# COVID-19: Alerte aux courriels frauduleux

## Comment reconnaître les courriels d'hameçonnage ?

| | Comment reconnaître les courriels frauduleux sur le thème du coronavirus? | Ce qu'il faut faire? |
|---|---|---|
| **Demandes de renseignements personnels en ligne** | Un courriel, ayant pour sujet/ titre « Coronavirus », qui recherche des renseignements personnels comme votre numéro de sécurité sociale et/ou vos identifiants est une arnaque d'hameçonnage.<br><br>Les organismes légitimes, publics et privés, ne demanderont jamais cette information par courriel ou même par téléphone. | Ne jamais répondre au courriel avec vos données personnels. |
| **Vérifier l'adresse du courriel ou le lien** | Vous pouvez vérifier un lien en passant votre souris sur l'URL pour savoir où il mène.<br><br>Parfois, il est évident que l'adresse Web n'est pas légitime. Mais soyez conscient que les hameçonneurs peuvent créer des liens qui sont presque des sosies parfaits comme ceux des adresses légitimes. | Si vous n'êtes pas sûr à 100% de l'authenticité du lien de redirection, ne cliquez pas dessus |
| **Attention aux fautes d'orthographe et de grammaire** | Si un courriel comprend des erreurs d'orthographe, de ponctuation et de grammaire, il est très probable qu'il s'agisse d'un courriel d'hameçonnage. | Veuillez ne pas agir sur le courriel jusqu'à ce que vous avez un moyen de contre-vérifier et de confirmer son authenticité. |
| **Rechercher des salutations génériques** | Il est peu probable que les courriels d'hameçonnage utilisent votre nom. Des salutations comme « Cher monsieur ou madame » indiquent qu'un courriel pourrait ne pas être légitime. | Veuillez ne pas agir sur le courriel jusqu'à ce que vous avez un moyen de contre-vérifier et de confirmer son authenticité. |
| **Évitez les courriels qui vous obligent à « agir maintenant » ou donnent un sentiment d'urgence de quelque façon que ce soit pendant cette période** | Les courriels d'hameçonnage tentent souvent de créer un sentiment d'urgence ou d'exiger que vous preniez des mesures immédiates. Le but est de vous faire cliquer sur un lien et de fournir des informations personnelles sur place. | Ne divulguez jamais de renseignements personnels à ce type de courriels et signalez ces courriels comme des « spam » dans votre boîte aux lettres. |

# COVID-19: Alerte aux courriels frauduleux

**Exemples de courriels frauduleux que vous pourriez recevoir pendant cette période pandémique :**

### Alertes par courriel

Les courriels qui semblent provenir d'organisations comme le CDC (Centre pour le contrôle et la prévention des maladies) ou l'OMS (Organisation mondiale de la santé) où ils pourraient prétendre d'établir un faux lien vers une liste de cas de COVID-19 dans votre région.

### Courriels sur les conseils de santé

Les hameçonneurs ont envoyé des courriels qui offrent de prétendus conseils médicaux pour vous protéger contre le COVID-19. Les courriels pourraient prétendre provenir d'experts médicaux près de Wuhan, en Chine, où l'éclosion a commencé. Ces courriels pourraient mentionner :

- « Cette petite mesure peut vous sauver »
- « Utilisez le lien ci-dessous pour télécharger les mesures de sécurité. »


### Courriels sur la politique en lieu de travail

Les cybercriminels ont ciblé les comptes de courriel des employés en lieu de travail.

Les courriels d'hameçonnage pourraient mentionner le nom d' « AfrAsia Bank » vous donnant l'impression que le courriel provient de la Banque.

Un exemple pourrait être « Tous, en raison de l'épidémie de COVID-19, AfrAsia Bank prend activement des mesures de sécurité en instaurant une politique de gestion des maladies transmissibles.» Si vous cliquez sur la fausse politique de l'entreprise, vous pouvez télécharger des logiciels malveillants.


### Des cartes COVID-19 en temps réelles

Les cartes qui prétendent suivre l'épidémie de virus est en fait une tactique de manipulation par les hackers pour injecter des malwares sur vos postes de travail, les permettant ainsi de voler vos données personnelles.