ÊTES-VOUS COMPATIBLES AVEC LE RGPD ?

VOTRE VIE PRIVÉE EST IMPORTANTE

Sécuriser vos données quand vous vous déplacez est notre première préoccupation, pas seulement d'un point de vue professionnel, mais aussi d'un point de vue personnel.

Que se passe-t-il si un employé ramène les données d'un client chez lui sur un disque dur et le perd ou se le fait voler ? Ou si vous égarez une clé USB contenant des fichiers détaillant vos relevés de compte ?

À l'échelle globale, plus de 2 millions de ces petits appareils de stockage sont perdus chaque année,et des études ont montré que plus de la moitié des clés USB égarées sont branchées.

Utiliser des périphériques sécurisés est un moyen facile de réduire ce risque. Ces appareils brouillent les données de manière à ce que seule une personne disposant du code ou de la clé correcte puisse les lire.

Pouvez-vous vous permettre de **ne pas** encrypter vos données ?

Verbatim™

Technology you can trust

LE SAVIEZ-VOUS ?

14,717,618,286

DOSSIERS DE DONNÉES ONT ÉTÉ PERDUS OU VOLÉS DEPUIS 2013

Dans seulement **4 %** de ces cas, les données volées étaient **encryptées**, les rendant ainsi inutilisables pour les voleurs.

Sur l'ensemble total des dossiers volés, le secteur des **réseaux sociaux** a vu la plus forte hausse dans l'augmentation des incidents liés à la sécurité, passant de 1,51 % en 2017 à **56,18 %** en 2018. Dans le même temps, le nombre d'effractions dans le secteur médical a connu une baisse importante. Au premier semestre 2018, les secteurs du gouvernement, de l'éducation, du divertissement, des services financiers et des organisations à but non lucratif ont déclaré avoir connu **une diminution de 50 à 100 % des effractions liées à la sécurité** par rapport à l'année précédente.

Source : Breach level index 17/04/19

LES DOSSIERS DE DONNÉES SONT PERDUS OU VOLÉS AUX FRÉQUENCES SUIVANTES

Chaque jour	Chaque heure	Chaque minute	Chaque seconde
6 404 534	266 856	4 448	74

QU'EST-CE QUE LE RGPD ?

RGPD - RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

L'application du RGPD a rendu la loi sur la protection des données identique pour l'ensemble du marché européen.

Il a donné aux entreprises un environnement juridique plus simple et plus clair dans lequel évoluer et les employés ont davantage un droit de regard sur ce que les entreprises peuvent faire de leurs données.

Les entreprises ne se conformant pas à ce règlement seront passibles d'amendes plus lourdes. Les entreprises risquent une amende pouvant atteindre jusqu'à 4 % de leur chiffre d'affaires annuel ou 20 millions d'euros.

Tout cela fait qu'il est plus important que jamais de s'assurer que vos informations critiques et sensibles sont correctement protégées.

LE MALWARE EXPLIQUÉ

Virus : en se fixant aux fichiers et en infectant d'autres fichiers, ils peuvent se propager de manière incontrôlable, endommager les fonctionnalités principales d'un système et supprimer ou corrompre des fichiers.

Rootkits : logiciel permettant à un intrus d'obtenir l'accès root du système d'un ordinateur. Il est souvent caché et peut ne pas être détecté ni éliminé par l'antivirus.

Spyware: programme qui se cache dans l'arrière-plan et espionne les utilisateurs, prend des notes sur leur activité en ligne, y compris les mots de passe, les numéros de carte bancaires, les habitudes de navigation et plus encore.

Les chevaux de Troie : se faisant passer pour un logiciel légitime, les utilisateurs les téléchargent en pensant qu'il s'agit de logiciels utiles,et se retrouvent avec un ordinateur infecté.

Vers : il s'agit de programmes auto-répliquants qui ont pour intention de propager un code malveillant. En utilisant des interfaces réseau, ils peuvent infecter des réseaux entiers, soit localement, soit via Internet.

Un **ransomware** est un type de programme malveillant pouvant crypter silencieusement vos fichiers et rendre votre système inutilisable, avant d'exiger un paiement de rançon en ligne en échange d'une clé de déchiffrement.

CHIFFREMENT AES 256 BITS

QU'EST-CE QUE L'ENCRYPTAGE AES 256 BITS ?

AES est l'abréviation de Advanced Encryption Standard. Il s'agit d'un encryptage par bloc symétrique qui est adopté partout dans le monde pour crypter les données sensibles.

256 bits fait référence à la longueur de la clé d'encryptage utilisée pour crypter un flux de données ou un fichier. Un hacker ou un pirate aura besoin de 2^{256}* combinaisons pour décrypter un message encrypté en 256 bits.

L'encryptage AES n'a jamais été décrypté et est sûr contre toute attaque par force brute.

*2^{256} =115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 9 13 129 639 936

STOCKAGE DE DONNÉES AVEC ACCÈS PAR EMPREINTES DIGITALES

Utilisez vos données biométriques uniques pour une sécurité des informations totales.

DISQUE DUR SÉCURISÉ PAR EMPREINTES DIGITALES

- Disque dur portable USB-C™ avec scanner d'empreintes digitales intégré
- Accès par les empreintes digitales de l'utilisateur autorisé
- Encryptage de sécurité matériel AES 256 bits
- Jusqu'à huit empreintes d'utilisateurs autorisés et un administrateur (via mot de passe)
- Emmagasine et contient les données confidentielles tout en étant protégé en cas de perte ou de vol
- Câble USB-C™ vers USB-A et adaptateur USB-C™
- Logiciel de sauvegarde Nero Backup inclus

53650 1 To | 53651 2 To

CLÉ USB SÉCURISÉE PAR EMPREINTES DIGITALES

- Clé USB 3.0 élégante avec scanner d'empreintes digitales intégré
- Accès par les empreintes digitales de l'utilisateur autorisé
- Encryptage de sécurité matériel AES 256 bits
- Jusqu'à cinq utilisateurs autorisés et un administrateur
- Emmagasine et contient les données confidentielles tout en étant protégée en cas de perte ou de vol

49337 32 Go | 49338 64 Go | 49339 128 Go

CLÉ USB PRO SÉCURISÉE

USB CHIFFRÉ

- Encryptage du lecteur obligatoire à 100 %
- Mode de passe à 12 chiffres maximum
- Encryptage AES 256 bits avec matériel basé sur un contrôleur de sécurité
- Préchargé avec une application de sécurité avec exécution automatique intuitive
- Algorithme de hachage de mot de passe
- Saisie de mot de passe anti-hacking, s'efface après 10 tentatives infructueuse
- Aucun droit d'administrateur requis sur le PC hôte
- Compatible PC et Mac

98664 16 Go | 98665 32 Go | 98666 64 Go

PÉRIPHÉRIQUES DE STOCKAGE AVEC ACCÈS SÉCURISÉ PAR CODE PIN

Nécessite de saisir votre mot de passe personnel pour accéder à toute donnée

DISQUE DUR PORTABLE SÉCURISÉ AVEC ACCÈS CLAVIER

- Encryptage matériel AES 256 bits obligatoire à 100 %
- Mode de passe de 5 à 12 chiffres
- Logiciel de sauvegarde NERO
- Compatible MAC et PC
- Type-C, USB 3.1 Gen 1
- Saisie de mot de passe anti-hacking, s'efface après 20 tentatives infructueuse

53401 1 To | 53403 2 To

SSD PORTABLE SÉCURISÉ AVEC ACCÈS CLAVIER

- Les disques SSD utilisent le stockage de mémoire flash pour des vitesses plus rapides, des performances plus élevées et une plus grande fiabilité
- Encryptage matériel AES 256 bits obligatoire à 100 %
- Mode de passe de 5 à 12 chiffres
- Logiciel de sauvegarde NERO
- Compatible MAC et PC
- Type-C, USB 3.1 Gen 1
- Saisie de mot de passe anti-hacking, s'efface après 20 tentatives infructueuse

53402 256 Go

CLÉ USB PORTABLE ET SÉCURISÉE AVEC ACCÈS PAR CLAVIER

- Encryptage matériel AES 256 bits, chiffre en temps réel de façon transparente toutes les données présentes sur le disque
- Clavier intégré pour saisir le mot de passe (jusqu'à 12 chiffres)
- Peut être utilisée avec une télévision (caractéristique impossible avec les appareils chiffrés habituels)
- Témoins LED de statut de l'alimentation/du chiffrement
- Compatible PC et Mac
- Disponible en USB 3.0 ou USB 3.1 GEN 1 avec connexion USB-C™

USB 3.0 : 49427 32 Go | 49428 64 Go | 49429 128 Go **USB-C™ :** 49430 32 Go | 49431 64 Go | 49432 128 Go

DISQUE DUR DE BUREAU SÉCURISÉ KIT BOÎTIER AVEC ACCÈS CLAVIER

- Clavier intégré pour saisir le mot de passe
- Encryptage matériel AES 256 bits
- Boîtier pour disque dur 3,5”
- Est compatible avec n’importe quel disque dur SATA interne de 3,5”
- Installation facile. Pas de connaissances techniques avancées nécessaires
- Câble USB-C™ vers USB-A

53405

SAUVEGARDE ET ARCHIVAGE

Les sauvegardes régulières protègent contre la perte de données accidentelle ou malveillante, qu'il s'agisse de pannes matérielles et de virus, d'erreurs humaines ou de vol. Ces sauvegardes peuvent être utilisées pour restaurer des fichiers de données d'origine.

Le choix du bon média et de la procédure de sauvegarde dépend de nombreux éléments :

- La quantité de données à sauvegarder
- La valeur perçue des données
- Les niveaux de risque acceptés
- La durée pendant laquelle vous souhaitez conserver les données

MEILLEURE PRATIQUE - APPLIQUER LA RÈGLE DE SAUVEGARDE 3-2-1

3

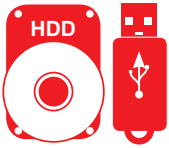
CONSERVEZ AU MOINS TROIS COPIES DE VOS DONNÉES

En plus de votre sauvegarde principale, vous devriez en avoir deux autres, ce qui aidera à réduire considérablement le risque de perdre des données. Il peut s'agir de solutions physiques et / ou de cloud.

2

STOCKEZ LES COPIES SUR AU MOINS DEUX SUPPORTS DIFFÉRENTS

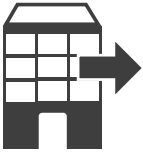
Il est recommandé de conserver des copies de vos données sur au moins deux types de stockage différents, tels que des disques durs internes ET des supports de stockage amovibles (cassettes, disques durs externes, clés USB, cartes SD, CD, DVD).



1

GARDEZ AU MOINS UNE COPIE DE SAUVEGARDE HORS LIGNE

Cela paraît évident, mais ce n'est pas une bonne idée de garder votre périphérique de stockage externe dans la même pièce que votre stockage de production. S'il y a un incendie, une inondation ou un cambriolage, vous perdrez toutes vos données.



LA MEILLEURE PROTECTION CONTRE LES ATTAQUES ARCHIVEZ VOS DONNÉES

Pour être complètement protégé, un utilisateur ou une entreprise doit avoir des données sauvegardées et archivées hors ligne.

Tout périphérique connecté à un système ou à un réseau attaqué est vulnérable.

Si votre disque dur de sauvegarde est branché sur votre ordinateur portable lorsqu'un ransomware est installé, il sera également crypté. Avoir vos données les plus importantes archivées sur un support optique peut éliminer ce risque.

MÉDIAS ET LECTEURS OPTIQUES POUR ARCHIVAGE

- Blu-ray, DVD, CD : la meilleure solution pour le stockage à long terme (25 - 100 ans)
- Utilisation avec les graveurs DVD et Blu-ray externes de Verbatim
- Logiciel Nero Burn&Archive gratuit avec les graveurs DVD et Blu-ray de Verbatim

43888 | 43889 | 43890 | 98938 | 43894

SACS SÉCURISÉS RFID

SACS SÉCURISÉS AVEC POCHE DE SÉCURITÉ RFID

- La gamme comprend des sacs à roulettes, des sacs à dos, des sacs pour appareils photo, des housses pour ordinateur portable et des sacoches
- Inclut une poche RFID pour protéger les cartes bancaires d'actes malveillants

Paris 49852 | London 49855

ÊTES-VOUS COMPATIBLES AVEC LE RGPD ?

Bureau de Verbatim

Verbatim GmbH
Düsseldorfer Str. 13,
D - 65760 Eschborn,
Allemagne
T : +49 (0) 6196 900 10
E: info.germany@verbatim-europe.com

Verbatim™
Technology you can trust

www.verbatim-europe.com/security