

Phishing : ne vous faites pas avoir !



Depuis le confinement de nombreuses démarches administratives peuvent désormais se faire à distance, directement sur Internet. Cependant, attention ne vous connectez jamais à un site web en suivant un lien reçu par mail ou par SMS, car c'est par là que les pirates vont essayer de récupérer vos informations personnelles et bancaires pour les utiliser ensuite à votre insu.

- **Le phishing c'est quoi ?**
- **De nombreux recensements au phishing depuis le début de l'année**
- **Les réflexes essentiels à adopter contre les fraudes en ligne**
- **Vous avez fourni vos informations personnelles ?**

Le phishing c'est quoi ?

Le **phishing** ou "hameçonnage" est une technique de piratage, destinée à récupérer vos informations personnelles et données bancaires. Les **fraudes** sont diverses et parce que plus c'est gros, plus ça passe, les escrocs se font régulièrement passer pour un tiers de confiance : **banques**, impôts, CAF, assurances, fournisseurs d'énergie...

Ces **arnaques** sont menées par courrier électronique, et même si la raison peut varier, souvent, vous êtes invités à vous connecter à votre compte, à un site commercial, ou à un site de paiement, à partir d'un lien présent dans l'email, pour :

- mettre à jour vos informations (modifier vos identifiants et mot de passe),
 - envoyer des pièces justificatives d'identité,
 - obtenir un remboursement ou régler une **facture** en précisant vos coordonnées bancaires...
- En réalité, le lien vous conduit vers un **site frauduleux**, qui est d'ailleurs très réussi puisqu'il ressemble fortement au site original. Vos **données personnelles** sont ensuite récupérées par des arnaqueurs qui ont ensuite le champ libre pour effectuer des achats sur Internet à votre insu ou se faire passer pour vous.

Ne répondez surtout pas à ce genre de sollicitation et n'en faites pas la promotion autour de vous.

De nombreux recensements au phishing depuis le début de l'année

L'actualité se prête souvent aux arnaques et cette année avec le Covid-19, les escrocs en ont beaucoup profité pour renouveler leurs **attaques** : faux sites, faux investissements, faux produits bancaires, faux appels aux dons...

Et ce n'est pas fini (d'ailleurs ce n'est jamais fini), le service des impôts a annoncé avoir été victime d'une **fraude au phishing**, un message frauduleux, demandant aux destinataires une copie de leur carte d'identité.

Soyez toujours extrêmement vigilant face à ce genre d'approche, avec vos pièces d'identité une personne malveillante pourrait se faire passer pour vous et/ou souscrire à des produits et services, comme un **crédit** par exemple.

Les réflexes essentiels à adopter contre les fraudes en ligne

De manière générale, vous devez faire preuve d'une grande prudence avec vos informations personnelles et vos données bancaires.

- Méfiez-vous des messages (emails, SMS...) ou appels téléphoniques d'origine inconnue ou inattendus
- Ne répondez pas aux sollicitations
- Tapez vous-même l'adresse du site, sans suivre de lien
- Vérifiez que le site est sécurisé, notamment qu'il commence par https avec la présence d'un cadenas
- Prenez le temps de faire les vérifications nécessaires, surtout si le message est alarmiste et demande une action urgente
- Ne communiquez pas vos informations personnelles
- Ne donnez jamais les données de votre **carte** bancaire
- Mettez régulièrement à jour vos appareils et installez des anti-virus et pare-feux efficaces

A savoir

Les sites souvent ciblés par les **arnaques au phishing** (**banques**, CAF, etc.) proposent souvent des alertes de sécurité, que vous pouvez consulter sur Internet.

[Retour haut de page](#)

Vous avez fourni vos informations personnelles ?

Si vous avez fourni vos informations personnelles et/ou données bancaires, contactez immédiatement votre **banque** pour lui signaler et faire **opposition** sur votre **carte**. Pensez aussi à consulter régulièrement votre compte bancaire pour identifier toute fraude. En cas de **débit frauduleux**, contestez l'opération au plus vite.

Si vous n'avez pas fourni vos informations personnelles et numéros de carte, rassurez-vous, sans ces informations les malfaiteurs ne peuvent rien faire.

Si vous êtes victime d'une **escroquerie**, rendez-vous sur la plateforme Pharos pour signaler l'abus. Vous pouvez aussi contacter info-escroquerie au 0 805 805 817 (service et appels gratuits).

Votre signalement sera examiné par des policiers et des gendarmes rattachés à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (police judiciaire).

Juillet 2020