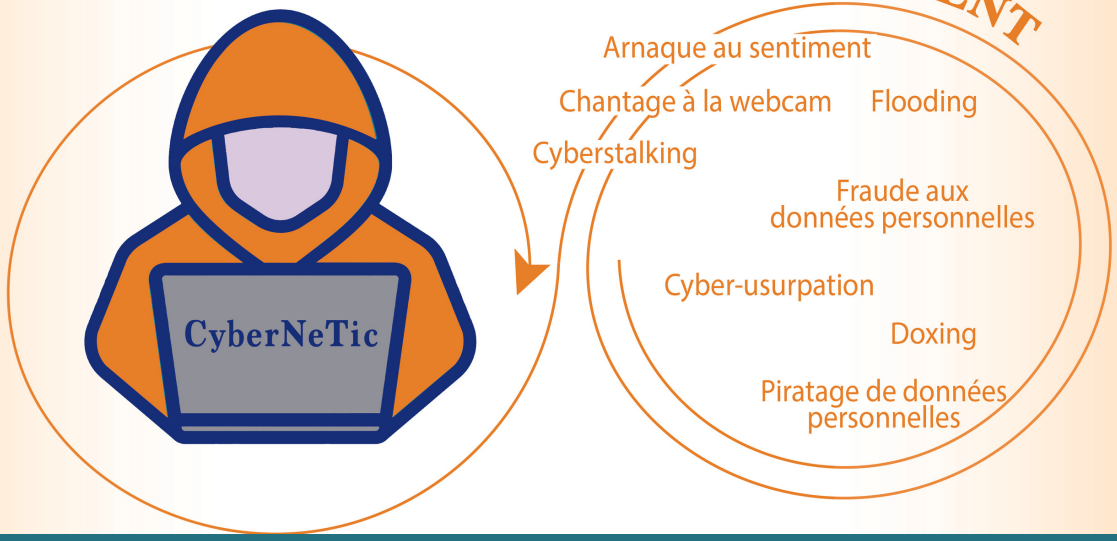
FRAUDE AUX DONNEES PERSONNELLES



SYNONYMES

- Escroquerie aux données personnelles
- Usage frauduleux de données personnelles

Définition

Concept-clé :

Dans le cadre de pratiques de cyberharcèlement, la fraude aux données personnelles consiste à mettre en place des techniques d'escroquerie numériques afin de dérober des informations personnelles, professionnelles et/ou bancaires, souvent à des fins d'enrichissement(revente des données, transactions frauduleuses, etc.)., dans le but de porter préjudice à une victime ciblée.

L'usage frauduleux de ces données recourt généralement à l'art de la manipulation et fait appel à des mécanismes de **conditionnement des comportements** pour duper les personnes. Plus communément appelé "**ingénierie sociale**" ou "**processus d'élicitation**" (qui signifie étymologiquement "tirer de", "faire sortir de"), cette démarche exploite les failles humaines et instrumentalise certains **biais cognitifs** (biais de cadrage, biais de confirmation, biais de distorsion perceptive, etc.) pour inciter de façon détournée les victimes à **enfreindre elles-mêmes les procédures de sécurité** de leurs appareils numériques.

Ce type d'approche relationnel se fonde principalement sur **l'abus de confiance** et profite du manque de connaissance informatique, d'une faille des logiciels de sécurité, d'une incrédulité ou d'une fragilité momentanée des personnes, etc., pour leur soutirer des renseignements sensibles et stratégiques (mot de passe, codes d'accès, etc.) afin de commettre leur forfait.

Ce qu'il faut retenir...

Plusieurs **techniques d'ingénierie sociale en ligne** sont utilisées pour leurrer les victimes et les inciter à communiquer leurs données sensibles :

- L'hameçonnage (phishing) s'appuie sur un message électronique frauduleux qui présente toutes les apparences d'un **message authentique** provenant d'une **source fiable** et qui incite le destinataire à **cliquer** sur un lien suspect, à **télécharger** une pièce jointe malveillante ou à **partager** directement ses informations personnelles ou financières.

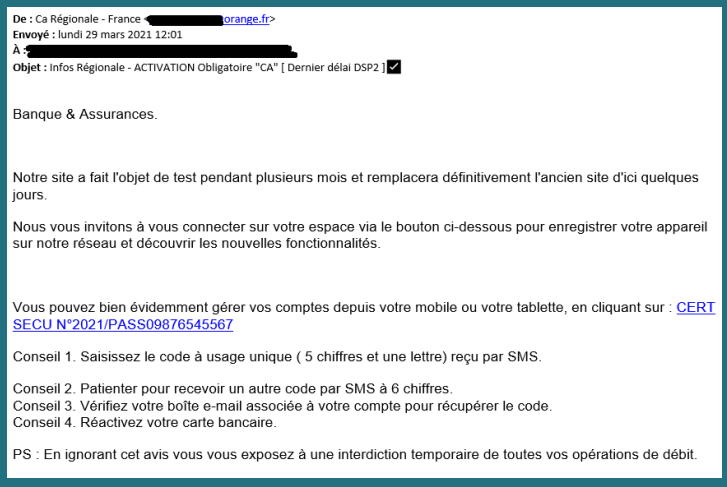
- Le harponnage (spear-phishing) est une variante très efficace de l'hameçonnage qui vise à **collecter en amont des informations** sur une victime bien ciblée afin de personnaliser le message qui lui est envoyé (par exemple en liant l'objet du courriel et le corps du message à son activité). Est souvent invoqué un **caractère d'urgence** dans le message de manière à assaillir la personne, l'exhortant à « agir avant qu'il ne soit trop tard », annihilant ainsi sa capacité de réflexion.

- L'appâtage (baiting) est une méthode un peu différente car elle sous-tend l'utilisation d'un **composant physique**, comme par exemple une clé USB qui contient un maliciel, et mise sur la **curiosité** de la victime pour la **brancher sur son ordinateur**, ce qui exécutera automatiquement le code malveillant, donnant accès à ses activités en ligne et hors ligne, dossiers personnels, etc.

- Le faux-semblant (pretexting) consiste à mobiliser un **prétexte solide** pour rentrer en contact avec la victime. Pour cela, le cyberharceleur emprunte généralement les traits d'une **figure d'autorité** ou d'un **tiers de confiance** (une banque, une compagnie d'assurance, l'administration fiscale, etc.) qui nécessite que la cible confirme son identité (par son numéro de téléphone, par son adresse mail, par des informations relatives au service qu'elle utilise, etc.) afin de débloquer une situation problématique.

> *Ce lien m'a amené sur un site web identique à celui de l'administration fiscale. Je ne suis pas naïf et pourtant je suis tombé dans le panneau...*

Un exemple concret :



De : Ca Régionale - France <[redacted]orange.fr>
Envoyé : lundi 29 mars 2021 12:01
À : [redacted]
Objet : Infos Régionale - ACTIVATION Obligatoire "CA" [Dernier délai DSP2]

Banque & Assurances.

Notre site a fait l'objet de test pendant plusieurs mois et remplacera définitivement l'ancien site d'ici quelques jours.

Nous vous invitons à vous connecter sur votre espace via le bouton ci-dessous pour enregistrer votre appareil sur notre réseau et découvrir les nouvelles fonctionnalités.

Vous pouvez bien évidemment gérer vos comptes depuis votre mobile ou votre tablette, en cliquant sur : CERT SECU N°2021/PASS09876545567

Conseil 1. Saisissez le code à usage unique (5 chiffres et une lettre) reçu par SMS.

Conseil 2. Patienter pour recevoir un autre code par SMS à 6 chiffres.
Conseil 3. Vérifiez votre boîte e-mail associée à votre compte pour récupérer le code.
Conseil 4. Réactivez votre carte bancaire.

PS : En ignorant cet avis vous vous exposez à une interdiction temporaire de toutes vos opérations de débit.

Aux origines...

Les origines du phishing remontent aux années **90**, à l'époque où la société **AOL** était l'un des principaux fournisseurs de services Internet et comptait plus d'un million de clients abonnés.

Cette popularité grandissante a attiré l'attention de pirates qui se sont constitués en un groupe s'identifiant comme la "c**ommunauté Warez**". Ils volaient les données sensibles des clients (leur nom d'utilisateur, leur mot de passe, etc.), puis grâce à un algorithme, généraient de manière aléatoire des **numéros de carte de crédit** qu'ils réutilisaient pour créer de faux comptes AOL.

En mettant à jour ses mesures de sécurité, AOL réussit à freiner à cette extorsion organisée de cartes de crédit, ce qui obligea les pirates à rechercher d'autres techniques pour tromper les utilisateurs. Ils ont alors commencé à utiliser AOL Messenger et créé de faux e-mails se faisant passer pour des employés de la société.

Pour enrayer ce nouveau mouvement de **phishing** (hameçonnage), AOL s'est mis à **détecter des mots-clés** dans les salons de conversation afin d'identifier tout vocabulaire qui pourrait les conduire jusqu'aux malfrats.

De manière à ne plus se faire repérer, les hackers ont alors cessé d'utiliser des mots, remplaçant simplement par la **chaîne de caractères « <>< »** toute référence à leurs activités illégales. Omniprésent dans toutes les pages HTML, ce **symbole** proche de la **forme d'un poisson** était devenu indétectable.

Que dit le cadre légal...

Dans le cadre d'une fraude aux données personnelles, plusieurs atteintes aux STAD sont sanctionnées par le code pénal et le code monétaire et financier. Nous pouvons retenir principalement :

- "**Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite**" qui est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18) ;

- "**Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données**" (article 323-2) qui est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende ;

- "**Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient**" (article 323-3) qui est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende ;

- "**Le fait de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions**" (article L. 163-3 du Code monétaire et financier) qui est puni de sept ans d'emprisonnement et de 750 000 euros d'amende ;

-"**Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions**" (article 323-3-1 du Code pénal) qui est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Pour aller un peu plus loin...

Quelques références scientifiques :

BATTISTI Michèle, Malwares, ransomwares, phishing,... et les autres », *I2D - Information, données & documents*, Volume 54, n° 3, 2017, pp. 1-1.

BEAUVOIS Jean-Léon, *Les influences sournoises. Précis des manipulations ordinaires*, François Bourin éditeur, 2011.

BENBOUZID Bilel, PEAUCELLIER Sophie, L'escroquerie sur Internet. La plainte et la prise de parole publique des victimes, *Réseaux*, Volume 197-198, n° 3-4, 2016, pp. 137-171.

DECLOQUEMENT Franck, LEHMANN Emmanuel, *Petit Traité d'Attaques Subversives Contre les Entreprises : théorie et pratique de la contre-ingérence économique*, Éditions Chiron, 2009.

DOUZET Frédérick, SAMAAN Jean-Loup, DESFORGES Alix, Les pirates du cyberespace, *Hérodote*, Volume 134, n° 3, 2009, pp. 176-193.

HADNAGY Christopher, *Social engineering. The art of human hacking*, John Wiley & Sons, 2010.

JOULE Robert-Vincent, BEAUVOIS Jean-Léon, *La soumission librement consentie*, Presses universitaires de France, 1998.

PENVEN Alain, *L'ingénierie sociale. Expertise collective et transformation sociale*, Érès, 2013.

RIVIERE Joël, Criminalité et Internet, une arnaque à bon marché, *Sécurité globale*, Volume 6, n° 4, 2008, pp. 67-82.