RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

mémo

COMPRENDRE LES RISQUES

# L'HAMEÇONNAGE

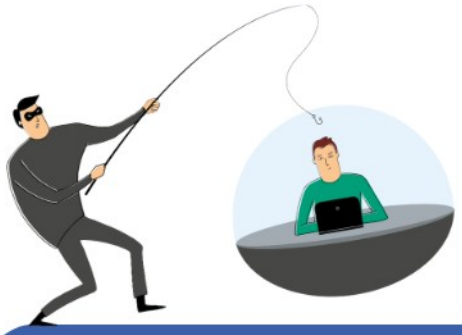

Vous recevez un message ou un appel inattendu, voire alarmant, d'un tiers qui vous demande des informations (personnelles ou bancaires), vous incite à cliquer sur un lien ou à ouvrir une pièce jointe ? Vous êtes probablement face à une tentative d'hameçonnage (phishing en anglais) !

## BUT

- Dérober des informations personnelles ou professionnelles (informations d'identité, coordonnées, mots de passe, codes de validation, données bancaires…) pour en faire un usage frauduleux ;
- Infecter un équipement par un virus pour en prendre le contrôle.

## MÉTHODE

Technique frauduleuse menée par mail, SMS, messagerie instantanée, message sur un réseau social ou par appel téléphonique qui usurpe l'identité d'un tiers de confiance : administration, entreprise (banque, livraison de colis, autoroute, commerce en ligne, réseau social…) voire d'un proche ou d'une connaissance (parents, amis, contacts en ligne…).



**S'informer :**
Cybermalveillance.gouv.fr

**Se faire assister :**
17Cyber.gouv.fr


## COMMENT RÉAGIR ?

• **Ne répondez pas** au message, **ne cliquez pas** sur les liens et **n'ouvrez pas** les pièces jointes d'un message suspect ou provenant d'un émetteur inconnu ;

• Au moindre doute, **vérifiez l'information** directement auprès de l'organisme ou de la personne qui vous sollicite.

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

mémo

COMPRENDRE LES RISQUES

# 9 POINTS DE CONTRÔLE
# POUR DÉTECTER UNE TENTATIVE D'HAMEÇONNAGE

1. Une alerte de votre logiciel de messagerie ou de votre antivirus
2. Un message d'un service, d'un organisme ou d'une entreprise dont vous n'êtes pas client ou utilisateur
3. Un nom ou une adresse d'expéditeur inhabituel, incohérent voire fantaisiste
4. Un objet de message succinct ou alarmiste
5. Une apparence suspecte (mauvaise mise en forme ou logo), une absence ou des erreurs dans la personnalisation
6. Un message aguicheur, inquiétant ou bien une demande inhabituelle
7. Des fautes de français surprenantes
8. Une incitation à cliquer sur un lien ou ouvrir une pièce-jointe
9. Un appel provenant d'un numéro de téléphone inconnu ou masqué

**Ces conseils vous aident à identifier un message malveillant mais les cybercriminels travaillent en permanence à rendre l'hameçonnage plus crédible.**
**Restez vigilant et, face à une sollicitation inhabituelle, vérifiez toujours par vous-même !**

**Si vous pensez être victime, rendez-vous sur 17Cyber.gouv.fr**