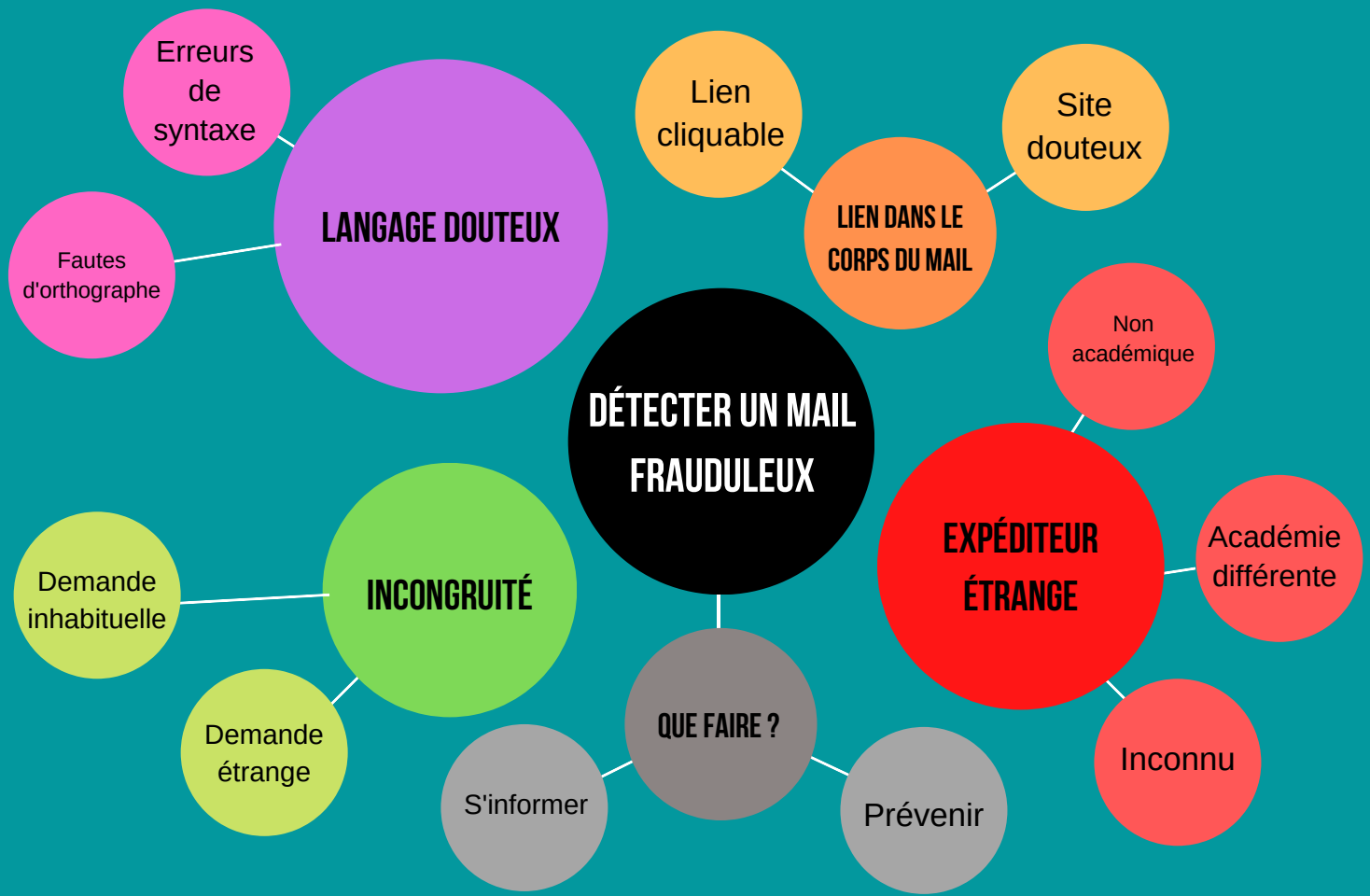
COMPRENDRE LE PHISHING

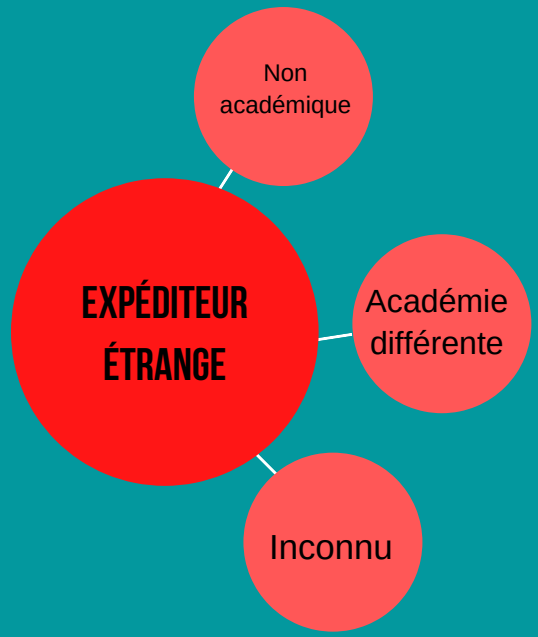
± "Le "phishing" (ou hameçonnage) est une technique d'escroquerie ou de fraude qui vise à pirater vos données et vos identifiants.

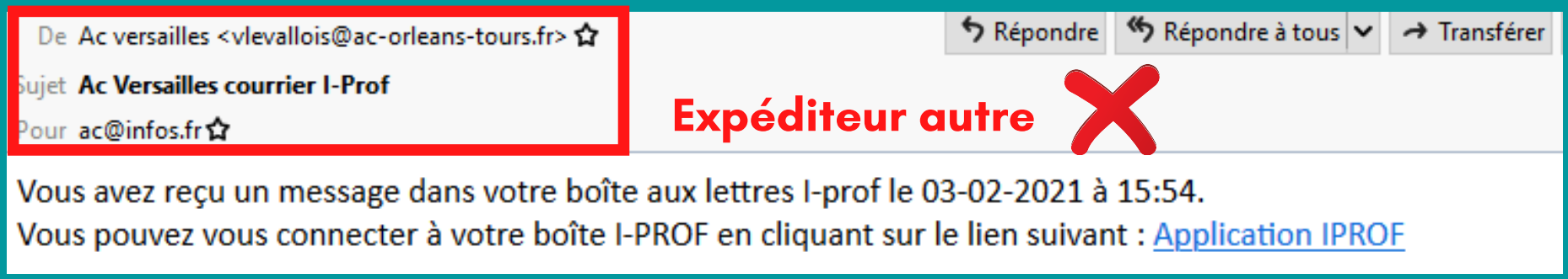


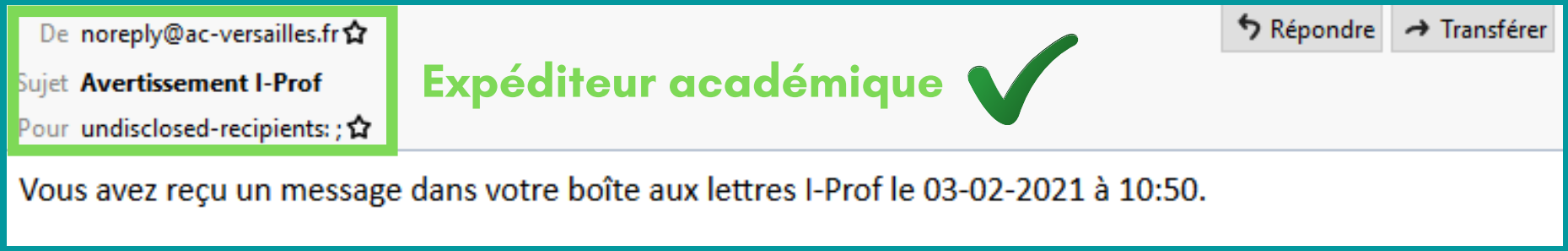
EXPÉDITEUR

Les expéditeurs qui n'ont pas d'adresse institutionnelle (ac-versailles, gouv.fr....) ou avec une adresse totalement inconnue avec des caractères étranges ou des chiffres, constituent un indice crucial.

Vérifiez toujours l'expéditeur.

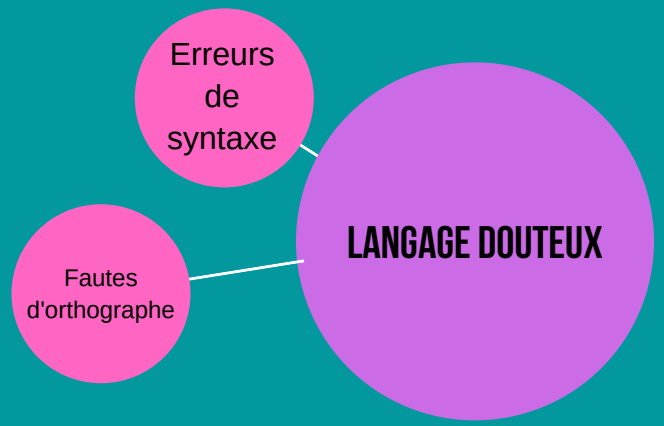






LANGAGE DOUTEUX ?

Si le message contient des erreurs d'orthographe manifestes, une syntaxe aléatoire ou des phrases qui ont peu de sens (termes techniques trompeurs)..., c'est un indice non négligeable d'un mail frauduleux.



"Client Webmail,"

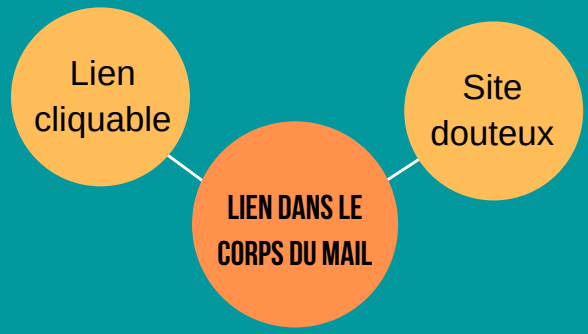
"Si après 72 heures, vous ne parvenés pas a mettre a niveau votre compte, ..."

"Vous avez épuisé l'espace de bande passante de 2000 Mo de votre compte de messagerie..."

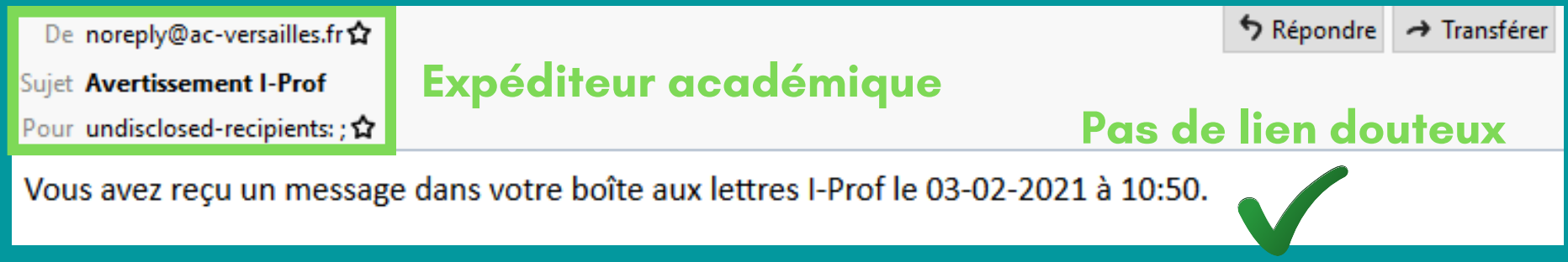
"Cher utilisateur Versailles..."

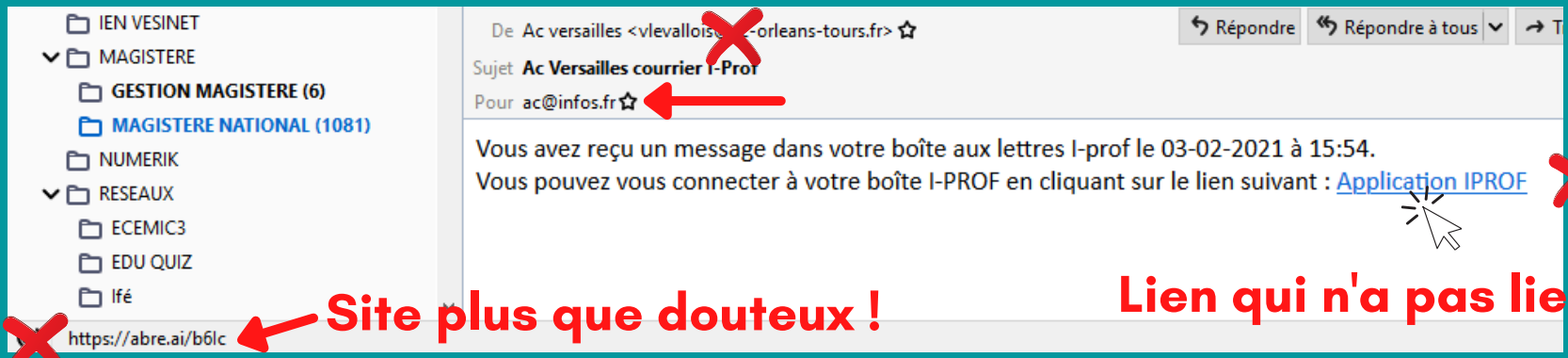
M. le modérateur Mail

LIEN



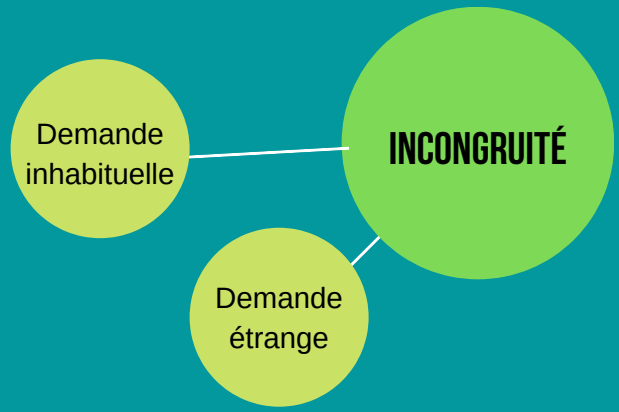
Si le message contient un lien cliquable, il constitue déjà en soi une menace.
Avant de cliquer, assurez-vous du lien. Il suffit la plupart du temps de déplacer le curseur avec la souris sur le lien, pour voir apparaître l'adresse du site vers lequel il pointe.





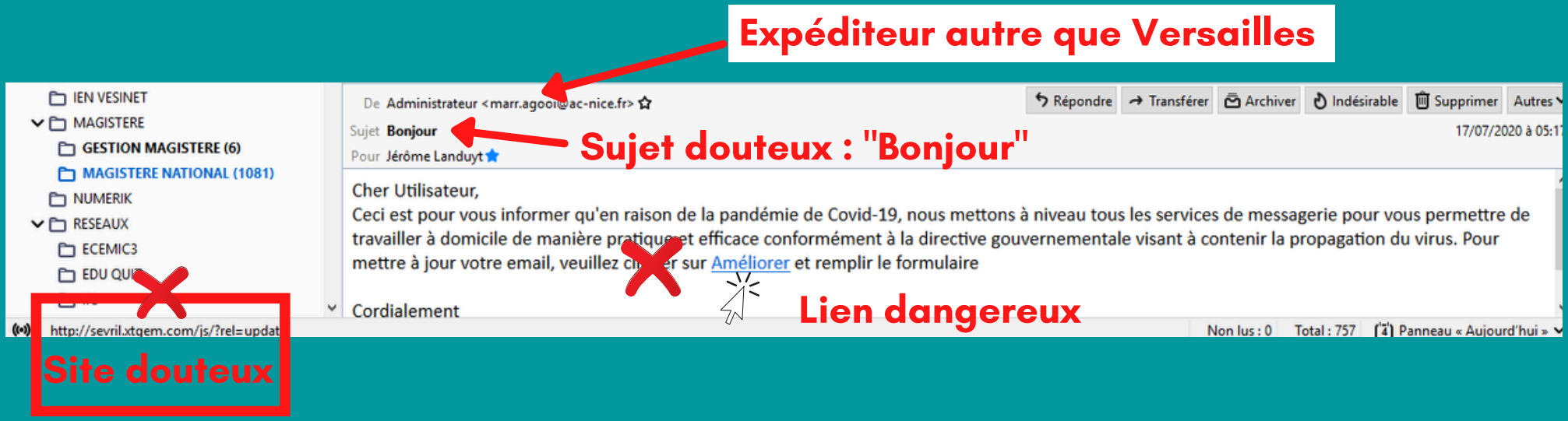
https://abre.ai/b6lc

INCONGRUITÉ



La demande est inhabituelle, étrange ou contient des éléments inconnus, commencez par douter ! Surtout quand le Sujet (ou Objet) n'a rien à voir avec le corps du message.

Un bon exemple de message frauduleux qui contient presque tous les indices d'hameçonnage :



QUE FAIRE ?

En premier lieu, il convient, au moindre doute, de ne pas cliquer sur les liens présents dans le corps de mail ou même de répondre. Ensuite, pensez à prévenir la cellule du rectorat qui gère le phishing.

ACADÉMIE DE VERSAILLES
Liberté
Égalité
Fraternité

Infographie Arena

Vidéo MN78

Podcast DSDEN