

HAMEÇONNAGE

On vous incite à communiquer des informations importantes ?
Ne tombez pas dans le piège.

QUE SE PASSE-T-IL ?



1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :

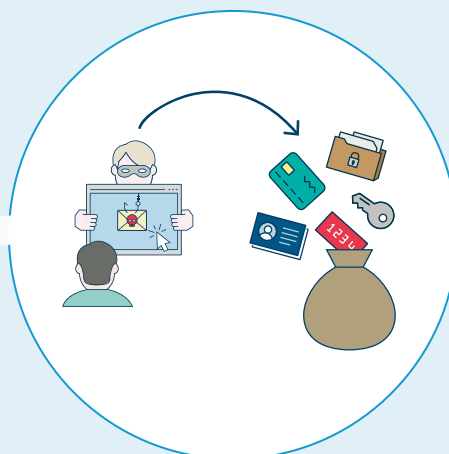
- cliquer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles



2. L'attaquant se fait passer pour une personne ou un tiers de confiance

L'attaquant est en mesure de :

- prendre le contrôle de votre système
- faire usage de vos informations



Impact de l'attaque



Intégrité



Disponibilité



Confidentialité



Authenticité

Motivations principales



Atteinte à l'image



Appât du gain



Revendication



Espionnage



Nuisance



Sabotage

COMMENT RÉAGIR ?

Vous êtes victime - Ne perdez pas un instant !



1 - Renouvelez immédiatement les identifiants des comptes compromis



2 - Contactez votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)



3 - Signalez l'incident sur PHAROS (www.internet-signalement.gouv.fr)



4 - Portez plainte auprès des services compétents (www.ssi.gouv.fr/en-cas-dincident)



5 - Plus de conseils avec INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit)

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

- Ne cliquez jamais sur un lien ou une pièce-jointe qui vous semblent douteux.
- Ne répondez jamais à un courriel suspect. Au moindre doute, contactez l'expéditeur par un autre canal.
- Évitez l'effet boule de neige ! Disposez d'un mot de passe unique pour chaque application.
- + de conseils avec la CNIL : www.cnil.fr/fr/tag/mots-de-passe
- Vérifiez les paramètres de sécurité de votre compte de messagerie.
- Activez l'authentification à double facteur

En savoir plus sur les attaques par hameçonnage :
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/arnaques-par-message-electronique-comment-identifier-et-dejouer-lhameconnage