



Pourquoi la formation des employés est une priorité en matière de sécurité

RAISON N° 1

Les brèches de données ont triplé au cours des 5 dernières années.¹ En 2017, plus de 235 millions de dossiers ont été perdus ou volés.²

RAISON N° 2

Avant une brèche de données, **le cours moyen des actions d'une entreprise augmente de 45,6 % sur trois ans**, mais, après une brèche, **l'augmentation n'est que de 14,8 %.**³

RAISON N° 3

De 2014 à 2017, le coût moyen du cybercrime a augmenté de plus de **40 % partout dans le monde** dans le secteur des services financiers.¹

LES EMPLOYÉS SONT VOTRE MEILLEURE DÉFENSE.

L'industrie des services financiers est ciblée par les voleurs de renseignements 65 % plus souvent que toute autre industrie.⁷ Les employés formés à repérer les risques peuvent, à long terme, faire économiser des millions de dollars à votre entreprise.

Nous protégeons ce qui compte.



POURQUOI LA FORMATION DES EMPLOYÉS EST UNE PRIORITÉ EN MATIÈRE DE SÉCURITÉ

La plupart des cabinets de services financiers comprennent l'importance des systèmes évolués de cyberdéfense, mais une formation continue de sensibilisation à la sécurité est également essentielle. Les employés peuvent aider à réduire le risque de brèche de données et à éviter les coûts qui en découlent.

Voici 5 façons :

1. LES MENACES ENTRANTES

Un rapport de 2017⁴ indique que 58 % des causes de brèches de données dans l'industrie des services financiers viennent de l'intérieur de l'entreprise, des employés et d'autres personnes de confiance, dont la majorité a été dupée afin d'aider les criminels à perpétrer leurs attaques.



LA SOLUTION :

Apprenez à vos employés à reconnaître les fraudes par courriel et aidez-les à se familiariser avec les autres procédés d'hameçonnage afin d'éviter qu'ils ne cliquent sur des liens ou des courriels suspects. Informez-les qu'ils doivent rapporter immédiatement tout incident.

2. LES HABITUDES DE TRAVAIL NÉGLIGENTES

25 % des brèches de données survenant sur les lieux de travail découlent d'une négligence.⁵ Cela inclut la divulgation de mots de passe, le transport inutile de renseignements confidentiels et l'élimination inadéquate des données confidentielles.



LA SOLUTION :

Instaurez des politiques de lieux de travail sécurisés et enseignez les pratiques exemplaires en matière de sécurité des données.

3. LES APPAREILS MOBILES

Les environnements de travail « apportez vos appareils personnels » d'aujourd'hui font en sorte que de nombreux employés se connectent aux ressources de l'entreprise lorsqu'ils sont à l'extérieur du bureau, exposant ainsi leurs appareils personnels et le réseau de l'entreprise aux menaces. La perte ou le vol d'appareils mobiles et le téléchargement d'applications inconnues augmentent également le risque de brèche de données.



LA SOLUTION :

Instaurez une politique exhaustive concernant les appareils personnels au bureau et apprenez à vos employés à protéger leurs appareils en tout temps. Veillez à chiffrer toutes les données de votre entreprise afin d'avoir une protection supplémentaire.

4. LA NON-CONFORMITÉ

Le secteur des services financiers est très réglementé, et les violations peuvent être très coûteuses en raison des amendes et des dommages à long terme à la réputation.



LA SOLUTION :

Présentez à vos employés les lois sur la protection des renseignements personnels qui les concernent, comme la Loi sur la protection des renseignements personnels et les documents électroniques, la Gramm-Leach-Bliley Act et la Sarbanes-Oxley Act. Assurez-vous d'inclure des lignes directrices strictes en matière de conformité dans la formation.

5. LA PERTE DE CLIENTS

La perte de clients contribue au coût élevé des brèches de données dans ce secteur. Une étude antérieure a révélé que, de tous les répondants, 12,3 % avaient quitté leur coopérative de crédit en raison de transactions non autorisées sur leur compte, et 28 % avaient quitté leur banque pour cette même raison.⁶



LA SOLUTION :

Adoptez une approche descendante pour souligner la relation qui existe entre la fidélisation de la clientèle et la sensibilisation à la sécurité. Les employés comprendront ainsi l'importance qu'a la sécurité de l'information pour l'entreprise.

Sources:

- 2017 Cost of Cyber Crime Study, Ponemon Institute et Accenture
- Breach Level Index, Gemalto, 2018
- Analysis: How Data Breaches Affect Stock Market Share Prices, Comparitech Ltd., 2017 <https://www.comparitech.com/blog/information-security/data-breach-share-price/>
- 2017 IBM X-Force Threat Intelligence Index, IBM
- 2017 Cost of a Data Breach Study, Ponemon Institute
- White Paper: The Impact of Cybersecurity Incidents on Financial Institutions, 20 février 2018, generalglobalassistance.com
- Security Trends in the Financial Industry, IBM Security, 2017

Pour avoir la certitude que les données de vos clients sont protégées, contactez Shred-it dès aujourd'hui.

888-227-0923 | shredit.com/finance

Shred-it® est une solution Stericycle. © 2018 Shred-it International. Tous droits réservés.

 Shred-it®