# SE PROTEGER DU HAMEÇONNAGE

## QU'EST-CE QUE L'HAMEÇONNAGE ?

L'hameçonnage, en anglais « phishing », est une technique par laquelle un attaquant usurpe l'identité d'un tiers légitime dans le but d'obtenir des informations sensibles.

## OBJECTIFS DE L'ATTAQUE

L'objectif est de récupérer des informations sensibles/confidentielles qui serviront à des fins illégales en amenant la cible à agir (soit en cliquant sur un lien, soit en exécutant la pièce jointe, soit en répondant au mail, etc.).

## RISQUES

- ➔ **VOL DE DONNEES SENSIBLES**
- ➔ **PERTE FINANCIERE**

## SYMPTOMES

**EXEMPLE DE COURRIEL D'HAMEÇONNAGE:**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES 01/09/2010

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez ici

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

**ELEMENTS CARACTERISTIQUES D'UN MAIL DE PHISHING :**

- Pas de signature, numéros d'identification, etc.
- Demande d'informations confidentielles, ou autres
- Nombreuses fautes de français (e.g : « S'il vous plaît, soumettre la demande …»). (Attention de moins en moins vrai)
- Le lien affiché ne correspond pas au lien réel

En cas de doute, se rendre sur le site officiel sans suivre les liens du courriel et consulter les informations.

- La cible du lien présent dans le courriel ne possède pas de certificat valide

Vérifier dans la barre d'adresse qu'un cadenas soit présent, certains navigateurs affichent la mention « Sécurisé ». (Rester tout de même vigilant, ceci ne garantit pas l'absence de tentatives de phishing).

## QUOI FAIRE

- **NE PAS CLIQUER SUR LE LIEN/PIECES JOINTES**
- **NE PAS SUIVRE LES INSTRUCTIONS**
- **TRANSFERER LE MAIL AU SUPPORT INFORMATIQUE EN CAS DE DOUTE**
- **AVERTIR LES TECHNICIENS**
- **SIGNALER LE MESSAGE COMME ETANT DU SPAM**

# SE PROTEGER DU HAMEÇONNAGE

## GRAVE OU PAS ?

L'hameçonnage est considéré comme grave lorsque des informations sensibles ont été divulguées

## LES BONNES PRATIQUES

- Les organismes sociaux, bancaires et autres ne demandent jamais d'information sensible par courriel
- S'assurer de l'authenticité de la source du message (e.g: demander confirmation par téléphone)
- Ne jamais effectuer d'actions dans la précipitation
- Ne jamais répondre ou faire suivre ces mails exceptés auprès de personnes compétentes (RSSI, Support..)
- Attention à la forme (fautes de français, style grammatical, homographe etc.)
- Utiliser un logiciel de filtre anti-courriel malveillant
- Pour un site web, s'assurer de la validité du nom de domaine
- Se méfier des liens courts (bit.ly, goo.gl..). Vérification avec unshorten, checkshorturl,getlinkinfo

## ORIGINES

- Mails (premier vecteur)
- Sites web malveillant
- Publicités malveillantes

## RESSOURCES

Attaque par hameçonnage ciblé

## SE PROTEGER DU PHISHING

**PREVENTION •**

- **Utiliser des outils anti-phishing**

Des solutions anti-phishing pour les boites mails ou les navigateurs web. existent.(SpamAssassin, ClamAV, …)

- **Utiliser un serveur DNS sécurisé (e.g : OpenDNS)**

Cela permet de se protéger du phishing et d'autres contenus indésirables.

- **Sensibilisation**

Il est indispensable de sensibiliser les utilisateurs afin d'éviter une reproduction de l'incident. Cela peut se faire au moyen de quizz/présentations.
Aussi, des sites de référencement et signalement de phishing existent (e.g : https://www.phishtank.com/ ),

**EN CAS DE PHISHING CONSTATE •**

- **Changer son ou ses mots de passe**

Sans changement des mots de passe, l'attaquant peut utiliser les accès obtenus.

- **Si vol de données sensibles**

Alerter les services concernés afin que des dispositions soient prises (e.g : blocage de compte bancaire…).

- **Si une application a été installée**

Il faudra : Identifier l'infection, désinfecter ou réinstaller le système (restaurer les données le cas échéant).

- **Identifier les possibilités de rebond**

Lorsqu'un attaquant récupère un accès, l'exploitation de ressources associées à la victime est légion.

Si la machine infectée est présente dans un réseau interne, analyser les machines connectées afin de déterminer si d'autres accès ont pu avoir lieu. Si l'attaquant a récupéré des identifiants, analyser les possibles informations qui servirait à élargir son champs d'attaque.

- **Comment signaler une tentative de phishing ?**

- En installant l'add-on « Signal Spam » sur www.signal-spam.fr, celui-ci permet de signaler et de mieux se protéger des mails de phishing
- Directement sur le site : www.internet-signalement.gouv.fr
- Pour un SMS, le transférer au 33700 -Bouygues, Orange et SFR (gratuit)

- **Alerter les utilisateurs du réseau.**