Eléments pédagogiques et messages pour alerter les bénéficiaires de démarchages abusifs, d'arnaques et de messages électroniques douteux

26/11/2020

Contexte

Les périodes de crise ou de troubles génèrent une recrudescence d'arnaques, de démarchages abusifs,… profitant du confinement des personnes les plus fragiles, notamment les personnes âgées, et de la peur de la contagion du Covid-19, de nouvelles escroqueries ont vu le jour.

Le domaine de l'Assurance santé représente un « terrain » propice à ce type de pratique : en effet, dans le secteur des assurances, il est, par exemple, possible de souscrire un contrat avec uniquement un consentement oral, et donc via téléphone. De même, certains messages frauduleux utilisent l'argument de mise à jour de données personnelles ou d'échéancier,… pour obtenir les coordonnées bancaires de personnes retraitées.

Vous trouverez ci-dessous quelques éléments pour se prémunir contre ce type d'agissement.

Démarchage abusif

- **Comment repérer un démarchage abusif ?**

Il est possible de souscrire une mutuelle senior par téléphone. Néanmoins, on considère que le démarchage devient abusif lorsque la personne en ligne se montre insistante et tente d'obtenir vos données personnelles (nom, adresse, relevé d'identité bancaire…).
Sachez qu'un simple accord verbal est suffisant pour conclure un contrat d'assurance. Il n'est pas obligatoire de signer un contrat pour y souscrire : on peut se retrouver engagé après une signature électronique qui peut revêtir plusieurs formes :

- **un code envoyé par SMS et qu'il faut répéter à voix haute,**
- **une touche de téléphone sur laquelle appuyer.**

Lors de l'appel, le procédé peut à priori sembler rassurant, mais en demandant l'accès au dossier d'offre personnalisée de la personne et l'envoi d'un simple code SMS – prétendument pour des raisons sécuritaires –, le démarcheur fait adhérer le particulier à une offre d'assurance santé.
Résultat : vous pouvez vous retrouver avec une mutuelle senior non désirée, à la suite d'un banal appel téléphonique.

De même, de nombreux démarchages frauduleux usurpent le nom de l'Assurance Maladie. Par exemple, lors d'un appel téléphonique, l'émetteur de l'appel se présente comme de l'Assurance Maladie et laisse un message demandant de rappeler la CPAM à un numéro différent du 3646 et fortement surtaxé.

- **Comment s'en prémunir ?**

Pour contourner tout risque de démarchage abusif, vous pouvez :

- **inscrire votre numéro de téléphone sur liste rouge, de façon à ne pas figurer dans les annuaires. Cela dissuadera de nombreux solliciteurs (mais pas tous, la plupart d'entre eux achetant des listes de contacts toutes faites) ;**
- **profiter du dispositif Bloctel mis en place en juin 2016. L'inscription sur cette liste d'opposition au démarchage téléphonique abusif est gratuite et peut se faire via le site internet qui lui est consacré. Les entreprises ont interdiction de démarcher les personnes dont les numéros y sont inscrits, à l'exception des professionnels auprès desquels le particulier dispose d'un contrat.**

En cas de doute, vous avez toujours la possibilité de demander à ce que l'on vous envoie les éléments par courrier.

Pour l'Assurance Maladie, seul le 3646 (service gratuit + coût de l'appel) vous permet de joindre votre CPAM.
Bon à savoir : lorsque l'Assurance Maladie vous contacte par téléphone, le numéro de l'appelant qui s'affiche à l'écran de votre téléphone peut être le 3646 (service gratuit + coût de l'appel) ou le 05 53 35 62 37 (ce numéro est un numéro officiel provenant de l'Assurance Maladie, utilisé pour des entretiens téléphoniques en vue d'améliorer la qualité de la relation avec le public et de promouvoir ses offres de service).
Enfin, l'Assurance Maladie assure que ses agents ne demandent jamais les coordonnées bancaires (n° de compte bancaire, RIB, n° de carte bancaire...) par téléphone.

En cas de démarchage abusif dans le but de vous faire signer une mutuelle senior ou tout autre contrat, n'hésitez pas à faire un signalement à la DGCCRF. Cela permet à cet organisme de sanctionner les entreprises qui ne respectent pas la loi.

SMS frauduleux

Le nombre de détenteurs de téléphones mobiles attire la convoitise des escrocs qui n'hésitent pas à envoyer des SMS frauduleux en utilisant les mêmes techniques que les courriels.

- **Comment repérer les SMS frauduleux ?**

Un SMS frauduleux est un message qui invite fortement son destinataire à rappeler un numéro surtaxé (de type 0 899 XX XX XX) ou à remplir un formulaire pour transmettre ses données personnelles ou ses coordonnées bancaires.
Parmi les arnaques les plus courantes, on trouve une nouvelle fois les mutuelles ou l'Assurance Maladie.
Des adhérents reçoivent des SMS au nom de leur mutuelle signalant par exemple des anomalies concernant leur RIB et les invitant à rappeler un numéro surtaxé pour transmettre leurs coordonnées bancaires.
Ce même type d'arnaque a été repéré pour l'Assurance Maladie, en utilisant une fausse offre de remboursement à valider à travers un simple clic où l'on vous demande de remplir vos coordonnées bancaires pour recevoir le remboursement.

- **Comment s'en prémunir ?**

Comme pour les démarchages téléphoniques ou les courriels, il est essentiel d'être vigilant et de se poser quelques questions avant de réagir :

- **le message vous concerne-t-il ?**
- **ne tapez pas sur les liens dans les messages suspects (souvent les liens ne correspondent pas à l'organisme qui est censé vous écrire)**
- **ne tombez pas dans un site Web convaincant**
- **faites attention à la grammaire**
- **Ne faites pas confiance à un message personnalisé**
- **Contacter directement la société**

Dans tous les cas, que ce soit votre mutuelle ou l'Assurance Maladie, ils ne demanderont pas vos coordonnées personnelles et bancaires par SMS.

<u>Messages électroniques douteux</u>

Via votre messagerie ou votre boîte mail, certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles en utilisant des techniques d'hameçonnage (phishing) ou d'escroquerie de type fraude 419 (scam) : ces techniques d'attaque évoluent constamment.

- **Comment repérer des messages électroniques douteux ?**

Certaines escroqueries par e-mail peuvent être très convaincantes, avec des logos de marque et un langage officiel. N'oubliez pas de prendre le temps de réfléchir chaque fois qu'un e-mail vous demande de prendre des mesures immédiates qui pourraient révéler des informations confidentielles.
Ex : l'Assurance Maladie dont l'utilisation du logo connait une recrudescence ces derniers temps. Or, l'Assurance Maladie ne demande jamais la communication d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par e-mail en dehors de l'espace sécurisé du compte ameli. Tous les messages de ce type en dehors de l'espace du compte ameli sont des mails frauduleux.

- **Comment s'en prémunir ?**

Vérifiez la présence de ces éléments indiquant généralement une escroquerie par e-mail :

- Le nom de l'expéditeur est imprécis et l'adresse électronique de l'expéditeur est longue ou complexe.
- L'objet de l'e-mail est attrayant ou alarmiste.
- L'e-mail appelle à une action immédiate.
- L'e-mail fait miroiter une offre alléchante.
- L'e-mail utilise un prétexte pour obtenir vos informations personnelles, y compris vos informations de connexion à un site Web.
- L'e-mail vous invite à cliquer sur un lien hypertexte sans préciser clairement la destination de ce lien.

Pour limiter la réception de ce type de courriel :

- Utilisez un logiciel de filtre anti-pourriel (par exemple, Bitdefender et AVG qui proposent des fonctions de protection de messageries électroniques) ou activer l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs.
- Installez un anti-virus et mettez-le à jour.
- Désactivez le volet de prévisualisation des messages.
- Lisez vos messages en mode texte brut.

/!\ Dans tous les cas, par téléphone, SMS ou courriel, il est important de ne jamais communiquer ses informations bancaires et ses données personnelles (numéro de sécurité sociale,…).