Services à la clientèle et gare aux faux numéros

Protégez-Vous :

Certains numéros de service à la clientèle trouvés sur un moteur de recherche sont faux. Voici quelques conseils pour rester vigilant et éviter qu'un appel finisse par vous coûter très cher…

Il y a quelques semaines, *Le Journal de Québec* relatait l'histoire d'Hélène Ménard, convaincue d'appeler le service à la clientèle d'Amazon en tapant « service à la clientèle » avec le nom de l'entreprise dans la barre de recherche de Google.
La dame de Terrebonne s'est fait voler près de 5 000 $ en contactant un faux numéro de téléphone...

L'arnaqueur au bout du fil lui a offert un service courtois et rassurant, avant de lui demander de télécharger une application sur son téléphone pour « l'aider » à résoudre le problème.
Une fois l'application téléchargée, le fraudeur avait accès à toutes ses informations et a immédiatement commencé à soutirer l'argent de son compte bancaire.

Comment éviter qu'une telle situation puisse nous arriver ?

Les faux numéros de service à la clientèle comblent un vrai besoin

De faux numéros de service à la clientèle existent bel et bien pour plusieurs vraies entreprises — évidemment à leurs dépens !

Certaines entreprises préfèrent gérer le service à la clientèle en ligne et évitent de mettre en évidence un numéro de téléphone sur leur site internet.
Exaspérés de ne pas trouver un numéro, les clients qui veulent absolument parler à quelqu'un finissent par utiliser un moteur de recherche et tombent sur un numéro d'appel. Or, il s'agit d'un faux numéro.

Les arnaqueurs paient afin que ces faux numéros de téléphone soient affichés en premier dans les moteurs de recherche.
À moins d'une plainte explicite, les entreprises qui gèrent les moteurs de recherche ne font pas systématiquement la vérification de tels numéros.

Si vous recevez un appel non sollicité

« Si c'est notre service aux membres qui vous appelle, on a déjà des informations sur vous », mentionne Valérie Parente, conseillère en prévention de la fraude chez Desjardins.
Vous n'avez pas à fournir d'informations personnelles.

Lors d'un appel non sollicité, c'est plutôt à vous d'interroger votre interlocuteur.
Le fait de lui demander quelques informations pour valider son identité pourrait le faire sortir de son rôle d'acteur.

Demandez à l'appelant la raison de son appel, son identifiant d'employé et l'entreprise qu'il représente ainsi qu'un numéro de téléphone pour le joindre.
Prenez en note toutes ces informations, qui vous seront utiles dans un cas de signalement de fraude.

« Si on vous dit qu'il y a des activités inhabituelles sur votre compte bancaire, connectez-vous pendant l'appel et allez vérifier en direct », conseille Valérie Parente.

Attention ! Ne vous fiez pas à l'identifiant sur votre afficheur qui pourrait être une identité volée.
Le Service de police de la Ville de Montréal (SPVM) rappelle que les fraudeurs vont usurper des numéros de téléphone en utilisant une application leur permettant d'afficher le numéro de téléphone de leur choix.
Votre afficheur vous indiquera un identifiant de confiance comme un service de police, mais, au bout du fil, ce sera un escroc.

Vous avez un doute ? Raccrochez !

Ce qui doit vous faire sourciller

- Une pression pour agir rapidement en vous disant, par exemple, que faute de paiement, vous allez perdre un service dans les heures qui suivent (comme l'électricité).

- L'interlocuteur ne s'est pas identifié et n'a pas nommé la compagnie pour laquelle il travaille ; parfois, les arnaqueurs gèrent plusieurs faux services clients en même temps.

- On vous appelle à des heures indues, où les personnes sont occupées. Comme l'arrivée des enfants de l'école ou la préparation du souper.
  « Les fraudeurs aiment bien téléphoner dans les moments où ils savent que les gens sont distraits », ajoute la conseillère en prévention de la fraude.

Ce qui doit activer le voyant rouge

- On vous demande de télécharger une application sur votre ordinateur ou téléphone portable afin de vous « aider » à régler le problème.
  De tels téléchargements peuvent permettre à l'escroc de prendre le contrôle de votre ordinateur ou d'y loger des virus qui lui fourniront vos informations personnelles.

- On vous demande de faire un transfert d'argent, un paiement en cryptomonnaie ou d'envoyer des cartes-cadeaux ou de l'argent liquide.

- On vous demande le mot de passe ou le numéro d'identification personnel (NIP) de votre carte de crédit ou débit.

- Si on vous envoie un virement plus élevé que le prix demandé, le virement envoyé sera faux, mais l'argent que vous enverrez pour rembourser la différence sera bien réel.

Plutôt que de recourir à un moteur de recherche, trouvez le numéro de service à la clientèle sur le site officiel de l'entreprise que vous aurez tapé vous-même dans la barre d'adresse.
Si vous cliquez sur une adresse internet apparue dans le moteur de recherche, il est possible que vous accédiez à un faux site internet.

Dans le doute, vous pouvez effectuer une recherche internet avant d'appeler un numéro de service à la clientèle.
Recherchez des termes comme « faux numéro de service à la clientèle XWZ entreprise ».
Plusieurs entreprises affichent les numéros de téléphone qui ont tenté d'usurper leur identité.

Si vous voulez joindre votre institution financière, téléphonez au numéro indiqué au dos de votre carte de débit ou de crédit, prévient la Fédération des caisses Desjardins du Québec.

Faites aussi une vérification auprès du Centre antifraude du Canada.
Mais il ne faut pas oublier que les fraudeurs ont souvent une longueur d'avance sur les autorités.
Demeurez donc vigilant même si le numéro ou l'entreprise n'apparaît pas sur la liste des fraudeurs.

Si vous réalisez que vous avez sans doute affaire à un fraudeur, raccrochez et communiquez immédiatement avec votre poste de police de quartier ou le 911.

Contactez aussi immédiatement votre votre institution financière et votre compagnie de surveillance de crédit pour les aviser.
Il est également recommandé de geler son dossier de crédit pour contrer le vol d'identité.

- Equifax Canada : 1 800 465-7166
- TransUnion : 1 877 713-3393

Si vous croyez que vos informations bancaires ont été compromises, changez vos mots de passe.

Signalez la fraude en communiquant avec le Centre antifraude du Canada ou le site Fraude-Alerte de la Clinique de cyber-criminologie.

La vigilance reste la meilleure manière de se prémunir.
Soyez plus prudent que pas assez pour éviter le stress des pertes financières associées à une fraude.

Il est complexe de récupérer des montants donnés à un fraudeur.
Pour recouvrer les sommes perdues, il faut retrouver le fraudeur derrière les faux numéros et les faux sites, tâche ardue, voire impossible, d'autant que la plupart sont situés à l'extérieur du pays.

Même si les principales compagnies de cartes de crédit, telles Mastercard, Visa, American Express et Interac ont des programmes de protection contre la fraude, le remboursement des montants n'est pas garanti.

Leur protection est valide à condition que vous ayez fait preuve de « soin raisonnable » dans le partage de vos données personnelles.
Cela signifie entre autres que vous n'avez pas divulgué votre NIP, vos mots de passe ou que vos mots de passe n'étaient pas trop simples à deviner.

« Les institutions financières ne sont pas tenues responsables en cas de fraude et elles ne sont pas obligées de vous rembourser les montants que vous auriez perdus en donnant vos renseignements personnels à un fraudeur », rappelle M^{e} Marc-Antoine Harvey, d'Éducaloi.
L'organisme a d'ailleurs produit un outil pour tester vos réflexes en cas de fraude.
Autant se pratiquer sans risque !

À lire aussi : Fraudes : trois manières de déjouer votre vigilance

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230804
"C'est ensemble qu'on avance"