MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Le phishing

Gendarmerie nationale

Le Phishing : une technique bien rodée

L'hameçonnage ou le phishing consiste à obtenir du destinataire d'un courriel, **d'apparence légitime**, la transmission de **ses coordonnées bancaires ou ses identifiants de connexion à des services financiers**, afin de lui **dérober de l'argent**.

Pour renforcer sa crédibilité, l'expéditeur du mail frauduleux n'hésitera pas à utiliser logos et chartes graphiques des administrations ou entreprises les plus connues. Le contenu du message repose en général sur deux stratégies :

- soit il vous est **reproché de ne pas avoir réglé une certaine somme d'argent** (factures, impôts, électricité...) et on vous enjoint de le faire sous peine de pénalités de retard voire de saisine de la justice
- soit on vous **signale une erreur d'ordre financier en votre faveur** (impôts, banque...) et on vous invite à suivre des indications pour vous faire rembourser. D'autres méthodes existent (colis en attente, cadeaux, offre exceptionnelle etc.).

Conseils pour vous protéger

- **Ne répondez pas au message** ou mail frauduleux
- **Ne communiquez jamais vos données personnelles**, votre numéro de compte ou de carte bancaire
- **Ne cliquez pas sur le lien contenu dans le mail et n'ouvrez pas les pièces jointes**
- En cas de doute, **contactez directement l'organisme concerné par téléphone ou en saisissant manuellement l'adresse du site**
- **Signalez le mail frauduleux** sur le site Signal Spam

Vous avez répondu à un message frauduleux : Quoi faire ?

Si vous avez communiqué votre numéro de compte bancaire, de carte bancaire ou toutes autres données personnelles suite à un message frauduleux, réagissez rapidement :

1) Faites opposition auprès de votre banque très rapidement, en cas de débits frauduleux de votre compte suite à l'utilisation de votre carte bancaire.

2) Modifiez vos mots de passe et codes d'accès aux sites concernés. Si nécessaire, demandez au site l'attribution d'un nouveau code confidentiel.

3) Si vous avez envoyé copie de votre pièce d'identité, passeport ou permis de conduire, portez plainte auprès de la gendarmerie ou du commissariat ;

4) Signalez l'escroquerie sur le portail officiel de signalement des contenus illicites de l'internet : Plateforme PHAROS

Page d'accueil

Pour entrer en contact directement avec un gendarme 24/7 cliquez ➔

BRIGADE numérique

RÉFÉRENT SURETÉ PRÉVENTION TECHNIQUE DE LA MALVEILLANCE