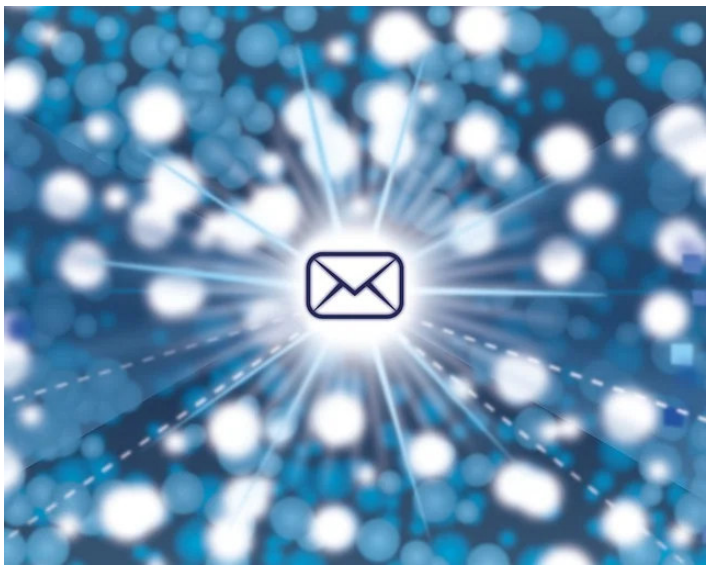
LE GLOSSAIRE DES ARNAQUES : LE SMISHING

Les arnaques sur internet se voient attribuer des « noms de baptême » permettant de les qualifier. Il s'agit de termes anglais qui bénéficient le plus souvent d'une traduction française.

Les deux termes les plus connus restent le « phishing » (hameçonnage) et le « scamming » (arnaque par ruse). Dans le premier cas, il s'agit de vous faire cliquer sur un lien frauduleux dans votre messagerie alors qu'il peut paraître officiel pour communiquer des informations confidentielles. Dans le second cas il s'agit d'un scénario frauduleux (fausse succession, faux gain au loto, faux amoureux) visant à régler des sommes d'argent par des moyens atypiques (recharge de cartes de crédit par exemple).

Le **Réseau Anti-Arnaques** se propose d'évoquer chaque mois un terme spécifique. Aujourd'hui, pour cette première présentation, l'invité est le « smishing ».

Le smishing est en fait un hameçonnage, réalisé par le biais d'un SMS (et non plus par le biais d'un mél). Par définition ce SMS frauduleux est bref, et vise à obtenir des informations confidentielles (informations personnelles, identifiants de connexion…). Le consommateur a tendance à le traiter (trop) rapidement.



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). Elle alimente la page **Facebook** du **RAA**.
SIRET : 503 805 657 00049

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