VIROFLAYSIENS VIGILANTS
Participation Citoyenne

Comment se prémunir contre *le phishing* ?

Usagers du web, vos données sont précieuses et les pirates le savent. C'est pourquoi ils redoublent d'imagination pour tenter de vous les soutirer. L'un de ces moyens est ***le phishing***.

Qu'est-ce que le phishing ou hameçonnage ?

Le **phishing** ou **hameçonnage** consiste à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses **coordonnées bancaires** ou ses **identifiants de connexion à des services financiers**, afin de lui **dérober de l'argent**.

Il s'agit de l'un des principaux vecteurs de la cybercriminalité.

Pour renforcer sa crédibilité, le courriel frauduleux n'hésitera pas à utiliser **logos** et **chartes graphiques des administrations ou entreprises** les plus connues. Le contenu du message repose en général sur 2 stratégies :

- soit **il vous est reproché de ne toujours pas avoir réglé une certaine somme d'argent** (factures, impôts, électricité,...) et on vous enjoint à le faire sous peine de pénalités de retard voire de saisine de la justice ;
- soit **on vous signale une erreur d'ordre financier en votre faveur** (impôts, banque,...) et on vous invite à suivre des indications pour vous faire rembourser.

D'autres méthodes existent (fax en attente, cadeaux,...). **Surtout restez vigilant !**

Comment vous protéger contre le phishing ?

Voici quelques conseils pour vous protéger contre le phishing :

- Si un courriel vous semble douteux, **ne cliquez pas sur les pièces jointes ou sur les liens** qu'il contient ! Connectez-vous en saisissant l'adresse officielle dans la barre d'adresses de votre navigateur.
- Si vous réglez un achat en ligne et que vous devez donc fournir des informations relatives à votre carte bancaire, **vérifiez que vous êtes sur un site web sécurisé dont l'adresse commence par « https »**.
- **Ne communiquez jamais d'informations confidentielles par mail**. Aucun site web fiable ne vous le demandera !
- **Vérifiez que votre antivirus est à jour** pour maximiser sa protection contre les programmes malveillants.

En cas d'agression ou si vous remarquez un comportement étrange : appelez le 17

- **Utilisez le filtre contre le filoutage du navigateur internet** : la plupart des navigateurs existants proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé, etc.), mais toutes ces fonctions aident à maintenir votre vigilance.
- **Utilisez un logiciel de filtre anti-pourriel** ou les fonctionnalités de classement automatique en tant que spam de votre boite de réception : même si ces filtrages ne sont pas exhaustifs, ils permettent de réduire le nombre de ces courriels.

Signalez l'abus d'utilisation d'informations personnelles aux autorités compétentes

Si vous pensez avoir été victime d'une escroquerie ou d'une tentative d'escroquerie par phishing signalez-le sur **signal-spam.fr**. Signal Spam donne la possibilité aux internautes de **signaler tout ce qu'ils considèrent être un spam dans leur messagerie** afin de l'assigner ensuite à l'autorité publique ou au professionnel qui saura agir pour lutter contre le spam signalé.

Exemples de messages frauduleux reçus par e-mail :

En cas d'agression ou si vous remarquez un comportement étrange : appelez le 17