Info-Alerte n° 2140 du 23 avril 2020

Détecter une tentative de PHISHING

Les tentatives de phishing *(hameçonnage)* se multiplient. Sous couvert d'une information semblant émaner, le plus souvent, d'un opérateur de téléphonie, d'un établissement bancaire ou d'une administration, les escrocs visent à obtenir la communication du numéro de carte bancaire ou la copie de documents officiels *(pièce d'identité, quittance de loyer, bulletin de salaire)*.

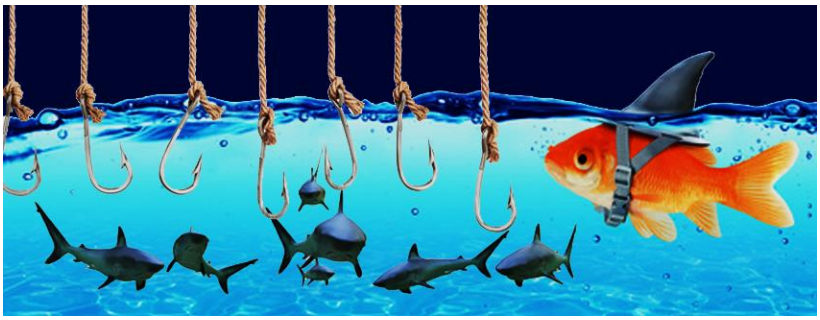
Les messages frauduleux qui sont diffusés actuellement sont bien plus performants que dans les années précédentes : une orthographe améliorée, une mise en page de qualité avec des logos à jour.

L'une des pistes pour détecter une tentative de phishing consiste à observer l'adresse de l'émetteur. En toute logique, elle sera construite selon le libellé suivant : mention « contact » ou « service clients » suivi de l'intitulé de la société. Si vous découvrez une adresse « exotique », il s'agit bien d'un message frauduleux.

Quelques exemples sélectionnés par le **Réseau anti-arnaques** :

- souscription-1@services-sg-notifications.com *(faux message **SOCIÉTÉ GÉNÉRALE**)* ;
- service.depot-chronopost.fr@contact-infos.mondovino.com *(faux message **CHRONOPOST**)* ;
- contact@bnpnb-propriv.ml *(faux message **BNP-PARIBAS**)*.

D'autre part, l'internaute désireux de contacter un fournisseur ou une administration, doit se connecter sur l'espace clients du site plutôt que de cliquer sur un lien présent dans un message reçu. Autrement dit, le consommateur doit rester maitre de l'initiative du contact.



INFO-ALERTE est une mise en garde hebdomadaire diffusée par le :
Réseau anti-arnaques, association partenaire de l'UFC-Que Choisir
BP 40179 – 79205 PARTHENAY cedex
(contact@arnaques-infos.org) - Site : www.arnaques-infos.org
SIRET : 503 805 657 00049

Directeur de la publication :
Pascal TONNERRE (president@arnaques-infos.org)