



Comment détruire de manière sûre les données d'un disque dur

Les disques durs modernes peuvent contenir une...

Rédigé par: Philip Le Riche



INTRODUCTION

Les disques durs modernes peuvent contenir une énorme quantité de données, même celui d'un ordinateur mis au rebut il y a 10 ou 15 ans. Les gens disent souvent « Personne ne serait intéressé par mes données ! » Vous pourriez être surpris.

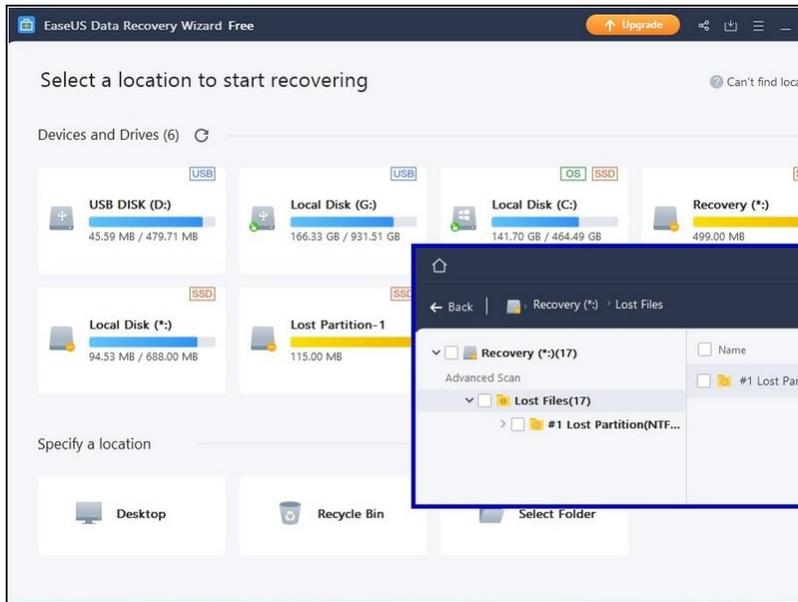
Les identifiants de connexion aux emails et aux réseaux sociaux sont très prisés par les pirates. L'accès à votre messagerie permettra à un pirate informatique de réinitialiser les mots de passe sur bon nombre de vos autres comptes, tels que PayPal, Amazon, les réseaux sociaux, le stockage sur cloud et peut-être même les services bancaires (bien que nous espérons que vous utilisez l'authentification à 2 facteurs pour les comptes plus sensibles). Une liste de vos contacts permettrait à un pirate de se faire passer pour vous et de leur envoyer des arnaques convaincantes.

Un pirate informatique pourrait être en mesure de récupérer des extraits de toutes sortes de données vous concernant, inoffensifs en eux-mêmes, mais utiles pour construire une tentative d'usurpation d'identité. Et plus.

Il est donc important qu'un disque dur ne quitte jamais votre possession sans que les données ne soient détruites de manière sécurisée.

La destruction des données sur les SSD, les clés USB et les cartes mémoire nécessite des méthodes assez différentes. Voir mon [tutoriel compagnon pour les SSD et les clés USB](#) si c'est votre problème.

Étape 1 — Ce qu'il ne faut pas faire



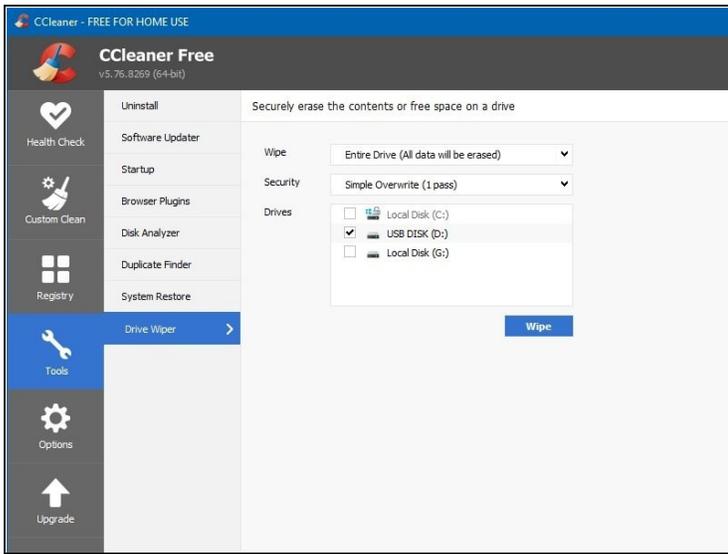
i Voici ce qu'il ne faut PAS faire :

⚠ Ne vous contentez pas de supprimer vos fichiers. Même si vous videz ensuite la corbeille, de simples outils disponibles gratuitement peuvent probablement les récupérer.

⚠ Ne pensez pas que le reformatage de votre disque va tout effacer. Cela ne fait que réinitialiser les index. La plupart de vos données resteront.

⚠ De même, n' imaginez pas que la réinstallation de votre système d'exploitation fera mieux. Cela écrasera uniquement le début de votre disque, laissant la plupart de vos données intactes.

Étape 2 — Destruction non physique



- La destruction physique est de loin la méthode la plus sûre et la plus rapide. Mais si vous DEVEZ VRAIMENT conserver l'ancien disque dur, vous avez le choix entre plusieurs utilitaires d'effacement de disque :
 - [Ccleaner](#) effacera un disque dur, mais pas celui à partir duquel vous avez démarré. Vous pouvez connecter votre ancien disque dur à un autre ordinateur avec un adaptateur USB-SATA afin de l'effacer.
 - Vous pouvez créer une clé USB ou un CD amorçable contenant [DBAN](#), qui effacera votre disque dur.
 - Les deux éléments ci-dessus peuvent laisser des fragments de données dans des secteurs de disque remappés et cachés. Blancco (de la même source que DBAN) est l'utilitaire de nettoyage de disque professionnel, doté de diverses certifications et approbations standard du gouvernement et de l'industrie. Une licence d'évaluation est disponible.
- ① Aucun de ceux-ci n'est rapide. Cela peut prendre de 12 à 24 heures pour un disque de 1 To. Voulez-vous vraiment attendre aussi longtemps ?

Étape 3 — Visez votre cible !



- Jetez un coup d'œil à votre disque dur. Depuis le dessus, vous devriez pouvoir distinguer le contour de l'emplacement du disque.
- En cas de doute, sur le dessous du disque, vous devriez pouvoir voir le moteur qui entraîne directement l'axe du disque.
- Sous le disque se trouve la broche de l'actionneur de la tête de lecture/écriture.
- Notez un point situé à environ la moitié ou les trois quarts du centre du disque et de sa circonférence. C'est là que vous ferez les dégâts !

Étape 4 — Facultatif : ouverture du disque dur



- Si vous avez des difficultés à déterminer où se trouve le disque, ou si vous êtes simplement curieux de voir à l'intérieur, vous pouvez dévisser le couvercle.
- Vous aurez généralement besoin d'un tournevis Torx. Il y a normalement 6 vis autour du périmètre du lecteur. Enlevez-les.
- La plupart des disques d'ordinateurs portables ont une vis de plus sous l'étiquette. Vous devrez la repérer au toucher, ou en la regardant avec la lumière juste au bon angle.
- Grattez l'étiquette autour de la tête de vis, à l'aide d'un cutter ou similaire. Sous l'étiquette, il y a probablement une couche de papier d'aluminium. Grattez-le également, pour faire apparaître la tête de vis. Retirez la vis.
- Les disques d'ordinateurs de bureau peuvent avoir plus de vis, que vous devrez repérer et retirer de la même manière.
- Une fois que vous avez retiré toutes les vis, vous devriez pouvoir retirer le couvercle. Un joint en caoutchouc peut le rendre un peu réticent à se détacher.

⚠ Remplacez le couvercle et fixez-le avec au moins 2 ou 3 vis avant de passer à l'étape suivante.

Étape 5 — La méthode du marteau et du clou



- La méthode la plus simple consiste simplement à enfoncer un clou dans le lecteur, ce qui brisera le disque. Un clou de maçonnerie de 25 mm x 2,5 mm est idéal – un clou plus gros sera plus difficile à retirer et il y aura plus de chances que des éclats s'échappent par le trou. Les clous standard pour bois se plieront simplement.
- Placez le lecteur sur un morceau de bois de rebut sur une surface ferme telle qu'un sol en béton ou un établi solide. En tenant le clou (de préférence) avec une pince, enfoncez-le dans et à travers le lecteur au point choisi.
- ① Le clou n'a pas besoin de traverser et de pénétrer dans la ferraille, tant que vous pouvez voir qu'il a commencé à pénétrer dans le circuit imprimé à l'arrière du lecteur.

- ① Si, après avoir pénétré le couvercle supérieur, le clou n'arrive pas à briser ou pénétrer le disque, il est très probable que ce soit l'un des rares à avoir un plateau métallique. La méthode alternative décrite à l'étape suivante fonctionnera très bien.
- Éloignez les éclats du clou avant d'essayer de le retirer. Si vous avez utilisé un marteau arrache-clou, vous pouvez utiliser l'arrache-clou pour retirer le clou très facilement, sinon utilisez une pince.
- Pour être sûr, enfoncez le clou à travers un second point à peu près diamétralement opposé.
- Couvrez les deux trous avec du ruban adhésif de n'importe quelle sorte.

Étape 6 — À l'aide d'une perceuse



- Si vous avez une perceuse à colonne, vous constaterez peut-être que cela vous permet de faire le travail plus rapidement. Un foret en acier rapide de 3 à 4 mm fera parfaitement l'affaire.
 - En perçant le couvercle et en appliquant une pression modérée, vous pouvez sentir le plateau de disque s'écraser lorsque le foret le frappe, ainsi que le second plateau s'il y en a un. Continuez à percer jusqu'à ce que vous arriviez de l'autre côté.
 - Si le plateau ne se brise pas même avec un peu de pression supplémentaire de la perceuse, enfoncez un clou ou un poinçon central dans le trou et frappez-le assez fort avec un marteau jusqu'à ce que vous brisiez le ou les plateaux.
 - Si la perceuse n'a pas pénétré à travers le lecteur, éloignez les éclats du trou et regardez à l'intérieur. Si vous pouvez voir une autre surface brillante ininterrompue, il y a un second plateau de disque. Écrasez-le de la même manière.
- ① Les disques très anciens, en particulier les disques d'ordinateurs de bureau (3,5") ainsi que quelques disques plus modernes peuvent avoir des plateaux en aluminium. Vous devriez pouvoir les percer sans difficulté.

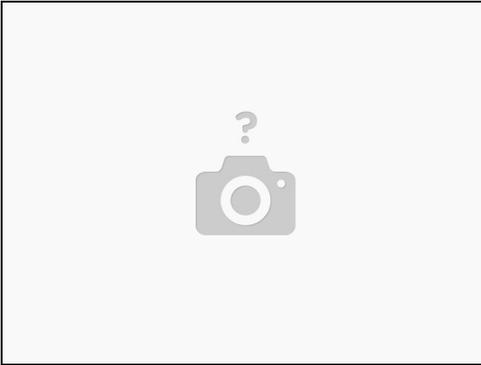
Étape 7 — Sécuriser avant de terminer



- Les éclats à l'intérieur seront extrêmement tranchants et certains d'entre eux très petits. Attention qu'ils ne s'échappent pas ! Avant de terminer, couvrez les trous des deux côtés avec du ruban adhésif ou similaire afin qu'aucun éclat ne puisse s'échapper. (Vous pouvez même utiliser un pansement !)

⚠ Il est toujours possible que de petits éclats s'échappent entre la carte de circuit imprimé et la coque métallique, alors continuez à traiter le lecteur avec soin. Pour éviter cela, vous pouvez dévisser et retirer le circuit imprimé avant de commencer.

Étape 8 — Un moyen plus facile la prochaine fois



- Le cryptage complet du disque dur est le moyen le plus simple de vous simplifier la vie la prochaine fois. Vous pouvez utiliser Bitlocker sous Windows ou Filevault sous MacOS. Si vous utilisez Linux, Veracrypt est disponible.
- ⚠ Il est important que vous cryptiez complètement votre disque dur immédiatement après l'installation du système d'exploitation et avant d'y écrire des données ou de vous connecter à des messageries emails, des réseaux sociaux ou tout autre site Web ou application, sinon des données non cryptées peuvent rester sur votre disque dur.**
- Lorsque vous souhaitez vous débarrasser de votre ordinateur ou du disque qu'il contient, tout ce que vous avez à faire est de changer le mot de passe de cryptage en quelque chose de long et totalement aléatoire, puis de détruire tous les enregistrements du mot de passe.
- ① Le chiffrement complet du disque appliqué comme décrit ci-dessus est le seul moyen simple et sûr de détruire les données sur un SSD.

Pour remonter votre appareil, attendez que quelqu'un invente une machine à remonter le temps, puis faites un voyage jusqu'à hier. Sérieusement, il n'y a pas d'autre moyen !

Mais si cela ne fonctionne pas pour vous, veuillez éliminer les restes de votre journée de travail de manière responsable, et appropriée pour les déchets électroniques.