07/06/2020

L'administration fiscale met en garde les contribuables face à la recrudescence des tentatives d'escroquerie par e-mail et téléphone. Soyez vigilant.

Prudence même en période de crise sanitaire ! **Des envois d'e-mails frauduleux et des appels ont été constatés par l'administration fiscale.** En se faisant passer pour la direction générale des Finances publiques, ils annoncent **des remboursements d'impôts** à leurs destinataires. Pour en bénéficier, les internautes doivent fournir des informations personnelles, dont leurs données bancaires…

Ces emails sont des pièges. Il s'agit de courriels envoyés par des individus ayant pour unique but de soutirer des informations personnelles et des données bancaires. On parle de "phishing" ou d'**hameçonnage** : en usurpant l'identité d'une administration ou d'une banque, les fraudeurs tentent de récupérer des données sensibles.

Aucune administration n'est autorisée à demander les coordonnées bancaires via internet (par courrier électronique, site web, forum). Ne les communiquez jamais via internet ou téléphone.

• Comment repérer ces faux e-mails ?

La direction des Finances publiques rappelle sur son site quelques règles de sécurité à observer face à ce type de courriels frauduleux.

Les autres éléments qui doivent vous alerter :

- **Les fautes d'orthographe** sont courantes (accords, accents…).
- **Le graphisme du logo et la typographie utilisée ne sont pas celles de l'Administration.**
- En passant votre souris sur les liens (**sans cliquer !**), vous pouvez parfois constater que **la page pointe vers une adresse web qui ne correspond pas du tout à celle de l'administration fiscale.**
- **L'adresse de l'expéditeur**, si elle commence par l'administration usurpée, finit souvent par **yahoo.fr, google.net.**
- En cas de doute, contactez l'administration fiscale via la rubrique "Contacts" du site officiel.

• Que faire si vous recevez un e-mail de ce type ?

- **Ne pas répondre.**
- **Ne pas cliquer sur les liens** du message qui dirigent vers des faux sites gouvernementaux.
- Consulter le site impots.gouv.fr ou les réseaux sociaux (Twitter ou Facebook) qui donnent des informations officielles sur le sujet.
- **Copier-coller le message aux services de la police judiciaire et dénoncez-le sur le site** internet-signalement.gouv.fr

- Vous pouvez également contacter le numéro vert mis en place par le gouvernement : **0 805 805 817.**
- **Le mettre dans la corbeille de votre boîte mail.**

• Des appels frauduleux en augmentation

La méthode utilisée est toujours la même : l'interlocuteur signale à l'usager une anomalie sur son dossier fiscal et l'invite, afin d'éviter d'éventuelles sanctions, à rappeler au plus vite un numéro de téléphone surtaxé à 5€ la minute !

En cas de besoin, **seuls les numéros de téléphone figurant sur les documents officiels des impôts** ou le **numéro Impôts Service 0 810 467 687 sont fiables.**

Ces pratiques ne se limitent pas à l'administration fiscale, les assurances, l'Assurance maladie, les fournisseurs d'énergie en sont victimes également. Soyez vigilant.

Pour signaler une escroquerie, vous pouvez contacter le numéro vert mis en place par le gouvernement : **0 805 805 817.**

07/06/2020

Des faux mails et appels de l'Assurance maladie circulent. Comment les reconnaître ?

Les arnaques dans les boîtes de réception se succèdent avec toujours le même but: **récupérer vos données personnelles**. De faux messages impliquant l'Assurance maladie, via des appels ou emails, sévissent.

• Attention aux emails frauduleux...

L'Assurance maladie alerte à nouveau les particuliers sur une récente vague de "phishing", ou hameçonnage, qui sévit dans les messageries.

L'Assurance maladie rappelle qu'elle ne demande **jamais d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par e-mail** en dehors de l'espace sécurisé du compte Ameli.

Elle n'écrit **jamais en rouge** dans ses courriers et ne se présente jamais comme un service client.

Si c'est le cas, il s'agit d'un mail frauduleux qui vise à récupérer vos données personnelles. **Ne répondez pas et supprimez-le de votre messagerie.**

Vous pouvez également signaler le mail frauduleux sur ce site : www.phishing-initiative.com

Si vous avez déjà communiqué vos coordonnées bancaires, contactez votre banque pour faire opposition.

... Et aux appels

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 ou le 05 53 35 62 37** (numéro officiel utilisé pour des entretiens téléphoniques en vue d'améliorer la qualité de la relation avec le public). **Elle ne vous demandera jamais vos coordonnées bancaires (n° de compte bancaire, RIB, n° de carte bancaire...) à cette occasion.**

Si l'appel est frauduleux, l'émetteur vous laissera un message sur votre répondeur **vous demandant de rappeler votre CPAM à un numéro différent du 3646**. Son but est de vous faire appeler un numéro fortement surtaxé dans le but de vous soutirer de l'argent indirectement. **Vous ne devez pas y donner suite.**

07/06/2020

La crise sanitaire n'inspire pas que de la solidarité à certains. Fausses cagnottes en ligne, remèdes "miracles", emails frauduleux ... La DGCCRF appelle à la vigilance même en ce moment !

Face à l'épidémie de CoVid19, les escrocs ne manquent pas d'imagination. La DGCCRF ***(Direction générale de la concurrence, de la consommation et de la répression des fraudes)*** **appelle les consommateurs à la vigilance, notamment sur internet. Remèdes miracles, vente de masques, mails frauduleux, fausses cagnottes en ligne...** Soyez prudent ! **Voici les mises en garde de la DGCCRF :**

- **Malheureusement, à ce jour, il n'existe pas d'aliments miracles, de vaccins, de purificateurs d'air, de lampes, de compléments alimentaires** ou **d'huiles essentielles qui protègent** ou permettent de **guérir du Coronavirus**. Il s'agit de pratiques commerciales trompeuses.

- **Il n'existe pas non plus de kit dépistage** semblant émaner des services de l'État. Il s'agit d'une arnaque pour obtenir vos données personnelles, en particulier vos coordonnées bancaires.

- **Vente de médicaments en ligne :** des sites internet frauduleux cherchent à vendre certains médicaments. Les acheter en ligne est illégal et peut vous exposer à des **risques graves pour votre santé** (effets indésirables ou même faux médicaments). Concernant le **paracétamol**, sa vente en ligne a été suspendue. Si une publicité vous propose d'en acheter, ne cliquez pas. Pour vous en procurer, **direction votre pharmacie, toujours ouverte durant le confinement.**

- **On vous propose une décontamination de votre logement recommandée par l'Etat ?** Rien n'est prévu à ce jour. **Ne laissez personne rentrer chez vous** sous ce prétexte-là.

- **Vous souhaitez aider les soignants** ou **la recherche médicale en participant à une cagnotte en ligne ?** Assurez-vous de l'identité du professionnel et de la destination de vos dons avant d'effectuer un transfert d'argent.

- **Prudence aussi dans votre boîte mail,** plus encore en ce moment : vente de masques, de gel hydroalcoolique... de nombreux **emails frauduleux** autour du Cov19 arrivent chez les particuliers. **Vérifiez l'expéditeur, n'ouvrez aucune pièce jointe et ne cliquez pas sur un lien suspect**. Bloquez l'expéditeur, supprimez le mail et signalez-le sur www.internet-signalement.gouv.fr