10 nouvelles arnaques très sophistiquées.

Un banal numéro commençant par "01, 02, …" ou "09" 'Spam SMS, vocal, téléphonique ou par mail... Attention aux nouvelles arnaques.

La consigne reste la même pour les nouveaux types de spams : "Ne rappelez pas".
De plus en plus sophistiqués, les spams sur mobile gardent le même objectif : vous faire rappeler, par tous les moyens, un numéro surtaxé. L'une des dernières formes de spams répertoriées par la plateforme de lutte contre les spams 33700.fr concerne les spams vocaux, suite à une alerte de la police nationale. "Votre téléphone sonne brièvement sans laisser de message ? (…) Ne rappelez pas, le numéro peut être surtaxé. Signalez-le par sms au 33 700". Ces appels frauduleux commencent par un indicatif régional français anodin (01, 02...) ou un numéro en 09. Les numéros commençant par "01 86 85" sont souvent pointés.

Un "contrôle d'alarme incendie"

Si vous appelez le numéro surtaxé, il vous sera répondu au bout de plusieurs minutes que "tous les agents sont en ligne".
Cette arnaque pas comme les autres se déroule ainsi : un automate vous contacte par téléphone en pleine nuit pour vous signaler un "contrôle" de vos installations de "détecteurs de fumée". La nouvelle arnaque ne prend pas de gants : l'une de ses dernières victimes, une habitante de Condéon, en Charente, a été réveillée à 4h30 par un appel du 09 75 12 42 52, l'invitant à rappeler un autre numéro dans la foulée, raconte Sud-Ouest. Il s'agissait du 089 963 05 24, surtaxé à 3 euros. L'astuce des escrocs : jouer sur l'effet de surprise, à des heures indues.

Les émissaires de fausses compagnies.

Les appels sur ligne fixe n'échappent pas aux spams. Et se corsent avec l'apparition, dans la plupart des cas, d'un vrai interlocuteur au bout du fil. Sur la plateforme de signalement http://www.arnaques-internet.info/, un internaute raconte par exemple avoir été contacté par le 09 80 09 04 28 par une personne se faisant passer pour un émissaire de la Sécurité sociale et essayant de lui soutirer des informations à domicile. Or, les véritables organismes, qu'il s'agisse de compagnie d'assurance, de banques ou d'administrations, ne font pas ce genre de démarche.

La "consultation des points du permis de conduire"

N'appelez surtout pas le numéro indiqué : il s'agit à coup sûr d'une arnaque. L'arnaque à la "consultation des points de permis" consiste à recevoir un appel traitant du sujet sensible du nombre de points sur votre permis. L'escroquerie au numéro surtaxé prend l'apparence d'un coup de fil de soi-disant employés du service permis de conduire de la préfecture. Ils vous informent alors de votre solde de points actuel en vous précisant généralement qu'il "vient d'être mis à jour" et vous demandent de rappeler un numéro (surtaxé). Or les préfectures ne donnent jamais par téléphone le nombre de points du permis de conduire.

Une "livraison de colis"

Colis or not colis, that is the question.
De nombreux Français font état d'arnaques à la livraison de colis, généralement par SMS. Si cette dernière n'est pas le plus récent des spams, elle montre le degré de sophistication atteint depuis le début des années 2000. Hautement résistant (il sévit toujours), ce spam fait croire aux gens que le transfert d'un colis à leur intention est suspendu. Et ressemble à ça : "Votre colis est en attente sur notre plate-forme/dans notre entrepôt. Veuillez nous rappeler sous peine d'annulation de votre commande". Facile à débusquer quand vous n'attendiez aucune commande, mais plus difficile dans le cas contraire.

Les faux bons d'achat

Carrefour et Electro Dépôt ont également été contactés de victimes de ce type d'arnaques.
Les faux bons d'achat correspondent à une forme de spam émergente, qui vous parvient sous forme de message vocal sur votre répondeur. Plutôt convaincant à l'écoute, ce dernier vous annonce que vous avez remporté un bon d'achat, souvent conséquent, dans une grande enseigne. Les victimes sont invitées à rappeler un numéro pour fournir leurs coordonnées et récupérer leur bon d'achat. Sauf qu'il s'agit d'un numéro surtaxé (même si on vous dit que l'appel est gratuit dans le message). Les deux enseignes les plus touchées par l'arnaque sont Conforama et Ikea.

Les SMS EDF bidons

L'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) est notamment chargé de lutter contre le phishing téléphonique.
La pratique est récente et particulièrement vicieuse : des SMS frauduleux envoyés au nom d'EDF ou d'autres sociétés au nom bien connu. De ceux qui vous demandent, par exemple, de fournir votre email complet pour "mieux vous informer". Objectif réel ? Comme pour tout spam qui se respecte, vous soutirer des informations mais aussi vous

pousser à rappeler des numéros surtaxés, commençant en général par 08 99. La société EDF elle-même enjoignait en décembre dernier de "ne pas répondre et ne pas cliquer sur le lien", assurant au passage que quand elle cherche à contacter un client, c'est "par téléphone ou courrier".

Le "lien à cliquer" pour obtenir un MMS, lire ou écouter un message

Les spams SMS nouvelle génération ressemblent à s'y méprendre à un message d'opérateur.
Les spams SMS sont devenus une routine pour certains utilisateurs de smartphones. Mais il en existe depuis peu une version "perfectionnée" : ces SMS, qui s'apparentent à ceux d'opérateurs, sont plus vrais que nature. Ils vous enjoignent de cliquer sur un lien pour accéder, suivant les cas, à un MMS, un message vocal ou écrit, et même un message "non-réceptionné". Beaucoup d'entre nous cliquent dessus sans rien obtenir, persuadés ensuite qu'ils ne savent pas bien utiliser leur téléphone. Et recommencent leur tentative la fois suivante, faisant l'affaire des émetteurs de spams.

L'arnaque spécial fêtes de fin d'année.

Les nouveaux escrocs savent jouer les faux père-noëls.
Va-t-on retrouver cette arnaque à Noël prochain dans nos téléphones ? Les escrocs savent désormais calquer leurs messages sur les événements, y compris les plus populaires. Les dernières fêtes de fin d'année ont été marquées par la réception massive de SMS signalant une réception de colis (plutôt courant avant Noël - CQFD) alors qu'il n'en était rien. Les missives demandaient au destinataire d'appeler un numéro surtaxé pour obtenir le suivi de leur colis. S'il peut arriver qu'on vous contacte pour un vrai colis, renseignez-vous via Internet sur le numéro indiqué avant d'appeler.

Les faux mails de sociétés

Le phishing de messagerie avec société fictive ou des spams de messagerie d'un nouveau genre. © SEBASTIEN SALOM-GOMIS/SIPA
Avant, on reconnaissait les spams de messagerie au premier coup d'œil : généralement truffés de fautes d'orthographe, leur contenu était souvent plus gros qu'une maison, comme avec ces fameux expéditeurs "orphelins", "veufs" ou "fortunés" vous priant dans leur mail de les aider à toucher une forte somme d'argent moyennant récompense. A présent, d'autres tentatives de Phishing, plus dangereuses, colonisent les boîtes mails : celles qui ont l'air de provenir de véritables sociétés basées en France.

Les arnaques téléphoniques via Le Bon Coin

Les arnaques téléphoniques prennent aussi appui sur des sites internet en apparence inoffensifs. Dorénavant, les arnaques téléphoniques ne sont pas toujours là on croit les trouver. Elles se cachent aussi, par exemple, sur les sites Web de petites annonces type Leboncoin.fr. Ce dernier, gratuit et sans commission, a beau permettre, entre autres, de vendre ou de louer un bien immobilier, il est très déconseillé, comme sur d'autres sites d'annonce du même type, d'y afficher votre numéro de téléphone en ligne ou vous risqueriez d'avoir de mauvaises surprises. Autrement dit, d'être assailli de spams vocaux ou de SMS publicitaires. Surtout, vous pourriez même être contactés par de faux acheteurs potentiels…

Les sms, appels en absence ou mails de "copains"

Face aux spams "copains", il faut savoir rester zen et surtout... silencieux.
Un appel qui vous dit "Allo ? Allo ? Ça capte mal… Rappelle-moi s'il-te-plaît ". Un message Facebook ou un mail en forme d'au secours qui vous demande une somme d'argent pour dépanner. Les messages de faux proches sont tellement "spontanés" et personnalisés qu'ils vous font croire illico que l'émetteur est quelqu'un que vous connaissez vraiment. Souvent, il faudra vous être laissé prendre une fois pour ne pas tomber dans le panneau ensuite. Mais ensuite, vous êtes généralement vacciné sur cette arnaque-là. Et c'est sans doute là la faille de ces spams de plus en plus sophistiqués.

La fausse arnaque à 150 000 dollars.

Des trésors peuvent se cacher dans votre dossier spam de messagerie et sa montagne de "pourriels". Parfois, malgré tous ceux que l'on vient de vous citer, les spams apparents n'en sont pas. Le mois dernier, Helen Garner, une écrivaine australienne, a tout de suite cru à une arnaque en découvrant un mail dans ses messages indésirables lui apprenant qu'elle venait de gagner 150 000 dollars (136 103 €). Il s'agissait pourtant, après vérifications, d'un mail de l'Université de Yale pour l'informer qu'elle avait remporté le prix littéraire Windham-Campbell et la copieuse somme d'argent allant avec. Une particularité du Prix en question peut expliquer la situation : il ne comporte pas de système de candidature et les auteurs sont évalués sans qu'ils le sachent.

Doc : Linternaute.com