

Connexion**Ontario**

# Consignes sur le cryptage et la transmission de fichiers

Version : 2

Identificateur de document : 2551

Responsable du document : Services de sécurité

## **Avis de droit d'auteur**

© cyberSanté Ontario, 2016.

## **Tous droits réservés**

Il est interdit de reproduire le présent document, en totalité ou en partie, de quelque manière que ce soit, y compris par photocopie ou transfert électronique vers n'importe quel ordinateur, sans le consentement écrit préalable de cyberSanté Ontario. Les renseignements contenus dans le présent document sont la propriété de cyberSanté Ontario. Il est interdit de les utiliser ou de les divulguer sans une autorisation écrite expresse de cyberSanté Ontario.

## **Marques de commerce**

Les autres noms de produits mentionnés dans le présent document peuvent être des marques de commerce ou des marques de commerce déposées et sont ici reconnus comme étant la propriété de leurs entreprises respectives.

## Introduction

*En vertu des politiques de cyberSanté Ontario, des mesures de protection appropriées doivent être prises chaque fois qu'un document ou un fichier contenant des données sensibles est stocké ou transféré au moyen de canaux de communication qui ne sont pas entièrement sûrs (courriel, CD, DVD, clé USB, carte mémoire flash, etc.).*

Le présent document explique la procédure à suivre pour appliquer un niveau de protection élevé aux fichiers et aux rapports contenant des données sensibles à l'aide de WinZip, une application commerciale qui permet de réduire la taille d'un document et de lui appliquer un niveau de protection élevé.

Il est important de garder à l'esprit que l'outil présenté dans ce document est un système de cryptage par mot de passe. Le fichier crypté peut être lu si la sécurité du mot de passe est compromise. Par conséquent, toute personne qui utilise cet outil pour crypter un fichier doit suivre les instructions sur la protection du mot de passe figurant à la section « Communiquer le mot de passe ».

## Utilisations autorisées

*Vous pouvez suivre cette procédure pour envoyer ponctuellement des données sensibles, notamment des documents contenant des renseignements personnels, sur la santé ou autres, par courriel, conformément à vos processus administratifs habituels.*

Si l'envoi de renseignements sensibles par courriel non sécurisé fait partie de vos processus administratifs actuels, vous devriez songer à automatiser ce processus et à utiliser un mécanisme d'entreprise pour transférer vos données de façon sécuritaire.

cyberSanté Ontario limite la taille des pièces jointes à 10 Mo par courriel.

Pour obtenir de l'aide, veuillez appeler le Service de dépannage de cyberSanté Ontario au 1 866 250-1554.

## Crypter des fichiers avec WinZip

*cyberSanté Ontario utilise la version standard de **WinZip 16.0** pour crypter et compresser des fichiers. Si WinZip n'est pas installé sur votre ordinateur, demandez de l'aide à votre service de dépannage, ou utilisez Microsoft Word ou Excel pour crypter vos fichiers. Vous trouverez ci-dessous la procédure d'utilisation de WinZip, de Microsoft Word et d'Excel.*

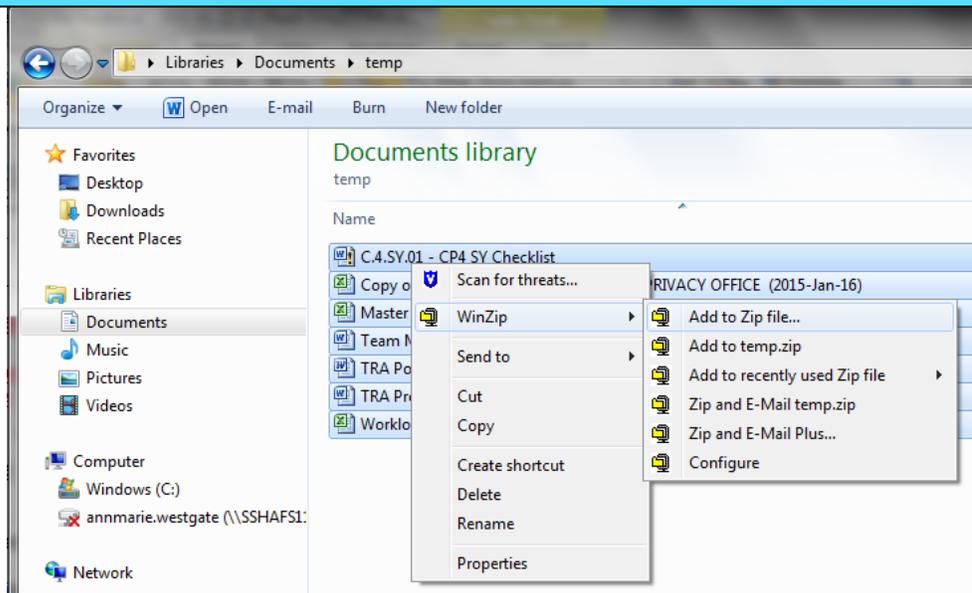
## Crypter des fichiers avec WinZip

### Étape 1 : Créer une archive

Ouvrez l'emplacement du fichier.

Ouvrez le dossier où se trouvent les fichiers. Sélectionnez les fichiers que vous souhaitez compresser. Dans la boîte de dialogue, placez le curseur de la souris sur WinZip et cliquez sur **Ajouter au Zip...**

Donnez au fichier le nom que vous voulez.



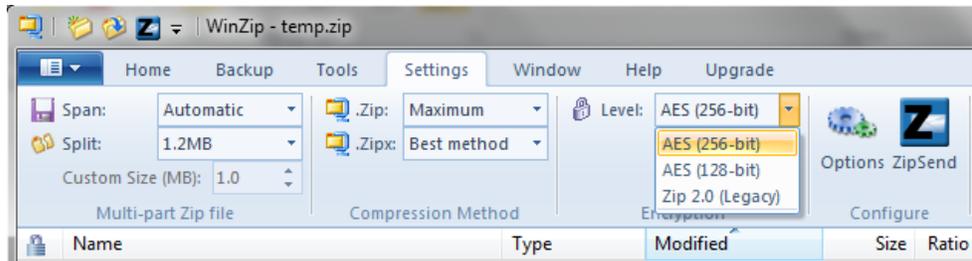
Étape 1 : Ajouter des fichiers à une archive.

### Étape 2 : Ouvrir l'archive

Double-cliquez sur le fichier Zip pour ouvrir l'archive.

### Étape 3 : Choisir un niveau de cryptage élevé

Utilisez le cryptage AES 256 bits. Dans l'onglet **Réglages**, assurez-vous que le niveau de cryptage sélectionné est **AES (256 bits)**.

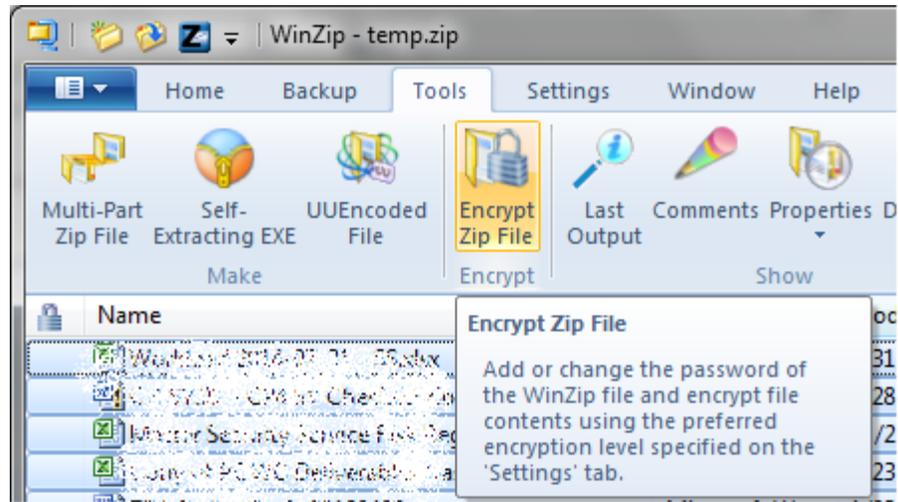


Étape 3 : Choisir un niveau de cryptage.

## Crypter des fichiers avec WinZip

### Étape 4 : Crypter le fichier

Dans le menu **Outils**, cliquez sur **Crypter le fichier Zip**.



Étape 4 : Crypter le fichier Zip.

### Étape 5 : Créer un mot de passe fort

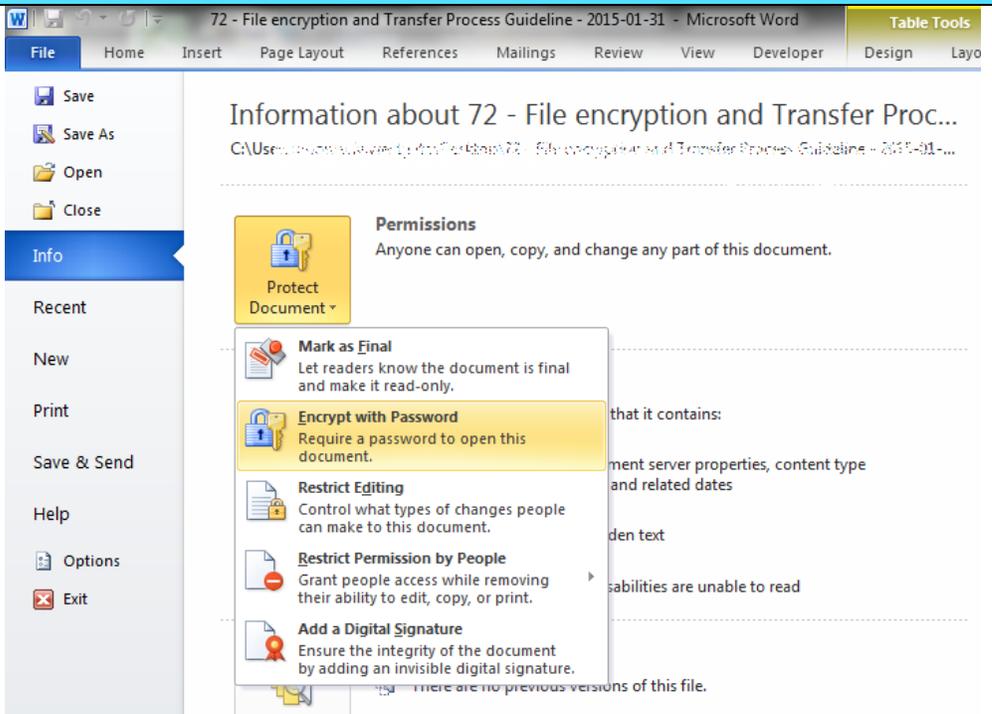
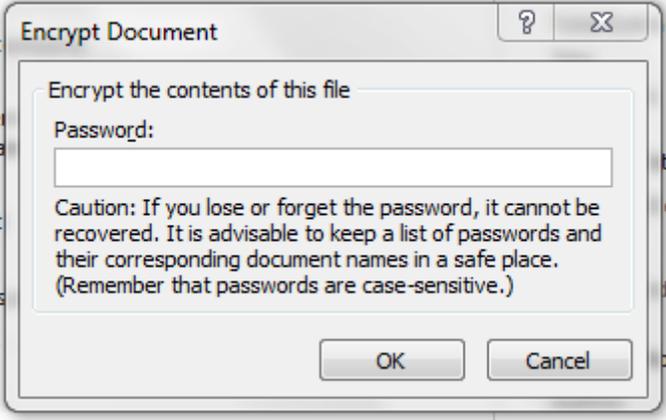
Entrez un mot de passe puis confirmez-le.

Pour savoir comment créer un mot de passe difficile à deviner, consultez la section « Créer un mot de passe » ci-après.

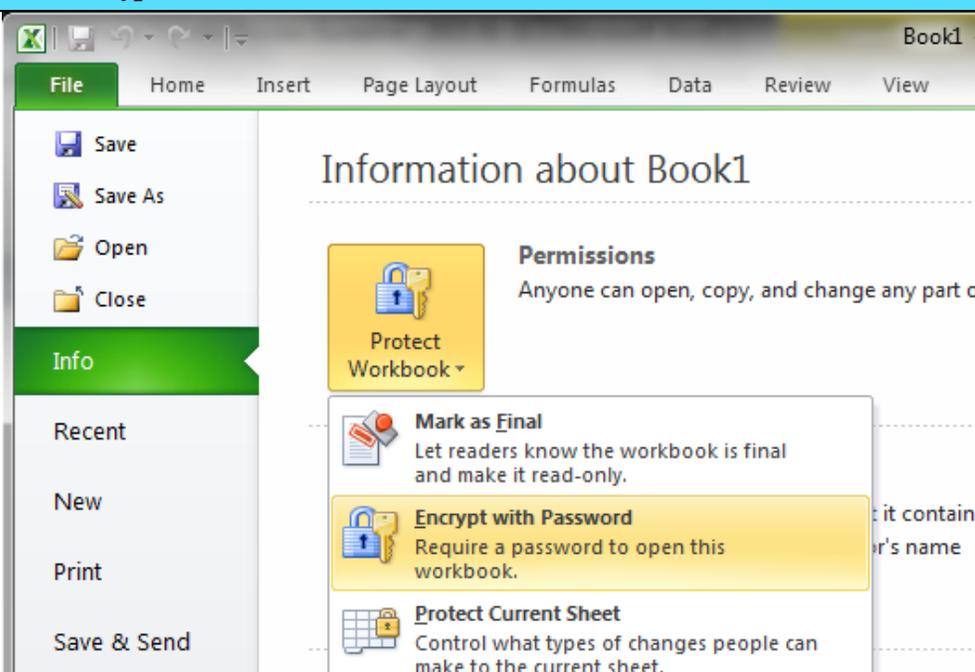
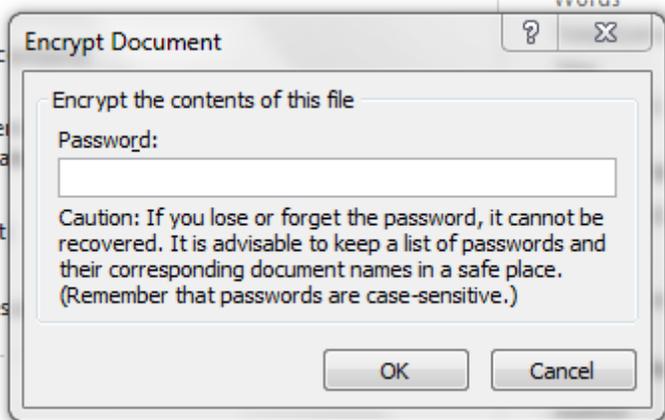


Figure 4 : Créer un mot de passe difficile à deviner.

# Crypter un document Microsoft Word

Crypter un fichier avec Microsoft Word 2010	
<p><b>Étape 1 : Protéger le document</b></p> <p>Ouvrez le document.</p> <p>Cliquez sur l'onglet <b>Fichier</b>, puis sur <b>Informations</b>.</p> <p>Cliquez sur <b>Protéger le document</b>.</p> <p>Dans le menu déroulant, cliquez sur <b>Chiffrer avec mot de passe</b>.</p>	 <p>The screenshot shows the Microsoft Word 2010 interface. The 'File' tab is active, and the 'Info' section is expanded. The 'Protect Document' dropdown menu is open, showing several options: 'Protect Document', 'Mark as Final', 'Encrypt with Password' (highlighted), 'Restrict Editing', 'Restrict Permission by People', and 'Add a Digital Signature'. The 'Encrypt with Password' option is selected, and a tooltip is visible over it.</p>
<p><b>Étape 2 :</b> Entrez un mot de passe, puis confirmez-le.</p> <p>Pour savoir comment créer un mot de passe difficile à deviner, consultez la section « Créer un mot de passe » ci-après.</p>	 <p>The screenshot shows the 'Encrypt Document' dialog box. It has a title bar with a question mark and a close button. The main text reads 'Encrypt the contents of this file'. Below this is a 'Password:' label followed by a text input field. A caution message states: 'Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)'. At the bottom, there are 'OK' and 'Cancel' buttons.</p>

# Crypter un document Excel

Crypter un fichier avec Microsoft Excel 2010	
<p><b>Étape 1 : Protéger le document</b> Ouvrez le document.</p> <p>Cliquez sur l'onglet <b>Fichier</b>, puis sur <b>Informations</b>.</p> <p>Cliquez sur <b>Protéger le document</b>.</p> <p>Dans le menu déroulant, cliquez sur <b>Chiffrer avec mot de passe</b>.</p>	 <p><b>Étape 1 : Protéger le document.</b></p>
<p><b>Étape 2 : Entrez un mot de passe puis confirmez-le.</b></p> <p>Pour savoir comment créer un mot de passe difficile à deviner, consultez la section « Créer un mot de passe » ci-après.</p>	 <p><b>Étape 2 : Entrer un mot de passe et le confirmer.</b></p>

## Créer un mot de passe

Il est important de créer un mot de passe fort pour protéger les fichiers chiffrés.

- Créer et utiliser des mots de passe différents pour chaque document chiffré.
- Utiliser au moins huit caractères.
- Les mots de passe doivent comprendre au moins trois des quatre types de caractères suivants : lettre majuscule (de A à Z); lettre minuscule (de a à z); chiffre (de 0 à 9) et caractère spécial (p. ex., !, \$, #, \_, ~, % et ^).
- Exemple d'un mot de passe faible : 1234motdepasse!.
- Exemple d'un mot de passe difficile à deviner : C\_35t\_Un3\_B3ll3\_Journé3.

Une fois le fichier chiffré, il faut envoyer le mot de passe au destinataire désigné du fichier à l'aide d'une méthode « hors bande » (p. ex., si le document est envoyé par courriel, transmettre le mot de passe par téléphone, par télécopieur ou par la poste). En d'autres termes, le mot de passe ne doit pas être envoyé en même temps que le fichier crypté à l'aide de la même méthode.

Le fichier doit être crypté et protégé par un mot de passe avant d'être envoyé par courriel sous forme de pièce jointe.

Le logiciel WinZip décrit dans le présent document emploie une cryptographie symétrique qui nécessite la communication d'un secret (en l'occurrence, un mot de passe). En d'autres termes, l'expéditeur du fichier crypté doit communiquer le mot de passe au destinataire prévu du fichier. En cas d'oubli du mot de passe, il sera impossible de récupérer les fichiers se trouvant dans l'archive cryptée. Le processus de création et de communication du mot de passe nécessite donc une attention particulière.

## Communiquer le mot de passe

Les dépositaires de renseignements sur la santé (DRS) doivent communiquer les mots de passe à cyberSanté Ontario de façon sécuritaire.

Voici la procédure à suivre :

- Déterminer qui est le destinataire autorisé de l'information.
- Mettre le fichier crypté à la disposition du destinataire selon le processus convenu (p. ex., SFTP, courriel).
- Le demandeur appelle l'expéditeur par téléphone.
- L'expéditeur vérifie oralement l'identité du destinataire :
  - Nom
  - Titre, division, organisation
  - Nom du fichier crypté reçu ou récupéré
- L'expéditeur fournit oralement au destinataire le mot de passe permettant d'ouvrir le fichier crypté.
- Il demande et obtient la confirmation orale que le destinataire a pu extraire les fichiers s'y trouvant.

- Le cas échéant, l'expéditeur détruit de façon sécuritaire la copie écrite du mot de passe ainsi que toute copie du fichier se trouvant sur le réseau ou le disque local.

## Récupérer le mot de passe

WinZip ne prévoit aucun mécanisme de récupération du mot de passe. Par conséquent, en cas de stockage à long terme de fichiers cryptés, une méthode de récupération du mot de passe doit être mise en place pour accéder aux fichiers (comme au cas où des fichiers d'un employé ayant quitté l'organisation devraient être consultés).

Par exemple, le mot de passe peut être conservé aux fins de récupération dans une enveloppe scellée accessible uniquement par la haute direction.

## Supprimer un fichier

Une fois qu'un fichier crypté n'est plus utile, il doit être supprimé par son expéditeur et son destinataire.