



U M I H

UNION DES MÉTIERS ET
DES INDUSTRIES DE L'HÔTELLERIE

Fiche n°1 : Les courriels frauduleux ou *phishing*

(maj DGCCRF 21/10/2016)

Nous vous avons déjà alerté sur cette pratique frauduleuse à l'occasion de notre circulaire de vigilance n°13.15.

Le *phishing* est une technique par laquelle **des personnes malveillantes se font passer pour de grandes sociétés ou des organismes financiers** qui vous sont familiers en envoyant des mails frauduleux **aux fins de récupérer vos mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.**

➤ Quel est le principe du *phishing* ?

Le principe du *phishing* est de récupérer des données personnelles sur internet, en usurpant l'identité d'une banque ou d'un fournisseur de service par exemple.

L'escroquerie repose le plus fréquemment sur :

- la contrefaçon du site internet de l'entreprise en question, et l'adresse URL du lien comprise dans le mail est également « masquée » afin de paraître authentique.
- des mails envoyés massivement, dans lesquels se trouvent une contrefaçon du logo et de l'adresse mail. Le message est souvent à connotation alarmiste ou allègue un prétendu remboursement en faveur de l'internaute.

Cela semble provenir d'une source de confiance (banque, CAF, impôts, etc.) et invite à se rendre sur une page de formulaire afin de fournir des données personnelles et souvent à caractère financier.

Ces informations sont ensuite récupérées par les *phishers*. Pendant toute la procédure, la victime croit avoir à faire à un site officiel d'un opérateur qu'elle connaît. Les liens figurant sur la page internet du formulaire sont souvent inactifs.

➤ Comment s'en protéger ? (Source : www.securite-informatique.gouv.fr)

- ✉ **Les centres des impôts n'envoient jamais ce genre de courriel.** Ils ne passent jamais par un courrier électronique pour demander à leurs assujettis de saisir leurs informations personnelles.
- ✉ **Les banques et organismes sociaux (CAF, mutuelles, etc.) n'envoient jamais non plus ce genre de courriel :** Ils ne passent jamais par un courrier électronique pour demander à leurs clients de saisir leurs informations personnelles. Pour se connecter au site de sa banque il vaut mieux entrer manuellement l'adresse réticulaire (URL) du site dans votre navigateur.
- ✉ **Préférer saisir des informations personnelles (coordonnées bancaires, identifiants, etc.) sur des sites internet sécurisés :** un cadenas apparaît dans le navigateur et l'adresse du site commence par HTTPS au lieu de HTTP.

- ↵ **Ne pas cliquer sur les liens contenus dans ces courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.
- ↵ **Être vigilant lorsqu'un courriel demande des actions urgentes.**
- ↵ **Utiliser le filtre contre le filoutage du navigateur internet** : la plupart des navigateurs (Microsoft Internet Explorer 7, Mozilla Firefox, Opéra) proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé, etc.) et sans être parfaites, ces fonctions aident à maintenir la vigilance de l'utilisateur.
- ↵ **Utiliser un logiciel de filtre anti-pourriel** : la plupart du temps ces tentatives d'escroquerie se diffusent par le biais de courriers électroniques. Même si les logiciels de filtrage ne sont pas parfaits, ils permettent de réduire le nombre de ces courriels.
- ↵ **Ne jamais répondre ou transférer ces courriels.**
- ↵ **En cas de doute ou de problème, prendre contact rapidement avec son agence bancaire ou l'organisme qui aurait envoyé ce courriel.**
- ↵ **D'une manière générale, être vigilant et méfiant.**

➤ **Signaler l'abus d'utilisation d'informations personnelles aux autorités compétentes**

Si vous pensez avoir été victime d'une escroquerie par *phishing*, signalez le immédiatement sur la plateforme « PHAROS » (plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements) à l'adresse suivante : www.internet-signalement.gouv.fr

Cette plateforme permet de signaler les sites internet dont le contenu est illicite, mais aussi la réception de *phishing*.

Votre signalement sera traité par un service de police judiciaire spécialisé dans ces questions, l'office central de lutte contre la criminalité et de la communication (OCLCTIC).

Enfin, vous pouvez également signaler les tentatives de phishing sur le site www.phishing-initiative.com, édité par l'association Phishing Initiative et destiné à alimenter les principaux navigateurs afin que l'accès à ces sites soit bloqué.