Protection de ses données

Quelques notes (liste non exhaustive) sur les possibilités simples de protéger ses données personnelles soit pour être stockées localement dans son PC ou un disque extérieur, soit pour leur transfert par Mél sur Internet.
Un lieu à craindre : le "Cloud" (quel nom idiot mais qui veut bien dire ce qu'il est !), normalement à éviter sauf à crypter tout ce que l'on y met.

Le niveau d'une protection dépend de l'importance de ce qui est à protéger, mais pourquoi laisser des informations personnelles aux quatre vents ?

KeePass

C'est un système de coffre permettant de stocker en lieu sûr vos mots de passe et identifiants, numéro de CB, de compte en banque, divers numéros de série d'appareils, de licences informatiques, ... **KeePass est l'élément le plus important de votre sécurité** car avec un seul mot de passe, il vous permet de stocker et d'utiliser facilement des mots de passe compliqués pour toutes vos applications qui en nécessitent un.
Il peut être installé complètement sur PC fixe, PC portable, tablette ou téléphone genre Smartphone ou être utilisé en mode portable placé sur mémoire (clé) USB sans installation et utilisé depuis un PC fixe, PC portable. C'est le même fichier coffre qui sert dans tous les cas.
Le fichier coffre (élément séparé de l'application KeePass) peut être copié, collé, renommé. Il peut contenir également de petits fichiers personnels à protéger, mais n'est pas en premier lieu fait pour sécuriser des fichier/dossiers.
Téléchargeable sur le site de l'auteur : http://keepass.info/download.html, ainsi qu'un patch de mise en français. Choisir la version "Classic" (version 1.xx).
Si besoin, se reporter aux fiches pour sa mise en œuvre sur PC ou en version portable sur http://www.rakforgeron.fr
Notez le mot de passe dans votre tête !

7-Zip

7-Zip permet de zipper (et dé-zipper) un/des fichiers et/ou un/des dossiers avec leur contenu et si vous le désirez de crypter le fichier zip final. Le destinataire doit avoir 7-zip installé pour en récupérer le contenu.
On peut zipper et crypter en générant un fichier exécutable qui pourra, avec le mot de passe, s'auto dé-zipper chez le destinataire sans qu'il ait 7-Zip installé. Dans ce cas, il convient de choisir le codage .7z.
Le décodage restituera toute l'arborescence qui a été précédemment zippée.
Si besoin, se reporter à la fiche s'y rapportant sur http://www.rakforgeron.fr
Le mot de passe doit être échangé avec le destinataire par une autre voie que celle du fichier lui-même.
Notez le/les mots de passe utilisés et leurs destinataires respectifs en lieu sûr (dans KeePass par exemple).

AxCrypt

AxCrypt permet de crypter un/des fichiers et/ou un/des dossiers avec leur contenu et les décrypter. A utiliser plutôt pour des cryptages au coup par coup, et notamment pour envoyer des documents personnels joints à des Mél.
On peut générer soit un fichier crypté simple qui nécessite, outre le mot de passe, d'avoir l'application installée sur le PC destinataire.
Sinon, on peut générer un fichier crypté auto-extractible sans avoir besoin d'avoir l'application installée chez le destinataire.
Le mot de passe doit être échangé avec le destinataire par une autre voie que celle du fichier lui-même.
Téléchargeable sur le lien : http://www.axantum.com/AxCrypt/Downloads.html
Existe en version à installer ou portable à placer sur une mémoire USB par exemple.
Attention : Il semble qu'à partir de la version 2, une adresse Mél est demandée pour utiliser le logiciel, même avec la version portable. Je préfère utiliser la dernière version 1.7.3156 qui semble être plus anonyme. Vous trouverez

facilement des sites la proposant.
Notez le/les mots de passe utilisés et leurs destinataires respectifs en lieu sûr (dans KeePass par exemple).

VeraCrypt remplaçant de TrueCrypt

L'histoire de ces applications semble labyrinthique ! Elles permettent de créer et gérer un fichier coffre fort de grande capacité (à votre choix) qui, une fois ouvert, se raccorde à l'arborescence de votre PC. Vous pouvez alors y placer, copier, coller, effacer et lancer tout fichier ou programme comme partout ailleurs dans l'arborescence du disque dur.
Ce coffre, quand il est fermé se présente sous l'aspect d'un fichier que l'on peut déplacer, copier…
TrueCrypt n'est plus maintenu par son concepteur mais est toujours parfaitement fonctionnel, est téléchargeable sur le lien https://truecrypt.ch/downloads/ . La dernière version est la 7.1a.
Son installation n'est pas compliquée, mais un peu longue. Un patch de mise en français est disponible dans la même page.

TruCrypt est remplacé par VeraCrypt téléchargeable sur le lien https://veracrypt.codeplex.com/
Utilisez un mot de passe "sérieux" noté en lieu très sûr (dans KeePass par exemple).

Audité par des structures sérieuses, il semble que l'assurance de la sécurité totale de ce nouvel outil ne soit pas évidente... Je garde TrueCrypt sous la main pour le moment, en attendant d'avoir une solution fiable disponible.

Suites bureautique

Les suites bureautique gratuites telles que libreOffice, OpenOffice ou celles payantes, permettent de crypter les fichiers de documents au format .doc, les fichiers de tableur .xls, ...
La mise en oeuvre du cryptage s'effectue au moment de l'enregistrement du document dans le menu "Enregistrer sous" en choisissant l'option correspondante.
Notez le/les mots de passe utilisés en lieu sûr (dans KeePass par exemple).

Ouadelse ?

Il existe également des possibilités de crypter ses Méls. Documentation à venir.
D'autres programmes sont utilisables pour chacune des différentes tâches couvertes par ceux proposés ici. J'ai présenté uniquement ceux que j'utilise.

Important

- Il est recommandé d'utiliser des mots des passe différents pour les systèmes de stockage de sécurité.
- Stockez vos mots de passe principaux en lieu sûr. Ceci est plus particulièrement important pour KeePass car si vous perdez le mot de passe d'entrée, son contenu est alors irrémédiablement perdu sans aucune récupération possible.
- Protéger ses données dans tel ou tel coffre ne dispense pas d'en effectuer des sauvegardes régulières.
- Chargez toujours les fichiers de vos applications sur le site de leur concepteur.
- N'utilisez aucun moyen de stockage de mots de passe déporté !