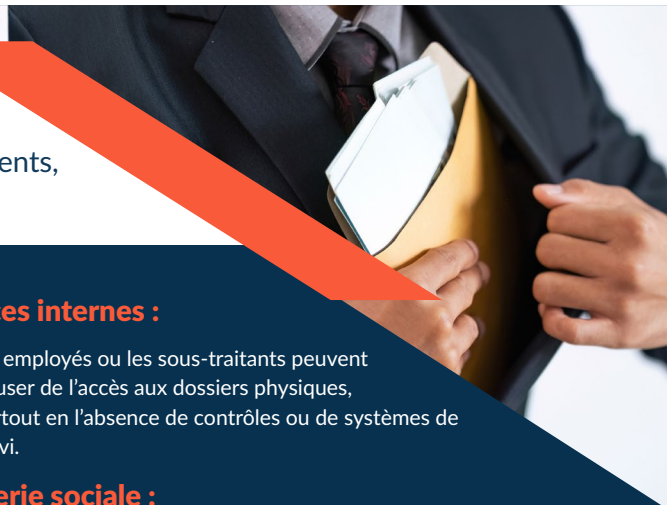
FICHE D'INFORMATION

La fraude n'est pas seulement numérique. Elle est aussi physique.



La fraude est souvent considérée, à tort, comme un simple problème numérique, comme c'est le cas pour les incidents de piratage informatique. Mais elle peut prendre de nombreuses formes, notamment l'exposition physique de documents, tout aussi dangereuse et souvent négligée.

Voici quelques mesures qui pourraient contribuer à mettre votre entreprise en danger :

Exposition physique des documents

- **Documents non déchiquetés** : les documents contenant des informations sensibles, tels que les factures, les contrats, les dossiers médicaux, les dossiers des employés laissés dans les poubelles, sur les bureaux ou dans les bacs de recyclage, peuvent être volés ou utilisés à mauvais escient.
- **Élimination inadéquate :** jeter des documents sans les détruire de manière sécurisée, par exemple en les déchiquetant, ouvre la porte au pillage des poubelles et à l'usurpation d'identité.

Menaces internes :

- les employés ou les sous-traitants peuvent abuser de l'accès aux dossiers physiques, surtout en l'absence de contrôles ou de systèmes de suivi.

Ingénierie sociale :

- les fraudeurs peuvent utiliser des documents physiques pour usurper l'identité de personnes ou d'entreprises, et ainsi accéder à des systèmes ou à des ressources financières.

Attaques hybrides :

- les documents physiques peuvent être utilisés pour faciliter la fraude numérique, par exemple en utilisant un relevé bancaire imprimé pour contourner la vérification d'identité dans le cadre d'escroqueries en ligne.

Comment pouvez-vous contribuer à prévenir la fraude au-delà des menaces numériques ?

Effectuez une évaluation de la sécurité des données

- Examinez comment les informations confidentielles sont stockées, consultées et éliminées, tant sous forme numérique que physique.
- Identifiez les vulnérabilités dans la gestion des documents, les zones de stockage et les processus d'élimination.
- Utilisez cette évaluation pour mettre à jour les politiques et former le personnel en conséquence.

Mettez en œuvre une politique de bureau propre

- Exigez que les employés retirent de leur bureau tous les documents sensibles à la fin de la journée.
- Rangez les documents, les clés et les périphériques USB sous clé lorsqu'ils ne sont pas utilisés.
- Cela réduit le risque d'exposition accidentelle ou de vol, notamment dans les bureaux partagés ou en espace ouvert.

Formez le personnel à la gestion des informations confidentielles

- Assurez-vous que tous les employés comprennent ce qu'est une donnée confidentielle.
- Fournissez des directives claires sur la manière de stocker, de partager et d'éliminer les documents sensibles.
- Incluez des exemples concrets de fraude physique pour mettre en évidence les risques.

Adoptez une politique de déchiquetage intégral des documents

- En cas de doute, utilisez Shred-it. Cela évite les interrogations et garantit qu'aucun document sensible ne tombe entre de mauvaises mains.
- Faites la promotion de cette politique comme un moyen simple et efficace de protéger les données des clients et de l'entreprise.
- Désignez une personne au sein de votre entreprise pour superviser le processus de destruction de tous les documents, par exemple en vérifiant les imprimantes pour repérer les documents égarés.

Pour plus d'informations, contactez-nous au 0800 844 848 ou rendez-vous sur : Shredit.fr

Nous protégeons ce qui compte.

Shred-it®
Une Solution Stericycle®