



# L'HAMEÇONNAGE

CYBERCRIMINEL



## VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

### BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

### TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...



VICTIME



## COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir liens utiles)

*Pour en savoir plus ou vous faire assister, rendez-vous sur [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)*

## LIENS UTILES

• [Signal-spam.fr](http://Signal-spam.fr)

• [Phishing-initiative.fr](http://Phishing-initiative.fr)

• Info Escroqueries  
0805 805 817 (gratuit)



## DISPOSITIF NATIONAL D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

Assistance aux victimes  
Information et sensibilisation  
Observation du risque numérique



avec

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉCONOMIE  
ET DES FINANCES

MINISTÈRE DE L'INTÉRIEUR

SECRÉTARIAT D'ÉTAT CHARGÉ  
DU NUMÉRIQUE

**RETROUVEZ TOUTES NOS PUBLICATIONS SUR :**

[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

