Workforce Security and Risk Training

La lettre d'information mensuelle sur la sensibilisation à la sécurité pour vous

Notification de fuite de données ? Ne paniquez pas, récupérez le contrôle

Un e-mail a tout changé

Justin venait de terminer son dîner lorsqu'il a remarqué un e-mail provenant du garage où il s'était récemment rendu pour faire réparer le moteur de sa voiture. Le sujet de l'e-mail était :

"Information de sécurité importante à propos de votre compte"

Au début, il allait le supprimer en se disant que c'était sûrement une autre arnaque. Puis la curiosité a pris le dessus. L'e-mail expliquait que l'entreprise avait subi une fuite de données et que les informations des clients, y compris les noms, les adresses e-mail, les adresses postales et les numéros de téléphone, avaient été divulguées. La bonne nouvelle était qu'aucune information bancaire n'avait été compromise. Comme son emploi du temps était chargé, il a décidé de laisser cette histoire de côté.

Quelques jours sont passés. Puis Justin a commencé à recevoir des e-mails étranges de l'entreprise du garage concernant de nombreuses factures impayées. Les e-mails le menaçaient de l'envoyer en prison s'il ne payait pas immédiatement. Ces e-mails semblaient authentiques, car non seulement ils comportaient le logo de l'entreprise, mais leurs auteurs connaissaient également son nom, son numéro de téléphone et son adresse personnelle. Paniqué, Justin a cliqué sur le lien et a payé la facture. Plusieurs semaines plus tard, alors qu'il discutait avec un ami, il s'est rendu compte que l'e-mail et les factures n'étaient pas authentiques. Ce n'étaient pas des e-mails d'hameçonnage que des cybercriminels avaient créés en utilisant les informations qu'ils avaient volées lors de la fuite de données du garage. En utilisant les informations volées à Justin, les cybercriminels ont pu mettre en place une attaque plus réaliste. Malheureusement, l'histoire de Justin est de plus en plus courante.

Qu'est-ce qu'une fuite de données ?

Une fuite de données désigne le fait que des données à caractère personnel détenues par une organisation ont été soit volées par des cybercriminels, soit divulguées par accident. Dans certains cas, ces entreprises sont tenues par la loi d'informer les clients ou partenaires dont les données auraient pu être perdues ou volées à la suite de cette violation de données. La question qui se pose alors est la suivante : que faire si vous recevez une notification ?

Que faire en cas de fuite de données ?

La bonne nouvelle, c'est qu'une faille de sécurité ne signifie pas automatiquement que vous en serez victime. Le plus important est votre réaction.

1. **Changer son mot de passe immédiatement**. Si vous avez un compte en ligne sur l'entreprise touchée, changez votre mot de passe. Et plus important, si vous avez utilisé ce mot de passe pour d'autres comptes, changez également ces mots de passe. Chacun de vos comptes devrait avoir un mot de passe

unique. De cette manière, si un compte est piraté, le mot de passe volé ne peut pas être utilisé pour accéder à vos autres comptes. Les cybercriminels savent que les gens réutilisent souvent leurs mots de passe, et ils essaieront d'utiliser les mots de passe volés sur vos autres comptes. La manière la plus simple de gérer tous vos mots de passe uniques est avec un gestionnaire de mots de passe, qui peut créer, stocker et compléter automatiquement les mots de passe pour vous.

2. **Activer l'authentification multi-factorielle**. L'authentification multifactorielle, souvent appelée MFA, ajoute un niveau de protection supplémentaire à vos comptes, au-delà du simple mot de passe. Même si un cybercriminel parvient à voler votre mot de passe, l'authentification multifactorielle (MFA) peut empêcher cette personne de se connecter.
3. **Se méfier des tentatives d'escroquerie qui pourraient suivre**. À la suite d'une fuite de données, des cybercriminels peuvent envoyer de faux e-mails, SMS ou passer de faux appels téléphoniques en se faisant passer pour l'entreprise concernée, votre banque ou un service d'assistance. En utilisant vos informations volées, ils peuvent créer des e-mails et des SMS bien plus réalistes. Ce n'est pas parce qu'une personne connaît des informations personnelles vous concernant, comme votre adresse, votre employeur ou le modèle de votre voiture, qu'elle est pour autant de bonne foi. Ne pas cliquer sur des liens ou appeler des numéros venant de ces messages. Rendez-vous directement sur le site officiel ou l'application mobile de l'organisation pour vérifier si ces problèmes sont réels.
4. **Surveiller ses comptes en banque**. Surveillez vos comptes bancaires et vos comptes de carte de crédit afin de détecter toute activité suspecte, telle que des achats inattendus, des retraits d'espèces, des notifications de réinitialisation de mot de passe ou des modifications apportées à votre profil. De nombreuses banques et plateformes en ligne vous permettent d'activer des alertes par SMS ou par e-mail pour toute nouvelle transaction ou tout changement concernant votre compte. Ces alertes peuvent vous aider à détecter rapidement les problèmes.

Dans certains cas, les entreprises qui ont été victimes d'une fuite de données vous proposeront également une forme de protection contre l'usurpation d'identité par le biais d'un service tiers. Même si ces services ne contribuent guère à protéger vos données, ils peuvent vous aider à surveiller vos comptes financiers, à mettre en place une surveillance du crédit et, souvent, vous offrir une assurance ou d'autres protections si vous êtes victime d'une usurpation d'identité à la suite de cette violation. Vérifiez la fiabilité de la société de surveillance d'identité, car vous devrez lui communiquer des informations personnelles pour créer votre compte.

Malheureusement, vous ne pouvez pas faire grand-chose pour protéger les données que d'autres entreprises collectent, car dans la plupart des cas, vous n'avez aucun contrôle sur celles-ci. Mais en suivant ces quelques conseils simples, vous pouvez grandement contribuer à renforcer votre sécurité en cas de violation de données.

Rédacteur invité

Brandi Narvaez est consultante senior en cybersécurité et compte plus de 25 ans d'expérience dans la mise en œuvre de projets liés à la sécurité de l'information et aux infrastructures. Elle est spécialisée dans la protection des utilisateurs et des actifs des entreprises, la sécurisation des données sensibles et l'alignement des stratégies de cybersécurité sur les objectifs métier afin de renforcer la cyber-résilience et d'optimiser l'efficacité opérationnelle.

Ressources

Comment les cybercriminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
Le pouvoir des phrases de passe : https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
FIni la souffrance des mots de passe : utilisez un gestionnaire de mots de passe : https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Se protéger quand la véritable confidentialité est impossible : https://www.sans.org/newsletters/ouch/protecting-yourself-when-true-privacy-is-impossible

Traduit pour la communauté par : Juliette Busson