

A

A

Entreprises, faites attention aux tentatives d'escroqueries !

<

LECTURE : 4 MINUTES

Par **Bercy Infos** , le 11/09/2023 - **Sécurité numérique**

Vous pensez que seuls les particuliers sont la cible de tentatives d'escroquerie ? Détrompez-vous ! De nombreuses pratiques frauduleuses touchent également les entreprises. On vous rappelle à quoi vous devez faire attention pour vous prémunir contre ce type d'arnaques.

Faites particulièrement attention aux fraudes qui consistent à usurper l'identité de l'administration

Il existe de nombreuses tentatives d'escroquerie, mais beaucoup d'entre elles consistent à vous faire des demandes en **usurpant l'identité d'une administration**. Tous les services peuvent être concernés par ces usurpations, mais généralement c'est l'identité de la **Direction générale des Finances publiques (DGFiP)** < <https://www.economie.gouv.fr/dgfi>>, ainsi que de ses services régionaux, qui est particulièrement utilisée par les fraudeurs.

Plus concrètement, des demandes par courriel (parfois accompagnées de faux formulaires en PDF) et de fausses signatures, usurpent l'identité et les adresses électroniques de la DGFiP.

L'objectif ? Vous faire communiquer à votre insu des informations sensibles et vous soutirer de l'argent.

À savoir

- La DGFiP reporte que beaucoup d'entreprises reçoivent également des demandes de règlement de factures prétendument non payées de leurs principaux clients, français et européens, qui règlent habituellement leurs prestations par **virement SEPA** < <https://www.economie.gouv.fr/cedef/espace-unique-de-paiement-en-euros-sepa>>. Si vous recevez ce type de message, **soyez donc particulièrement vigilant**, il s'agit très probablement d'une arnaque !

<

- D'autres types d'arnaques existent. La **Douane signale**, par exemple, l'existence de sites frauduleux se faisant passer pour un service d'accompagnement à la demande d'enregistrement de **numéro EORI** < <https://www.economie.gouv.fr/entreprises/numero-eori>>. Ces sites vous proposent d'effectuer les démarches à votre place, mais après avoir payé, le service n'est pas rendu et vous n'avez plus aucune possibilité d'entrer en contact avec

<

vos interlocuteurs. Pourtant, solliciter un numéro EORI est une démarche **simple et gratuite**. Derrière ces « annonces », à l'apparence légale sur les moteurs de recherche, se cachent des escrocs.

Comment faire pour repérer une tentative d'escroquerie ?

De nombreux indices doivent vous mettre sur la piste d'une éventuelle tentative de fraude. Soyez particulièrement attentif au **contenu des messages**. Certaines choses doivent vous alerter. Voici une liste non-exhaustive des éléments les plus récurrents à repérer :

- les **fautes d'orthographe** ou de **syntaxe**
- les demandes d'**informations détaillées** sur l'entreprise ou ses **coordonnées bancaires**
- l'**interlocuteur** ou une **forme de demande inhabituelle** (adresse de messagerie très proche de l'adresse officielle mais néanmoins différente)
- les **fausses adresses courriel** (les adresses authentiques de la DGFIP contiennent, par exemple, le suffixe @dgfip.finances.gouv.fr : toute autre dénomination doit donc vous alerter)
- etc.

À savoir

- Sachez également que 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.
- Ces pratiques frauduleuses ne se limitent pas aux usurpations de l'identité de l'administration fiscale mais touchent d'autres secteurs comme les banques, les assurances, ou encore les distributeurs d'énergie.

Que faire en cas de doute ?

Ne répondez pas !

En cas de doute sur un message, surtout si celui-ci ne provient pas de l'adresse électronique de vos interlocuteurs habituels

<

(notamment du **service des impôts des entreprises (SIE)** dont vous dépendez), adoptez la conduite suivante :

- **ne répondez pas**
- **ne cliquez pas sur les éventuels liens** à l'intérieur du message (ils peuvent vous rediriger vers un faux site)
- **supprimez le message** de votre boîte aux lettres.

Signalez la 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, contactez le portail des pouvoirs publics : **internet-**

<

signalement.gouv.fr.

Vous pouvez également passer par le téléphone, via le numéro vert gratuit : **0 805 805 817**.

Vous pouvez également contacter directement votre Centre des Finances publiques, lorsque le message porte un en-tête de l'administration fiscale, dont le numéro de téléphone figure sur vos documents officiels (avis ou déclarations d'impôts, etc.).

Nos autres conseils pour vous prémunir des tentatives d'escroquerie

Plus généralement, il vous est conseillé d'adopter quelques bons réflexes de prudence au quotidien pour **vous prémunir au maximum** < <https://www.economie.gouv.fr/entreprises/methodes-piratage>> de tentatives frauduleuses :

- Si un message suspect est envoyé de la part d'un interlocuteur habituel, **contactez-le directement** avec les coordonnées que vous utilisez habituellement.
- Ne cédez pas à la pression et à l'urgence souvent invoquées dans les tentatives d'arnaques. **Prenez toujours le temps d'analyser les messages** qui vous paraissent suspects avant de répondre.
- D'une manière générale ne **divulgez jamais à l'extérieur des informations sur l'organisation de l'entreprise**.
- Diffusez en interne **les alertes sur les arnaques**, notamment celles transmises par les fournisseurs, et sensibilisez vos employés aux différents risques d'escroquerie.
- Instaurer des **procédures de vérification complémentaires** (pour les paiements internationaux notamment).
- Si vous avez été victime d'une escroquerie, **bloquez immédiatement les coordonnées bancaires frauduleuses** et identifiez les paiements déjà réalisés, à venir ou en instance, pour effectuer les rejets et blocages nécessaires.

Ces contenus peuvent aussi vous intéresser

- Comment lutter contre les spams ? < <https://www.economie.gouv.fr/entreprises/comment-lutter-contre-spams>>
- Sécurité de vos données : comment vous protéger des méthodes de piratage ? < <https://www.economie.gouv.fr/entreprises/methodes-piratage>>
- Piratage : bénéficiez d'un accompagnement sur-mesure avec [cybermalveillance.gouv.fr](https://www.economie.gouv.fr/entreprises/site-cybermalveillance) < <https://www.economie.gouv.fr/entreprises/site-cybermalveillance>>
- Entrepreneurs : quelles règles de cybersécurité appliquer ? < <https://www.economie.gouv.fr/entreprises/createurs-dirigeants-regles-cybersecurite>>
- Numéro EORI : pourquoi et comment l'obtenir ? < <https://www.economie.gouv.fr/entreprises/numero-eori>>

Pour en savoir plus sur les tentatives d'escroqueries

- **Attention aux arnaques !** [sur le site impots.gouv.fr](https://www.impots.gouv.fr)

- **Sécurité informatique : soyez vigilants !** [sur le site impots.gouv.fr](https://www.impots.gouv.fr)

- **Tentatives d'arnaques à la demande de numéro EORI** [sur le site douane.gouv.fr](https://www.douane.gouv.fr)

- **Guide de prévention contre les arnaques** de la Task-Force nationale de lutte contre les arnaques [PDF – 1 232 Ko]

Thématiques : [Sécurité numérique](#)

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières... utiles à la gestion de votre activité.

