

# PHISHING (Hameçonnage)



# Exemple de phishing

*De : webmaster@universite.fr [mailto:albert.duchmoll@univ-ville.fr]*

*Envoyé : jeudi 12 novembre 2015 08:21*

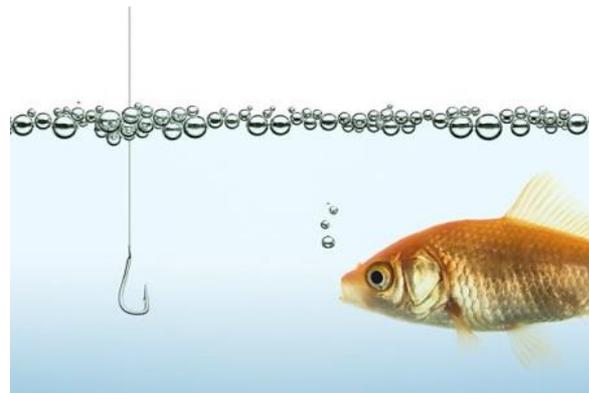
*Objet : Alerte*

Votre limite de stockage de boîte aux lettres a été dépassé en raison du taux élevé de Spam / ordure de tous les messages entrants sont rejetés.

Pour re-valider votre email. Cliquez sur le lien ci-dessous et envoyer le formulaire de revalider leur e-mail.

CLIQUEZ ICI: <http://upgrade-001-dept-akd12389754.tropid.com/>

© 2,015 équipe de support technique.



# Autre exemple, moins trivial



## Votre espace Client

Chère cliente, cher client,

Suite au refus de votre banque lors d'un prélèvement de facture ,Votre paiement a été malheureusement refusé .

A fin de résoudre ce dernier nous avons mis au point en accord avec votre banque une nouvelle tentative avec des vérifications plus approfondis .Veillez cher client suivre la procédure ci-dessous , toutes nos excuses pour ce désagrément .

[Résoudre ce problème maintenant.](#)

Cordialement,  
Votre conseiller **EDF**

Retrouvez tous vos services sur  **votre espace Client**

Ce message vous est adressé automatiquement. Nous vous remercions de ne pas répondre, ni d'utiliser cette adresse email.  
**ATTENTION** : Ce message est strictement confidentiel. Son intégrité n'est pas assurée sur Internet. Si vous n'êtes pas destinataire du message, merci de le détruire.

**EDF SA** au capital de 924 433 331 €, RCS Paris n° 552 081 317, siège social 22-30 av de Wagram 75382 Paris cedex 08.

Copyright © **EDF** 2010

## Définition

Techniques d'ingénierie sociale incitant un utilisateur à fournir « en toute bonne foi » des données sensibles ou d'autres ressources (argent, par exemple) à des personnes mal intentionnées, ou amenant l'utilisateur à installer à son insu des logiciels malveillants sur son poste de travail.

Le média utilisé pour effectuer un « phishing » est généralement la messagerie électronique, mais le téléphone, le fax ou l'écrit peuvent également être mis à contribution (cf. « arnaque au président »).



## Comment augmenter le niveau de vigilance ?

➤ campagnes régulières de faux phishing

## à quelles techniques d'ingénierie sociale se limite-t-on (pour l'instant 😊) ?

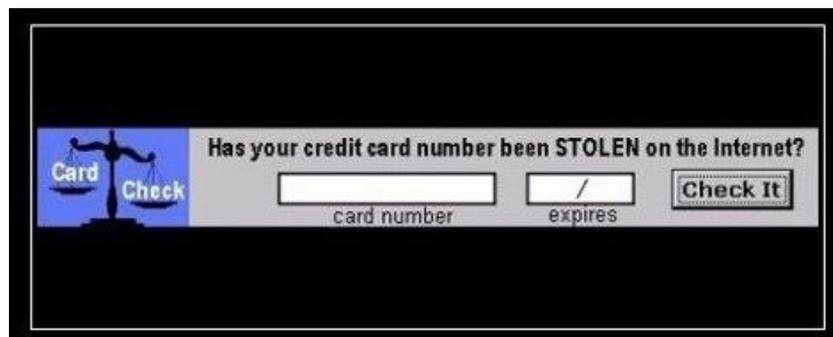
➤ envoi de mails incitant l'utilisateur à fournir des informations confidentielles

## Quels indicateurs (au minimum) ?

➤ pourcentage de personnes « piégées »

➤ noms des victimes (*Q : comment les prévenir avec tact ?*)

➤ délai entre le début de l'opération et premier signalement au CRI ou aux RSSI



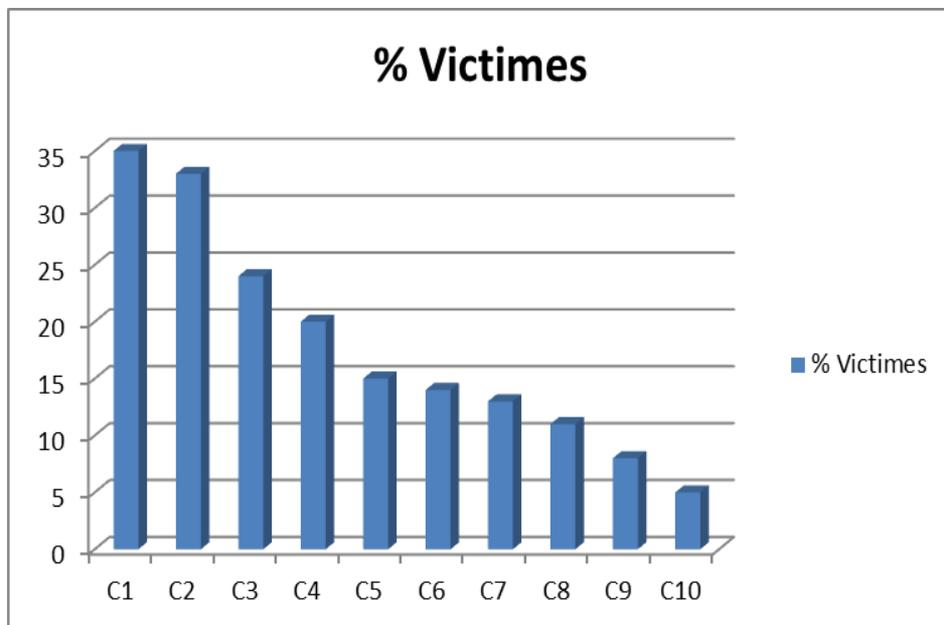
## Quelles sont les personnes ciblées ?

➤ À déterminer... (choix politique)

## Y-aura-t-il d'autres campagnes ?

➤ chaque année, il faut au minimum sensibiliser les nouveaux arrivants

➤ il faudra varier les méthodes de phishing 😊 tout en permettant une comparaison des indicateurs



Bonsoir,  
J'espère que je ne te dérange pas ?  
j'ai besoin sérieusement de ton aide. Contacte-moi par mail en toute discrétion, je suis en déplacement pour des raisons personnelles et je suis tombé dans une situation embarrassante. C'est vraiment délicat. J'ai besoin de ton assistance financière, juste un prêt que je te rembourserai dès mon retour de voyage. Je reste dans l'attente urgente de te lire.  
Cordialement