Signaler un courriel malicieux MS Outlook

MISE EN CONTEXTE:

Certains messages, reçus dans votre boîte courriel, peuvent parfois s'avérer être des tentatives d'hameçonnage ou du contenu indésirable qui pourraient ne pas être détectés par nos systèmes.

Il existe 2 façons de voir un courriel d'hameçonnage :

1. un véritable courriel d'hameçonnage envoyé par un acteur malveillant qui tente de vous soutirer de l'information ou de vous faire prendre une action.
2. une simulation d'hameçonnage dans le cadre de nos campagnes de sensibilisation.

Pour ces deux, le Cégep vous demande de les signaler, en prenant bien soin **de ne pas exécuter les actions demandées dans le courriel**.

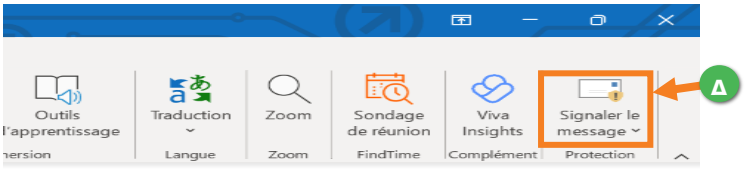
Cette procédure remplace le besoin de créer un billet Synapse ou d'effectuer un appel au Centre de services pour signaler un courriel suspect. Si vous pensez avoir exécuté une action demandée dans le courriel, vous devez, rapidement et obligatoirement, ouvrir un billet Synapse.

Malgré le filtrage de courriels, vous n'êtes pas entièrement à l'abri de recevoir des courriels frauduleux. Si vous ne connaissez pas l'expéditeur d'un courriel, nous vous recommandons de ne pas cliquer sur les liens contenus dans le courriel et de ne pas ouvrir les fichiers qui y sont joints.

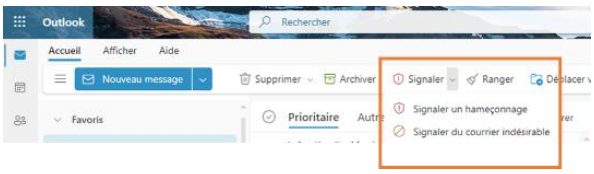
DÉMARCHE :

Lorsque vous recevez un courriel suspect (hameçonnage ou courriel indésirable) dans votre boîte de réception Outlook ou Outlook pour le Web, vous devez rapidement signaler celui-ci.

A. Lorsque vous êtes sur le courriel suspect en question, vous devez cliquer sur le bouton **Signaler le message.**

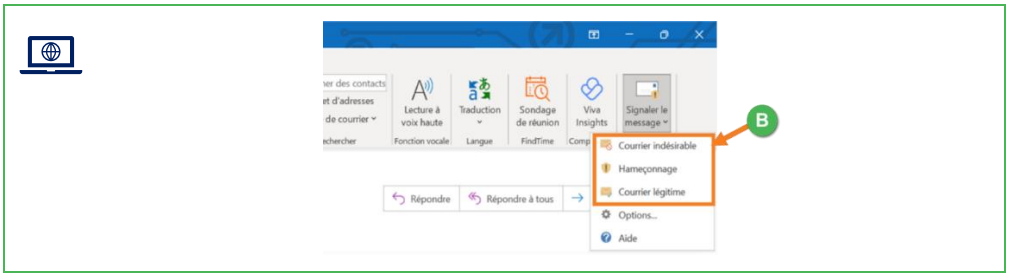


Le bouton de signalement sur Outlook pour le Web peut ressembler à ceci.



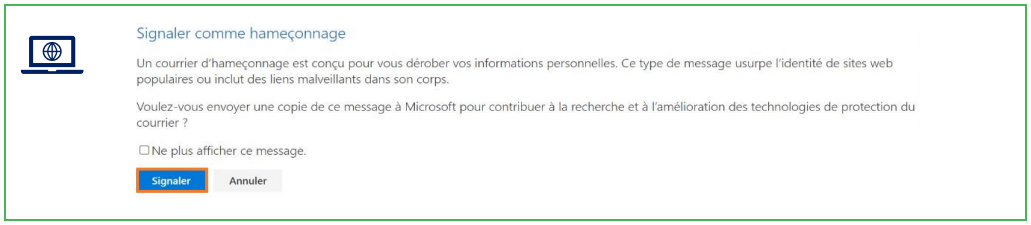
Date de mise à jour : 2023-02-08

B. Cliquer sur l'une des options selon le classement du courriel :

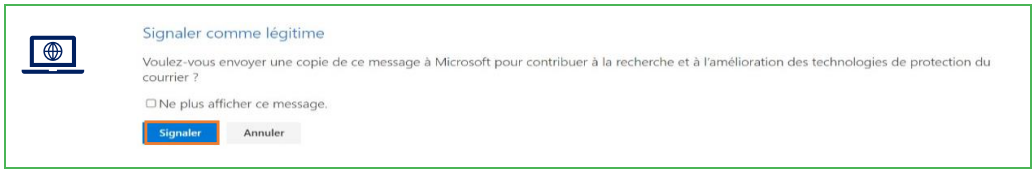


- **Courrier indésirable ou spam** si vous jugez qu'il s'agit d'un courriel indésirable, c'est-à-dire une communication électronique non sollicitée dans votre boîte de réception (publicité, campagne non sollicitée, etc.)

- **Hameçonnage** ou **Phishing** si vous jugez qu'il s'agit d'un message qui se veut légitime, mais qui a tout l'air d'une usurpation d'identité. C'est une personne qui vous envoie un message en se faisant passer pour une institution financière ou une entreprise afin de vous induire en erreur ou de vous inciter à leur révéler des informations sensibles.



- **Courrier légitime** si vous jugez après avoir regardé tous les éléments du courriel comme le nom complet, l'adresse courriel, la signature, le logo, le contenu du message, etc. qu'il s'agit bien d'un expéditeur connu. Ce type de courriel légitime se classe souvent dans votre dossier des courriels indésirables.



C. Un message vous demandera si vous souhaitez envoyer une copie du message à Microsoft. Cette étape est facultative, vous pouvez répondre par l'affirmative ou non.

Fin de la procédure

Date de mise à jour : 2023-02-08