Fraudcast : histoires de tromperies et de trahisons

Épisode 5 : Hameçonnage, harponnage et vol d'identité

Jazz Clemente

Bonjour à tous, et merci d'écouter le balado sur la fraude de KPMG, au cours duquel nous discutons des cas de fraude qui font la une de l'actualité pour comprendre ce qui s'est passé et en tirer des leçons. Je m'appelle Jazz Clemente.

Frédéric LeBlond

Et je suis Frédéric LeBlond.

Jazz Clemente

Nous sommes tous deux conseillers principaux au sein du groupe Juricomptabilité de KPMG au Canada.

Frédéric LeBlond

Les histoires dont il sera question dans cette série sont des cas réels, mais les noms ont été changés pour protéger pour la vie privée de toutes les personnes concernées. Bien que KPMG n'a pas travaillé sur ces affaires en particulier, nous nous penchons souvent sur des cas semblables à ceux dont il est question ici et qui sont connus du public.

Jazz Clemente

Dans cet épisode, nous discuterons des stratagèmes utilisés par les fraudeurs pour obtenir des renseignements personnels. Les cas dont nous allons parler montrent que ces stratagèmes peuvent causer des pertes financières, et même mener à la mort.

Tout d'abord, nous allons discuter de la façon dont un stratagème d'hameçonnage a fait perdre des millions de dollars à un homme. Tout a commencé par deux adolescents canadiens qui ont usurpé une adresse courriel des services de police de l'Ontario pour envoyer un faux bulletin d'information d'une agence de presse concernant une arnaque en cryptomonnaies. Ce faux bulletin indiquait également que les services de police locaux collaboraient avec le FBI et le United Secret Service Electronic Crimes Task Force dans le cadre de cette enquête. Une victime, vivant quelque part aux États-Unis, a perdu une valeur de 4,2 millions de dollars en Ethereum et en bitcoins après avoir cliqué sur un lien dans le faux bulletin.

Frédéric LeBlond

Peu importe le nombre de contrôles de sécurité en ce qui concerne la crypto, cliquer sur un seul lien frauduleux est tout ce qu'il faut faire pour perdre des millions de dollars en investissements.

Jazz Clemente

Perdre toutes les économies d'une vie en un clic. La police locale a confirmé que l'enquête décrite dans le faux bulletin n'a jamais eu lieu et qu'elle n'avait aucun lien avec les conseils offerts dans le bulletin. La police (la vraie!) a également indiqué que cette histoire a retenu l'attention aux échelles locale et internationale car le bulletin ressemblait à un communiqué de presse légitime. La confiance du public envers la police est précieuse, et de tels incidents peuvent miner cette confiance.

Frédéric LeBlond

Les dommages à la réputation très difficiles à réparer, et ce type d'incident n'aide certainement pas. C'est particulièrement vrai en ce qui concerne la police, qui dépend de la confiance du public pour s'acquitter de ses fonctions de manière adéquate.

Jazz Clemente

Le harponnage (spear fishing) est l'une des formes d'hameçonnage les plus courantes, visant plus particulièrement les entreprises et les grandes sociétés. Tout d'abord, les fraudeurs recueillent des renseignements sur leur cible afin de pouvoir envoyer des courriels convaincants, d'une source qui semble fiable. Ainsi, ils s'infiltrent à l'aide du compte courriel de l'entreprise ou d'un employé.

Fred, peux-tu parler de certaines variantes d'attaques par harponnage?

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.

Frédéric LeBlond

Certainement. Voici certains exemples d'attaque : une entreprise reçoit une demande de modification des renseignements concernant un paiement, provenant d'un soi-disant fournisseur existant. L'employé de la comptabilité reçoit ensuite une demande de retrait importante, qui semble provenir de son client. Ou le service de paie reçoit un courriel prétendant provenir d'un employé qui cherche à mettre à jour les renseignements de son compte bancaire. On peut aussi voir des membres d'un groupe religieux qui reçoivent une demande de don prétendant provenir du leader du groupe.

Jazz, quels sont les signaux d'alarme pour ces attaques?

Jazz Clemente

Certains signaux d'avertissement comprennent des courriels non sollicités, une communication directe provenant d'un membre de la haute direction avec qui vous n'êtes pas normalement en contact, une personne qui met beaucoup de pression pour une demande ou encore une demande inhabituelle, qui ne correspond pas aux procédures internes.

Il est important de demeurer vigilants afin de se protéger contre le harponnage. Évitez d'ouvrir ou de répondre aux courriels non sollicités et de cliquer sur des pièces jointes ou des liens suspects.

Jazz Clemente

Nous allons maintenant parler d'un cas où un vol d'identité a conduit un homme à tout perdre, y compris la vie.
John Harper était autrefois parmi les criminels les plus recherchés du Canada, figurant également sur la liste des criminels recherchés d'Interpol. De col blanc, il est devenu un criminel qui a presque réussi à passer à travers les mailles du filet. Il pensait avoir commis le meurtre parfait, mais il avait oublié un témoin important – la montre Rolex de la victime.

John Harper, un Ontarien, vit une vie parfaite. Marié, père de trois enfants, il fonde une petite entreprise de tenue de livres qui s'est développée pour devenir une importante société financière comprenant plusieurs succursales et de nombreux employés.

Frédéric LeBlond

Oh wow, ça commence bien! J'aime beaucoup les histoires où les gens font leur propre fortune.

Jazz Clemente

Mais il semble que ce n'était pas suffisant pour lui, car il a été révélé qu'il fraudait ses clients, leur volant un montant de 3,2 millions de dollars.

Frédéric LeBlond

Ah, je reprends ce que j'ai dit. Quel revirement!

Jazz Clemente

Mais il y a toujours un piège… Faisant face à 18 chefs d'accusation de fraude, de blanchiment d'argent et de vol, Harper s'enfuit en Europe en 1990, avec l'une de ses filles. Il s'installe dans une petite ville d'Angleterre sous le nom d'Aaron Allen. Comme il ne détenait pas les pièces d'identité requises pour obtenir un emploi, il a conclu un accord avec un compatriote canadien qui vivait en Angleterre, rencontré peu après sa fuite : Robert Scott, un réparateur de télévision. Harper a donc utilisé l'argent qu'il avait détourné au Canada pour lancer une entreprise de réparation de télévision avec Scott. Comme Robert Scott parlait souvent de son désir de retourner au Canada, Harper a saisi l'occasion et lui a « généreusement » offert de lui payer un aller simple pour le Canada… à la condition qu'il lui laisse son permis de conduire, son certificat de naissance et un exemple de sa signature. Le prétexte de Harper était qu'il souhaitait poursuivre les activités de leur entreprise en Angleterre.

Frédéric LeBlond

Ne me dis pas que Scott a accepté l'offre de Harper!

Jazz Clemente

Bien sûr. Sinon, nous n'aurions pas d'histoire à raconter.

Frédéric LeBlond

Dommage que Robert Scott n'ait pas eu la chance d'écouter notre balado, il n'aurait sûrement pas fait ça. Ce type d'entente n'est jamais une bonne idée. Ce n'est pas comme demander à un ami d'aller chercher votre commande au resto à votre place!

Jazz Clemente

Une fois Scott reparti au Canada en 1992, Harper a utilisé son certificat de naissance et son permis de conduire pour voler son identité. Malheureusement, en 1995, Scott est retourné en Angleterre. Comme il ne pouvait y avoir deux Robert Scott, il n'y avait qu'une seule solution pour Harper.

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.

En 1996, il invite son ancien associé d'affaires à excursion de pêche.

Frédéric LeBlond

Pour lui rendre ses papiers d'identité?

Jazz Clemente

Plutôt pour lui prendre quelque chose de bien plus précieux. Une fois en mer, Harper assomme Scott, l'attache à l'ancre à son corps et le jette par-dessus bord. Puis il continue sa vie en tant que Robert Scott, pensant qu'il venait de commettre le crime parfait. Le corps du vrai Scott a été retrouvé par un pêcheur deux semaines plus tard. Comme il était en état de décomposition avancé, il n'était pas possible de l'identifier. Mais il portait toujours sa montre Rolex. Rolex tient des dossiers très précis sur les ventes et le service, et leurs montres sont faites pour durer. Le numéro de série de la Rolex a permis aux policiers de savoir que son propriétaire était Robert Scott. De plus, les Rolex indiquent non seulement la date et l'heure, mais aussi les périodes d'inactivité. En vérifiant l'information de la montre, la police a établi le moment du meurtre, presque à la seconde.

Frédéric LeBlond

Et voilà donc, mesdames et messieurs, une autre bonne raison d'acheter une montre authentique.

Jazz Clemente

La police a rapidement trouvé que Robert Scott vivait toujours en Angleterre, ce qu'ils ont trouvé fort intéressant puisqu'ils venaient de trouver son corps. Ainsi, John Harper a été démasqué et arrêté, au grand plaisir d'Interpol et du gouvernement canadien. Harper a été jugé pour ce crime en Angleterre, et condamné à la prison à perpétuité. Ainsi, il ne peut malheureusement être extradé au Canada pour faire face aux accusations de fraude et de vol qui pèsent sur lui.

Jazz Clemente

Maintenant, accueillons Imraan Bashir, associé et leader national, Cybersécurité, Secteur public. Imraan compte plus de 20 ans d'expérience dans les domaines de la cybersécurité et des technologies de l'information, notamment en matière de gouvernance, de stratégie, de gestion d'incidents, de sécurité infonuagique, de gestion des risques et d'identité numérique. L'excellence de son travail dans ce domaine est reconnue à l'échelle mondiale et en 2019, il a été nommé au palmarès mondial des 100 personnes les plus influentes en gouvernement numérique par la plateforme Apolitical. Bienvenue Imraan!

Imraan Bashir

Merci Jazz. Merci de m'avoir invité.

Jazz Clemente

Imraan, peux-tu nous expliquer ce qu'est l'hameçonnage et la façon dont ça fonctionne? Quelles sont les techniques courantes utilisées par les cybercriminels pour perpétrer des attaques?

Imraan Bashir

L'hameçonnage, en termes simples, est une façon de tromper les gens pour les amener à faire quelque chose qu'ils ne feraient pas en d'autres circonstances. Je pense que le meilleur exemple et le plus courant – vous le savez sûrement – est d'envoyer un courriel au nom d'une source officielle, par exemple de l'agence du revenu, ou encore d'une compagnie de livraison, ce qui est très populaire dans le temps des Fêtes. Le courriel vous invite à cliquer sur un lien pour, soi-disant, suivre votre colis ou vérifier l'état de votre déclaration de revenus. Mais ce lien vous dirige vers un site frauduleux, qui fait en sorte que vous téléchargez un programme malveillant ou qui vous demande d'entrer votre nom d'utilisateur et mot de passe, qui sont ensuite utilisés à des fins frauduleuses.

L'hameçonnage va de faux courriels aux faux textos, ou peut faire appel à l'ingénierie sociale; par exemple dans le cas où un fraudeur se fait passer pour le PDG auprès d'un employé pour que celui-ci effectue une transaction urgente. Récemment, les fraudeurs tentent de pousser des employés à acheter plusieurs cartes-cadeaux iTunes pour une raison quelconque, pour payer une facture. Ces fraudeurs misent sur la bonne volonté des employés, qui veulent simplement aider. Malheureusement, on abuse de leur confiance.

Jazz Clemente

Quelles sont les tendances et les techniques émergentes en matière de cyberfraude et de vol d'identité, que les particuliers et les entreprises devraient connaître?

Imraan Bashir

Je pense que la première chose est de savoir que les techniques changent vraiment rapidement. Il y a cinq ans, les courriels d'hameçonnage étaient plutôt amusants, en ce sens qu'ils étaient mal rédigés et pleins de fautes d'orthographe. C'était vraiment évident, par exemple, un grand prince du Nigeria souhaite léguer un gros montant d'argent en échange d'un virement. C'était avant.

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.

Au cours des dernières années, les techniques sont devenues beaucoup plus sophistiquées, et beaucoup plus ciblées. Par exemple, on cible l'adjoint administratif d'un chef de la direction, en lui envoyant un message qui semble provenir de son patron. Ou encore, on trouve le moyen d'imiter une demande de paiement de facture du chef des finances, et ainsi de suite.

Aujourd'hui, l'émergence des technologies comme l'IA change complètement la donne. Les courriels rédigés de façon bizarre sont chose du passé. Maintenant, certains courriels frauduleux sont très bien structurés, et on voit même apparaître de nouvelles fraudes par téléphone. J'ai lu un article qui expliquait qu'en utilisant environ cinq secondes de la voix d'une personne – par exemple, enregistrée lors d'une conférence, il est possible de cloner sa voix et de lui faire utiliser tous les mots du dictionnaire. Vous pouvez imaginer les répercussions de l'utilisation de votre empreinte vocale pour mener une arnaque par téléphone.

Récemment, un fraudeur a cloné la voix d'une jeune fille pour appeler ses parents et leur dire « Maman, Papa, je suis en prison au Mexique et j'ai besoin que vous m'envoyiez X $ par virement sur ce compte. » En tant que parent, dans une telle situation, la première chose que vous voulez faire est de vous assurer que votre enfant est en sécurité. Alors tu fais ce qu'on te demande. Et bien sûr, c'est une arnaque. Dans cette histoire, la jeune fille était bien au Mexique, dans un tout inclus, ce que les parents savaient, sans plus. Quand ils se sont posé des questions, il était trop tard. C'est là un exemple de la vitesse à laquelle la fraude évolue; passant de courriels mal écrits à des arnaques vocales sophistiquées par IA, ce qui les rend beaucoup plus difficiles à détecter.

Jazz Clemente

Les cybercriminels ont un objectif lorsqu'ils se lancent dans une activité frauduleuse. Pouvez-vous nous expliquer certains des principaux objectifs derrière les stratagèmes d'hameçonnage et de cyberfraude? Y a-t-il des différences selon le type de fraudeur?

Imraan Bashir

Il y a un large éventail de fraudeurs, qui ont divers objectifs, d'un gain financier rapide, à l'espionnage ou à la manipulation politique. Il y a aussi ceux qui le font simplement pour nuire, des idiots, bien franchement. Si les objectifs varient, malheureusement, l'impact est toujours le même. En général, les conséquences sont financières. Par exemple, le vol de propriété intellectuelle cause ultimement des dommages financiers à une organisation. L'incidence sur la réputation est également importante. Une fois qu'une entreprise a été la cible de fraudeurs, la confiance du public et des clients s'en ressent. Les dommages à la réputation à eux seuls peuvent parfois être plus coûteux que les dommages financiers.

En fin de compte, je dirais que l'objectif varie selon le fraudeur et ce qu'il recherche. Malheureusement, le résultat pour l'organisation qui est victime tend à être très similaire – des dommages financiers ou d'atteinte à la réputation qui finissent par nuire à l'organisation à long terme.

Jazz Clemente

Notre prochain sujet est le concept d'identité numérique, qui semble être un sujet brûlant dans le monde entier. Pouvez-vous nous expliquer ce qu'est exactement une identité numérique et quel rôle elle pourrait jouer dans l'atténuation de la fraude?

Imraan Bashir

Je suis un grand fan de l'identité numérique. Essentiellement, il s'agit d'une représentation électronique de vous. Elle prouve que vous êtes bien qui vous affirmez être dans vos échanges en ligne. Je pense que nous savons tous ce que l'identité signifie dans un contexte qui n'est pas numérique; quand on veut acheter de l'alcool avant l'âge légal, on a besoin d'une preuve, comme un permis de conduire. Si on achète un billet d'avion, il faut prouver sa citoyenneté avec un passeport. Nous avons l'habitude et nous savons que ces documents prouvent notre identité. Dans le monde numérique, c'est plus compliqué puisque nous n'avons pas de version électronique officielle de tels documents. Nous n'avons donc aucune preuve numérique solide de notre identité.

L'identité numérique est une preuve fiable et sûre en ligne. La raison pour laquelle je m'y intéresse autant est que je pense qu'elle peut jouer un rôle majeur dans la lutte contre la fraude. Par exemple, si on revient à mon exemple de tentative d'hameçonnage par courriel ou par texto, qui vous mène à un site web frauduleux où il faut entrer son nom d'utilisateur et son mot de passe. Dans un monde parfait, une telle tentative ne fonctionnerait pas; avec une identité numérique robuste, personne ne pourrait utiliser vos identifiants parce qu'ils ne pourraient satisfaire aux autres demandes d'authentification. Autrement dit, ils ne pourraient prouver… qu'ils sont vous.

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.

Je préfère vivre dans un monde où ces erreurs peuvent se produire, parce que nous sommes tous humains. Les humains commettent des erreurs. Les humains cliqueront toujours sur des liens douteux, peu importe la sensibilisation et ce que nous faisons pour l'éviter. Ce que je voudrais par contre, c'est un monde où si on fait l'erreur de cliquer sur un lien douteux, l'impact n'est pas si important parce notre identité numérique est solide. Je veux être rassuré en sachant que personne ne peut utiliser mon nom d'utilisateur et mon mot de passe sans connaître le contexte supplémentaire qui forme mon identité. Donc des niveaux de vérification supplémentaires de l'identité numérique confirmeront qu'elle est émise par une autorité réelle, par exemple un gouvernement, et non pas créée dans le sous-sol d'un adolescent qui utilise l'ordinateur de sa mère. Ce serait un bon début, parce que l'identité numérique sera vérifiée et confirmée de façon cryptographique et ne pourrait pas être dupliquée.

Ainsi, il serait plus difficile pour les fraudeurs d'usurper une identité et assurerait les entreprises, les gouvernements, les consommateurs et qui que ce soit que l'identité utilisée est réelle et ne provient pas d'une activité frauduleuse. Je pense également que l'identité numérique fournirait une transparence totale; on saurait où et quand votre identité est utilisée, de quelle façon et pourquoi. Certains pays d'Europe proposent une identité numérique aux citoyens, ce qui leur permet de savoir qui a effectué des recherches sur leur identité par l'entremise d'un portail. Par exemple, si vous recevez une contravention de la police pour excès de vitesse, vous rentrez chez vous et ouvrez le portail. Vous seriez en mesure de voir qu'à disons 13 h 15, la police a vérifié votre identité pour la contravention.

Vous sauriez en toute transparence quand et pourquoi votre identité est utilisée et cela protégerait mieux la vie privée. Vous auriez l'assurance que votre identité est utilisée dans le but prévu. En ce moment, nous n'avons aucune idée de qui peut avoir une copie de notre permis de conduire ou de notre passeport; on ne sait pas ce qui se passe dans les coulisses jusqu'à ce qu'il soit trop tard. En résumé, je pense que l'identité numérique aiderait à prévenir et à détecter les fraudes et le vol d'identité.

Jazz Clemente

Quels sont les risques ou les défis associés à la mise en œuvre de l'identité numérique au Canada?

Imraan Bashir

Je connais très bien ce sujet puisque c'est ce que je faisais avant de me joindre à KPMG. Le Canada est un pays intéressant en ce sens qu'il est une fédération composée de provinces et de territoires qui ont chacun le pouvoir sur certains éléments identitaires. Par exemple, le gouvernement fédéral, notamment le ministère de l'Immigration, émet certaines pièces d'identité. Le défi que nous avons, comparé à certains pays européens qui ont un gouvernement centralisé, est que nos données sont disséminées dans le pays car les gouvernements provinciaux émettent aussi des pièces d'identité, par exemple la carte d'assurance maladie.

Nous devons créer un écosystème identitaire ouvert; par exemple, si je suis né en Ontario, mon certificat de naissance a été délivré par le registraire de l'Ontario et les autres provinces y ont accès. Mes parents sont immigrants; quand ils ont obtenu leur résidence permanente, ils ont pu demander un passeport canadien, un permis de conduire et ainsi de suite. Toutes ces pièces d'identité sont donc dérivées de la carte de citoyenneté. L'écosystème est une toile complexe. Pour que l'identité numérique fonctionne correctement au Canada, tous les gouvernements doivent pouvoir interagir et partager des données, avec le consentement de la personne concernée. C'est difficile pour un pays si vaste, dont les gouvernements sont indépendants.

Je voudrais également parler de l'importance de la protection de la vie privée. Je pense qu'il ne fait aucun doute que notre pays prend ce point très au sérieux, et à juste titre. Je suis également très conscient du fait que nous devons le faire correctement. La gestion de la confidentialité n'est pas un système qu'on lance sans trop le tester, en espérant qu'il fonctionne. Si nous ratons notre tentative, nous perdons la confiance des citoyens et cela ne sera pas de bon augure. Une grande partie des travaux effectués à cet égard sont liés à la mise en œuvre d'un tel système. Il faut s'assurer que les utilisateurs exercent un contrôle total sur leur vie privée, qu'ils peuvent donner leur consentement et le révoquer à tout moment et qu'il y a transparence complète sur les activités liées à leur vie privée. Les données recueillies à leur égard doivent être réduites au minimum et les utilisateurs doivent pouvoir décider des données qu'ils souhaitent partager ou non. C'est très long à programmer.

Je crois que c'est la bonne chose à faire que de s'assurer qu'un tel système soit mis en œuvre de manière responsable. Certains pays plus autoritaires ont recueilli un grand nombre de données sur les particuliers, ce que je ne

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.

voudrais certainement pas en tant que professionnel en cybersécurité et défenseur de la vie privée. Tout ceci pour dire qu'il y a beaucoup de défis à relever au Canada. Heureusement, de nombreuses personnes qualifiées se penchent sur le sujet et je suis optimiste quant à leur réussite dans un futur proche.

Jazz Clemente

C'était vraiment intéressant, merci beaucoup Imraan!

Imraan Bashir

Ça me fait plaisir. Merci de m'avoir invité!

Frédéric LeBlond

Comme à chaque épisode, nous vous offrons quelques conseils accroître la sensibilisation à la fraude. Voici donc Jazz, qui nous présente le stratagème de fraude de la semaine : le vol d'identité.

Jazz Clemente

Avez-vous de la difficulté à vous connecter à vos comptes en ligne? L'interface est-elle différente lorsque vous vous connectez? Y a-t-il des montants que nous ne connaissez pas qui ont été portés à votre compte? Votre cote de crédit a-t-elle soudainement chuté? Il peut s'agir de signes indiquant que votre identité a été volée. Le vol d'identité consiste à obtenir les renseignements personnels ou financiers d'une autre personne, ce qui permet au voleur de commettre des fraudes, comme des transactions ou des achats non autorisés. Les victimes de vol d'identité sont généralement confrontées à des dommages financiers ainsi qu'à leur réputation, auprès des organismes de crédit entre autres.

Il y a deux types principaux de vol d'identité. Dans le cas d'un vol d'identité traditionnel, le fraudeur usurpe l'identité de quelqu'un d'autre et utilise des documents volés pour effectuer une fraude. En général, ils maximisent les cartes de crédit immédiatement, ce qui avertit la victime de la fraude. Ce vol d'identité est signalé assez rapidement. Les victimes de vol d'identité « synthétique » ne sont pas aussi rapidement alertées puisque le fraudeur utilise une combinaison de vrais et de faux renseignements. Par exemple, ils utilisent le numéro d'assurance sociale d'une personne avec d'autres renseignements sur une autre personne pour créer une nouvelle identité et ensuite commettre des crimes financiers.

Frédéric LeBlond

Jazz, que faut-il faire pour prévenir un tel vol?

Jazz Clemente

Il y a plusieurs conseils à retenir pour réduire le risque d'être victime d'un vol d'identité. D'abord, ne gardez pas trop de renseignements personnels dans votre portefeuille. Vérifiez votre boîte aux lettres régulièrement. Déchiquetez tous les documents qui comportent des renseignements personnels avant de les jeter. Informez-vous sur les personnes qui vous sollicitent au téléphone, en ligne ou en personne en prétendant opérer pour une entité légitime. Conservez vos documents financiers, vos cartes de crédit et vos carnets de chèques dans un endroit sûr, comme un coffre-fort. Portez attention aux dates de vos relevés de carte de crédit; s'ils n'arrivent pas, ils ont peut-être été volés. Utilisez une connexion internet sécurisée si vous devez transmettre des renseignements personnels et pensez-y à deux fois avant de vous inscrire auprès d'un site web qui demande des renseignements personnels.

Frédéric LeBlond

Les professionnels en juricomptabilité de KPMG aident leurs clients à modifier leurs méthodes de détection, d'atténuation et de gestion des risques, leur faisant ainsi gagner temps et argent. Nous aidons les particuliers et les organisations à se tenir au fait de la fraude, et nous serions ravis de vous aider. Au nom de toute l'équipe de Juricomptabilité de KPMG au Canada, je vous remercie d'avoir écouté cet épisode du balado sur la fraude de KPMG.

Jazz Clemente

Au plaisir de vous retrouver bientôt!

© 2024 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG.