UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide sur le chiffrement des courriels dans Microsoft Outlook

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

INDRODUCTION

Le courriel est un outil indispensable dans les opérations quotidiennes de chaque établissement du milieu de l'enseignement supérieur. À chaque jour, les utilisateurs reçoivent et envoient une multitude de courriels contenant diverses informations, certaines à caractères sensibles, d'autres de nature anodine. Pourtant, la sécurité du courriel n'est pas sans failles. C'est pourquoi il est **primordial** d'employer de bonnes pratiques et de développer des habitudes saines lors de la manipulation et de l'envoi de données.

QUELS SONT LES RENSEIGNEMENTS PERSONNELS ?

Les renseignements personnels sont des informations qui peuvent permettre à un acteur malveillant d'identifier une autre personne et de voler en partie ou en totalité son identité à des fins néfastes. Les renseignements personnels peuvent contenir, entre autres :

- Un nom associé à une date de naissance
- Une adresse civique
- Un numéro de compte bancaire
- Un numéro d'assurance sociale
- Mots de passe

QUELS SONT LES RENSEIGNEMENTS CONFIDENTIELS ?

Les renseignements confidentiels sont des informations qui sont critiques au maintien et au développement d'une organisation. Dans le cas des établissements d'enseignement supérieur, les renseignements confidentiels pourraient inclure, sans être limités à :

- Contrats
- Ententes syndicales
- Documents légaux, avis juridiques
- Données de recherche
- Documents stratégiques restreints
- Relevés de notes
- Documents soumis aux droits d'auteur

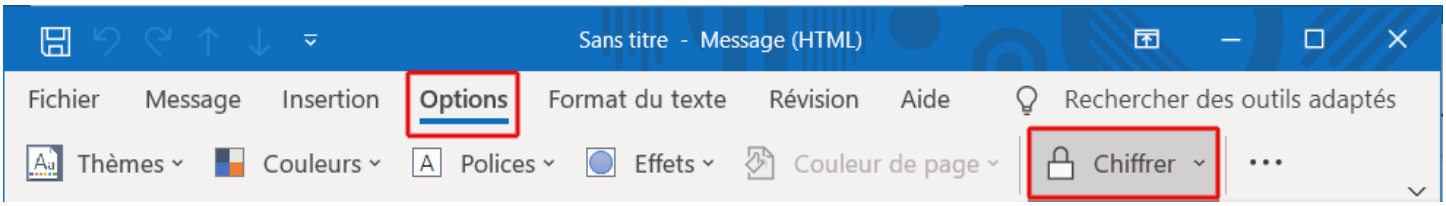
Dans ce guide, nous utiliserons les outils de chiffrement disponibles dans le logiciel Outlook, inclus dans la suite Office 365 de Microsoft, afin de sécuriser l'information que nous distribuons.

Pour plus d'informations sur ce qu'est le chiffrement, et les avantages qu'il apporte dans la sécurité de l'information, voici quelques ressources que vous pouvez consulter :

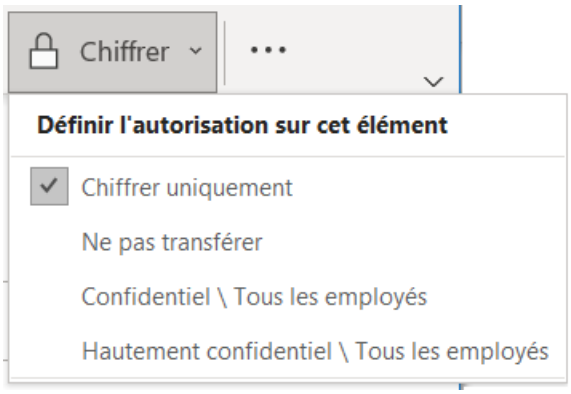
- Le chiffrement : qu'est-ce que c'est ? Comment ça marche ? - Blog TheExpert (squad.fr)
- Le chiffrement informatique - Proxival
- Chiffrement des données et données de chiffrement | Kaspersky

COMMENT ACCÉDER AUX OPTIONS DE CHIFFREMENT ?

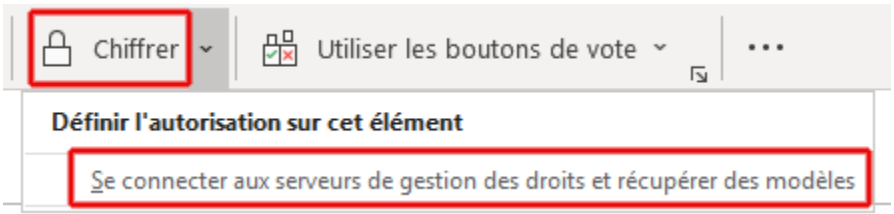
Lorsque nous commençons la rédaction d'un nouveau courriel, afin d'accéder aux options de chiffrement, sélectionnez l'onglet « Options » dans la barre de menu de la fenêtre du courriel en question. Dans les outils qui s'afficheront, vous pourrez utiliser l'outil « Chiffrer » qui fera défiler une liste de chiffrements possibles.



Les choix qui seront dans la liste peuvent varier dépendant de votre organisation, mais les choix usuels devraient ressembler à ceci :



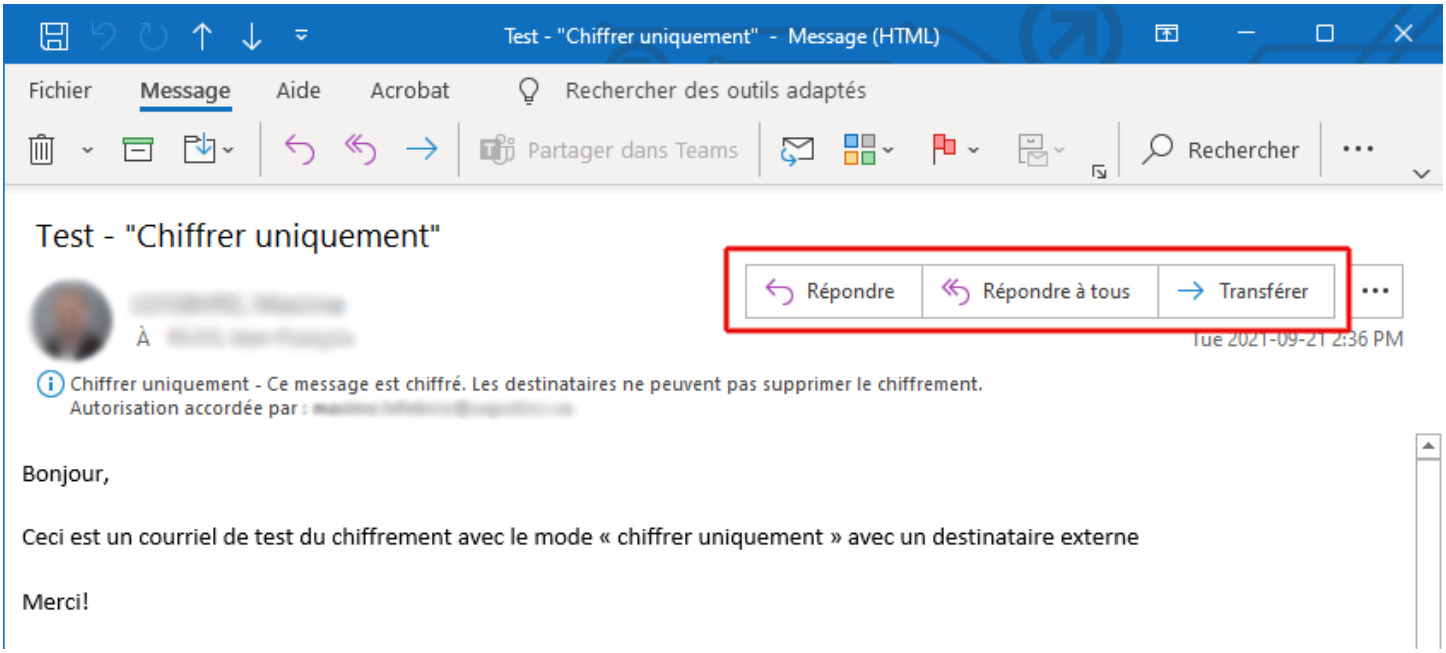
Il est possible que la seule option dans la liste soit « **Se connecter aux serveurs de gestion des droits et récupérer des modèles** ». La raison est simple : c'est la première fois que vous tentez de faire du chiffrement sur votre appareil ! Vous n'avez qu'à choisir l'option présentée. Le processus prendra quelques secondes, et ira récupérer les modèles de chiffrement configurés par votre organisation et les ajoutera à votre liste de choix.



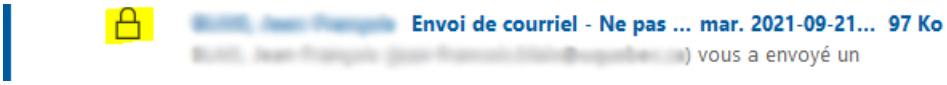
OPTION « CHIFFRER UNIQUEMENT »

Lorsque vous choisissez l'option de chiffrement « Chiffrer uniquement », les messages sont encryptés et protégés contre des attaques du genre « intermédiaire », ou « l'homme au milieu ». C'est-à-dire que si vous vous branchez sur un réseau sans-fil non-sécurisé, une personne ne pourrait pas espionner les données qui transigent sur le réseau pour lire vos courriels. Tout ce que cette personne verrait est un message encodé et illisible.

C'est l'option de chiffrement la plus générique. Elle permet tout de même la réponse et le transfert du courriel vers d'autres destinataires tout en conservant le chiffrement sur le courriel. Vous pourrez voir dans la fenêtre du courriel quel type de chiffrement est actuellement appliqué.



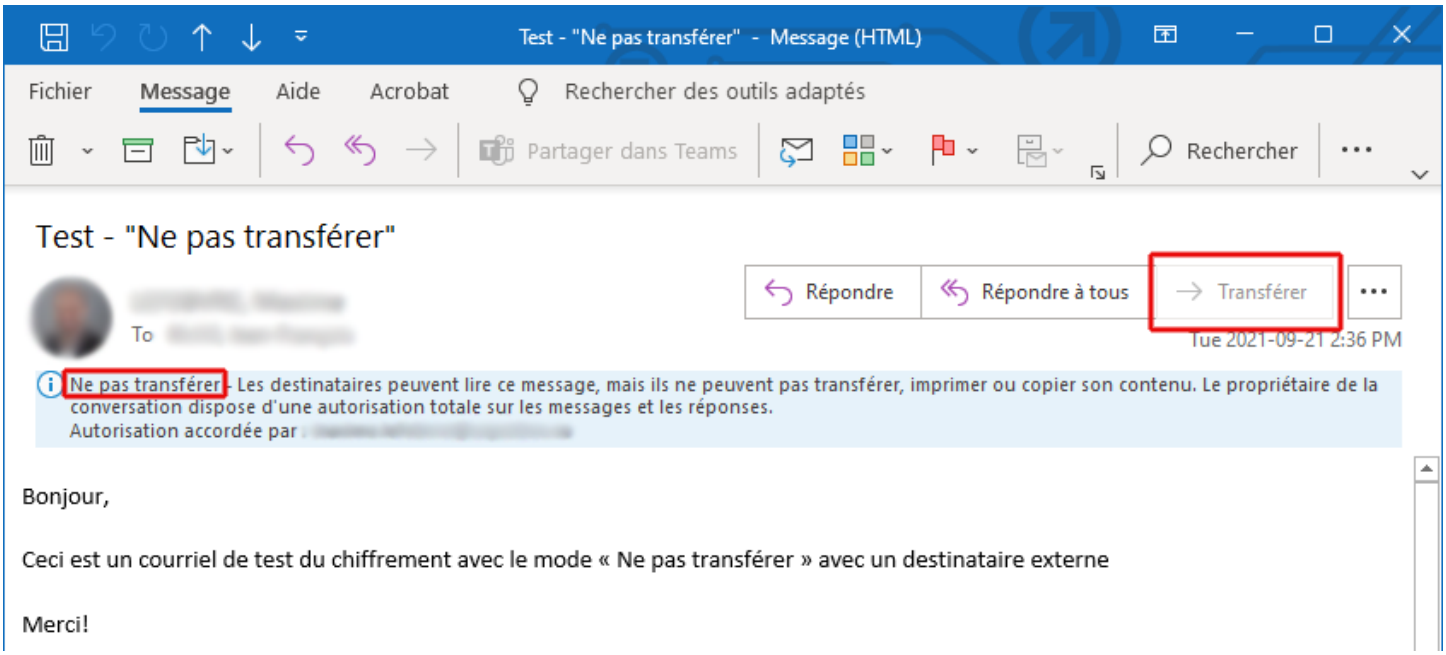
Lorsque vous recevez un courriel sécurisé, dans la liste de vos courriels entrants, vous pourrez voir un petit graphique d'un cadenas barré à droite du titre du courriel. C'est le symbole qui signifie que le courriel a été chiffré.



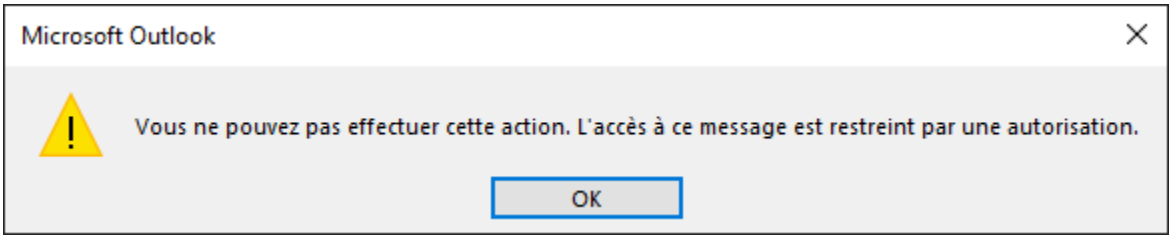
OPTION « NE PAS TRANSFÉRER »

L'option de chiffrement « Ne pas transférer » empêche les membres de la discussion de transférer les courriels vers des destinataires externes à la discussion. Il empêche aussi, lorsqu'ils répondent aux messages, d'ajouter des destinataires. Seule la personne qui a rédigé le courriel initial peut ajouter ou modifier les destinataires. Nous pouvons déterminer qui est le propriétaire de la discussion sous la bannière bleue, où il est indiqué « Autorisation accordée par ».

Nous pourrons voir que le bouton « Transférer » devient grisé, démontrant que le chiffrement fonctionne.



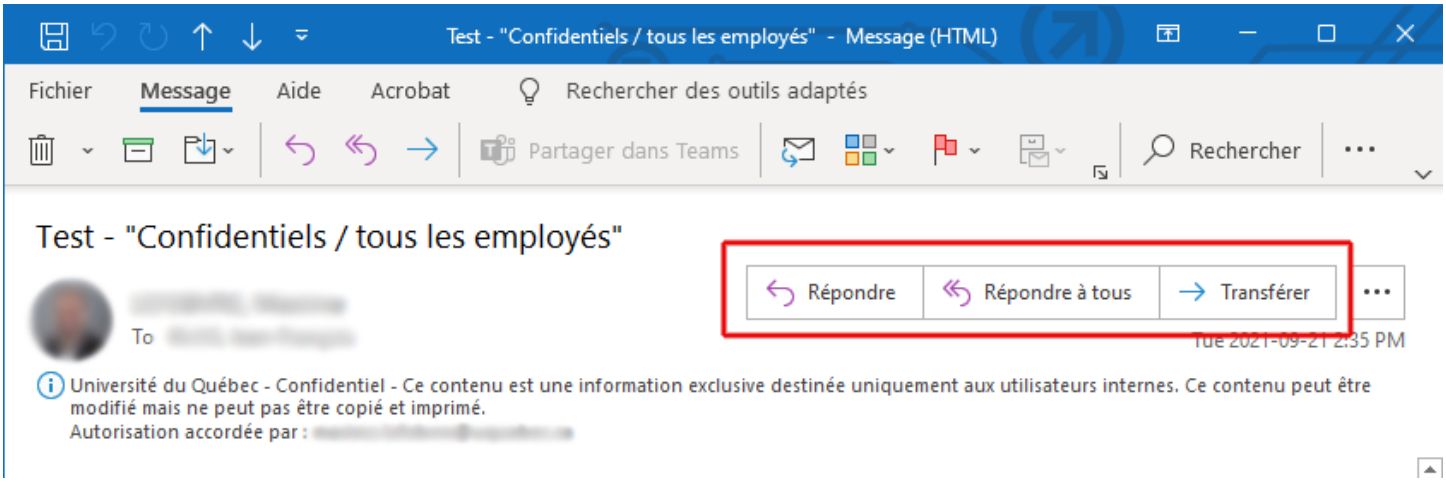
Dans certaines versions d'Outlook, le bouton « Transférer » pourrait ne pas être grisé. Lorsque vous tentez de l'utiliser, cependant, un message indiquant que vous ne disposez pas des autorisations devrait apparaitre, vous empêchant de procéder au transfert.



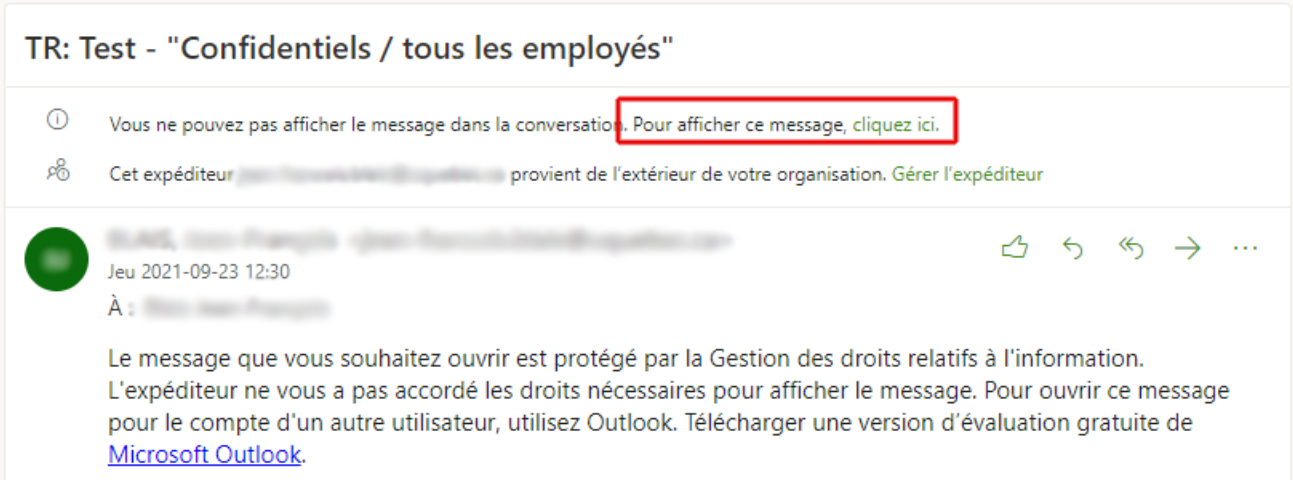
OPTION « CONFIDENTIEL \ TOUS LES EMPLOYÉS »

L'option de chiffrement « Confidentiel \ Tous les employés » permet aux employés d'une organisation d'initier des fils de discussion avec d'autres membres de leur organisation, tout en s'assurant qu'un utilisateur externe à l'organisation ne puisse pas consulter son contenu. Les utilisateurs ne pourront pas copier ou imprimer le contenu du courriel.

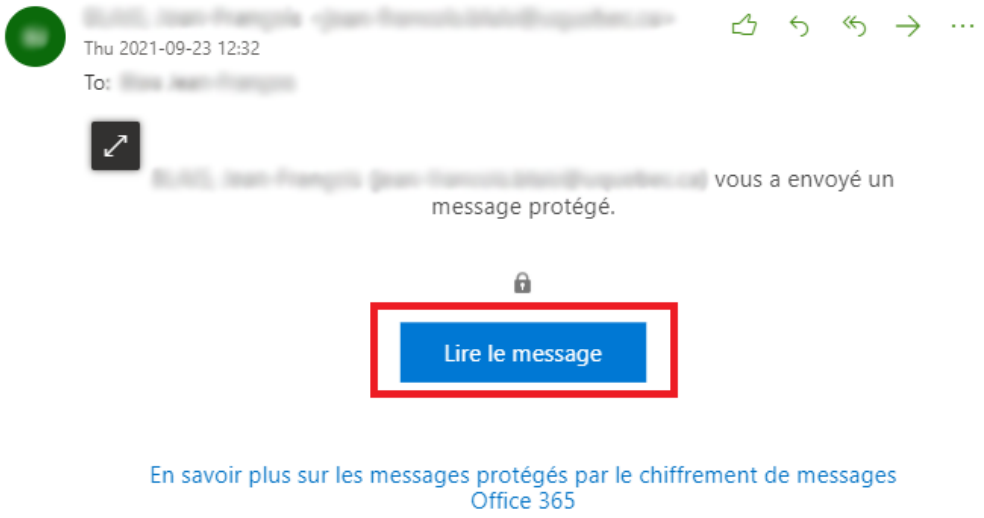
Lorsqu'un utilisateur interne à l'organisation reçoit un message protégé par ce mode de chiffrement, il conserve la possibilité de répondre et de transférer le courriel. Il peut ajouter d'autres destinataires, même des destinataires externes, mais ceux-ci ne pourront pas consulter le courriel.



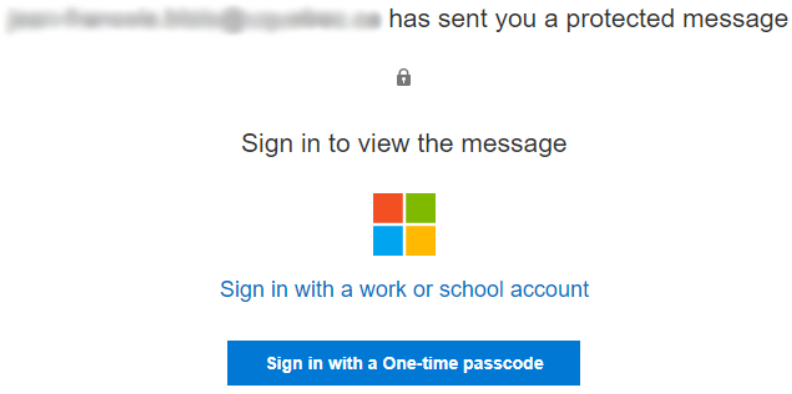
Pour un utilisateur externe, le message qu'il recevra ressemblera à la capture suivante. L'utilisateur devra cliquer sur un lien afin de visualiser le courriel. Une nouvelle fenêtre Outlook s'ouvrira.



Dans cette nouvelle fenêtre, l'utilisateur pourra appuyer sur un lien « Lire le message », qui ouvrira un navigateur, et proposera deux choix d'autentification à l'utilisateur. Notez que l'adresse dans la barre d'adresse du fureteur internet devrait débuter par : **https://outlook.office365.com/Encryption**.



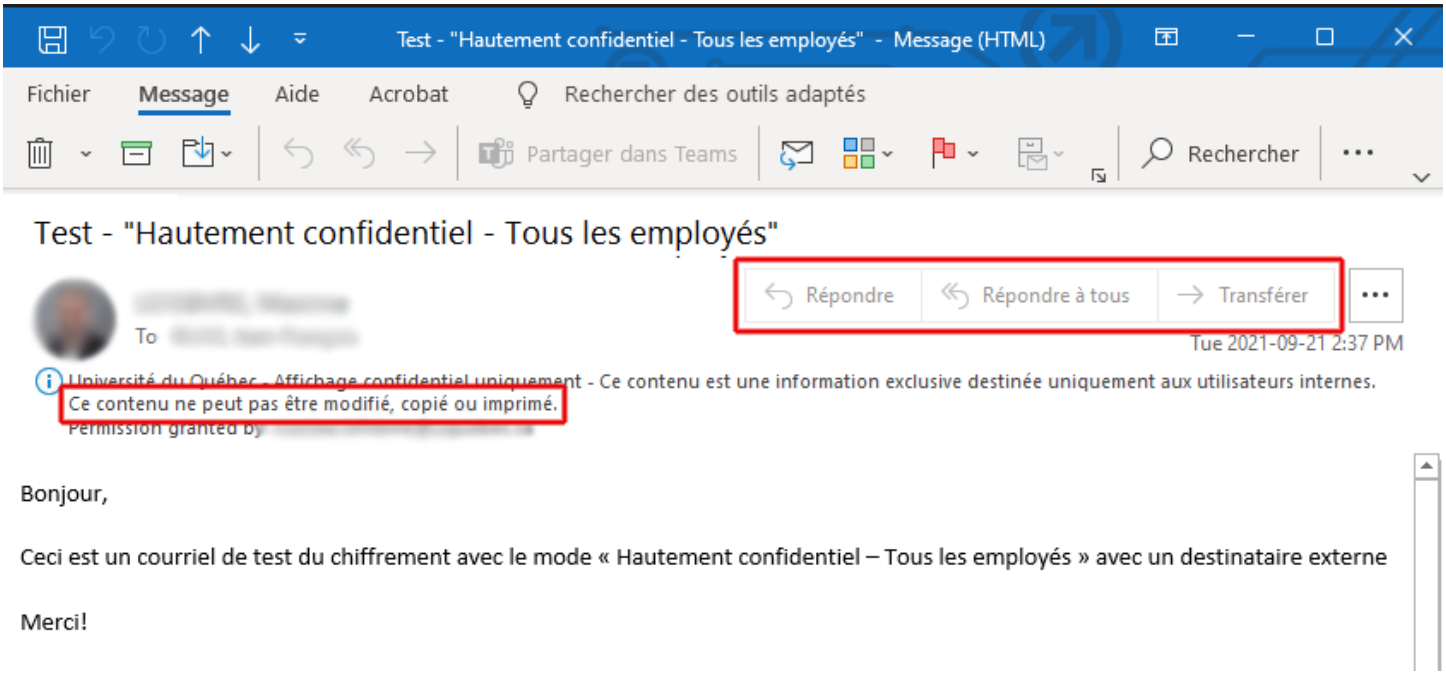
L'utilisateur aura le choix de s'authentifier avec un compte d'entreprise, ou un code à usage unique. Si l'utilisateur ne possède pas de compte faisant partie de l'organisation, l'accès au message lui sera refusé.



OPTION « HAUTEMENT CONFIDENTIEL \ TOUS LES EMPLOYÉS »

L'option de chiffrement « Hautement confidentiel \ Tous les employés » est le mode de chiffrement le plus élevé et le plus restrictif. Il permet aux employés d'une organisation d'envoyer un message unique aux autres utilisateurs de l'organisation. Les récipients du message ne pourront pas imprimer, copier, répondre ou transférer le message vers d'autres destinataires.

Tout comme le mode « Confidentiel \ Tous les employés », il est possible que celui qui rédige le courriel initial ajoute des utilisateurs externes à l'organisation. Ceux-ci recevront des messages qui exigeront une authentification avec un compte interne à l'organisation, sous faute de ne pouvoir accéder au message envoyé.



RESSOURCES ADDITIONNELLES

Le chiffrement de courriel permet d'ajouter plusieurs couches de sécurité additionnelles lors de l'envoi d'information. Il prévient plusieurs types de cyberattaque, mais il demeure que les causes les plus fréquentes de fuite d'information sensible sont liées à des habitudes de travail qui ne tiennent pas compte de la sécurité de l'information.

C'est pourquoi il est important de bien s'informer et de rester vigilant lorsqu'on manipule des données.

Voici quelques ressources et lectures additionnelles qui expliquent comment maintenir une bonne cyberhygiène, et qui permettent de développer de bonnes habitudes en lien avec la sécurité de l'information.

- Comment éviter de partager trop de renseignements en ligne — Pensez cybersécurité (pensezcybersecurite.gc.ca)
  Les 7 signaux d'alarme de l'hameçonnage — Pensez cybersécurité (pensezcybersecurite.gc.ca)

RÉVISIONS

Date	Action	Auteur	Ver.
2023-01-17	Ajustement du modèle	Jean-François Blais CESI de l'UQ	1.2
2022-08-03	Ajustement du modèle	Jean-François Blais CESI de l'UQ	1.1
2022-03-11	Première version	Jean-François Blais CESI de l'UQ	1.0