# Quelques règles de sécurité

*Les documents anciens qu'ils soient sur papier ou parchemin, les vieilles photos sur cadre de verre, papier, ou films négatifs, sont venus jusqu'à nous malgré l'apparente fragilité de leur support.*
*Aujourd'hui, nous numérisons beaucoup de documents, nous réalisons un grand nombre de photos numériques. Vont-ils arriver jusqu'à nos arrière-petits-enfants ? Rien de moins sûr !*

Sont rassemblés ici quelques conseils de sécurité relatifs notamment au classement et à la pérennisation des documents de documents informatiques liés à la généalogie et la paléographie.
Bien sûr ces conseils peuvent être mis en œuvre par tout utilisateur d'un PC.

## Fichiers

*Nommez les fichiers "logiquement".* C'est le meilleur moyen de s'y retrouver.

- Utilisez des noms de fichier "logiques", ayant un sens avec leur contenu, cela facilitera les recherches et regroupements.
- Ne jamais travailler sur vos fichiers originaux, ne travaillez que sur des copies.
- Si vous y avez apporté une modification, évitez d'enregistrer en écrasant votre fichier de départ, sauf si vous le désirez.
- Il est recommandé d'enregistrer un fichier modifié en gardant le même nom que celui du fichier de départ mais en lui ajoutant une ou un groupe de lettres ("m" comme modifié, ou "nb" pour Noir et Blanc par exemple) afin de le distinguer de l'original que l'on garde intact.

## Dossiers (répertoires)

*Nommez les dossiers "logiquement".* C'est le meilleur moyen de s'y retrouver.

- Un grand nombre de documents nécessite un classement rigoureux.
- Le nom des dossiers doit, comme pour les fichiers, avoir un sens logique associé au type de documents (fichiers) qu'il contient. C'est la meilleure façon de s'y retrouver par la suite.
- Ne pas hésiter à créer des sous-dossiers afin d'éviter un le nombre de fichiers trop important dans chacun d'eux.

## Sauvegardes

*Pensez à sauvegarder !*

- Pensez à effectuer une ou plusieurs sauvegardes de vos fichiers que vous rangerez en différents lieux sûrs.
- Quels qu'ils soient, tous les supports de stockage d'information ont une durée de vie différente, mais limitée, une sensibilité aux agents extérieurs (température, chocs, rayons du soleil, ...) qui varie d'un type à l'autre, d'où la nécessité de les multiplier en les variant.
  Diversifiez les formes de sauvegarde : disque dur extérieur sur port USB ou sur réseau, CD, DVD, dans une mémoire SD Card, mémoire USB (clé USB), ..., chaque forme de sauvegarde ayant ses qualités et ses défauts.
  Avoir au moins une sauvegarde sous deux formes différentes.
- Diversifiez les lieux de rangement des sauvegardes (on ne met pas tous ses oeufs dans un même panier).
- Ne pas jamais penser qu'une sauvegarde est sûre et définitive.
- Effectuez des mises à jour de vos sauvegardes régulièrement à l'aide de SyncBack Free* par exemple, pour des sauvegardes sur mémoire USB, SD Card, ou disque dur externe ou réseau.
- Effectuez des sauvegardes en changeant le nom de la sauvegarde, en y rajoutant la date par exemple de manière à ne pas écraser la sauvegarde précédente.
- Générez de nouvelles sauvegardes sur des supports neufs, si les précédentes sont trop anciennes.
- Attention au "Cloud". Préférez des systèmes privés en qui vous aurez plus confiance.
  N'y placez que des éléments neutres et impersonnels. Sinon, encryptez avec mot de passe !

Note importante : Ne débranchez pas un élément USB (mémoire dite "clé USB" ou disque extérieur) de manière "brutale".

Suivez toujours la procédure qui consiste à cliquer gauche sur l'icône de la connexion UBS  sous Windows 7 ou  sous Windows XP situé dans la barre des tâches en bas à droite de votre écran, puis cliquez sur "*Ejecter*" (dans Windows 7) ou "*Fermer*" (dans Windows XP).
Attendez que le système vous dise que "*Le matériel peut être retiré en toute sécurité*" pour débrancher votre

périphérique USB.

## Stockage de sécurité

*Il faut judicieusement répartir les lieux de sauvegarde.*

- Pour la sauvegarde de vos mots de passe il est conseillé d'utiliser un logiciel "coffre" qui permet de les rassembler et les stocker de manière protégée et sûre, dont l'accès est contrôlé par un mot de passe unique. On peut par exemple, utiliser *KeePass**.
- Les fichiers peuvent être entreposés dans un coffre fort (réalisé à l'aide d'un gros fichier protégé) qui ne sera accessible qu'avec un mot de passe. Utiliser par exemple *TrueCrypt**.
- La fonction ZIP (compression de fichiers) permet de rassembler en un seul fichier tout un ensemble de dossiers et les fichiers qu'ils contiennent, en maintenant l'organisation de ceux-ci. De plus, ils peuvent être protégés par un mot de passe. On peut utiliser *7-zip** par exemple.

## Envoi de fichiers par Mél

*Si besoin, les fichiers joints à des mails que vous envoyez à vos correspondants peuvent être protégés.*

- On peut utiliser la fonction ZIP (programme *7-zip** par exemple) qui, outre le regroupement dans une seule entité informatique (fichier au format .zip), permet une protection par mot de passe.
- L'utilisation d'un logiciel de cryptage permet de protéger efficacement un fichier ou des dossiers. Le logiciel *AxCrypt** peut être utilisé efficacement. Le destinataire n'a pas besoin de l'avoir installé sur son PC, le fichier étant auto extractible chez le destinataire dès l'entrée du mot de passe.
- Le mot de passe doit bien sûr être communiqué au correspondant par un moyen séparé.
- Voir les informations sur les mots de passe ci-dessous.

## Réception de fichiers par Mél

*Attention aux messages issus d'expéditeurs inconnus.*

- N'ouvrez aucun fichier joint à un message reçu d'un expéditeur inconnu.
- N'ouvrez aucun message reçu d'un expéditeur inconnu. Mettre le message et son contenu joint directement dans la poubelle !
- Jetez directement tout document joint qui vous semble suspect, même venant d'un expéditeur connu. Certains peuvent s'être fait pirater leur agenda.
- Enregistrez dans le dossier adéquat les fichiers joints à des messages d'expéditeurs que vous connaissez.
- Tout bon anti virus peut automatiquement scanner un fichier joint à un message, ou vous pouvez lui demander un scan du fichier que vous venez "d'enregistrer sous..." pour s'assurer de son intégrité.
- Videz régulièrement votre logiciel de messagerie.

## Mots de passe

*Un mot de passe doit toujours être choisi avec soin. Vous en aurez plusieurs !*

- Bien sûr la qualité d'un mot de passe doit être à la hauteur de ce qui est à protéger.
- Utilisez un mot de passe d'au moins 8 caractères composé de caractères numériques, alphabétiques majuscules et minuscules mélangés (et signes de ponctuation si nécessaire).
- Ne pas utiliser son numéro de carte bleue comme mot de passe !
- Evitez d'utiliser de mot de passe personnellement explicite comme sa date de naissance, le prénom de ses enfants ou le nom de sa mère, ...
- Avoir plusieurs mots de passe pour des besoins différents :
  - les mots de passe de boite à lettres
  - les mots de passe de forums
  - les mots de passe d'accès à des serveurs (ftp, connexion Internet, ou autres)
  - les mots de passe d'accès à des abonnements (Généanet, ...)
  - le mot de passe de réseau Wifi (préférez le protocole WPA)
- Il vaut mieux avoir un mot de passe complexe. On peut le stocker dans un coffre à mots de passe comme par exemple *KeePass** qui peut fonctionner sur une mémoire USB (clé USB). Des logiciels "coffre" comme *KeePass** ont un générateur de mot de passe intégré.
- Assurez-vous de respecter les règles dans le choix du mot de passe du site sur lequel vous désirez en entrer un. Ces règles pouvant imposer un nombre de caractère minimum et/ou maximum, autorisant ou pas certains caractères au-delà des caractères alphanumériques minuscules et majuscules, tels que *%^$)~+/...*

** Il existe un grand nombre de programmes gratuits, libres ou payants, permettant de réaliser des fonctions de sécurité plus ou moins complètes. Quelques uns d'entre eux ont été cités ici, ne présumant pas de leur qualité et de leur capacité ni de celle de tous les autres.*
*Certains d'entre eux peuvent être inclus de base dans l'OS (Operating Système) de votre PC : Windows 7, Xp ou Vista, distribution Linux. Reportez-vous aux éléments d'aide fournis avec votre ordinateur.*

## Aide à distance

***L'aide à distance peut être pratique, mais attention…***

- Ne demandez ou n'acceptez de l'aide que d'une personne que vous connaissez et en qui vous avez confiance.
- A tout moment vous pouvez fermer la session.
- Suivez toutes les opérations effectuées, l'Aidant doit expliquer son intervention au fur et à mesure.
- Ne se faire aider qu'avec une conversation téléphonique pendant tout le temps de l'intervention, afin d'avoir des explications au fur et à mesure.
- Si vous avez des documents confidentiels, ne pas les laisser visibles sur le bureau, les placer dans un dossier ou un sous dossier, ou mieux dans un "coffre" (*TrueCrypt** par exemple).
- Conservez vos mots de passe dans un environnement sécurisé (*KeePass**, logiciel libre et gratuit, par exemple).
- Assurez-vous de bien refermer le programme qui a permis l'aide à distance à la fin de la session.

## Et votre PC …

***Il faut aussi penser à appliquer quelques règles pour son PC lui-même.***

- Activez la mise à jour automatique, téléchargement et installation, de l'Operating Système (OS) de votre PC, que ce soit XP ou Windows 7 ou autre.
- Activez la mise à jour automatique de votre antivirus.
- Activez votre pare-feu.
- Activez la mise à jour automatique, sinon accepter toutes celles proposées, de toutes vos applications de communication comme FireFox ou Internet Explorer, Thunderbird, Filezilla, …
- Assurez-vous de toujours utiliser la dernière version de vos principaux logiciels.
- Ne téléchargez des mises à jour ou des logiciels nouveaux que depuis le site de leur concepteur. Attention aux sites "parasites" qui vous fournissent un fichier de téléchargement qui une fois lancé, va effectuer des opérations complémentaires au téléchargement de ce qui vous intéresse.
- Lors de l'installation d'applications (programme) faites attention à n'installer que ce dont vous avez besoin : décochez les options de toutes les barres d'outils et options invasives proposées.
- Regardez attentivement toutes les options proposées lors de l'installation ou de la mise à jour d'une application.
- Lancez une analyse complète de tous les disques de votre PC par votre anti-virus au moins une fois par mois.

## Liens de téléchargement des logiciels conseillés

***Ne téléchargez les applications ou leur mise à jour que depuis le site de son concepteur****, ou depuis un site connu. Assurez-vous de télécharger la dernière version (si elle est toujours proposée gratuitement).*

- **KeePass** logiciel libre et gratuit : *http://keepass.info/download.html*
  Pour le passer en français : *http://keepass.info/translations.htm*
  Une version sans installation qui peut être utilisée sur une mémoire USB (Clé USB) est proposée.
- **7-Zip** logiciel libre et gratuit : http://www.7-zip.org/
- **AxCrypt** : http://www.axantum.com/axcrypt/Downloads.html
- **TrueCrypt** logiciel libre et gratuit, malheureusement plus maintenu, son successeur **VeraCrypt** :
  https://veracrypt.codeplex.com/wikipage?title=Downloads
- **TeamViewer** logiciel gratuit pour un usage personnel :
  *http://download.teamviewer.com/download/TeamViewer_Setup_fr.exe*
  Il existe une version simple "QuickSupport" sans installation :
  *http://download.teamviewer.com/download/TeamViewerQS_fr.exe*
- **SyncBackFree** logiciel version gratuite :
  *http://www.2brightsparks.com/download-syncbackfree.html*