RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

mémo

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
- Au moindre doute, contactez directement l'organisme concerné pour confirmer

COMMENT DÉTECTER UN MESSAGE D'HAMEÇONNAGE ?

7 points de contrôle qui doivent vous alerter :

- Une notification de la messagerie ou de l'antivirus
- Un nom d'émetteur inhabituel
- Une adresse d'expédition fantaisiste
- Un objet de message succinct ou alarmiste
- Un message aguicheur ou inquiétant
- Des fautes de français surprenantes
- Une incitation à ouvrir un lien ou une pièce-jointe

PLUS D'INFORMATIONS SUR :
www.cybermalveillance.gouv.fr