Penser en « biais » … pour comprendre les attaques par ingénierie sociale

Mme Nathalie GRANIER *– Cyber-Psychologue, experte en Threat Intelligence*

Depuis la nuit des temps, la supercherie est un art qu'il faut savoir maîtriser pour gagner des guerres. C'était d'ailleurs l'un des points clés évoqués par Sun Tzu, dans son « Art de la Guerre » dont il dit qu'il est entièrement « *basé sur la duperie.* »

Sun Tzu[1] n'imaginait sans doute pas qu'avec ce manifeste, il allait à jamais marquer de son empreinte les sciences militaires, pour les faire graviter autour d'un concept simple : « the deception ».

« Deception », ce terme anglais, qui pourrait passer pour un faux-ami, mais qui désigne en fait l'ensemble des mesures et contremesures à utiliser pour induire en erreur son ennemi. On y retrouve évidemment les ruses, les leurres, les déformations de la réalité et les falsifications.

La supercherie est donc là, présente au cœur de chaque combat, de chaque assaut, de chaque victoire. Celui qui en maîtrisera l'art sortira vainqueur de sa bataille.

Mais revenons au sujet qui nous occupe.

L'ingénierie sociale.

Définir l'ingénierie sociale est une tâche ardue, car elle peut prendre un certain nombre de formes en fonction du contexte de son utilisation.

Nous pourrions simplifier les contextes en quatre grands ensembles : les sciences sociales, les sciences politiques, la sécurité de l'information et la psychologie.

Si dans les deux premiers, la définition de l'ingénierie sociale peut sembler une pratique saine (et encore, nous pourrions en débattre j'en suis sûre), les deux derniers cadres d'utilisation de l'IS relèvent plutôt de la manipulation psychologique individuelle à des fins malveillantes.

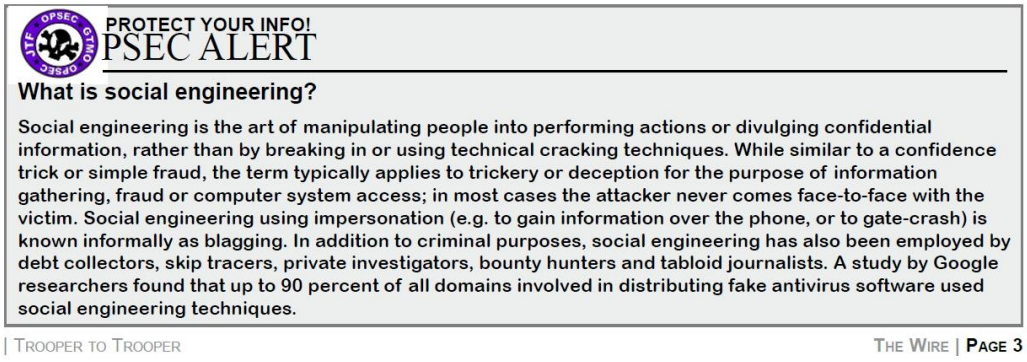
Concentrons-nous sur le domaine de la sécurité de l'information.

Dans le contexte de la cybersécurité, l'ingénierie sociale revêt une forme particulière. En effet, même si sa base première reste identique dans chaque contexte (pratique de manipulation), l'ingénierie sociale en cybersécurité est une forme de manipulation psychologique, plus ou moins élaborée, plus ou moins lente, dont la seule finalité est de contrôler ou influencer la pensée, les choix, les actions d'un individu, via un rapport de pouvoir ou d'influence, afin de mettre en place une arnaque, une usurpation ou tout autre forme d'escroquerie.

(Illustration de César Leal Jiménez sur « le lavage de cerveau »)

L'ingénierie sociale et la sécurité de l'information

ou l'art d'obtenir une information importante pour l'utiliser à des fins malveillantes mais relutives.



PROTECT YOUR INFO!

PSEC ALERT

What is social engineering?

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases the attacker never comes face-to-face with the victim. Social engineering using impersonation (e.g. to gain information over the phone, or to gate-crash) is known informally as blagging. In addition to criminal purposes, social engineering has also been employed by debt collectors, skip tracers, private investigators, bounty hunters and tabloid journalists. A study by Google researchers found that up to 90 percent of all domains involved in distributing fake antivirus software used social engineering techniques.

| TROOPER TO TROOPER THE WIRE | PAGE 3

Une définition posée, en 2011, par un employé des forces armées ou du département de la Défense des États-Unis.

Dans le contexte IT, les attaques par ingénierie sociale sont devenues légions et certaines d'entre elles sont si sophistiquées qu'il est particulièrement compliqué de les détecter simplement. En exploitant les faiblesses d'un individu ou d'une organisation, l'attaquant a un but précis : récupérer un bien, un service, un virement bancaire, un accès physique ou informatique, une information confidentielle, etc.

Et la méthode utilisée, appelée processus « d'élicitation », est toujours la même : fausser la perception de la réalité de sa victime en usant notamment d'un rapport de séduction, de suggestion, de persuasion, de soumission.

[1] TZU Sun, l'art de la guerre - Coll Mille et une nuits - 1996

Un petit retour en arrière

C'est en 2002 que le monde a pu enfin comprendre ce qu'était une attaque par ingénierie sociale. En effet, cette année-là, Kevin Mitnick, le plus célèbre des arnaqueurs par IS, et sans doute fils spirituel de Sun Tzu, publiait son fameux « Art de la supercherie ».

Kevin Mitnick[2] a été l'un des « ennemis publics » les plus recherchés par le FBI parce qu'il avait piraté près de 40 grandes entreprises rien que pour relever des défis.

De grands noms comme Nokia, Fujitsu, NEC, Novell, Sun Microsystems, Motorola, Apple ont compté comme étant ses victimes.

En 1980, Kevin Mitnick pénètre physiquement dans le central téléphonique COSMOS qui servait de base de données pour archiver les appels téléphoniques, ainsi que la facturation de la Pacific Bell à Los Angeles. Le pirate de génie se procura une liste des mots de passe des utilisateurs, les combinaisons de fermeture des portes des bureaux centraux de Pacific Bell, etc.

En 1983, Kevin Mitnick fait une intrusion dans le réseau du Pentagone en se servant d'une machine de l'Université de Californie du Sud. Il parviendra à se connecter à l'ARPAnet, l'ancêtre d'Internet, et obtiendra un accès illégal à tous les fichiers du département de la Défense américaine !

Et tout ça, sans violence…

Ses méthodes : utiliser la terminologie de l'entreprise ciblée, trouver les bons contacts, usurper la bonne personne pour réussir son attaque, utiliser la crédulité de sa victime en prétextant un problème ou la résolution d'un problème.

Plus proche de nous

Entre 2005 et 2006, un certain Gilbert Chikli [3]réussira à récupérer près de 60 millions d'euros auprès d'employés de 33 sociétés françaises !

Chikli est l'inventeur de la juteuse escroquerie aux faux ordres de virements (FOVI) aussi appelée « L'arnaque au Président ».

Sur un simple coup de fil, il parvient à « isoler » psychologiquement son interlocuteur avant de le manipuler à sa guise en se faisant passer pour le PDG de groupes ciblés et avant de leur ordonner le virement d'importantes sommes vers des comptes bancaires à l'étranger.

Cette technique est d'ailleurs toujours en vigueur en 2019 !

Et non content d'avoir réussi ce coup de maître, Chikli est suspecté d'avoir mis sur pied une arnaque encore plus osée, l'escroquerie dite du « faux Le Drian » !

En effet, il est suspecté de s'être glissé dans la peau de l'ancien ministre de la Défense pour récupérer d'importantes sommes d'argent auprès de richissimes contacts (particuliers, hommes politiques, représentants religieux, grands chefs d'entreprise). Son argumentaire rodé s'appuyait sur des faits qui secouaient alors le monde : les rançons réclamées par le groupe État islamique en échange de la libération de soldats ou de journalistes français…

Les arnaques au Président, les attaques FOVI, aux faux fournisseurs, au faux changement de RIB, ou aux faux supports techniques se sont généralisées depuis 10 ans. On estime d'ailleurs aujourd'hui qu'elles coûtent plus de 6 milliards de dollars par an aux victimes !

Ces deux grands génies de l'arnaque ont joué de leurs connaissances, de leur charisme, de leur sens de l'imposture et bien sûr de leur culot pour abuser de la confiance, de l'ignorance et de la crédulité de leurs cibles et ainsi obtenir ce qu'ils cherchaient.

Mais alors pourquoi ça fonctionne ?

Comme je l'ai dit précédemment, pour atteindre son objectif, le pirate va utiliser différentes méthodes, techniques et psychologiques.

Partant du constat que les êtres humains ne sont pas toujours rationnels et qu'ils prennent parfois les mauvaises décisions et selon un schéma que l'on ne comprend pas toujours, le pirate va manipuler la pensée, le mode de décision de son interlocuteur afin d'obtenir les premières informations, qui lui serviront pour ses futures attaques. L'ingénierie sociale sera une de ses premières armes. Les cyber-attaquants exploitent les facteurs de comportement sociaux, émotionnels et psychologiques pour influencer et manipuler.

90% DES CYBERATTAQUES DÉBUTENT PAR UN LEURRE NUMÉRIQUE ADRESSÉ À UN HUMAIN.

Et c'est en faisant ce constat que l'on comprend que toutes les techniques d'ingénierie sociale sont basées sur un point commun : les biais cognitifs qui permettent à une personne de prendre une décision. Une attaque par les biais cognitifs consiste donc à « dévier la pensée logique et rationnelle » de sa victime pour obtenir d'elle ce que l'on souhaite. Et bien sûr, le choix des leviers doit être adapté à la situation et à la cible.

[2] Mitnick, l'art de la supercherie - Coll CampusPress - 2005

[3]SELLAMI Stéphane et LEPLONGEON Marc, Faux Le Drian : une arnaque spectaculaire - Le Point, Avril - 2018, https://www.lepoint.fr/faits-divers/exclusif-l-escroc-gilbert-chikli-futur-repenti-23-04-2018-2212668_2627.php

Selon les travaux de Wason et Evan, mis en exergue par Kahneman et Tversky[4] , la cognition humaine repose sur deux grands ensembles de processus cognitifs :

- Les processus du système 1, rapides et automatiques, qui comprennent les processus débouchant sur une pensée intuitive.
- Les processus du système 2, lents et contrôlés, qui regroupent les processus cognitifs amenant à une pensée analytique.

On parle alors de Biais Heuristique : les informations qui sont répétées et auxquelles nous adhérons fortement deviennent des réponses intuitives.

Et de biais analytique, par lequel nous essaierons de justifier nos réponses en cherchant d'autres données qui confortent nos croyances tandis que les informations contradictoires seront écartées ou interprétées dans le sens de nos croyances.

Et évidemment, c'est en abusant du biais heuristique que les meilleures attaques par ingénierie sociale fonctionnent.

Quelques exemples de biais

Tous les sentiments peuvent être utilisés comme leviers d'influence. Le choix des biais employés par le pirate va être mûrement réfléchi et devra s'adapter à la situation et à la victime.

Pour cela, il prendra le temps nécessaire à la récolte d'informations sur le web, à défaut ou en complément il tentera la manipulation téléphonique (extorsion d'information), par mail, sur les réseaux sociaux et peut même être amené à user de manipulation directe (accès physique à des installations).

Plus le pirate sera spontané, naturel, entrainé, plus facile il obtiendra les informations. Souvenez-vous de Mitnick ou de Chikli… Ils sont les exemples même des « parfaits » manipulateurs.

La plupart du temps les manipulateurs n'ont pas besoin de connaitre les quelques 250 biais référencés aujourd'hui. Ils n'en utilisent que quelques-uns. Et les maîtrisent à la perfection.

Voici les plus récurrents auxquels vous avez peut-être été déjà vous-même confronté(e) :

- **« Laissez-moi vous aider », l'effet Benjamin Franklin** ou le principe de réciprocité. (Ce biais cognitif a été étudié notamment par Robert Cialdini[5]) Chacun de nous se sent obligé de rembourser ou rendre ce qu'ils ont reçu des autres. Le pirate va tout faire pour vous rendre un service et vous demandera, un jour, de lui rendre en retour un service.

- **Le principe de contraste (dans le milieu de la vente on parle de 'porte dans le nez') :** Le pirate va donc ouvrir une conversation en demandant quelque chose d'extrême. Alors que la victime répondra forcément « non », elle «se retirera» pour une seconde demande plus «raisonnable».
  En demandant quelque chose de peu contraignant dans un second temps, la personne aura l'impression que cette nouvelle demande n'est pas si difficile à accorder, comparativement à la demande initiale et le fait qu'elle ait refusé lui donnera un sentiment de devoir accepter la deuxième demande, et aura l'impression de se 'racheter'.

- **« Instaurer la confiance »** : Le manipulateur anticipe la suspicion et la résistance. Il transforme la méfiance en confiance. Il prévoit les futures questions de sa victime. Pour ne jamais être pris au dépourvu, le manipulateur va tout préparer en avance de phase pour ainsi conforter sa victime dans le fait que tout est bien sous contrôle. L'attaquant exploite ici le principe de l'appropriation : les gens sont plus susceptibles de se conformer aux demandes de ceux qu'ils aiment, apprécient, croient bien connaître.

- **Suggérer indirectement,** Quand une idée vient de soi, on est beaucoup plus disposé à réaliser ce qu'on nous a demandé. Le pirate suggère à sa future victime de l'aider, sans le dire expressément, ainsi la victime va fort probablement penser que l'initiative vient d'elle, et donc elle acceptera de rendre service.

- **« La culpabilité, la compassion, l'intimidation »** : La serviabilité constitue un réel point faible qu'un manipulateur exploitera très souvent. En utilisant, par exemple, le principe de l'autorité, les gens suivent d'autres qui semblent savoir ce qu'ils font (courriels de phishing pour donner l'impression qu'ils ont été envoyés par des organismes faisant autorité).

On le comprend aisément, cette réalité de l'exploitation des biais cognitifs met l'humain au centre de la chaine de sécurité et l'identifie clairement comme le maillon le plus faible.

Et l'émergence et la démocratisation de l'intelligence artificielle renforce encore la menace en offrant aux attaquants des possibilités de création de leurres plus complexes, immersifs et cohérents.

Et enfin, comment ça peut fonctionner ?

C'est effectivement la question légitime que l'on peut se poser : comment peut-on encore aujourd'hui céder à ce genre d'attaques ?

---

[4] KAHNEMAN Daniel, Système 1 / Système 2 - Les Deux Vitesses De La Pensée - Coll Flammarion - 2012

[5] CIALDINI Robert, Influence et manipulation : Comprendre et maîtriser les mécanismes et les techniques de persuasion - Coll First Edition - 2004

On a vu que la manipulation psychologique était le moyen, mais avec quel support ?

Si l'accès physique à la victime n'est pas toujours possible, l'accès virtuel lui l'est quasiment toujours.

Il va donc falloir utiliser des techniques plus ou moins avancées pour porter et supporter l'attaque psychologique et l'utilisation des biais cognitifs.

Il existe un grand nombre de techniques, mais je vais me focaliser sur une en particulier, sans doute la plus connue et la plus répandue, encore de nos jours.

Le phishing et ses variantes.

Commençons par définir ce qu'est le « phishing » techniquement :

« Phishing = fishing + phreaking », c'est-à-dire « Pêche + Piratage de lignes téléphoniques ».

Plus globalement, le phishing (ou hameçonnage) est une forme d'escroquerie, par email ou par téléphone, qui consiste à prendre l'identité d'une personne ou d'une entreprise connue et/ou reconnue pour inciter le ou les destinataires à fournir des informations susceptibles de rapporter de l'argent ou de fournir des informations dites confidentielles.

Si l'on fait un état des attaques par phishing sur l'année 2018, le bilan est alarmant.[6]

Sur près de 300 milliards de mails échangés par jour, près de 65% sont des spams, soit environ 195 milliards… et plus de 500 millions de ces spams sont des emails de phishing !

Aujourd'hui, on considère que près de 150 millions de personnes répondent quotidiennement à des emails de phishing, et que 80% des entreprises dans le monde sont touchées. Montant total de la perte estimée… 12 milliards de dollars (près de 11 milliards d'euros).[7]

Ces chiffres donnent le vertige !

Et il existe quelques variantes à cette technique, qui permettent aux attaquants de diversifier le support d'attaque, et donc d'augmenter sa surface.

Si le phishing permet d'adresser un grand nombre de destinataires avec peu de personnalisation, il est nécessaire parfois pour les attaquants d'aller plus loin et de donner plus de crédibilité à leur arnaque. Il s'agit alors d'attaque par « Spear Phishing », appelée aussi harponnage. L'attaque est ciblée, personnalisée, et souvent quasi invisible.

On pourra également citer SMISHING (SMS Phishing), le VISHING (Voice Phishing) et une technique qui fonctionne également très bien, le Hard Phishing (appelée aussi USB Drop).

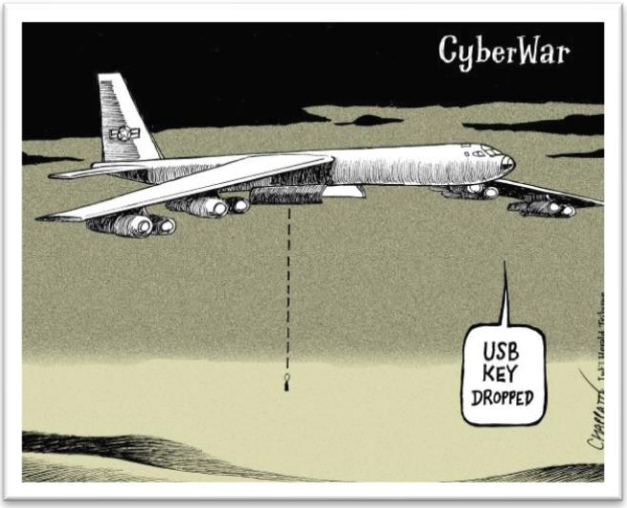


Illustration de Patrick Chappatte, dans « International Herald Tribune »

Comment reconnaître une tentative de phishing ?

Un des exemples les plus connus est le courrier électronique qui vous invite à vous connecter à un site de banque, un site commercial ou un site de paiement comme Paypal.

Le prétexte utilisé est souvent le même : on vous demande, pour des raisons de sécurité, de mettre à jour vos données personnelles, de changer votre code confidentiel ou bien de régulariser une facture impayée.

Dans cet email, il y aura toujours un lien qui conduira à un site pirate, copie visuellement quasi parfaite, afin de récupérer vos données confidentielles.

---

[6] Rapport Verizon "Databreach Investigation" - 2019

[7] The Evolution of Cyber Threat Intelligence (CTI): SANS CTI Survey 2019

Comment réagir face au phishing ?

Ne répondez jamais à ce type de courrier et prévenez le site usurpé au plus vite en lui faisant suivre ce message.

Ne cliquez jamais sur les liens des messages qui vous semblent suspects. Ne récupérez ou visionnez jamais les pièces jointes des courriers étranges.

Assurez-vous lors des sessions Internet de la sécurité et de l'authenticité du site sur lequel vous êtes, en repérant par exemple, le cadenas vert sur la barre de navigation.

Tapez vous-même l'adresse des sites institutionnels (impôts, assurance maladie, CAF, etc…) et des sites les plus importants (banque, fournisseurs d'énergie, sites de paiements…).

Faites aussi attention aux messages vous incitant à appeler votre banque : prenez le temps de vérifier le numéro de téléphone.

Signalez les tentatives d'escroquerie sur le site Internet d'assistance aux victimes d'actes de cybermalveillance (https://www.cybermalveillance.gouv.fr/).

Et quoi qu'il arrive, soyez toujours vigilants.

Pour finir

L'humain étant le maillon le plus faible de toute la chaîne de sécurité, l'ingénierie sociale a encore aujourd'hui de grandes et belles années à vivre.

Et puis comme je l'ai dit un peu plus tôt, l'arrivée de l'intelligence artificielle permet de créer des leurres numériques de plus en plus avancés, réalistes et crédibles. L'environnement numérique dans lequel chacun de nous se trouve est de plus en plus hostile, et il devient particulièrement compliqué de faire le bon choix.

Les données personnelles sont le Graal de chaque pirate informatique, et ce bien plus que des plans d'avions. Un numéro de carte vitale et une identité complète valent bien plus que plusieurs milliers de numéro de cartes bancaires.

L'enjeu individuel est désormais de savoir déceler le faux pour protéger le vrai et il devient urgent de changer le paradigme : agir pour ne plus subir.

- - - - - -

Biographie

Férue de psychologie et de sciences humaines et sociales depuis mon adolescence, j'en ai fait ma spécialité. Diplômée de l'Université de Bordeaux, je suis devenue psychologue en 2004, avec une spécialisation sur les interactions au sein des groupes, le comportementalisme, sur la cognition et ses biais, et évidemment sur la manipulation mentale. Cependant, consciente qu'il manquait une corde à mon arc, j'ai complété mes connaissances, par une formation et un diplôme en Ressources Humaines. J'ai exercé mes métiers dans des structures variées, tant dans leurs natures (cabinets spécialisés, PME, ou grandes ESN françaises), que dans leurs tailles (de 20 à plus de 70 000 salariés) ou leurs domaines (aéronautique, spatial, pétrochimie, finance, océanographie, informatique, cybersécurité).

Ce parcours très diversifié m'a menée un jour à intégrer une grande équipe de cybersécurité au sein d'une ESN française. On m'a confié deux grandes tâches : celle de piloter le delivery des activités SOC pour 4 grands clients français, et celle de développer une partie de l'activité de Threat Intelligence avec un focus sur l'aspect psychologique.

Au sein de la cellule de renseignement à laquelle j'appartiens, j'interviens en tant que cyber-psychologue et travaille sur le profiling des cyber-attaquants. Je surveille les acteurs et les groupes malveillants, j'en détermine les signatures comportementales, les relations humaines. J'essaie de mettre en lumière leurs profils en liant tactiques, techniques et procédures. J'interviens également sur les attaques par ingénierie sociale, avec un focus fort sur les manipulations psychologiques mises en œuvre.

- - - - - -

Références

- TZU Sun, l'art de la guerre - Coll Mille et une nuits - 1996
- Mitnick, l'art de la supercherie - Coll CampusPress - 2005
- SELLAMI Stéphane et LEPLONGEON Marc, Faux Le Drian : une arnaque spectaculaire - Le Point, Avril 2018, https://www.lepoint.fr/faits-divers/exclusif-l-escroc-gilbert-chikli-futur-repenti-23-04-2018-2212668_2627.php
- KAHNEMAN Daniel, Système 1 / Système 2 - Les Deux Vitesses De La Pensée - Coll Flammarion - 2012
- CIALDINI Robert, Influence et manipulation : Comprendre et maîtriser les mécanismes et les techniques de persuasion - Coll First Editions 2004
- Rapport Verizon "Databreach Investigation" - 2019
- The Evolution of Cyber Threat Intelligence (CTI): SANS CTI Survey 2019