CONSEILS EN MATIÈRE DE
PROTECTION DES DONNÉES

Protégez vos informations numériques et physiques avec les services Shred-it

Les données sont considérées comme le nouveau pétrole. Vos systèmes d'informations et dossiers en ligne, où sont généralement stockées vos données confidentielles, constituent donc des mines d'or (ou plutôt des champs de pétrole) pour les personnes malveillantes.

En effet, des milliers de systèmes en ligne sont compromis chaque jour. L'année dernière, 39 % des entreprises européennes ont déclaré avoir subi une cyberattaque[1], et le nombre de violations de données signalées jusqu'à présent cette année a déjà dépassé le total de 2020.

Pour faire face à cette menace, les entreprises doivent doter leurs collaborateurs du savoir-faire et des outils nécessaires pour protéger leurs informations confidentielles. Nos conseils essentiels sur la protection des données vous aideront sur cette voie.

[1] Source: Statista

01

Mettre en place une politique de gestion des risques

Une politique de gestion des risques permet aux entreprises d'identifier et de comprendre les menaces, puis d'éliminer ou de réduire ces risques en sécurisant la technologie, les systèmes et les informations.

02

Sécurisez vos réseaux

Les pares-feux et les programmes antivirus sont deux éléments essentiels de la cybersécurité. Vérifiez systématiquement la nature et la provenance de vos e-mails et évitez de cliquer sur des liens. Soyez attentif aux signaux d'alarme comme les fautes d'orthographe, une mauvaise grammaire, une formulation étrange et les demandes urgentes d'argent.

03

Utilisez des mots de passe forts

Les mots de passe forts utilisent huit caractères ou plus et comprennent des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Conservez les mots de passe en lieu sûr, n'utilisez pas le même pour plusieurs comptes et changez-les tous les trois mois.

Nous protégeons ce qui compte.

Shred-it®
Une Solution Stericycle®

04

Protégez votre vie privée sur les réseaux sociaux

Les criminels peuvent obtenir vos informations confidentielles avec seulement quelques points de données, donc moins vous en partagez, mieux c'est ! Par exemple, si vous publiez le nom de votre animal de compagnie, vous pourriez exposer les réponses à une question de sécurité courante.

05

Formation et sensibilisation des collaborateurs

Créez des politiques de sécurité et dispensez une formation à la cybersécurité. Le personnel doit savoir comment identifier les e-mails ou liens douteux et doit se montrer vigilent quant aux sites Web qu'il visite et aux applications qu'il télécharge. Encouragez les équipes à signaler toutes les cyberattaques.

06

Utilisez les services de destruction de disque dur

Ne stockez pas d'ordinateurs et de données numériques obsolètes. Triez vos données numériques, maintenez-les à jour et purgez-les régulièrement. Une fois que votre ancienne technologie est obsolète, faites détruire en toute sécurité les disques durs d'ordinateurs anciens ou inutilisés.

07

Protégez les smartphones et autres appareils connectés

Les mobiles et autres appareils connectés peuvent être votre maillon faible. Ne les laissez jamais sans surveillance et activez la protection par mot de passe. Gardez vos applications et systèmes d'exploitation à jour et assurez-vous de suivre, verrouiller et effacer les appareils perdus ou volés.

08

N'oubliez pas les documents et les menaces physiques!

Les anciens documents présentent également un risque important s'ils ne sont pas manipulés, stockés et détruits en toute sécurité. L'établissement d'une politique de bureau propre peut renforcer la sécurité, tandis qu'une politique « Shred-it ALL» contribue à réduire l'erreur humaine qui est souvent responsable des violations de données.

Nous protégeons ce qui compte.

Shred-it®
Une Solution Stericycle®