

Communications par courriel sécurisé à l'aide de *Microsoft 365 Message Encryption*

Introduction

Le Collège Régional Champlain met à la disposition de ses employés et de ses étudiants un moyen de communication sécurisé et d'échange d'informations confidentielles ou sensibles par courriel.

Vous trouverez ci-dessous des instructions sur la façon d'utiliser le *Microsoft 365 Message Encryption*, permettant d'échanger en toute sécurité des informations confidentielles et sensibles avec des parties internes et externes. Le chiffrement des courriels fournit une couche de sécurité supplémentaire pour garantir que seuls les destinataires prévus peuvent accéder au contenu et le lire. En utilisant le chiffrement, nous pouvons empêcher tout accès non autorisé au contenu de notre courriel, protégeant ainsi à la fois notre vie privée et les informations sensibles de l'organisation. À une époque où les cybermenaces évoluent constamment, le chiffrement des courriels est une étape nécessaire pour maintenir l'intégrité et la sécurité de nos communications numériques.

Remarque sur le chiffrement

Microsoft 365 Message Encryption ne peut pas empêcher la suppression, le vol, la corruption ou la capture et la transmission du contenu par des programmes malveillants ou des virus informatiques. Il ne peut pas non plus empêcher le contenu restreint d'être copié ou retapé à la main ou d'être photographié ou capturé numériquement.

Remarque sur les pièces jointes

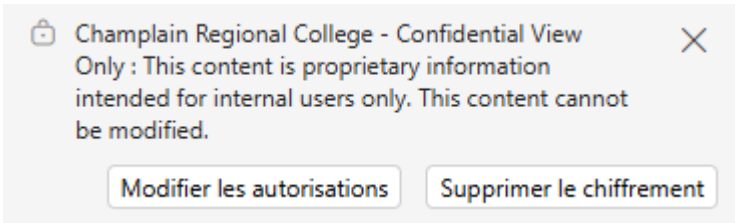
Toutes les pièces jointes du courriel sont chiffrées; cependant, elles se comportent différemment après leur téléchargement en fonction de l'option de chiffrement utilisée.

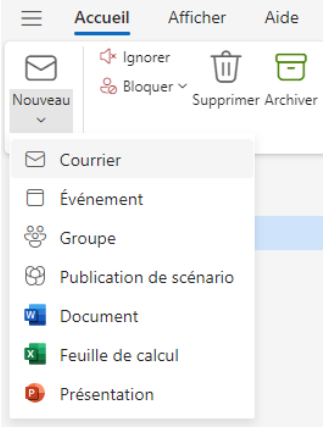
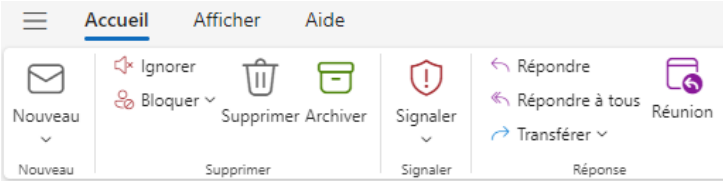
Si vous choisissez **Chiffrer**, les destinataires peuvent télécharger des pièces jointes sans chiffrement.

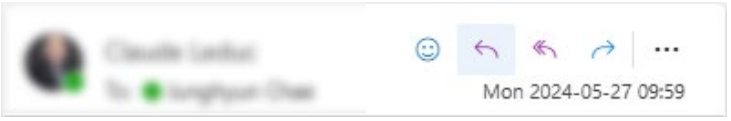
Si vous choisissez **Ne pas chiffrer**, il existe deux options concernant les pièces jointes :

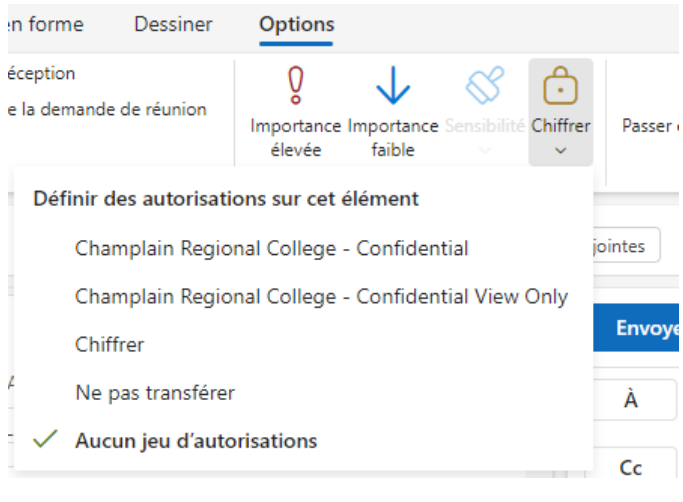
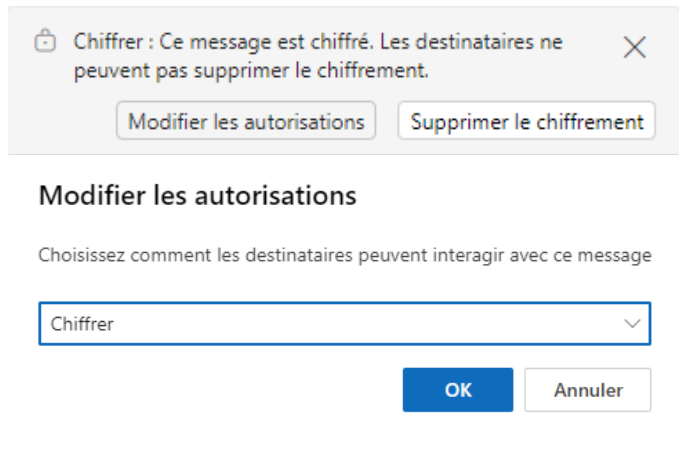
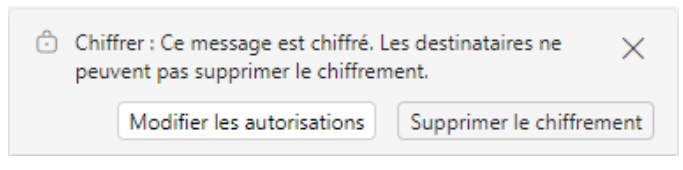
- Les pièces jointes Microsoft Office telles que les fichiers Word, Excel ou PowerPoint restent chiffrées même après leur téléchargement. Cela signifie que si le destinataire télécharge la pièce jointe et la transmet à quelqu'un d'autre, il ne pourra pas l'ouvrir car il n'a pas l'autorisation.
- Toutes les autres pièces jointes, telles que les fichiers PDF ou les fichiers image, peuvent être téléchargées sans chiffrement.

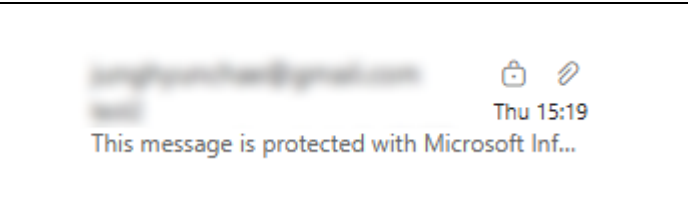
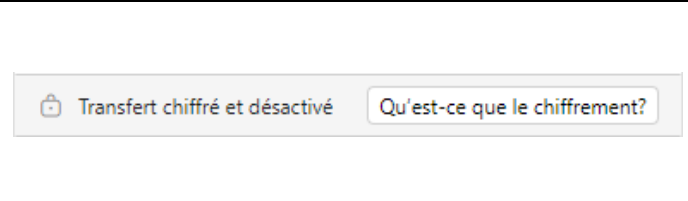
<u>Options de protection des messages disponibles dans Outlook (toutes versions)</u>	
1. Chiffrer 2. Ne pas transférer 3. <i>Champlain Regional College - Confidential</i> 4. <i>Champlain Regional College - Confidential View Only</i>	Définir des autorisations sur cet élément Champlain Regional College - Confidential Champlain Regional College - Confidential View Only Chiffrer Ne pas transférer ✓ Aucun jeu d'autorisations
Chiffrer	
Cette option vous permet d'envoyer des messages chiffrés à n'importe quel destinataire interne ou externe, qu'il se trouve ou non au sein de l'organisation.	 Chiffrer : Ce message est chiffré. Les destinataires ne peuvent pas supprimer le chiffrement.  Modifier les autorisations Supprimer le chiffrement
Ne pas transférer	
Cette option vous permet d'envoyer un message chiffré et limite également le transfert, l'impression ou la copie du contenu et du courriel.	 Ne pas transférer : Les destinataires ne peuvent pas transférer, imprimer ou copier du contenu.  Modifier les autorisations Supprimer le chiffrement
<i>Champlain Regional College – Confidential</i>	
Cette option permet uniquement aux destinataires internes du Collège Régional Champlain de lire et de modifier le contenu protégé.	 Champlain Regional College - Confidential : This content is proprietary information intended for internal users only. This content can be modified but cannot be copied and printed.  Modifier les autorisations Supprimer le chiffrement

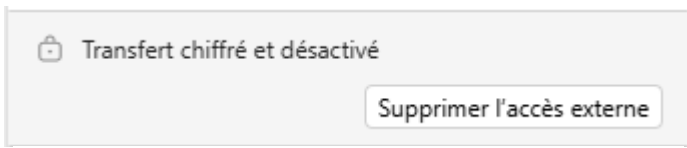
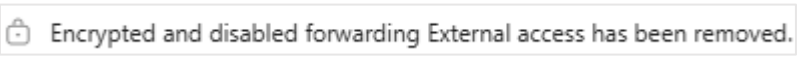
Champlain Regional College – Confidential View Only	
Cette option permet uniquement aux destinataires internes du Collège Régional Champlain de lire le contenu protégé (impossible de répondre, de transférer, de sauvegarder, d'exporter).	

Mise en route (New Outlook et Outlook Online)	
*** La procédure suivante s'applique uniquement au client New Outlook et Outlook Online. Si vous utilisez le client Outlook Classic, passez à la section Mise en route (Outlook Classic) ci-dessous. ***	
Ouvrez l'application New Outlook depuis votre bureau :	
Ou, à l'aide du navigateur Web (Edge, Chrome, Firefox, Safari, etc.) de votre choix, accédez à l'adresse suivante :	https://outlook.office365.com/mail/
Commencez un nouveau message en sélectionnant Nouveau dans le menu Accueil . Vous pouvez soit cliquer sur l'icône de l'enveloppe, soit cliquer sur la flèche en dessous et sélectionner Courrier .	
Vous pouvez également créer un nouveau message en répondant/transférant un message de votre boîte de réception – sélectionnez Répondre/Répondre à tous/Transférer dans le menu Accueil .	

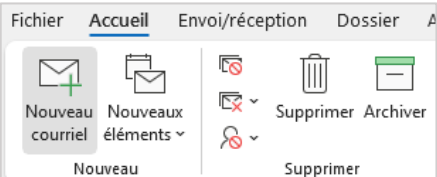
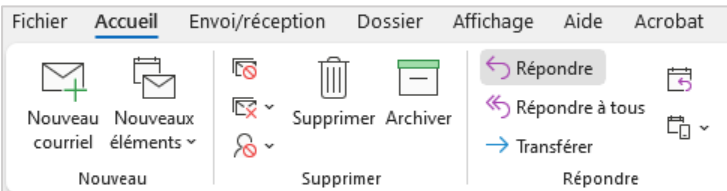
Ou cliquez sur l'icône Répondre/Répondre à tous/Transférer en haut du message, à côté des informations sur l'expéditeur.	
---	--

<u>Microsoft 365 Message Encryption (New Outlook et Outlook Online)</u>	
Dans le nouveau message, sélectionnez Options, sélectionnez Chiffrer et sélectionnez le chiffrement qui comporte les restrictions que vous souhaitez appliquer, telles que Chiffrer ou Ne pas transférer. Une icône de cadenas et les informations de chiffrement apparaissent en haut du message, ainsi que la possibilité de modifier ou de supprimer le chiffrement.	
Pour modifier le chiffrement, cliquez sur Modifier les autorisations. Sélectionnez l'autorisation souhaitée, puis cliquez sur OK.	
Pour supprimer le chiffrement, cliquez sur Supprimer le chiffrement ou sur X. L'icône du cadenas et les informations de cryptage disparaîtront du haut du message.	

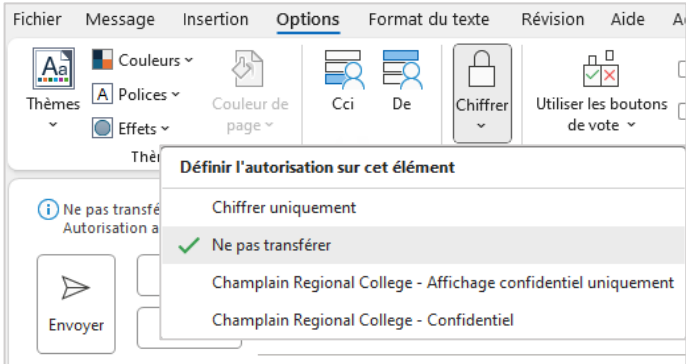
Terminez et envoyez le message comme d'habitude. Un message de courriel chiffré sera affiché avec une icône de cadenas.	
Si vous êtes le destinataire, une icône de cadenas et les informations de chiffrement s'afficheront en haut du message, ainsi qu'un lien pour en savoir plus sur le <i>Microsoft 365 Message Encryption</i> .	

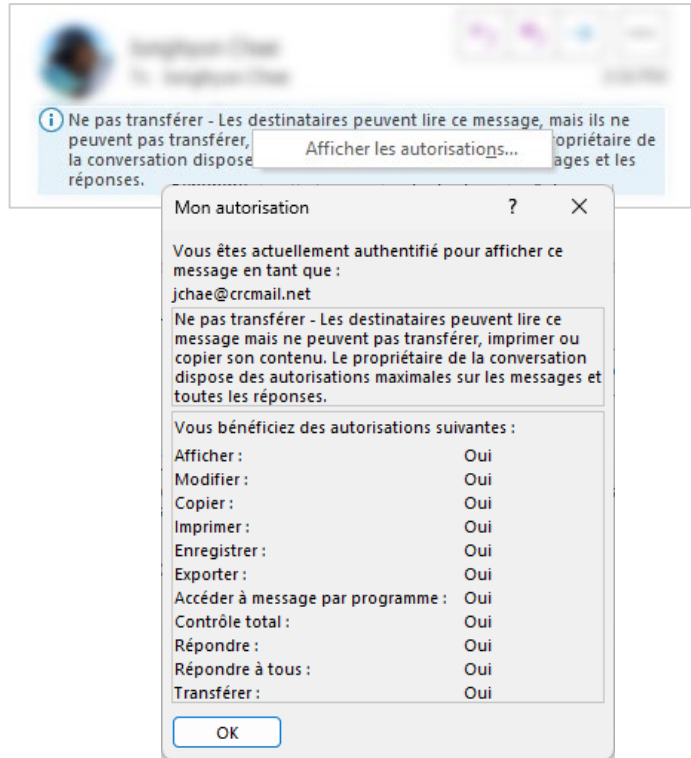
<u>Suppression de l'accès externe après l'envoi du courriel</u> <u>(New Outlook et Outlook Online)</u>	
Si vous êtes l'expéditeur, vous pouvez supprimer l'accès externe après l'envoi du courriel. Accédez à vos Éléments envoyés , sélectionnez le message chiffré, puis cliquez sur Supprimer l'accès externe . Cliquez sur OK .	 Supprimer l'accès externe Les destinataires externes qui ont reçu ce message ne pourront plus accéder à son contenu. OK Annuler
Une icône de cadenas et l'information indiquant que l'accès externe a été révoqué seront affichées en haut du message.	

Mise en route (Outlook Classic)

Ouvrez l'application Outlook Classic depuis votre bureau :	
Commencez un nouveau message en sélectionnant Nouveau dans le menu Accueil .	
Vous pouvez également créer un nouveau message en répondant/transférant un message de votre boîte de réception – sélectionnez Répondre/Répondre à tous/Transférer dans le menu Accueil .	
Ou cliquez sur l'icône Répondre/Répondre à tous/Transférer en haut du message, à côté des informations sur l'expéditeur.	

Microsoft 365 Message Encryption (Outlook Classic)

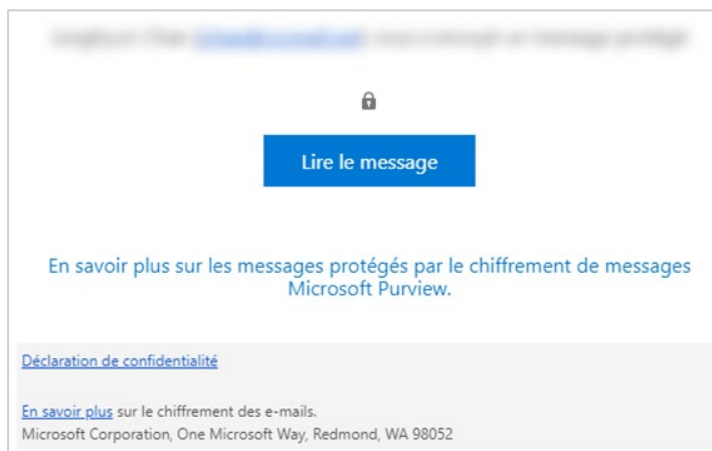
Dans le nouveau courriel, sélectionnez Options, puis sélectionnez Chiffrer. Les informations du chiffage apparaissent en haut du message. Par défaut, l'option Chiffrer Uniquement est sélectionnée. Pour sélectionner une autre option de chiffage, cliquez sur la flèche en dessous, puis sélectionnez l'option souhaitée.	
--	--

Terminez de composer et envoyez le message comme d'habitude. Lorsque vous envoyez un courriel chiffré, les informations de chiffrement s'affichent en haut du message.	
Vous pouvez afficher l'autorisation en cliquant sur le message chiffré et en sélectionnant Afficher l'autorisation.	

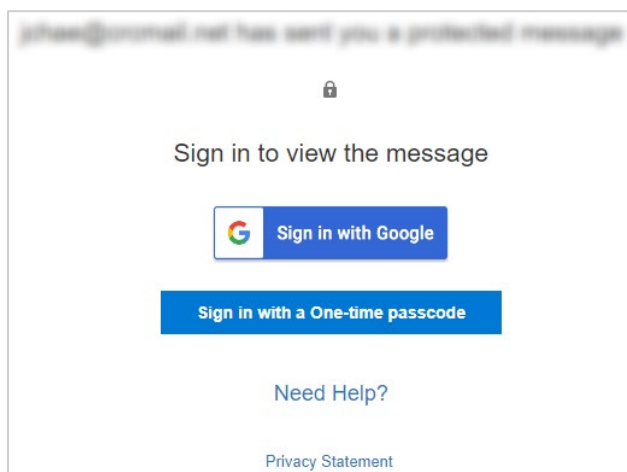
À quoi cela ressemble lorsque le courriel est reçu par un autre client (par ex., Gmail)

***** Cette section est fournie à titre d'exemple uniquement, afin d'illustrer la manière dont les gens reçoivent des communications chiffrées. Selon le client utilisé par le destinataire, le résultat peut varier. *****

Lorsqu'un message chiffré est envoyé à d'autres clients de messagerie tels que Gmail, le contenu n'apparaît pas dans le corps du message. Le destinataire est invité à cliquer sur le lien **Lire le message** pour visualiser le message.



Sélectionnez la méthode d'authentification de votre choix.



Une fois l'identité du destinataire validée, le message s'affiche dans une fenêtre séparée.

