



MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

Communiqué de presse

Communiqué de presse

Direction générale des Finances publiques
economie.gouv.fr
impots.gouv.fr

Paris, le 20 août 2019

Sécurité informatique, fraude à la carte bancaire, piratage d'adresses mails... la Direction générale des Finances publiques rappelle les bonnes pratiques afin d'éviter les arnaques aux impôts.

Des courriels, SMS et appels téléphoniques frauduleux usurpant l'identité de l'administration et de ses agents sont constatés chaque année par la Direction générale des Finances publiques, notamment pendant les périodes de grandes échéances (déclaration de revenus, réception des avis d'impôt sur le revenu, de taxe habitation, de taxe foncière, etc). Parmi les messages et appels frauduleux, les plus nombreux concernent :

1 – Les tentatives de fraude à la carte bancaire via la promesse d'un remboursement d'impôts par courriel (#phishing). Ces courriels sont des faux. L'administration fiscale n'est pas à l'origine de ces envois. Le numéro de carte bancaire ne vous est jamais demandé pour le paiement d'un impôt ou le remboursement d'un crédit d'impôt, ni pour compléter vos coordonnées personnelles par ce biais.

Que faire si vous recevez un courrier électronique de ce type ?

- > Ne répondez pas à ce message ;
- > Ne cliquez pas sur les liens à l'intérieur du message (ils peuvent vous rediriger vers un faux site) ;
- > Supprimez le message de votre boîte aux lettres.

De manière générale, nous vous recommandons de ne jamais communiquer votre numéro de carte bancaire (ou tout autre données personnelles) par courrier électronique ou par téléphone, sur ce motif.

Retrouvez des exemples de mails frauduleux sur ce lien :

<https://www.impots.gouv.fr/portail/securite-informatique-soyez-vigilants>

2 – Les appels vers des numéros surtaxés (#vishing)

La méthode utilisée, toujours la même, signale par voie téléphonique à l'utilisateur 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 facturé 5 € la minute.

La direction générale des Finances publiques est totalement étrangère à ces pratiques et invite les usagers à ne pas donner suite à ces appels. **Ces pratiques frauduleuses ne se limitent pas à l'administration fiscale mais elles touchent d'autres secteurs comme les banques, les assurances, ou encore les distributeurs d'énergie.**

Certains fraudeurs se font passer pour une administration afin de récupérer des données personnelles ou des identifiants de connexion au compte fiscal.

Exemple : Un appel d'un faux agent du ministère de l'écologie demandant à un usager de lui communiquer son numéro fiscal afin de lui faire bénéficier d'un chaudière gratuite.

3 – Le piratage d'adresses mails :

L'adresse mail est la clé d'entrée indispensable pour accéder à de nombreux services en ligne de sites administratifs ou de la sphère privée. C'est pourquoi il convient de bien sécuriser son accès afin qu'un pirate ne puisse pas accéder à vos données personnelles et ainsi réaliser des opérations à votre insu.

Le mois dernier, la Direction générale des Finances publiques a constaté une vague inhabituelle de renouvellement de mots de passe de plusieurs espaces particuliers sur impots.gouv.fr. En effet, des hackers ont piraté des comptes de messagerie personnelle chez plusieurs opérateurs ce qui leur a permis de renouveler le mot de passe pour accéder à l'espace particulier en ligne d'impots.gouv.fr de ces usagers.

La Direction générale des Finances publiques a immédiatement réagi suite à ces activités suspectes en :

- bloquant l'accès à ces comptes (environ 2 000 comptes ont été sécurisés)- accompagnant les usagers concernés via un dispositif personnalisé (courrier, téléphone, accueil physique)
- informant les différents opérateurs, les fournisseurs de boîtes mail et la CNIL
- déposant une plainte auprès des autorités compétentes.

Très rapidement, la DGFIP a ainsi mis en œuvre toutes les mesures permettant d'éviter tout dommage ou impact fiscal pour les usagers lié à une potentielle utilisation frauduleuse de ces accès.

Dans un souci permanent de mise à jour des normes de sécurité, des évolutions respectant les normes européennes et le règlement général sur la protection des données (RGPD) sont d'ores et déjà prévues, comme l'ajout d'une question secrète supplémentaire dès la fin du mois d'août, ou envisagées, comme l'envoi d'un code par SMS ou l'application d'un système biométrique comme le suggère l'UE pour mieux sécuriser les achats sur internet.

Néanmoins, la sécurisation de votre adresse mail reste indispensable. Pour cela, consultez le guide des bonnes pratiques de l'ANSSI (Agence Nationale des systèmes de sécurité informatique) : <https://www.ssi.gouv.fr/particulier/precautions-elementaires/dix-regles-de-base/>

Bon à savoir

Que faire si vous recevez ce type de messages
ou si vous êtes victime d'une arnaque ?

Signalez via la plate forme internet « internet-signalement.gouv.fr »
ou par téléphone via le numéro vert gratuit mis en place par le gouvernement :
0 805 805 817.

Contacts presse :

Direction générale des Finances publiques : 01 53 18 86 95