BERCY INFOS

Attention aux faux courriels et appels qui se font passer pour l'administration

Des courriels ou appels téléphoniques usurpent régulièrement l'identité de l'administration dans le but de pousser les usagers à communiquer des informations personnelles à des fins frauduleuses. Rappel des bonnes pratiques à adopter.

Quelles sont les pratiques frauduleuses les plus courantes ?

L'identité de l'administration est régulièrement utilisée pour des tentatives d'escroquerie réalisées par le biais de courriels ou d'appels téléphoniques.

La fraude à la carte bancaire

Même si **tous les services de l'administration peuvent être potentiellement utilisés dans le cadre de ces opérations frauduleuses**, l'identité de la Direction générale des finances publiques (DGFiP), ainsi que celle de ses services déconcentrés, est particulièrement utilisée par les fraudeurs.

En effet, parmi tous les courriels et appels frauduleux, les plus nombreux concernent les tentatives de fraude à la carte bancaire qui accompagnent la promesse d'une restitution d'impôts.

L'arnaque au Compte personnel de formation (CPF)

On constate une recrudescence de l'arnaque dite au « compte personnel de formation (CPF) ». Comme le rappelle le site Mon compte formation, le principe est généralement le suivant :

- vous recevez des appels téléphoniques, des courriels ou SMS d'une personne prétendant appartenir à la plateforme Mon compte formation ou à un autre organisme public (la Caisse des dépôts, Pôle emploi, le ministère du Travail, etc.),
- le message ou la communication vous prévient que vous allez bientôt perdre vos droits à la formation,
- l'escroc vous demande alors vos données personnelles pour accéder à votre compte formation. Il peut également demander votre mot de passe ou bien créer directement un compte par téléphone avec vous. Une fois la connexion effectuée, il peut vous inscrire avec ou sans votre consentement, à une formation factice ou frauduleuse,
- dans certains cas, l'escroc connaît déjà vos nom, prénom et numéro de sécurité sociale. Vous découvrez alors une inscription à une formation à votre insu en vous connectant à votre compte formation.

Il s'agit bien évidemment d'**arnaques**. Sachez que le CPF est valable **tout au long de carrière professionnelle**, il n'y a donc pas de date d'expiration au cours de cette période. Si vous recevez ce type d'appel, de courriel ou de SMS, ne donnez pas suite.

Pour en savoir plus sur cette tentative d'escroquerie et comment la signaler, vous pouvez consulter le site Mon compte formation, ainsi que la page dédiée sur le site de la DGCCRF. Retrouvez également des recommandations sur le site cybermalveillance .gouv.fr.

À savoir

Le démarchage téléphonique dans le cadre du CPF est désormais interdit. La loi du 19 décembre 2022 interdit en effet le démarchage des titulaires d'un CPF par téléphone, SMS, mail ou via les réseaux sociaux, si ce démarchage n'a pas lieu au titre d'une action de formation en cours entre le titulaire du CPF et l'organisme de formation.

Attention aux faux sites administratifs !

Certains sites commerciaux font tout pour tromper le consommateur en **prenant l'apparence d'un site officiel** (couleurs similaires, présence d'un drapeau…). Ils proposent bien souvent de réaliser pour vous des démarches administratives, moyennant rémunération.

En cas de doute, la première chose à faire est de **vérifier l'URL du site** en question. Sachez que les sites officiels de l'administration française doivent se terminer par **« .gouv.fr » ou « .fr »** et jamais par **« .gouv.org » ou « .gouv.com**.

Comment se prémunir contre les tentatives d'escroquerie par courriel ?

Le bon réflexe : ne pas communiquer vos informations bancaires ou personnelles

L'**administration fiscale ne demande jamais** à l'usager de lui communiquer ses coordonnées bancaires ou des informations personnelles par courriel, ni pour le paiement d'un impôt ou le remboursement d'un crédit d'impôt, ni pour compléter ses coordonnées personnelles. **Si de telles demandes vous sont faites, il ne faut donc pas y répondre**.

Il s'agit de tentatives d'hameçonnage (*phishing* en anglais), qui est une escroquerie au cours de laquelle l'émetteur se fait passer pour une administration ou un organisme public, et demande au destinataire de cliquer sur un lien pour accéder à son dossier personnel et renseigner des informations personnelles.

Ces messages imitent très souvent le style et le visuel des messages officiels, en faisant notamment figurer l'entête ou la signature de la DGFiP ou du ministère de l'Économie et des Finances.

Les bonnes pratiques à adopter

La Direction générale des Finances publiques (DGFiP) vous conseille de :

1. ne **pas répondre pas au message**
2. ne **pas cliquer sur les liens** à l'intérieur du message (ils peuvent vous rediriger vers un faux site)
3. **supprimer le message** de votre boîte aux lettres.

Comment se prémunir contre les tentatives d'escroquerie par téléphone ?

D'autres pratiques abusives existent en dehors de celle du hameçonnage par courriel. C'est le cas des **faux recensements**, ou encore des **appels téléphoniques frauduleux** (hameçonnage vocal ou *vishing*).

Le principe est le même que pour le courriel, à savoir : une usurpation de l'identité de l'administration et notamment de l'administration fiscale à des fins frauduleuses.

Savoir identifier un appel téléphonique suspect

La méthode utilisée est toujours la même : l'usager reçoit un appel lui signalant qu'une anomalie a été constatée sur son dossier fiscal et l'invitant à rappeler un numéro au plus vite afin d'éviter d'éventuelles sanctions. **Le numéro en question est surtaxé**, facturé plusieurs euros la minute et n'appartient bien évidemment pas aux services de l'État. Il ne faut donc pas appeler le numéro indiqué.

Ces pratiques frauduleuses ne se limitent pas à l'administration mais concernent d'autres secteurs comme la banque, l'assurance ou encore, les distributeurs d'énergie.

Les bonnes pratiques à adopter

L'administration, et l'administration fiscale en particulier, rappelle que :

- les numéros de carte bancaire des usagers **ne sont jamais demandés** dans le but d'effectuer des transactions ou des remboursements sur Internet,
- pour obtenir des renseignements fiscaux pour les particuliers, les numéros à utiliser sont : soit des **numéros de téléphone ordinaires** d'appels locaux (en 01, 02, 03, 04 ou 05) qui sont ceux des centres des Finances publiques et figurent souvent sur les documents officiels, soit **le numéro unique non surtaxé (prix d'un appel local) : 0 809 401 401**,
- vous pouvez consulter le site impots.gouv.fr pour obtenir des informations officielles sur le sujet.

Des liens et numéros utiles pour se renseigner ou signaler une tentative d'escroquerie

En cas de doute sur l'identité de l'expéditeur d'un courrier électronique (ou même postal) portant l'en-tête ou la signature d'une administration, ou bien pour signaler une tentative d'escroquerie, vous pouvez :

- vous rendre sur le site dédié « **internet-signalement.gouv.fr** » (Pharos)
- effectuer un signalement par téléphone *via* le numéro vert gratuit : **0 805 805 817**
- suivre nos conseils en cas de **détournement de vos coordonnées bancaires** et vous rendre sur **Perceval**, la plateforme dédiée au signalement d'une fraude à la carte bancaire.