03 mars 2017

Dans le cadre le cadre de votre travail ou chez vous, vous conservez des documents qui peuvent contenir des informations confidentielles qui ne devraient pas être accessibles à tous. Le chiffrement répond à cette problématique.

Pourquoi chiffrer ses documents et ses répertoires ?

Le chiffrement est une méthode qui consiste à protéger ses documents en les rendant illisibles par toute personne n'ayant pas accès à une clé dite de déchiffrement.
Pour en savoir plus, vous pouvez (re)lire notre fiche Comprendre les grands principes de la cryptologie et du chiffrement.

À titre personnel, le chiffrement peut être utile si vous souhaitez conserver des documents confidentiels sur un support qui pourrait être volé (clé USB, ordinateur portable, etc.) ou sur un ordinateur que vous partagez avec des personnes qui ne doivent pas pouvoir y accéder. Enfin, le plus souvent, lorsque vous stockez des documents dans le *cloud*, la confidentialité de ces fichiers n'est pas garantie. Ces données sont généralement stockées en clair sur les serveurs, elles sont potentiellement lisibles par tout utilisateur disposant de droits privilégiés sur ces serveurs (par exemple, des administrateurs ou pirates potentiels).

D'un point de vue professionnel, vous pouvez aussi être concernés :

- Si vous stockez des documents confidentiels sur un serveur partagé avec des collègues qui ne doivent pas en avoir connaissance.
- Si vous êtes avocat, médecin, journaliste, ou toute autre profession imposant un strict secret professionnel et que vous travaillez sur un ordinateur portable qui pourrait malheureusement vous être volé un jour.

Ça n'arrive pas qu'aux autres !

Une atteinte à la confidentialité des données peut avoir diverses conséquences. Il existe de nombreux exemples, autant :

- **À titre professionnel,** une liste de clients non chiffrée qui tombe entre les mains d'un mauvais destinataire peut nuire à la santé financière de l'entreprise ainsi qu'à sa réputation.

  La police de Manchester a ainsi été condamnée en 2012 par l'ICO (l'équivalent de la CNIL en Grande-Bretagne) à une amende de £120 000 pour s'être fait voler une clef USB non chiffrée, contenant les données d'environ 1 000 personnes liées à des enquêtes criminelles.

- **À titre personnel,** protéger ses données personnelles, c'est aussi prévenir les potentielles usurpations d'identité.

  La captation de documents ou d'informations personnelles peut permettre à des personnes malveillantes d'utiliser ces informations à votre insu, par exemple, pour souscrire en votre nom à un crédit, un abonnement, commettre des actes répréhensibles ou nuire à votre réputation.

INFOGRAPHIE | Comment chiffrer ses documents ?

Le tutoriel ci-dessous, et les logiciels proposés, s'adressent aux particuliers et aux professionnels qui souhaitent sécuriser leurs documents mais pour lesquels une faille dans la confidentialité pourrait être surmontée, même avec difficulté.

En particulier, il n'a pas vocation à traiter la sécurisation de documents soumis au secret de la défense nationale pour lesquels des mesures complémentaires doivent être apportées.

De même, si vous êtes journaliste, avocat ou encore médecin, le présent tutoriel peut être une introduction mais devrait être complété pour vous permettre de respecter votre secret professionnel que ce soit vis-à-vis de vos sources, vos clients ou vos patients.

Attention : le chiffrement est irréversible, si vous perdez la clé de déchiffrement ou le mot de passe qui la déverrouille vous ne pourrez plus accéder à vos données. Vous souhaiterez peut-être faire une copie de votre mot de passe ou de votre clé à conserver en lieu sûr, « au cas où ».

Technique n°1 : chiffrer un document pour l'envoyer

En pratique, pour chiffrer des données pour soi, le plus simple est le chiffrement symétrique c'est-à-dire celui pour lequel on utilise la même clé

- Peazip est un logiciel libre semblable à 7-Zip. Il est gratuit, téléchargeable sur www.peazip.org, disponible en français et librement redistribuable.
- AxCrypt est un logiciel libre édité par la société Axantum qui permet de chiffrer des fichiers sous Windows.
- Zed! est un outil de chiffrement plus avancé, développé par la société Prim'X, dont une version de découverte gratuite permet de chiffrer des fichiers jusqu'à 200 Mo.

Tutoriel : utiliser7-ZIP

Avec 7-Zip, la création d'une archive chiffrée s'effectue en quelques secondes en utilisant la méthode suivante :

1. Télécharger et installer 7-ZIP,
2. S'assurer que le destinataire dispose de 7-ZIP et lui envoyer le lien de téléchargement,
3. Sélectionner le ou les fichiers à chiffrer,
4. Effectuer un clic-droit sur les fichiers, menu « 7-Zip » puis ajouter à l'archive,
5. Vérifier que la méthode de chiffrement choisie est AES,
6. Que l'option « Chiffre les noms de fichiers » est cochée,
7. Entrer un mot de passe suffisamment long et complexe (voir Les conseils de la CNIL pour un bon mot de passe).

Technique n° 2 : abriter un ou plusieurs documents dans un répertoire chiffré

Plutôt que chiffrer les documents un par un, il est possible de créer des partitions chiffrées. Une partition chiffrée est une sorte de répertoire chiffré qui, une fois ouvert, se présentera comme un disque réseau supplémentaire.

Différents logiciels fournissent cette fonctionnalité, comme, par exemple, Zed! de Prim'X Technologies, Bitlocker de Microsoft ou encore Veracrypt. Ce dernier étant un logiciel libre et gratuit, c'est celui-ci que nous avons choisi pour notre tutoriel.

Tutoriel : utiliser Veracrypt

Ce tutoriel vous montre comment chiffrer un espace de travail sur votre PC en tout simplicité. Il s'adresse aux internautes qui souhaitent s'initier au chiffrement à des fins personnelles ou dans le cadre de leur travail.