Effacement sécurisé des données

Supprimer des données de façon définitive s'avère bien plus difficile qu'on le croit. Car il y a supprimer et supprimer... La solution la plus sûre – qui serait la destruction physique du support de stockage – n'est la plupart du temps pas envisageable dans la pratique. Or des alternatives existent.

Pour effacer des données de manière sécurisée,

- écrasez (plusieurs fois) les espaces libérés sur les supports magnétiques ou les bandes de données à l'aide d'utilitaires dédiés.
- écrasez l'ensemble de l'espace de stockage des supports de données électroniques tels que les clés USB, les cartes SD ou les disques durs SSD à l'aide d'utilitaires dédiés (une fois est suffisante).
- réinitialisez votre smartphone ou votre tablette en restaurant les paramètres d'usine avec activation du chiffrement de l'appareil.
- détruisez physiquement les supports optiques tels que CD-R/RW ou DVD-R-RW.
- chiffrez l'ensemble de l'espace de stockage ou les informations sensibles stockées sur vos supports, indépendamment de leur type, et détruisez la clé de chiffrement.
- détruisez physiquement le support

Les fichiers ayant été supprimés sans précautions particulières peuvent être récupérés la plupart du temps à l'aide de logiciels spécialisés. En effet, un fichier ne peut pas être considéré comme supprimé tant qu'il n'a pas été écrasé par d'autres données. La difficulté réside donc dans localisation et l'effacement de tous les espaces disque correspondants.

Pour effacer des données confidentielles de manière définitive et irrévocable, vous devez vous procurer des logiciels spécialisés et utiliser une méthode adaptée au support de données utilisé.

Les supports magnétiques (disques durs ou bandes de données)

Des logiciels spéciaux permettent de ré-écrire (écraser) le disque ou la bande à l'emplacement des données que l'on souhaite supprimer avec des schémas de données (parfaitement dénués de sens). Le processus de ré-écriture (écrasement) est souvent répété plusieurs fois. Cette méthode permet de supprimer les données de manière irrévocable.

Plusieurs logiciels, payants et gratuits, sont disponibles sur le marché comme par exemple :

Windows

- **Eraser** : Téléchargement : eraser.heidi.ie (https://eraser.heidi.ie)
- **Secure Eraser** : le site Web de la revue Computerbild propose une bonne présentation (https://www.computerbild.de/download/Secure-Eraser-1276072.html) du logiciel. Téléchargement : www.secure-eraser.com

(http://www.secure-eraser.com)

macOS

- **Permanent Eraser** : Téléchargement : www.edenwaith.com (http://www.edenwaith.com)

Les supports électroniques (disques durs SSD, clés USB ou cartes SD)

Pour des raisons techniques, les programmes susmentionnés ne permettent pas de supprimer de manière sûre des fichiers isolés enregistrés sur des supports électroniques.

La seule solution est de procéder au formatage complet et d'écraser l'ensemble de l'espace de stockage, ce qui comporte bien évidemment la perte de l'ensemble des fichiers. La solution alternative est de chiffrer les données stockées (cf. plus bas).

Smartphones et tablettes

Pour effacer définitivement les supports de stockage de données intégrés dans les smartphones et tablettes, il est possible de restaurer les paramètres d'usine si le chiffrement de l'appareil est activé. Mais attention : cette opération détruira toutes les données de l'utilisateur !

Android

1. Activez le chiffrement de l'appareil dans **Paramètres / Sécurité** et patientez jusqu'à la fin du processus (attention : cela peut prendre parfois beaucoup de temps !)
2. Pour restaurer les paramètres d'usine : **Paramètres / Système / Réinitialisation**.

iOS

1. Pour les dispositifs iOS actuels, le chiffrement est activé par défaut et ne peut pas être désactivé.
2. Grâce à votre identifiant Apple, votre appareil reste associé à vous même après avoir effacé toutes vos données. Si vous souhaitez donner votre appareil à quelqu'un d'autre, vous devrez au préalable (c.à.d. avant d'effacer vos données) supprimer l'association à votre identifiant Apple en vous déconnectant du service. Pour ce faire : **Réglages / Déconnexion / Désactiver**.
3. Puis, restaurez les paramètres d'usine dans **Réglages / Général / Réinitialiser / Effacer contenu et réglages**.

Une autre méthode simple pour effacer au moins les dossiers photos et vidéos consiste à réaliser, après avoir effacé manuellement leur contenu, une vidéo « vide », c'est-à-dire avec l'objectif dirigé sur une table par exemple, et de continuer à enregistrer jusqu'à ce que la mémoire soit pleine. (Attention : sachez que la vidéo enregistre aussi le son et que certains espaces de mémoire, tels que les messages par exemple, ne seront ni effacés, ni écrasés).

Les supports optiques (CD-R/RW ou DVD-R-RW)

Force est de constater que les supports optiques tels que les CD-R/RW ou DVD-R/RW sont trop souvent oubliés lorsque l'on aborde le problème de l'effacement des données. Lorsqu'ils ne sont plus utilisés, ils finissent souvent à la poubelle, avec toutes les données qu'ils contiennent, confidentielles ou pas.

Il est techniquement impossible d'effacer les CD-R / DVD-R de manière sécurisée. Quant aux supports réinscriptibles (CD-RW / DVD-RW), la procédure n'aurait aucun sens au regard de la valeur commerciale très faible du support en lui-même.

Dans ce cas précis, la destruction physique du support de stockage représente la méthode à la fois la plus sûre et la plus pratique.

La destruction physique du support de stockage

La destruction physique est une méthode d'effacement sécurisé des données qui peut être appliquée pour tous les types de supports. Pour cela, il suffit de détruire la puce-mémoire en perçant par exemple un trou dans un disque dur ou en écrasant une clé USB avec un marteau. Certaines sociétés offrent aussi une méthode plus professionnelle et garantissant un niveau de sécurité supérieur avec un destructeur de document conforme à la norme DIN 66399.

Bien sûr, lorsque vous détruisez physiquement un support de stockage, vous réduisez à néant sa valeur commerciale. Cette solution n'est donc généralement pas envisageable pour les supports de stockage plus chers comme les disques SSD d'une certaine capacité ou pour les dispositifs où le support de stockage est intégré dans l'appareil (ex. smartphones ou tablettes). Dans ce dernier cas de figure, le chiffrement des données représente une bonne alternative.

La protection des données par chiffrement

L'alternative la plus sûre et en même temps la plus flexible aux différentes formes de suppression des données consiste à chiffrer les informations et les fichiers les plus sensibles pour les rendre illisibles à toute autre personne autre que l'utilisateur. Contrairement aux méthodes d'effacement, cette protection est efficace pendant tout le cycle de vie des données et même au-delà. Une fois la clé de chiffrement supprimée, les données chiffrées seront irrémédiablement perdues.

Pour être certain qu'aucun contenu non protégé ne sera jamais enregistré sur un support de stockage, ce dernier devra être chiffré dès sa mise en service. Là encore, l'utilisateur dispose de plusieurs programmes :

Windows

- **BitLocker** est une fonction permettant de chiffrer des supports de données complets. Disponible dans les versions Windows Ultimate / Pro et Enterprise.
- **EFS** est une fonction Windows standard embarquée du système de fichiers NFTS qui permet de chiffrer ponctuellement certains fichiers ou dossiers.
- **VeraCrypt** est gratuit, puissant et simple d'utilisation.Téléchargement : www.veracrypt.fr (https://www.veracrypt.fr)

macOS

- **FileVault** est une fonction standard intégrée à macOS pour chiffrer des fichiers ou l'ensemble du disque dur.
- **VeraCrypt** est gratuit, puissant et simple d'utilisation. Téléchargement : www.veracrypt.fr (https://www.veracrypt.fr)

La destruction définitive et irrévocable des données passe par la destruction physique du support de données. Mais dans la pratique, on a recours à des programmes spécifiques qui suppriment les données par écrasement. L'alternative, valable tout au long du cycle de vie des données et même au-delà, est de les protéger par chiffrement.

Pour aller plus loin

Vider la corbeille ou formater son disque dur ne suffit pas

En informatique, la procédure normale de suppression d'un fichier prévoit tout d'abord son transfert dans la corbeille, À partir de là, ce fichier peut être rétabli ou définitivement supprimé (tout du moins en apparence) si l'on vide la corbeille. En apparence, car ce processus ne fait qu'effacer l'adresse du fichier dans le répertoire. Le fichier devient alors « invisible » aux yeux de l'utilisateur, et son emplacement sur le disque se trouve libéré et prêt à être réécrit. De cette manière, les données demeurent sur le disque jusqu'à ce qu'elles ne soient écrasées par un nouveau fichier venant s'enregistrer sur l'emplacement ainsi libéré.

Même chose pour le formatage des supports de données. Un formatage rapide consiste simplement à supprimer l'index du système de fichiers. Le contenu des fichiers est donc conservé, même si l'utilisateur n'y a plus accès.

Le formatage haut niveau est plus efficace. Cette procédure consiste à remplir entièrement le disque dur avec des zéros. Dans ce cas, toute récupération des données est dans la pratique impossible avec des moyens raisonnables.

C'est ce qui explique pourquoi il est possible de récupérer des fichiers supprimés, lorsque ceux-ci ont été supprimés mais pas écrasés. Cela peut d'ailleurs se révéler très utile en cas de suppression involontaire d'un fichier dont vous avez encore besoin. D'un point de vue de la sécurité, cette méthode n'est toutefois pas recommandée lorsque vous devez p. ex. supprimer définitivement un document confidentiel.

Pour effacer définitivement un fichier précis ou l'ensemble d'un support de stockage, il faut s'équiper de logiciels dédiés. La marche à suivre dépend alors du type de support utilisé et donc du processus d'enregistrement utilisé.

Les disques durs magnétiques

Sachant que l'emplacement d'un fichier est précisément défini sur les supports de données magnétiques, des logiciels dédiés permettent de localiser et d'écraser cet espace du disque dur, sachant que le processus est la plupart du temps plusieurs fois répété pour des raisons de sécurité. De cette manière, les données sont irrévocablement supprimées.

Lorsque vous souhaitez vous débarrasser ou vendre votre vieil ordinateur, il convient de commencer par en extraire le disque dur ou de supprimer au préalable toutes les données qui y sont stockées. Enfin, pour éviter que l'acheteur de votre appareil puisse récupérer vos données sensibles, le plus simple est d'utiliser un CD bootable contenant les utilitaires de suppression des données qui vont écraser complètement le disque dur (p. ex. DBAN (https://www.dban.org) pour Windows).

Les clés USB et les cartes SD

Sur les supports de stockage à base de mémoire Flash, tels que les clés USB ou les cartes de mémoire SD, un même contenu peut, pour des raisons techniques, être stocké dans plusieurs emplacements. Des copies sont ainsi créées automatiquement. Lors d'un effacement par écrasement, on ne supprime que la dernière copie utilisée, les autres étant conservées dans la mémoire.

Cela signifie que pour supprimer un fichier de façon sécurisée, il sera nécessaire de formater l'ensemble du support. Il faut donc garder à l'esprit que les clés USB et les cartes SD ne permettent pas de supprimer de façon sécurisée des fichiers isolés.

Les disques durs SSD

Les programmes mentionnés plus haut ne permettent pas l'effacement sécurisé des données stockées sur les disques durs SSD embarqués sur les ordinateurs les plus récents. Techniquement parlant, cela s'explique de la façon suivante : en vue d'assurer une usure uniforme des cellules de mémoire, les contenus enregistrés sur le disque durs sont automatiquement réorganisés à intervalles réguliers. Cette réorganisation génère des copies « perdues » des données et qui ne peuvent pas être écrasées. Un effacement des données par écrasement ne peut donc pas être considéré comme définitif et irrévocable.

Certains fabricants de disques durs SSD proposent des fonctions embarquées qui permettent de localiser et de supprimer ces données perdues, apparemment de manière définitive. Le fonctionnement et la fiabilité de cette fonction restent néanmoins difficiles à vérifier.

Outre la solution de la destruction physique du disque, là encore le meilleur moyen d'effacer définitivement des fichiers est de formater l'ensemble de l'espace disque.

Une alternative sûre consiste par ailleurs à chiffrer les dossiers sensibles ou directement l'ensemble de l'espace disque. Sans clé de chiffrement, personne ne pourra accéder à vos contenus confidentiels. Le chiffrement présente également l'avantage de protéger vos fichiers sensibles en cas de perte ou de vol de votre dispositif (votre ordinateur portable p. ex.). Sans le précieux sésame en main, impossible d'accéder à votre disque dur !

Les supports optiques

Dans le cas des supports optiques enregistrables, les données sont gravées au laser en créant des alvéoles sur une couche réfléchissante. Selon le type de support, le processus d'inscription peut avoir lieu une fois (dans le cas des CD-R) ou plusieurs fois (CD-RW ou réinscriptibles).

Étant donné la difficulté technique et le faible prix d'un CD, la solution de la destruction physique du support de stockage s'avère ici la plus adaptée pour supprimer les données.

Les bandes magnétiques

Les bandes magnétiques sont souvent utilisées pour la sauvegarde et l'archivage de grandes quantités de données, pour une durée relativement longue parfois. Elles permettent donc d'avoir un « coup d'œil sur le passé », même sur des données que l'on croyait perdues depuis longtemps.

Sur ce type de support, l'enregistrement des données est séquentiel. Les bandes magnétiques constituent en général une mémoire auxiliaire non modifiable et donc inviolable. Dans la mesure où il est impossible d'éliminer des fichiers isolés, La solution est de détruire l'ensemble du jeu de sauvegarde.