

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant 8 heures l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données professionnelles ni personnelles derrière soi.

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction ?

Denis Jacquot, l'ordinateur professionnel qui vous a été mis à disposition étant généralement en état de service, à moins d'être des circonstances ou des cas particuliers, vous devrez donc rendre cet appareil au mieux dans l'état initial.

En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.

De manière à vous empêcher d'être contacté une copie et de l'utiliser contre votre ancien employeur.

1. Identifier les données ayant un caractère confidentiel et qui nécessitent une sauvegarde dans un format protégé par un procédé tel que le cryptage tel que le logiciel de cryptage.
2. Identifier les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de assistance.
3. Identifier les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants.)
4. Identifier les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ce soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifier les fonctions de « Sauvegarde », « Exporter » ou « Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptés soit :

- à la confidentialité (tout support numérique en utilisant un logiciel de cryptage tel de logiciel de cryptage, par exemple un disque dur USB, un disque dur externe, un disque dur externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.
- à l'intégrité (utiliser le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à l'abandonnement pas perdre) ;
- à la longévité (utiliser des supports avec une durée de vie adaptée à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'évolution des versions, des formats et des logiciels). On peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité (plusieurs plateformes et les plusieurs lieux, comme le proposent les solutions cloud qui sont idéales) y a quelques dizaines d'années seulement ;
- à la rapidité (pour plusieurs plateformes et les plusieurs lieux, comme le proposent les solutions cloud qui sont idéales) y a quelques dizaines d'années seulement ;
- à la quantité (car vous devez rapidement stocker pour ensuite être en mesure de choisir un support adapté en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques :

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tombent un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tombent un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteurs DVD, lecteurs Blu-ray, lecteurs de bande etc. sont de plus en plus rares. Conservez des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant que vous souhaitez accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vie de vos données numériques entre les mains de Son Ciel.

Pensez, en fonction de vos données, à partir de ces conseils, si ne vous restes plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Conseils :

Disque dur : Quelque Soit à quelconque To – Son marché, rapide mais fragile.

Clé USB : Quelque Soit – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne

Cloud : Quelque Soit à quelconque To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdre tout.

Disques optiques (CD, DVD, Blu-ray, etc.) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (paramètres des lecteurs de disques) jusqu'à quand ?

Supports externes (ZIP, lecteurs DVD, lecteurs Blu-ray, lecteurs de bande etc.) : Supports fragiles, lecteurs trop rares pour garantir une lecture au-delà de 10 ans.

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé ?

La procédure élimine totalement :

- Les programmes installés ;
- Les e-mails ;
- Les traces de navigation ;
- Les fichiers téléchargés ;
- Divers identifiants et mots de passe ;
- Les fichiers temporaires.

Mais d'activer l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes installés :

Facile sur Mac et mettre le dossier d'un programme à la corbeille, s'utiliser surtout pas la corbeille pour supprimer des programmes sous Windows. Le plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

- soit par le recours de désinstallation que le programme a créé ;
- si il n'y a pas de recours prior à cet effet, passer par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
- Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails :

Selon le programme que vous utilisez, la suppression du dossier compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

- Fichiers dans « %userprofile%\local settings\application data\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- Les fichiers contenus dans « %localappdata%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird

Le dossier contenu dans « %local settings\application data\Microsoft » pour le programme InternetMail.

Concernant les traces de navigation :

De fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'« Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés :

De fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe :

De fait que le mot de passe de votre système d'exploitation stocke quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un backup de type « utilisateur ».

De fait que les mots de passe que vous avez mémorisés au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passe et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires :

En utilisant la fonction adéquate dans votre navigateur Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).

En utilisant la fonction adéquate dans votre système d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir :

Pensez qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore ».

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

- Accéder à vos documents et déjouer les informations qui peuvent être professionnelles et être utilisées contre vous, mais personnelles permettant à un copain de les utiliser contre vous tout en vous demandant de l'argent contre son silence ou pour avoir le paix ;
- Accéder aux identifiants et mots de passe des comptes Internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à vos comptes Facebook, Twitter, Dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement apposer des commentaires ou envoyer des e-mails en utilisant votre identité.

Auteur : Denis JACQUOT

Denis Jacquot anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du Travail de l'Emploi et de la Formation Professionnelle n°93 04 03041 04).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques de information, découvrir et comprendre les attaques et les stratégies informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL et le maître de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lanetsecur.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

IS

IS

IS

Rejoignez à cet article

Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr