

# L'HAMEÇONNAGE (phishing)

## VOL DE DONNÉES PERSONNELLES

### Technique :

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

### But :

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

CYBERCRIMINEL



Comment éviter de se faire hameçonner ?



### CONTACTS UTILES

- [Signal-spam.fr](http://Signal-spam.fr)
  - [Phishing-initiative.fr](http://Phishing-initiative.fr)
  - [Info Escroqueries](http://Info-Escroqueries.com)
- 0 805 805 817 (gratuit)

VICTIME



Ne communiquez jamais d'informations sensibles par messagerie ou téléphone



Confirmez avec l'organisme concerné



Vérifiez votre dernière connexion



Ne cliquez jamais sur un lien douteux



Utilisez des mots de passe différents et complexes



Activez la double authentification



Vérifiez l'adresse du site dans votre navigateur

SI VOUS AVEZ MALENCONTREUSEMENT COMMUNIQUÉ VOS DONNÉES PERSONNELLES, VOUS DEVEZ :

- Faire opposition immédiatement (en cas d'arnaque bancaire)
- Déposer plainte
- Changer vos mots de passe



**CYBERMALVEILLANCE.GOUV.FR**  
Assistance et prévention du risque numérique

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

### **Missions :**

Assistance aux victimes  
Information et sensibilisation  
Observation du risque numérique

**RETROUVEZ TOUTES NOS PUBLICATIONS SUR :**

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



avec

SECRÉTARIAT D'ÉTAT CHARGÉ  
DU NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉCONOMIE  
ET DES FINANCES