CYBER-SÉCURITÉ POUR LES ORGANISATIONS PLUS PETITES

LISTE DE CONTRÔLE DU RSSI : PROTÉGER VOS CLIENTS

CONSEILLER LES CLIENTS ET LES EMPLOYÉS SUR LA PROTECTION DES DONNÉES AU NIVEAU INDIVIDUEL

☐ **Fournissez aux employés et aux clients les recommandations personnelles suivantes à respecter pour mieux protéger leurs données :**

- Utilisez des mots de passe forts sur tous les appareils personnels et professionnels, et envisagez d'utiliser un gestionnaire de mots de passe.
- Gardez les systèmes d'exploitation et autres logiciels et applications à jour sur vos ordinateurs et appareils mobiles.
- Installez des logiciels antivirus, anti-logiciels malveillants et anti-ransomware qui empêchent, détectent et éliminent les programmes malveillants.
- Utilisez un programme pare-feu pour empêcher l'accès non autorisé à votre ordinateur.
- Utilisez uniquement des produits de sécurité d'entreprises réputées. Lisez les commentaires des publications d'ordinateurs et de consommateurs et envisagez de consulter le fabricant de votre ordinateur ou système d'exploitation.
- Soyez prudent avec les informations sensibles. N'envoyez pas de mots de passe de compte bancaire ou d'autres données de comptes financiers sensibles via un e-mail non chiffré.
- Faites preuve d'intelligence quant à l'endroit et à la manière dont vous vous connectez à Internet pour les services bancaires ou autres communications impliquant des informations personnelles sensibles.
- N'ouvrez pas automatiquement les pièces jointes des e-mails ou ne cliquez pas sur des liens dans des e-mails non sollicités ou suspects. Arrêtez-vous. Réfléchissez. Cliquez.
- Méfiez-vous si quelqu'un vous contacte soudainement en ligne ou par téléphone et vous demande vos informations personnelles. Même lorsque vous communiquez avec des adresses connues, essayez de réduire au minimum le partage d'informations personnelles par e-mail.
- N'oubliez pas qu'aucun établissement financier ne vous enverra un courrier électronique ou ne vous appellera et ne vous demandera des informations confidentielles qu'ils ont déjà vous concernant.
- Partez du principe qu'une demande d'information d'une banque où vous n'avez jamais ouvert un compte est une arnaque.
- Vérifiez la validité d'un e-mail suspect ou d'une fenêtre contextuelle avant de fournir des informations personnelles. Accordez une attention particulière à l'adresse e-mail.

ADMINISTRER DES COMPTES

☐ **Exigez que les clients utilisent des identifiants et des mots de passe forts pour se connecter à vos services. Recommandez-leur de ne pas utiliser un mot de passe déjà utilisé pour d'autres comptes.**

☐ **Utilisez la vérification instantanée, la vérification en temps réel, la vérification de dépôt d'essai, la vérification d'identité et/ou des questions à réponses ouvertes pour valider les clients réels et réduire l'opportunité de fraude.**

☐ **Proposez ou, idéalement, exigez l'utilisation de l'authentification à deux facteurs pour les clients lorsqu'ils se connectent à vos services.**

☐ **Vérifiez régulièrement les comptes des utilisateurs pour détecter des signes de fraude.**

PROTÉGER LES DONNÉES

- ☐ **Déterminez les données clients que votre organisation doit collecter pour exécuter ses services et soyez prudent si vous collectez des données clients qui vont au-delà.**
- ☐ **Définissez et distribuez des politiques de conservation des données. Supprimez les données clients lorsqu'elles ne sont plus nécessaires.**
- ☐ **Chiffrez les données clients en transit et au repos.**
- ☐ **Mettez en place des politiques de sécurité des données pour indiquer clairement quelles méthodes de transfert de données sont approuvées par rapport aux restrictions et pour spécifier ce qui est acceptable pour tous les employés lorsqu'ils traitent des données clients. Veillez à ce que ces politiques soient documentées, communiquées, appliquées pour tous les employés, et régulièrement examinées et mises à jour.**

SÉCURISER DES APPLICATIONS WEB PUBLIQUES

- ☐ **Appliquez le protocole HTTPS sur les applications Web publiques de votre organisation et redirigez tout le trafic HTTP vers HTTPS.**
- ☐ **Utilisez une politique de sécurité du contenu sur votre ou vos sites Web.**
- ☐ **Activez l'épinglage de clé publique sur votre ou vos sites Web.**
- ☐ **Assurez-vous que votre ou vos applications Web publiques n'utilisent jamais les cookies pour stocker des informations très sensibles ou critiques sur le client (comme les mots de passe) et qu'elles disposent de dates d'expiration conservatrices pour les cookies (mieux vaut tôt que tard).**
- ☐ **Pensez à chiffrer les informations stockées dans les cookies que vous utilisez.**
- ☐ **Envisagez d'embaucher un service de test d'intrusion pour évaluer la sécurité de votre ou vos applications Web publiques au moins une fois par an.**

FORMER LES EMPLOYÉS

- ☐ **Responsabilisez vos employés et apprenez-leur les stratégies pour minimiser l'erreur humaine qui pourrait exposer les données clients. Cela implique de leur recommander de :**
  - Minimiser leur accès et la transmission des données clients à seulement ce qui est nécessaire pour exécuter leur travail ;
  - Maintenir des pratiques de sécurité solides sur tous les appareils et comptes qui traitent des données clients en utilisant des mots de passe forts, en activant l'authentification à deux facteurs, en gardant les logiciels à jour et en ne cliquant pas sur des liens suspects ; et
  - Signaler tout incident de sécurité interne ou externe potentiel, menace ou mauvaise manipulation des données du client au personnel technique de votre organisation et/ou aux cadres supérieurs.
- ☐ **Assurez-vous que vos employés comprennent et ont signé des documents pour adhérer aux politiques de protection des données et de sécurité de votre organisation.**

INFORMER LES CLIENTS

☐ **Sensibilisez à l'environnement réglementaire de votre organisation en matière de gestion des violations de données clients afin de vous assurer que vous êtes prêt à vous y conformer en cas d'incident.**

☐ **Lorsque votre organisation prend connaissance d'un incident d'accès non autorisé à des informations sensibles du client, enquêtez pour déterminer rapidement la probabilité que les informations aient été ou seront mal utilisées. Suivez les bonnes pratiques de notification et informez le ou les clients concernés dès que possible avec :**

- Une description générale de l'incident et des informations qui ont été violées ;
- Un numéro de téléphone pour plus d'informations et pour obtenir une assistance ;
- Un rappel pour « rester vigilant » au cours des 12 à 24 prochains mois ;
- Une recommandation de signalement rapide des incidents d'usurpation d'identité suspectée ;
- Une description générale des mesures prises par l'établissement financier afin de protéger les informations d'un accès ou d'une utilisation non autorisé(e) ;
- Les coordonnées des agences d'évaluation de crédit ; et
- Toute autre information requise par les réglementations avec lesquelles votre organisation doit se conformer.