TERRANOVA SECURITY

Semaine de la protection des données : Six bonnes pratiques pour vos utilisateurs

Quelles connaissances ont vos employés de la confidentialité des données ? En réalité, les employés ne savent généralement pas comment leurs informations personnelles sont collectées et utilisées par la plupart des entreprises. Or avec la Semaine de la confidentialité des données 2022 approchant à grands pas, c'est l'occasion idéale d'en apprendre davantage à ce sujet, de sensibiliser les employés à la confidentialité des données en ligne et de leur apprendre à protéger leurs informations personnelles.

Du 24 au 28 janvier, les professionnels dans de nombreux pays à l'échelle du globe, notamment au Canada et aux États-Unis, peuvent participer à diverses initiatives en ligne associées à cet événement de sensibilisation en partageant des connaissances liées aux meilleures pratiques essentielles pour la sensibilisation à la confidentialité des données. Cet événement encourage également les entreprises à offrir une plus grande transparence sur la manière et les raisons pour lesquelles elles collectent les données des clients.

Profitez de ces conseils importants sur la confidentialité des données et partagez-les avec les membres de votre équipe, vos collègues, votre famille et vos amis pour les aider à protéger leurs données contre l'hameçonnage, l'ingénierie sociale, et d'autres formes de cyberattaques en 2022.

En quoi consiste la confidentialité des données?

La confidentialité des données englobe tout aspect lié à la mesure dans laquelle les données sensibles d'un utilisateur sont partagées en ligne avec des tiers. Les données sensibles peuvent inclure (sans s'y limiter) le nom, l'adresse, la date de naissance, la race, le sexe, les coordonnées, le numéro de carte de crédit, la photographie, le numéro de carte d'identité, l'adresse IP ou les données de localisation d'une personne.

Pour l'essentiel, les données sensibles représentent toutes les données liées à un comportement dans le monde réel ou en ligne, qu'il s'agisse d'une transaction financière sur un site de commerce électronique ou d'un engagement (par exemple, un « J'aime » ou un « Partage ») dans une publication sur les médias sociaux.

En quoi la confidentialité des données et la Semaine de la confidentialité des données 2022 sont-elles importantes ?

Dans bien des pays, la confidentialité des données est considérée comme un droit fondamental, protégé par des

réglementations très strictes. L'une des réglementations les plus connues à cet égard est le Règlement général sur la protection des données (RGPD) de l'Union européenne, qui précise les droits des résidents de l'UE concernant leurs données.

Du point de vue d'une personne ou d'un consommateur, les réglementations relatives à la confidentialité des données sont un élément essentiel de la protection contre l'accès non autorisé aux données sensibles par des annonceurs tiers ou des cybercriminels.

La confidentialité des données est tout aussi importante pour établir avec des clients internationaux une relation de confiance, fondée sur le traitement, le stockage et le partage de leurs informations. Si ces données ne sont pas sécurisées, l'entreprise met en danger les données de ses clients en cas de brèche de données, et elle s'expose en plus à des responsabilités réglementaires et à des amendes.

C'est pourquoi il est essentiel de participer à la Semaine de la confidentialité des données 2022, car elle offre aux entreprises et aux employés la possibilité de réexaminer leur approche de la confidentialité des données. C'est aussi un moyen de découvrir de nouvelles façons de mettre en œuvre des protections contre les utilisations ou les divulgations non souhaitées.

Six bonnes pratiques de confidentialité des données à présenter à ses utilisateurs en 2022

Pour préserver à tout moment la sécurité de l'information sensible, découvrez six bonnes pratiques de confidentialité des données que vous pouvez transmettre à vos employés cette semaine. Chaque d'entre elle favorise une meilleure sécurité des informations, aussi bien dans leur vie personnelle que dans leur vie professionnelle.

1. Apprenez à reconnaître des informations personnelles

Les informations personnelles se définissent comme les données qui peuvent être utilisées seules ou en combinaison avec d'autres informations, afin d'identifier une personne. Cette catégorie englobe les éléments suivants :

- Le nom, l'adresse et la date de naissance.
- Le numéro du passeport ou du permis de conduire.
- L'historique médical, criminel ou financier.
- L'origine ethnique ou raciale.
- L'adresse IP, si elle peut mener à une personne.
- L'ADN, l'empreinte digitale ou vocale.

Pour protéger ces informations, vous devez veiller à ne les partager qu'en cas de nécessité absolue et uniquement auprès de destinataires que vous connaissez et qui ont votre confiance.

2. Méfiez-vous des tentatives d'hameçonnage

Les courriels d'hameçonnage représentent l'une des menaces les plus importantes pour les informations personnelles de vos employés en 2022. Les cybercriminels les utiliseront pour tromper les personnes et les inciter à cliquer sur un lien suspect ou à télécharger un fichier afin de voler leurs données, d'installer des logiciels malveillants sur leur appareil, et plus encore. Pour vous défendre contre ces courriels frauduleux, vous devez adopter les mesures suivantes :

- Évitez d'ouvrir des courriels provenant d'expéditeurs inconnus. En cas d'incertitude sur l'identité de l'expéditeur, vous pouvez toujours le joindre par téléphone pour vous renseigner.
- Ne cliquez jamais sur les liens contenus dans des courriels non sollicités, car ils peuvent vous mener à un site d'hameçonnage ou télécharger un logiciel malveillant sur votre appareil.
- Ne répondez jamais aux courriels vous demandant de fournir des données confidentielles ou personnelles. Aucune entreprise digne de confiance ne vous demandera ce type d'informations de cette façon.
- Si une offre semble trop belle pour être vraie, elle l'est sûrement. Ignorez donc tous courriels e-mail vous annonçant que vous avez gagné un prix ou que vous pouvez bénéficier d'une remise spéciale.

3. Ne vous laissez pas duper par les tentatives d'hameçonnage vocal ou par message texte

Les courriels ne sont pas le seul moyen que les cybercriminels utilisent pour inciter leurs victimes à communiquer leurs informations personnelles. Ils utilisent également les messages textes et les messages vocaux pour inciter les utilisateurs à fournir des informations personnelles.

Par exemple, un pirate peut envoyer à une personne un message texte lui indiquant que ses données de paiement sont sur le point d'expirer, et contenant un lien l'invitant à les mettre à jour. Si l'utilisateur clique sur le lien, il sera dirigé vers un site d'hameçonnage sur lequel le pirate recueillera ses données.

Les employés peuvent contrer les tentatives d'hameçonnage vocal et d'hameçonnage par message texte en veillant à ne jamais cliquer sur des liens inclus dans ces messages et communiquer d'informations personnelles par téléphone.

4. Signalez tous courriels frauduleux

Si vous repérez une tentative d'hameçonnage dans votre boîte courriel, ne l'ignorez pas et signalez-le. Le fait de signaler un courriel à votre service informatique, votre fournisseur de services informatiques ou à un autre organe directeur peut contribuer à empêcher le pirate d'escroquer d'autres utilisateurs.

La plupart des solutions de messagerie personnelle et d'entreprise, dont Outlook, Gmail et Yahoo, offrent aux utilisateurs une option intégrée pour signaler les courriels frauduleux. Toutefois, il convient de noter que la plupart des pays disposent également d'un organisme chargé de traiter les fraudes par hameçonnage, que vous pouvez contacter par courriels pour signaler toutes tentatives. Voici quelques-uns de ces organismes :

- Au Canada : le Centre antifraude du Canada
- Aux États-Unis: la Cyber Security and Infrastructure Agency
- En France : Malveillance.GOUV.FR, Assistance et prévention en sécurité numérique

Contactez votre service informatique ou les forces de l'ordre locales pour vous renseigner sur l'organisme à contacter dans votre région.

5. Sécurisez vos achats en ligne

Si les achats en ligne se sont imposés dans la vie de tous les jours de nombreuses personnes, ils constituent également une cible de choix pour les cybercriminels. Il est donc essentiel de prendre des mesures supplémentaires pour sécuriser ses données lors de l'utilisation d'un site de commerce en ligne ou une plateforme de transactions tierce. Veillez donc à prendre les mesures suivantes pour sécuriser votre expérience d'achat en ligne :

- Confirmez la légitimité du site. Lorsque vous faites des achats sur un nouveau site de commerce en ligne, commencez par en vérifier la légitimité en procédant comme suit :
  - Vérifiez l'URL, en vous assurant qu'il commence par « HTTPS » (ce qui indique une communication cryptée entre votre navigateur et le site Web), et en vérifiant que le site Web présente un cadenas fermé qui signale une transaction sécurisée.
  - Examinez attentivement le certificat de sécurité du site. Dans certains navigateurs, vous pouvez cliquer sur l'icône de cadenas et sur une option « Afficher le certificat » pour voir l'émetteur du certificat et sa date d'expiration.
  - Prêtez attention aux sceaux d'approbation de fournisseurs de services de sécurité tiers.
- Méfiez-vous du vol d'identité et des fraudes associées. Rien qu'en 2020, la Commission fédérale du commerce a recensé 4 720 743 rapports de fraude et de vol d'identité. Les utilisateurs doivent donc être en mesure de repérer par eux-mêmes les tentatives d'escroquerie.
- Utilisez l'authentification à plusieurs facteurs à chaque fois que vous le pouvez. Bien des commerces en ligne vous demanderont de créer un compte lors du paiement de votre commande. Si vous choisissez de le faire, créez un mot de passe fort et configurez l'authentification à plusieurs facteurs lorsqu'elle est proposée.

6. N'utilisez pas de Wi-Fi public pour faire des achats

Il peut être pratique d'utiliser le Wi-Fi public pour les achats impulsifs et les achats d'urgence. Cependant, cela peut compromettre vos informations, car les pirates peuvent espionner les données transmises sur le réseau. Vous ne devriez jamais transmettre votre adresse et vos informations de carte bancaire sur une connexion Wi-Fi publique.

Si vous devez absolument faire des achats en ligne à partir d'un point d'accès Wi-Fi public, utilisez un réseau privé virtuel (VPN) pour protéger vos transferts de données afin de limiter leur suivi et leur collecte par des cybercriminels.

Bâtir une culture d'entreprise cybersécuritaire pendant la Semaine de la confidentialité des données 2022

Quels que soient leur secteur d'activité, leur taille ou leur emplacement géographique, toutes les entreprises peuvent être ciblées par des cybercriminels. Pour protéger vos données, vous devez donc vous attacher à instaurer une culture d'entreprise axée sur l'humain et la cybersécurité.

La Semaine de la confidentialité des données est l'occasion idéale de donner le coup d'envoi d'une campagne de sensibilisation à la confidentialité et à la sécurité des données, qui se poursuivra toute l'année. Présentez à vos employés lespratiques de sécurité les plus récentes à utiliser pour sécuriser leurs informations, qu'ils travaillent au bureau ou qu'ils fassent leurs achats à domicile.

Vous pouvez également consulter notre Kit gratuit de sensibilisation à la confidentialité des données pour lancer votre programme de sensibilisation à la confidentialité des données. Ce Kit propose un cours interactif gratuit et divers conseils pour former des cyberhéros, qui donneront l'exemple et contribueront à améliorer la sensibilisation de vos employés à la sécurité.

Il est important de noter que si la Semaine de la confidentialité des données 2022 est un moment crucial pour favoriser la sensibilisation à la confidentialité des données, cela ne signifie pas que vous devez cesser d'en parler le 29 janvier. La Semaine de la confidentialité des données doit être perçue comme l'opportunité de mettre en place un programme de sensibilisation à la sécurité et à communiquer sur les cybermenaces tout au long de l'année. Si vous souhaitez en savoir plus sur la confidentialité des données, vous pouvez utiliser ces ressources :

- Au Canada : Commissariat à la protection de la vie privée : Conservation et retrait des renseignements personnels : Principes et pratiques exemplaires
- Aux USA : l'Alliance nationale en cybersécurité (en anglais) :
  - › Participez à la Journée de la confidentialité des données
  - › Mettez à jour vos paramètres de confidentialité
  - › Devenez un champion de la Journée de la confidentialité des données
- En France : Commissions Nationale de l'Informatique et des Libertés : Les outils de la conformité

En connaître davantage sur la confidentialité des données

Alors que des mesures telles que le Règlement général sur la protection des données (RGPD) et le California Consumer Protection Act (CCPA) ont sensibilisé à la nécessité de protéger la confidentialité des données, les consommateurs prennent de plus en plus conscience de la façon dont les grandes sociétés mettent à profit, voire exploitent, leurs informations personnelles.

Même si ces lois ont fait l'objet d'un grand battage médiatique, nombreux sont ceux qui ne comprennent pas entièrement leur effet et leurs droits. Vous trouverez plus d'informations en matière de confidentialité des données dans les ressources que Terranova Security propose sur le GDPR et le CCPA.

En résumé

Parler ouvertement de la confidentialité des données est la première étape pour instaurer une culture de la sécurité. Lorsque vos employés comprennent comment les sites Web et les entreprises utilisent leurs données, ils sont plus enclins à y réfléchir à deux fois avant de partager en ligne leurs informations sensibles.