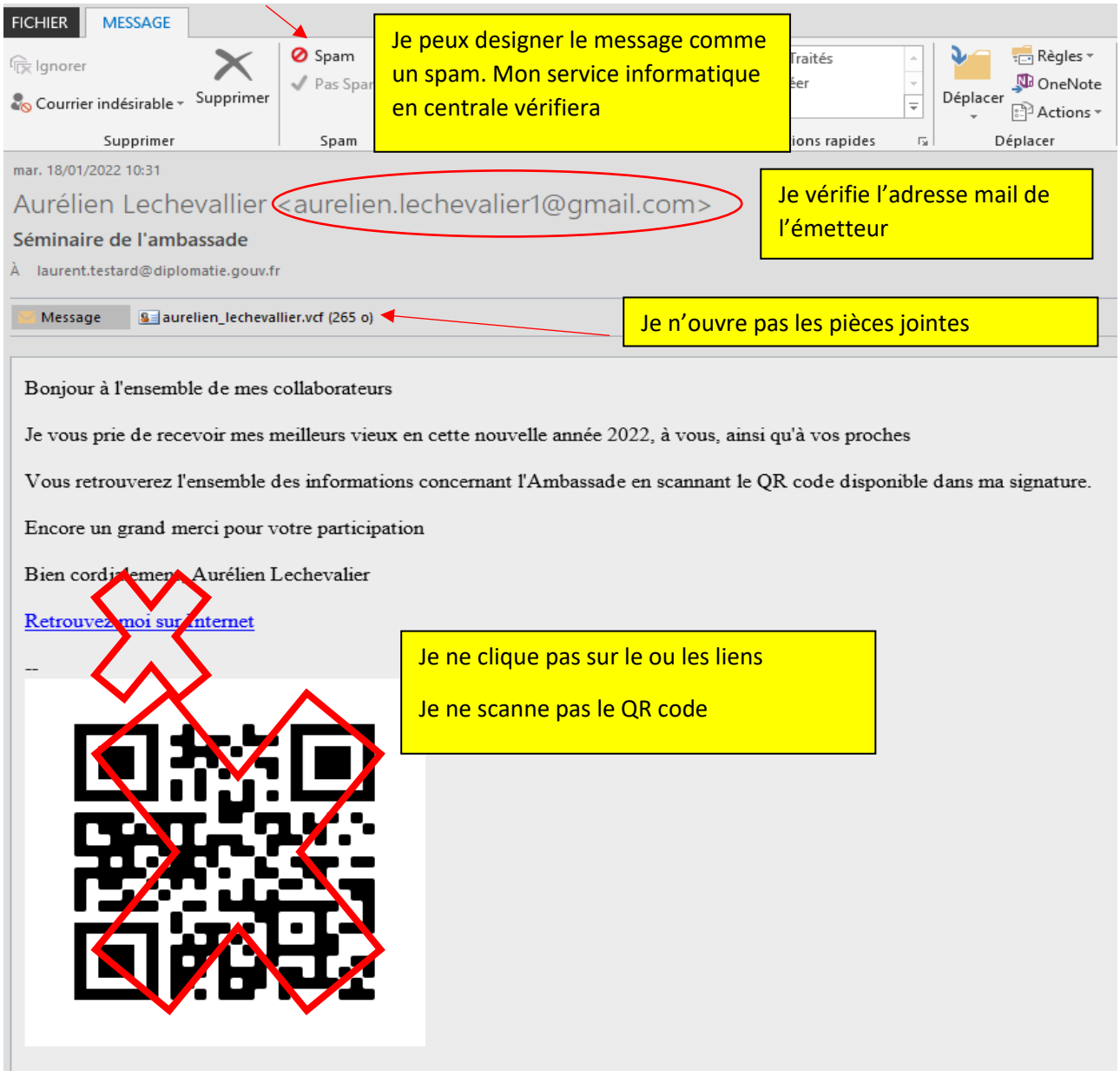
Je ne réponds pas
Je ne clique pas
Je ne scanne pas
Je n'affiche pas les images

2- Je vérifie

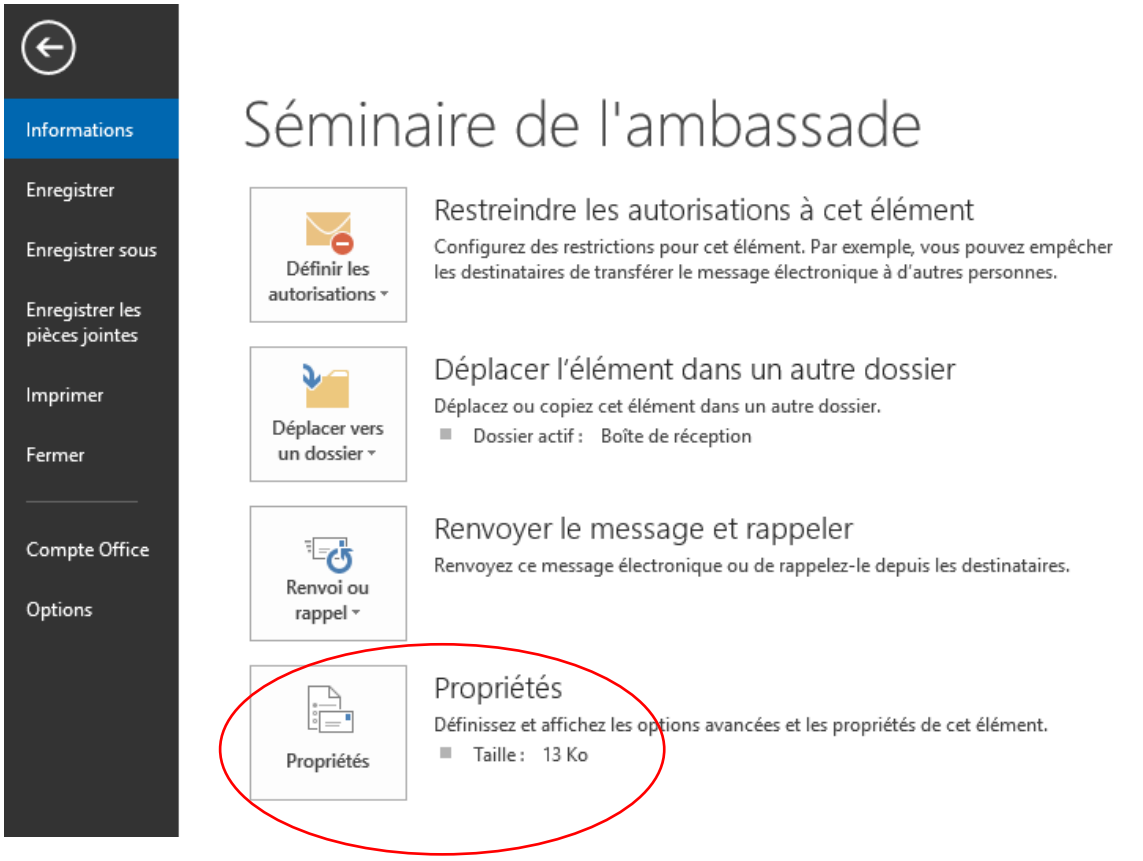
La provenance du message, selon le logiciel de mail utilisé :

- 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

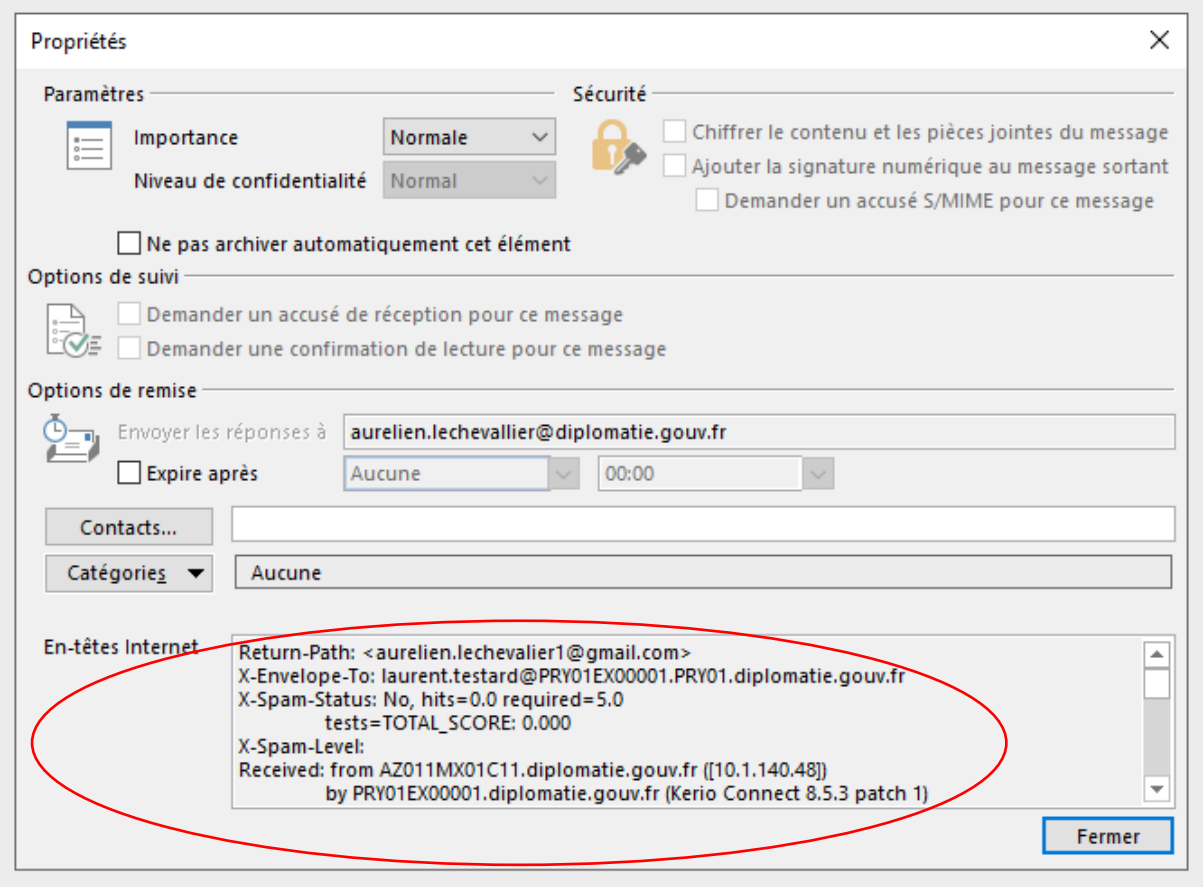
Pour trouver la source du message dans OUTLOOK, j'ouvre le message en double cliquant dessus



Lorsque le mail est ouvert je clique dans fichier et propriétés



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.



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