

Procédure Phishing

Procédure de gestion des e-mails suspects

La vigilance de chacun est la première ligne de défense de notre sécurité informatique. Voici la marche à suivre en cas de doute sur un message reçu.

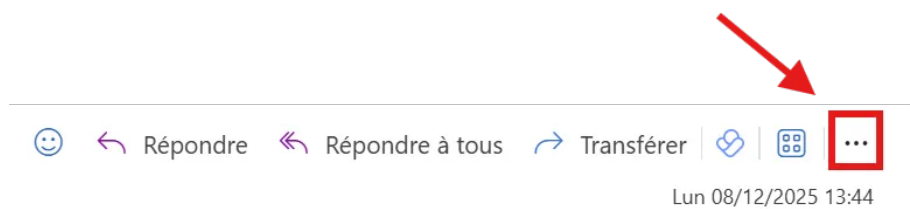
Comment signaler un e-mail suspect ?

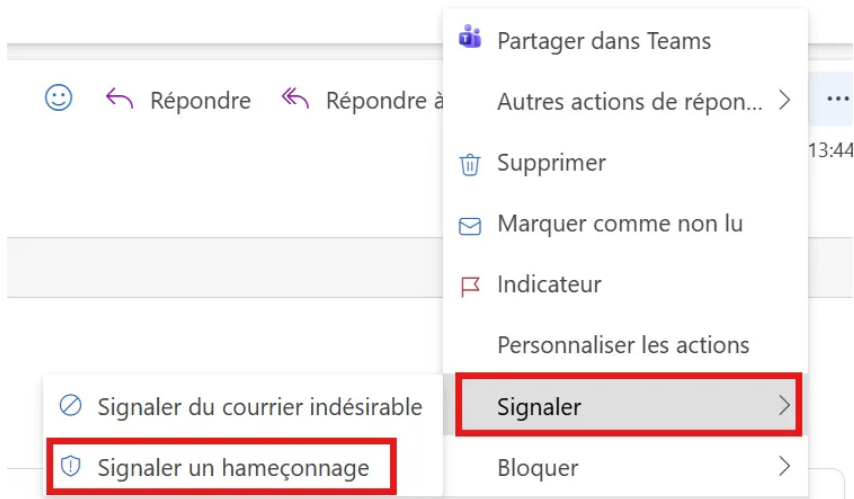
Si vous recevez un e-mail qui vous semble douteux (expéditeur inconnu, demande urgente, lien inhabituel).

- **Le signalement intégré** : Utilisez la fonction "Signaler l'e-mail comme phishing" directement dans votre boîte de réception. Cela nous transmet automatiquement une copie pour analyse.

Note importante : Même si vous savez que des collègues ont déjà effectué le signalement, transférez le **nous systématiquement**. Certaines campagnes de phishing utilisent des liens personnalisés et uniques pour chaque utilisateur. Pour neutraliser totalement la menace, nous devons identifier et bloquer toutes les variantes du message.

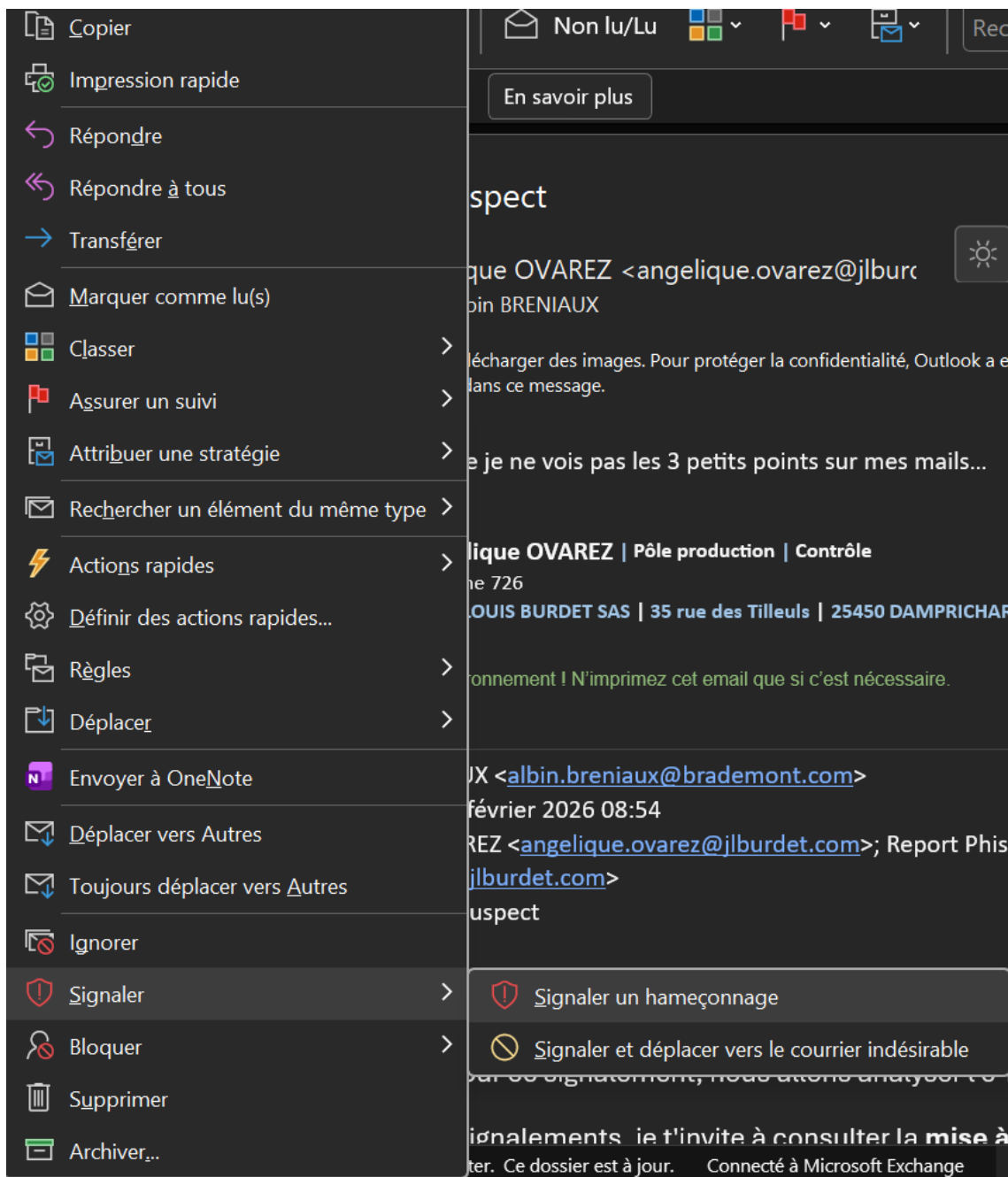
New Outlook





Outlook Classic

Faites un clique droit sur le mail en question puis Signalez le.



Ce système viendra alimenter automatiquement une mise à jour du filtre de nos différentes boîtes de messagerie

L'équipe interne reçoit une copie de ce message, l'étudiera et si besoin reviendra vers vous.

Que faire en cas d'interaction avec un phishing ?

Si vous avez cliqué sur un lien, ouvert une pièce jointe ou saisi vos identifiants par erreur, **contactez immédiatement le service informatique.**

Une intervention rapide est cruciale pour :

- **Sécuriser votre compte** : Réinitialisation immédiate de votre mot de passe.
- **Limiter la propagation** : Blocage définitif de la menace pour l'ensemble de l'entreprise.
- **Investiguer** : Vérifier si une intrusion ou un vol de données a déjà eu lieu sur votre session.

“ **Rappel** : La réactivité est la clé. Il vaut mieux un signalement pour rien qu'une intrusion non détectée.