Prévention des sinistres

Soyez proactif pour prévenir les accidents!

Prévenir les brèches de données dans un contexte de pandémie

Dans le contexte actuel, voici quelques rappels des meilleures pratiques de prévention à suivre afin d'éviter d'être victime d'une brèche de donnée.

Une **brèche de donnée** peut être d'origine volontaire, accidentelle et même être causée par inadvertance. Vous trouverez ci-dessous, quelques conseils afin de réduire les risques associés à la protection des renseignements.

- Ne laissez pas d'équipement et de documents dans un véhicule sans surveillance. Même faire une course très rapidement laisse amplement de temps à un voleur pour dérober un appareil ou un document laissé dans une voiture garée.

- On devrait appliquer les mêmes mesures de sécurité pour les équipements amenés à la maison**.** Verrouillez les systèmes lorsque vous quittez, même pour quelques minutes. S'assurer que l'équipement est rangé hors de la vue lorsqu'il n'est pas utilisé, ceci est non seulement vrai pour les ordinateurs portables et les tablettes, mais également pour les disques durs externes et même les serveurs domestiques, lesquels sont souvent beaucoup plus petits et faciles à voler.

- Assurer une sauvegarde de toutes les données de l'entreprise et conservée au minimum une copie l'extérieur des lieux (Infonuagique, disque dur externe, etc.). La fréquence de sauvegarde devrait être 1 fois par jour. Il est important qu'une personne soit attitrée au bon fonctionnement de cette opération et qu'une procédure soit en place afin d'assurer la récupération des données en cas d'incident. Utiliser également le chiffrement de donnée afin de protéger adéquatement les données et renseignements confidentiels de l'entreprise.

intact ASSURANCE

Prévention des sinistres

Soyez proactif pour prévenir les accidents!

Protection des données

- Il est inévitable que certaines données doivent circuler dans l'univers numérique, à partir d'un ordinateur ou téléphone portable, etc. Utiliser le chiffrement de données au moyen d'un réseau privé virtuel (VPN) afin d'éviter que ceux-ci ne soient interceptés. Il est également préférable d'éviter les connexions à des réseaux publics.

- Évaluez à l'interne les niveaux d'accès du personnel et supprimez les autorisations inutiles. Confirmez également que le pare-feu et les autres technologies (lesquels permettent souvent d'intercepter des courriels suspects avant qu'ils ne pénètrent dans votre réseau) disposent des derniers correctifs de sécurité et sont installés sur tous les équipements. Assurez la mise à jour constante des logiciels et systèmes d'exploitation de l'entreprise.

- L'utilisation de compte de messagerie personnel et de média social peut augmenter les risques de brèches de sécurité du réseau de l'entreprise. Par conséquent, le matériel fourni par l'entreprise aux employés (ordinateurs, téléphones, etc.) ne devrait pas servir à des fins d'utilisations personnelles.

Fraude et brèche de donnée

Malheureusement, des fraudeurs utilisent la crise sanitaire actuelle afin de tenter de leurrer des individus dans un but de les extorquer. Méfiez-vous des tentatives de fraude impliquant les transferts monétaires, demandes d'informations personnelles, ou le téléchargement de fichiers.

intact ASSURANCE

Prévention des sinistres

Soyez proactif pour prévenir les accidents!

Protection des données

L'ingénierie sociale c'est quoi:

Dans le contexte de la sécurité de l'information, ingénierie sociale consiste à recourir à la tromperie en vue d'amener des personnes, en les manipulant, à divulguer des renseignements personnels ou confidentiels, lesquels peuvent être utilisés à des fins de collecte d'information, de fraude ou d'accès à un réseau informatique de façon illégale. L'hameçonnage est une technique d'ingénierie sociale très répandue, mais la fraude peut aussi être perpétrée via téléphone, SMS, etc.

Méfiez-vous des appels, texto et courriels comprenant l'information suivante:

- Sentiment d'urgence d'agir
- Menaces et conséquences en cas d'inaction
- Appel ou courriel non sollicité
- Il vous est demandé de valider votre identité ou de fournir de l'information personnelle et/ou de transférer de l'argent
- On vous demande de cliquer sur un lien et/ou de télécharger un fichier.

intact ASSURANCE

Prévention des sinistres

Soyez proactif pour prévenir les accidents!

Protection des données

Éviter les fraudes

Sensibiliser les employés et gestionnaires à ne pas transmettre d'information et/ou cliquer sur des hyperliens ou fichiers douteux.

Revérifiez les adresses courriel. Commencez simplement par examiner le nom de domaine des messages entrants.

Revérifiez les demandes suspectes ou inhabituelles. Les criminels enverront souvent des messages qui demandent à un employé d'effectuer des transferts électroniques ou de fournir des renseignements sensibles.

Limitez l'accès aux données. Vous courez moins de risques lorsque l'accès à vos données les plus sensibles (les numéros de compte financiers ou les renseignements personnels des employés, par exemple) est limité à quelques personnes seulement.

intact ASSURANCE