RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

COMPRENDRE LES RISQUES

L'HAMEÇONNAGE

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…

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 ci-dessous)

LIENS UTILES

Signal-spam.fr

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

SES MISSIONS

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **INFORMATION ET SENSIBILISATION** À LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

QUI EST CONCERNÉ ?

- PARTICULIERS
- COLLECTIVITÉS TERRITORIALES
- ENTREPRISES

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 3.0