

Attention aux courriels et sites Internet frauduleux !

Votre caisse d'Allocations familiales vous met en garde contre le "phishing" : ce sont des messages frauduleux que vous avez peut-être reçus, par courriel ou par téléphone (SMS ou message vocal).

Dans tous les cas, votre Caf ne vous demande jamais votre numéro de carte de crédit, ni sur un site internet, ni par courriel, ni au téléphone.

Pour être sûr que vous consultez le site de votre Caf et non un site pirate qui imite celui de votre Caf, il suffit de **saisir manuellement l'adresse <http://www.caf.fr>** dans votre navigateur. A partir de la page d'accueil, vous pouvez naviguer en toute confiance à l'intérieur de ce site, et accéder à la page souhaitée.

QUE FAIRE SI VOUS AVEZ RECU UN MESSAGE FRAUDULEUX ?

- Ne répondez pas au courriel - ou au SMS - ou au message vocal frauduleux, ne remplissez pas les données qui vous sont demandées, et n'appellez pas le numéro de téléphone qu'il peut comporter.
- Ne cliquez pas sur les liens ni sur les boutons du courriel frauduleux, et n'ouvrez pas les pièces jointes.
- Nous vous invitons à participer à la lutte contre le piratage informatique en signalant l'adresse du site frauduleux sur la page suivante : <http://www.phishing-initiative.com>
- Supprimez le courriel - ou le SMS - ou le message vocal frauduleux de votre boîte de messages.
- Assurez-vous régulièrement que les systèmes de sécurité de votre ordinateur et de votre téléphone portable sont à jour. En savoir plus sur le site http://www.securite-informatique.gouv.fr/gp_mot5.html

QUE FAIRE SI VOUS AVEZ REPONDU A UN MESSAGE FRAUDULEUX ?

- Si vous avez communiqué vos coordonnées bancaires suite à un message frauduleux, faites immédiatement opposition auprès de votre banque.
- Si vous avez communiqué vos identifiants de connexion à "Mon Compte", sur un autre site que [caf.fr](http://www.caf.fr), signalez-le vite à votre Caf qui vous transmettra un nouveau code confidentiel.
- Si vous avez envoyé la copie de votre carte d'identité ou tout autre justificatif aux auteurs d'un message frauduleux, nous vous conseillons de porter plainte auprès de la gendarmerie ou du commissariat le plus proche de votre domicile.
- Si vous pensez avoir été victime d'une escroquerie par « phishing », vous pouvez aussi le signaler sur le site officiel suivant : www.internet-signalement.gouv.fr. Cette plateforme permet de signaler les sites internet dont le contenu est illicite, mais aussi les tentatives de "phishing".
- Supprimez le courriel - ou le SMS - ou le message vocal frauduleux de votre boîte de messages.

POUR EN SAVOIR PLUS

Pour en savoir plus et pour mieux vous prémunir, vous pouvez consulter les pages suivantes sur le site de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) :

- « 5 réflexes à avoir lors de la réception d'un courriel » :
http://www.securite-informatique.gouv.fr/gp_article707.html
- « Filoutage (phishing) » :
http://www.securite-informatique.gouv.fr/gp_article44.html