Aides et outils

- Les sites sécurisés ont une adresse commençant par « https » et précédé d'un cadenas
- En cas de hameçonnage consultez le site « PHAROS »
- Afin de vérifier les informations vous pouvez vous rendre sur le site « HOAXBUSTER .COM »
- Si vous êtes victime d'escroquerie contactez le numéro vert **0 805 805 817**

RAPPEL

15 SAMU	17 POLICE
18 POMPIERS	112 NUMÉRO INTERNATIONAL

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

GENDARMERIE NATIONALE
91
GROUPEMENT DE L'ESSONNE

M@lveillance numérique

Prendre la mesure du risque et comment l'éviter ?

CADETS DE LA GENDARMERIE
SNU
RGIF

par les cadets
de la Gendarmerie
de l'Essonne

Le hameçonnage

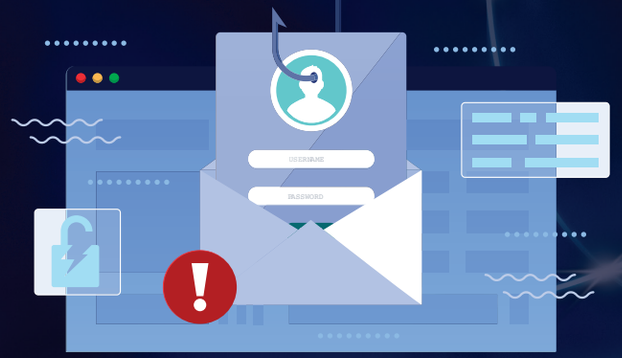
Qu'est-ce que c'est ?

Il s'agit d'une technique de fraude sur Internet visant à obtetnir des renseignements confidentiels (mots de passe, informations bancaires...) afin d'usurper l'identité de la victime.

Les règles à retenir :

- Aucune institution publique ne vous demandera de fournir vos informations privées et/ou confidentielles à partir de lien sur votre messagerie.
- Vérifier l'adresse mail de l'expéditeur, les fautes d'orthographes ou de formulations, les logos.

ATTENTION aux pièces jointes, aux liens et aux mails provenant d'organismes publics/privés inconnus.



Les mots de passe

- Choisissez un mot de passe complexe et évitez les suites de nombres ou de lettres (1234, AZERTY...)
- Choisissez un mot de passe différent pour chaque application ou pour chaque compte.
- Pensez à activer la double authentification.
- Gardez vos mots de passe à l'abris. Evitez de les noter sur des supports libres d'accès (post-it, carnet, téléphone...).

ATTENTION : évitez les wifi publics (sources d'arnaques).

Les réseaux sociaux

- Vérifiez vos paramètres de confidentialité (sélectionner le mode « privé »).
- Maitrisez vos publications (photos de familles, entre amis...).
- Faites preuve de discrétion sur vos publications.

ATTENTION : n'acceptez que les invitations des personnes dont vous connaissez l'identité !