JE SAIS QUI VOUS ÊTES

LE MANUEL D'ESPIONNAGE SUR INTERNET

CHARLES COHLE
AVEC L'INSTITUT PANDORE

JE SAIS QUI VOUS ÊTES

Le manuel d'espionnage sur Internet

Par Charles Cohle
jesaisquivousetes.com

Édité par l'Institut Pandore

Correction par Sophie Loir (sophie@institut-pandore.com)

ISBN : 978-2-9539663-5-0 (numérique)

Sommaire

Note au lecteur

Tout au long de votre lecture, vous serez amené(e) à visiter divers sites Internet par l'intermédiaire de petits blocs semblables à celui-ci :

> *Titre du site*
> *www.adresse-du-site.com*

Vous serez entre autres invité(e) à vous rendre sur le blog officiel du livre (jesaisquivousetes.com). Ne voyez rien de commercial dans cette démarche : beaucoup d'explications techniques ont été déportées sur le blog pour ne pas surcharger le livre inutilement.

De plus, certaines explications liées à des outils informatiques devront être mises à jour régulièrement afin de rester valables. Les figer sur le papier aurait rapidement rendu le livre caduc.

Pour vous faciliter la vie, les liens Internet ont été raccourcis au maximum pour vous permettre de les recopier très facilement si vous lisez la version papier ou liseuse.

Certains liens pourront pointer vers des pages d'erreur ou des sites web qui n'existent plus. Ne prenez pas cela pour de la publicité mensongère : un site présenté dans ce livre a pu fermer ses portes entre temps. Utilisez toujours les liens présentés dans les encarts pour accéder aux sites recommandés, car ces liens peuvent être corrigés à distance par l'auteur. De plus, n'hésitez pas à contacter Charles Cohle

par e-mail pour lui signaler un lien mort. Il aura à cœur de faire tout son possible pour corriger le problème.

Pour finir, l'achat de ce livre vous offre un accès gratuit et entier à de nombreux services web que l'auteur vous présentera au fur et à mesure de ses explications. C'est votre numéro de commande qui vous servira d'identifiant.

Avant-propos

À l'heure où j'écris ces lignes, une personne sur sept dans le monde possède un compte Facebook.

Le web est devenu un gigantesque annuaire que chacun s'obstine à mettre à jour en y publiant ses photos, ses humeurs et ses opinions politiques.

Pourtant les internautes en général – vous et moi y compris – savent comme il est important de protéger leur vie privée sur Internet.

Malheureusement, la confidentialité sur le web c'est comme l'écologie : tout le monde sait que c'est important, tout le monde y pense, mais personne ne fait vraiment d'efforts.

Je me suis longtemps demandé pourquoi les gens, aussi bien informés soient-ils, se fichaient complètement de leur vie privée. J'ai fini par comprendre.

Premièrement, une grande partie des internautes se croit protégée. C'est peut-être votre cas : vous avez bidouillé quelques réglages de confidentialité sur Facebook et vous pensez que vos photos personnelles sont en lieu sûr.

Deuxièmement, la majorité des internautes ne se doutent absolument pas des dégâts que peuvent provoquer quelques informations personnelles dispersées sur la toile.

Enfin la « protection de la vie privée » est un sujet moralisateur vu, revu et archi-revu. Oui, on sait, c'est important… mais laissez-nous vivre un peu ! On atteint l'overdose, tout le monde

nous dit de faire attention mais personne ne nous dit ni comment, ni pourquoi.

Ce livre aborde la question de la vie privée sur Internet d'une manière ouvertement provocatrice. Je le résumerais en citant Napoléon : « la meilleure défense, c'est l'attaque ».

Au lieu de vous rabâcher une énième fois les bonnes pratiques de confidentialité sur Internet, j'ai pris le parti de vous expliquer comment exploiter la négligence généralisée des gens qui utilisent Internet.

Vous apprendrez à exploiter des failles techniques mais aussi – et surtout – des failles humaines dans l'objectif de pister et d'espionner vos cibles de la même manière qu'un détective privé professionnel. Tout cela vous servira, je l'espère, à prendre conscience qu'aucune information n'est jamais en lieu sûr à partir du moment où elle est publiée sur Internet.

Dans la dernière partie du livre, je passerai en détails les moyens les plus efficaces pour vous protéger de toutes les techniques offensives que vous aurez appris durant votre lecture.

J'ai conscience que certaines techniques expliquées par la suite peuvent choquer les âmes un peu trop sensibles. C'est assumé.

Nous sommes aujourd'hui en 2014 et il ne sert plus à rien de rappeler qu'Internet est un lieu « dangereux ». Bien sûr qu'il l'est, puisque qu'il est occupé par l'Homme (et aussi par les chats, mais c'est une autre histoire).

Permettez-moi une parenthèse. Avez-vous déjà vécu la douloureuse expérience du « crash de disque dur » ? Vous allumez votre ordinateur un beau matin et surprise ! il ne

démarre plus. Vous venez de perdre (entre autres) toutes vos photos de vacances de ces six dernières années en quelques secondes.

Avant que cela ne vous arrive pour de vrai, le principe de sauvegardes informatiques vous semblait totalement inutile. « Prendre 10 minutes par semaine pour faire des sauvegardes sur clef USB ? Non merci, c'est pas la peine. »

La vie privée sur Internet fonctionne exactement de la même manière : le jour où un patron, un associé, un membre de votre famille ou un individu mal attentionné découvriront quelque chose de compromettant à votre propos, vous vous en mordrez les doigts. « Ho purée, j'aurais dû faire plus attention…. ».

Ce « quelque chose de compromettant » vous semble sûrement très abstrait. Vous découvrirez tout au long du livre de quoi il peut s'agir, et pourquoi cela vous concerne directement.

J'espère sincèrement que ce livre agira comme un électrochoc, vous évitant des situations embarrassantes.

Je termine avec un *disclaimer* : chacun a ses raisons lorsqu'il s'agit de pister ou d'espionner, il n'est pas question de vous juger. Bien souvent, nos intentions sont bénignes, futiles et sans conséquences. Malgré cela, vous serez tenu seul responsable de vos actes si vous décidez d'utiliser certaines méthodes de ce livre pour nuire à quiconque.

Bonne lecture.

Introduction

Hot-reading, *profiling*, *social-engineering* et *doxing*, ça vous dit quelque chose ? Je m'excuse auprès des anglophobes mais ces trois mots reviendront régulièrement. J'ai choisi de ne pas les traduire pour deux raisons. D'abord parce que les traductions françaises sont assez lourdes mais aussi et surtout parce que ces mots sont chargés des sens.

Le *hot-reading* (littéralement « lecture à chaud ») ou « profiling » consiste à déterminer le profil psychologique et émotionnel d'un individu sans jamais lui parler directement. Il s'agit donc d'exploiter toutes les informations que l'on trouvera au sujet d'une personne pour nous permettre de tracer son portrait.

Le *social-engineering* (« ingénierie sociale ») est un concept qui nous vient du monde du *hacking*, plus précisément du piratage informatique. Une grande partie des attaques informatiques reposent essentiellement sur l'exploitation de failles humaines : c'est ce qu'on appelle le *social-engineering*. On pourrait aussi parler de manipulation sociale.

Je vous invite à découvrir l'article du blog à ce propos. J'y explique trois attaques informatiques très impressionnantes qui se sont basées sur du *social-engineering* bien avant d'exploiter des failles informatiques.

> *3 attaques de social-engineering auxquelles vous n'auriez jamais pensé*
> *www.pandore.it/ase*

Enfin, le *doxing* (abréviation de « document tracing ») consiste à pister une personne sur Internet grâce aux traces qu'elle y laisse. Vous apprendrez entre autres à géolocaliser précisément une personne avec qui vous parlez sur Internet, à trouver l'appareil qu'elle utilise pour se connecter, à deviner ses heures de connexion, ses occupations, peut-être son métier, etc.

À ceux qui doutent encore de l'éthique et l'intérêt de ce livre – chose que je peux tout à fait comprendre à ce stade – j'aimerais présenter quelques situations du quotidien dans lesquelles il est important, voire primordial, de posséder des notions de cyber-espionnage. Je suis sûr que vous avez déjà vécu au moins l'une de ces situations.

- **Par curiosité mal placée :** vous voulez voir à quoi ressemble la vie d'un ancien proche mais vous n'avez pas envie de reprendre contact avec lui pour autant ;
- **Pour vous protéger :** un inconnu vous parle, vous menace ou vous agresse sur Internet, mais il ou elle se cache derrière un pseudonyme ;
- **Par besoin professionnel :** vous allez participer à un séminaire ou vous présenter à un entretien d'embauche et vous aimeriez en savoir plus sur les personnes que vous rencontrerez sur place. D'une part pour briller, d'autre part pour être plus confiant ;
- **Par besoin personnel :** vous allez rencontrer pour la première fois une personne avec qui vous avez pris contact sur un site de rencontre. Vous avez envie d'en savoir plus sur elle ou lui pour savoir de quoi discuter le jour J.

- **Par habitude :** vous fréquentez beaucoup de communautés Internet et vous avez besoin de savoir à qui vous parlez lorsque vous faites une rencontre virtuelle ;

Tout au long de ce livre, je m'efforcerai de vous proposer des situations du quotidien dans lesquelles vos nouvelles connaissances en *doxing* pourront être mises à l'épreuve.

Il est malheureusement très compliqué d'inventer de toutes pièces des exemples qui tiennent la route et qui correspondent à chaque lecteur. De ce fait, vous devrez absolument vous détacher de ces mises en situations, sans quoi le livre perdra tout son intérêt. Retenez les techniques de base, les astuces et les concepts mais ne retenez pas les situations en elles-mêmes.

Vous êtes prêt(e) à commencer ? Allons-y ! Dans cette première partie du livre, vous allez découvrir l'outil classique et indispensable du *doxing* : le *tracking link*.

Le *Tracking Link*, l'outil indispensable du *doxing*

1. Introduction

Le *Tracking Link* (« lien de traçage » en français) est un outil que j'ai commencé à utiliser il y a une dizaine d'années.

Le principe est simple. Il s'agit d'une page web qui enregistre l'identité de chacun de ses visiteurs. À partir du moment où quelqu'un consulte cette page, ses informations de connexion sont instantanément envoyées par e-mail au propriétaire de la page. Nous verrons un peu plus tard en quoi consistent ces fameuses informations de connexion.

Cette page « espionne » peut prendre l'apparence de n'importe quelle autre page web sans problème : un article du *Monde*, la page d'accueil du site de la Maison Blanche, etc. Ainsi, elle n'éveille absolument pas les soupçons des internautes.

I) À quoi ça sert ?

C'est une bonne question. Les informations que permet de récupérer le *tracking link* concernant un internaute sont assez techniques : il s'agit de l'adresse IP et de l'*user-agent*. À ce stade de votre lecture, vous ne savez peut-être même pas de quoi il s'agit. Pas de panique, nous le découvrirons ensemble un peu plus loin.

Concrètement, le *tracking link* permet de pister un internaute. En l'incitant à visiter votre (future) page web truquée, vous

obtiendrez immédiatement sa position géographique, l'appareil qu'il utilise pour se connecter à Internet, l'heure à laquelle il a cliqué sur votre lien, et d'autres informations plus approximatives que nous apprendrons à extraire par la suite.

Voici quelques situations de la vie quotidienne où l'utilisation du *tracking link* vous sera très utile :

- Vous parlez à un(e) inconnu(e) sur Internet (un vendeur sur Leboncoin, une fille ou un garçon rencontrée sur un tchat ou un forum) mais vous avez un doute sur son honnêteté. Vous pourrez utiliser le *tracking link* pour confirmer sa position géographique à son insu ;
- Vous pensez qu'un interlocuteur vous évite : vos e-mails et coups de téléphone restent tous sans réponse. Vous pourrez utiliser un *tracking link* pour savoir si cet interlocuteur lit vos messages ou non ;
- Vous pensez qu'une personne se fait passer pour un(e) autre. Exemple classique : un faux profil vous ajoute sur Facebook. Vous pourrez démasquer son créateur grâce à votre *tracking link* ;

2. Comment ça fonctionne ?

Tout se passe sur le site officiel du livre, à cette adresse :

Accéder au Tracking Link Creator
www.pandore.it/atlc

Le Créateur de *Tracking Link* est une petite application en ligne très simple d'utilisation qui vous permet de créer votre propre page espionne en quelques clics.

Connectez-vous sur le site puis complétez les étapes obligatoires. Vous obtiendrez alors l'adresse de votre propre page espionne. Quiconque accédera à cette page vous enverra, sans le savoir, toutes ses informations de connexion. Un schéma et des explications détaillées sont disponibles sur la page du *Creator*.

Ce système n'est ni illégal, ni dangereux. Il ne s'agit absolument pas d'un virus. À moins de remonter jusqu'à ce livre, il est impossible pour quiconque de deviner le fonctionnement de votre page espionne.

Votre seul travail dans tout cela : créer une page espionne grâce au Créateur de *Tracking Link* et inciter votre cible à se rendre dessus, pour une raison ou pour une autre.

Quelles informations allez-vous récupérer ?

Je vais être très clair : vous n'aurez pas accès à son nom, son numéro de téléphone ou son adresse e-mail. Au lieu de cela, vous aurez principalement accès à deux informations :

1. **Son adresse IP :** il s'agit d'une suite de chiffres qui permet d'identifier un ordinateur connecté à Internet. *Exemple d'une adresse IP : « 78.144.251.62 »*

2. **Le *user-agent* de son navigateur :** il s'agit d'une sorte de séquence – un peu incompréhensible pour le commun des mortels – qui identifie le navigateur et le système d'exploitation d'un internaute.

Exemple d'un user-agent : « Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36 »

Vous vous demandez peut-être à quoi tout cela rime. Que faire d'une adresse IP ? Que faire d'un *user-agent* ? Attachez vos ceintures : nous allons apprendre à transformer ces données brutes et compliquées en de précieuses informations.

3. Apprendre à exploiter l'adresse IP

L'adresse IP permet d'identifier une connexion internet. Si deux internautes ont la même adresse IP, alors cela veut généralement dire qu'ils se connectent à partir du même endroit. J'insiste sur « généralement » car il y a des exceptions bien particulières que je ne vais pas détailler ici. Si vous utilisez une box Internet chez vous, alors toutes les personnes de votre foyer qui se connectent à cette même *box* partagent la même adresse IP et seront reconnues comme étant la même personne sur Internet.

Vous venez d'apprendre votre première notion de *doxing* : en obtenant l'adresse IP de deux internautes et en les comparant, vous pourrez savoir s'il s'agit de la même personne.

Allons plus loin.

Une adresse IP permet de géolocaliser une cible de manière tout à fait précise. À partir d'une adresse IP, vous trouverez sans aucune difficulté le pays de connexion d'un internaute. Dans l'immense majorité des cas, vous pourrez même

connaître la ville depuis laquelle il se connecte (ou au moins la ville la plus proche).

Il existe des milliers de services Internet gratuits qui permettent de transformer une adresse IP en coordonnées géographiques. Vous trouverez une liste complète sur le blog du livre :

> *Comment localiser une adresse IP*
> *et comment ça marche ?*
> *www.pandore.it/ageo*

Allez sur n'importe lequel de ces sites web, recopiez bêtement l'adresse IP de votre victime dans la case prévue à cet effet puis validez. Vous obtiendrez immédiatement une carte avec sa position précise et d'autres informations à son sujet (son fournisseur d'accès Internet, entre autres).

La géolocalisation indique un pays bizarre, par exemple en Asie. Pourquoi ?

Certains internautes utilisent un proxy. Nous aborderons ce point en détails dans le dernier chapitre du livre. En quelques mots, il s'agit d'une technique de camouflage. Si votre cible utilise un proxy, vous aurez peu de chance de pouvoir connaître sa véritable adresse IP et donc sa véritable localisation géographique.

Pour savoir si l'adresse IP que vous avez récupérée est celle d'un proxy ou non, je vous recommande d'utiliser ce site web :

Is a proxy or not ?
www.pandore.it/apon

Le lien vers ProxyOrNot.com est déjà donné dans l'e-mail que vous recevrez contenant les informations de votre cible, suite à sa visite sur votre page espionne.

La géolocalisation m'indique souvent Paris, pourtant je suis sûr que ma cible n'y est pas. Pourquoi ?

Aujourd'hui, beaucoup de gens utilisent leur téléphone pour surfer sur le web. De ce fait, ils sont connectés par l'intermédiaire du réseau 3G ou 4G de leur opérateur. L'adresse IP qui les identifie lorsqu'ils utilisent le réseau Internet de leur opérateur mobile est partagée par des milliers d'autres utilisateurs. C'est l'une des spécificités des réseaux Internet mobiles : les adresses IP des utilisateurs 3G/4G ne sont pas aussi personnelles que les adresses IP de nos box Internet (celles que l'on utilise dans nos salons).

Cette différence est importante en *doxing* : si votre cible utilise son téléphone portable connecté en 3G/4G pour consulter votre page espionne, vous aurez une adresse IP biaisée et sans intérêt, qui pointera très probablement sur Paris (nœud des réseaux).

Pour résumer, l'adresse IP d'un utilisateur dépend du point d'accès Internet qu'il utilise :

- Si son point d'accès est sa box (Freebox, SFR Box, Bbox, etc.) » : l'adresse IP de l'utilisateur est personnelle et géolocalisable ;

- Si son point d'accès est un réseau 3G/4G : l'adresse IP de l'utilisateur n'est pas personnelle et n'a aucun intérêt pour nous (à part nous indiquer l'opérateur téléphonique de la cible).

C'est tordu, n'est-ce pas ? Mais rassurez-vous, l'analyse de l'adresse IP n'a pratiquement plus de secrets pour vous. Le *tracking link* est un outil puissant : en seulement quelques clics, vous êtes désormais capable d'en savoir beaucoup plus sur un internaute.

Allons encore plus loin.

4. Apprendre à exploiter un user-agent (UA)

L'*user-agent* (abrégé UA) offre lui aussi des informations très intéressantes, en l'occurrence le système d'exploitation utilisé par votre cible (Windows, OS/X, GNU/Linux, etc.) et la version de son navigateur web (Firefox, Chrome, Internet Explorer, etc.).

Pour rappel, voilà à quoi peut ressembler un *user-agent* :

> « Mozilla/5.0 (Windows NT 6.1)
> AppleWebKit/537.36 (KHTML, like Gecko)
> Chrome/27.0.1453.110 Safari/537.36 »

Tout comme l'adresse IP, ce machin compliqué plein de mots anglais peut sembler inutile à première vue. Et pourtant ! Voici deux manières de l'exploiter intelligemment.

Premièrement, vous pouvez utiliser l'*user-agent* pour tracer un internaute grâce à la machine qu'il utilise. En récupérant l'UA

de votre amie Alice par exemple, vous saurez si elle utilise à l'instant T son iPhone, son PC domestique ou encore sa tablette. Couplé avec la géolocalisation de l'adresse IP, il est possible de savoir si elle est partie en vacances, au travail ou chez elle.

Il existe une autre manière d'exploiter l'*user-agent*, plus originale encore : il s'agit d'utiliser des études statistiques et des stéréotypes.

Rappelez-vous : l'UA vous permet de connaître le système d'exploitation de votre cible (Windows, OS/X, etc.) mais aussi de connaître son navigateur Web (Firefox, Chrome, Internet Explorer, etc.).

Aujourd'hui, avoir un Mac ou un PC n'est plus complètement anodin. La marque de votre frigo ou de votre four micro-ondes n'intéresse personne, par contre la marque de votre ordinateur peut en dire beaucoup sur vous.

L'informatique est au cœur de nos vies et pour beaucoup d'entre nous, elle est même au cœur de toutes nos préoccupations (passion, vie sociale, vie professionnelle). Les marques de nos ordinateurs ne sont plus que de simples logos : chaque constructeur défend une philosophie et des valeurs. L'idéologie d'un constructeur se retrouve chez ses utilisateurs.

Acheter un Mac a un sens. Persévérer dans l'achat de PC pendant 20 ans a aussi un sens. En dehors des considérations financières (les produits Apple coûtent cher), il est clair que les utilisateurs se complaisent dans l'idéologie de leurs marques préférées.

C'est ainsi qu'ont lieu de véritables combats idéologiques :

- Firefox versus Internet Explorer ;
- Android versus iOS (iPhone) ;
- GNU/Linux versus Windows ;

Tous ces choix ont tellement de sens que de nombreux organismes publient des sondages et des statistiques sur la personnalité des utilisateurs en fonction de leur matériel et des logiciels qu'ils utilisent. C'est par exemple le cas de cette superbe étude statistique :

> *Une étude sociologique des utilisateurs de MAC et PC*
> *www.pandore.it/aetude*

Elle compare la personnalité et les habitudes de vie des utilisateurs de Mac avec celles des utilisateurs de PC. Il s'agit de statistiques, pas d'une liste de vérités scientifiques. Cela dit, il est évident que la notion de stéréotypes sociologiques s'appliquent aussi sur Internet.

Statistiquement, il y a peu de chance qu'un internaute qui utilise Internet Explorer pour naviguer sur le web soit un technophile. Pour cause : ce navigateur fait fuir les utilisateurs avancés à cause de son manque de fonctionnalités et ses failles de sécurité.

Il y a de fortes chances qu'un utilisateur du système GNU/Linux soit un utilisateur avancé, car ce système d'exploitation demande bien souvent quelques connaissances techniques.

En fonction de votre propre expérience du monde d'Internet, vous disposez sûrement d'une grille plus ou moins vaste de stéréotypes concernant les outils que chaque internaute est amené à utiliser.

Comment exploiter l'*user-agent* en pratique ?

Revenons à l'*user-agent* lui-même. Dans la forme, il s'agit d'une sorte de phrase informatique compliquée. Voici trois *user-agents* pris au hasard sur Internet que vous serez susceptibles de rencontrer en pistant une cible :

1. Mozilla/5.0 (Macintosh ; Intel Mac OS X 10.9 ; rv :27.0) Gecko/20100101 Firefox/27.0
2. Mozilla/5.0 (Windows NT 5.1 ; rv :15.0) Gecko/20100101 Firefox/15.0.1
3. Mozilla/5.0 (Windows NT 6.3 ; Trident/7.0 ; rv :11.0) like Gecko

Comprendre un *user-agent* requiert un peu de pratique.

Le premier *user-agent* de la liste révèle l'identité d'un internaute utilisant un Macintosh et le navigateur Firefox. Le second UA révèle l'identité d'un utilisateur de Windows XP utilisant aussi Firefox. Le dernier UA de la liste identifie un utilisateur de Windows 8 utilisant Internet Explorer.

Au lieu de vous assommer avec des explications techniques, je vous ai concocté une petite fiche en ligne qui vous explique très simplement comment analyser un *user-agent*. Les conventions des *user-agents* changent régulièrement, il serait donc idiot de les figer sur papier.

Comprendre et analyser un user-agent
en 10 secondes
www.pandore.it/aua

Exploiter un *user-agent* n'est pas toujours évident car c'est une donnée un peu technique, mais le jeu en vaut la chandelle.

5. Le tracking link comme accusé de réception

Une autre information extrêmement importante vous est offerte par votre page espionne : tout simplement le fait que votre cible l'ait visitée ! Puisque vous recevez un e-mail lorsque quelqu'un clique sur votre lien, vous pouvez utiliser cet outil comme une sorte d'accusé de réception.

Un *tracking link* est un excellent moyen de savoir si quelqu'un vous boycotte (la personne lit votre message, clique sur les liens qu'il contient mais ne vous répond jamais), ou ne lit tout simplement pas vos messages.

Vous connaîtrez aussi l'heure exacte à laquelle une personne a cliqué sur votre lien espion, simplement en relevant l'heure de réception du mail.

6. Inciter à cliquer sur votre lien espion

Voici un premier exercice de *social engineering* très basique : comment faire en sorte qu'une cible clique sur votre *tracking link* sans se douter du moindre piège ?

Il existe des millions de possibilités, votre imagination est la seule limite.

Voila deux façons simples d'inciter un proche à cliquer sur un *tracking link via* un message Facebook, un e-mail ou un SMS.

- Vous générez un *tracking link* élégant grâce à l'outil que je vous fournis. Cet outil permet de personnaliser l'adresse de votre page espionne, pour feindre un article du journal *Le Monde* par exemple ;
- Vous envoyez un message à votre cible avec un texte comme « *Ho purée, tu te rappelles d'elle ? On en avait parlé l'autre jour c'est hallucinant ce qui lui arrive : {url-de-votre-tracking-link.com}* »

Jouez sur des détails qui vous rapprochent de la personne, personnalisez l'accroche autant que possible.

Si vous ne pouvez pas vous permettre une approche très personnelle, n'hésitez pas à créer une fausse identité pour accoster virtuellement votre cible par e-mail, sur Twitter ou *via* Facebook. Nous aborderons la question des fausses identités plus tard dans le livre.

7. Résumé des informations extraites

Cette partie peut sembler un peu dense. Voici un résumé des informations que vous allez facilement obtenir concernant votre cible grâce à votre site espion :

- Son pays de connexion ;
- Sa ville de connexion ;

- Son fournisseur d'accès Internet (Bouygues, SFR, etc.) ;
- L'heure à laquelle elle a cliqué sur votre lien ;
- Des informations sur l'appareil qu'elle utilise pour se connecter ;
- Des informations sur son navigateur Internet ;
- Son profil stéréotypé si vous avez une « culture Internet ».

8. Pour aller encore plus loin

L e *tracking link* donne des informations très intéressantes, mais il en est une qu'on rêve souvent d'obtenir : l'identité réelle d'un interlocuteur virtuel.

J'ai mis au point une méthode, proche du *tracking link*, permettant d'obtenir à coup sûr le profil Facebook d'un internaute sans qu'il ne s'en rende compte. Par extension, vous obtiendrez son nom, son prénom et peut-être sa photo.

Vous trouverez l'explication entière sur le blog du livre :

Trouver le profil Facebook de n'importe qui
(sans qu'il le sache)
www.pandore.it/afb

Conclusion

L e *tracking link* vous délivrera des informations brute qu'il faudra apprendre à analyser et interpréter .

Vous devrez également être capable d'hameçonner convenablement votre cible pour l'inciter à cliquer sur votre lien. Il existe des millions de possibilités, à vous d'être imaginatif et subtil.

Puisque c'est l'objet de ce ouvrage, nous verrons à la fin du livre comment vous protéger efficacement d'une personne mal intentionnée qui tenterait de vous espionner par ce biais ou par un moyen similaire.

Qui se cache derrière l'écran ?

1. Introduction

On entend souvent dire que tout se sait grâce à Internet. Heureusement, c'est faux ! On trouve sur Internet ce que des gens ont bien voulu y laisser, rien de plus et rien de moins. C'est une remarque qui peut sembler tautologique mais elle mérite d'être discutée.

Nous allons apprendre à exploiter un numéro de téléphone, une adresse e-mail, un pseudonyme, une adresse postale. Bref, n'importe quelle petite information dont on dispose sur une personne pour remonter jusqu'à elle.

Lorsque vous ferez vos recherches, repensez à ce que vous venez de lire : on ne trouve sur Internet que ce qu'un être humain a bien voulu y laisser. Si votre cible n'a jamais publié son numéro de téléphone en ligne, vous n'aurez aucune chance de remonter jusqu'à elle. Ne pensez pas qu'Internet est un puits magique qui réfléchit et travaille à votre place. C'est pourtant ce que s'imaginent beaucoup de gens.

Parallèlement, ce chapitre vous fera prendre conscience, je l'espère, que tout ce que vous publiez en ligne fini par se retrouver en cherchant bien.

2. Savoir utiliser Google correctement

Je vais être clair : Google est votre meilleur ami dans la recherche d'informations. Nous utiliserons des méta-moteurs

de recherche un peu spécialisés pour peaufiner notre fouille mais ils ne nous aideront que très partiellement.

Il existe quelques astuces plus ou moins connues pour bien exploiter les fonctionnalités de Google. Voici des exemples de recherches un peu spéciales :

- **“michel sappin”**
  En ajoutant des guillemets autour de votre recherche, Google ne vous affichera que les résultats qui correspondent **exactement** à vos mots clefs. Les mots qui « ressemblent juste » (comme « sapin ») seront éliminés des résultats.

- **“michel sappin” site :www.cadremploi.fr**
  En ajoutant le mot-clef « site : » suivi d’une URL, vous n’effectuez la recherche que sur le site dont il est question. Très pratique pour passer au crible un trombinoscope par exemple.

- **site :michel-sappin.com ext :pdf**
  Si votre cible a un site Internet (*michel-sappin.com* dans cet exemple), vous pouvez rajouter le mot-clef « ext :pdf » dans votre recherche pour extraire tous les documents PDF que Google a trouvé sur ce site et uniquement sur ce site. Peut-être y trouverez vous un CV ou une lettre contenant des informations importantes (les lettres sont souvent au format PDF ou DOC/DOCX).

N'oubliez pas l'outil de recherche avancée de Google, extrêmement puissant et intuitif
www.pandore.it/agg

Passons maintenant au cas pratique : comment retrouver une personne lorsqu'on ne dispose que d'une information *a priori* peu bavarde à son sujet.

3. Que faire avec un numéro de téléphone ?

Voici un scénario classique : vous disposez d'un numéro de téléphone provenant d'un appel louche, d'un SMS ou d'un document quelconque, et vous aimeriez connaître l'identité de son propriétaire.

Vous trouverez ici trois solutions très efficaces dans la grande majorité des cas.

I) Google et les annuaires inversés

Première chose à faire : une recherche Google sur le numéro. Cependant, il ne vous suffira pas de le taper bêtement dans le champ de recherche pour avoir des résultats pertinents.

En tapant un numéro de téléphone dans Google, vous obtiendrez des milliers de résultats sans intérêt qui, par hasard, correspondent seulement à 3 ou 4 chiffres du numéro.

Autre problème : un numéro de téléphone peut se retrouver sous plusieurs formes. Voici les quatre principales (XX représente deux chiffres) :

1. XX-XX-XX-XX-XX (nombres séparés par des tirets) ;
2. XX. XX.XX. XX.XX (nombres séparés par des points) ;
3. XX XX XX XX XX (nombre séparés par des espaces) ;
4. XXXXXXXXXX (nombres collés).

Lorsque vous ferez votre recherche Google, utilisez l'opérateur « OR » (traduction de « ou » en français) pour rechercher toutes les formes possibles. Utilisez aussi les guillemets pour préciser à Google que vous ne vous intéressez qu'au numéro de téléphone entier (et pas simplement à 4 de ces chiffres).

Voici l'exemple d'une recherche Google pertinente sur un numéro de téléphone :

> "01 42 92 81 00" OR "01.42.92.81.00" OR "01-42-92-81-00" OR "0142928100"

Si le numéro de téléphone appartient à une entreprise, il devrait vite ressortir dans les résultats, en étant associé au nom de l'entreprise.

S'il appartient à un particulier, ça se corse. Vous allez remarquer dans les résultats, de nombreux sites qui listent des centaines de numéros de téléphone dont celui que vous venez de taper.comment cela se fait-il ?

Ces sites web, qui prétendent être des annuaires inversés, génèrent en réalité des milliers de pages web contenant toutes les combinaisons de numéros de téléphone possibles et imaginables. Ces pages ont été créées par un ordinateur.

Ainsi, lorsqu'un internaute tape un numéro de téléphone dans Google, il tombe immanquablement sur l'une de ces pages fictives bourrées de numéros de téléphone. Naïvement, le visiteur clique sur le résultat Google puisqu'il y voit apparaître le numéro qu'il recherche. Une fois sur le site en question, le processus est toujours le même.

On vous redemande le numéro de téléphone dont vous cherchez le propriétaire. Une fois que vous leur indiquez, ils vous affichent quelque chose comme « nous avons trouvé le propriétaire ». Enfin, on vous demande d'appeler un numéro surtaxé pour connaître le fameux propriétaire.

Il s'agit d'une arnaque dans 100 % des cas, ne vous laissez pas avoir. Le seul annuaire inversé gratuit et fiable est celui des Pages Jaunes.

Vous pouvez accéder à cet annuaire inversé ici :
www.pandore.it/aai

Tous les autres sites d'annuaire inversés que vous trouverez ne vous serviront absolument à rien.

II) L'accès au répondeur

90 % des abonnés téléphoniques personnalisent leur messagerie vocale en indiquant leurs nom et prénom.

L'astuce consiste donc à utiliser un service qui vous permet de tomber directement sur la messagerie vocale d'un abonné.

Il existe plusieurs services de ce genre. Personnellement j'utilise RepondeurDirect.com. Attention : ce site est payant. Vous devez d'abord appeler un numéro surtaxé et ensuite taper le numéro de la personne à appeler.

Au total, le procédé ne vous coûtera pas plus de 2 €. Les conditions tarifaires sont clairement indiquées sur le site.

Accéder au site de RepondeurDirect.com :
www.pandore.it/ard

Je ne suis absolument pas affilié à ce site web, je vous le recommande en tant qu'utilisateur satisfait.

III) Exploiter Leboncoin

Leboncoin, le célèbre site de petites annonces en ligne, est le 7e site web le plus visité en France en 2014. Un français sur cinq l'utilise pour acheter ou vendre des biens et c'est le deuxième mot-clef le plus tapé sur Google après « Facebook ».

Dans la majorité des cas, le vendeur laisse son numéro de téléphone sous l'annonce. Le site « lebonvendeur.com » a exploité le filon et aspire régulièrement les nouvelles annonces déposées sur Leboncoin pour créer un annuaire des vendeurs.

Si vous avez déjà posté une annonce sur le site en laissant votre téléphone, vous êtes sûrement fiché sur *lebonvendeur.com* comme des millions d'autres utilisateurs !

Accédez à Lebonvendeur :
www.pandore.it/albv

En tapant un numéro de téléphone sur ce site, vous pourrez retrouver toutes les annonces d'un vendeur. Si votre cible utilise Leboncoin pour vendre, alors bingo ! Les annonces de vente mentionnent généralement le nom du vendeur, son e-mail et même sa ville.

Note : utilisez la page de contact du site Lebonvendeur pour faire supprimer votre numéro de téléphone si vous avez été enregistré contre votre gré. C'est très rapide.

Ce que vous devez retenir

Le numéro de téléphone est une information assez difficile à exploiter sur Internet.

Si le propriétaire d'un numéro est sur liste rouge, il ne sera listé dans aucun annuaire. Si personne n'a jamais formellement associé son nom à son numéro sur une page web, vous n'avez aucune chance de le trouver.

La technique du répondeur reste malgré tout bien efficace. Une fois que vous aurez trouvé le nom du propriétaire du numéro, vous aurez besoin d'autres techniques pour remonter jusqu'à son compte Facebook, son e-mail ou son adresse postale. Nous découvrirons tout cela plus loin.

4. Que faire avec une adresse IP ?

Vous obtiendrez généralement l'adresse IP d'une cible grâce à votre *tracking link*. L'exploitation de l'adresse IP grâce au *tracking link* a été largement détaillée dans le chapitre précédent.

5. Que faire avec un pseudonyme ?

Les pseudonymes sont de moins en moins utilisés. La faute à Facebook et Google qui imposent à leurs utilisateurs d'utiliser leurs vrais noms sous peine de sanctions. Parallèlement, de plus en plus de services web proposent de vous inscrire en utilisant votre profil Facebook ou Google. Petit à petit, la possibilité de s'enregistrer anonymement disparaît.

Les tchats, les forums et les communautés technophiles restent tout de même très attachés au concept de pseudonyme. Si la cible que vous *doxez* fréquente ce type de communautés, vous aurez de bonnes chances de le retrouver.

On utilise généralement un pseudo pour s'inscrire dans une communauté d'intérêt dans laquelle on sera amené à dialoguer, échanger, publier du contenu.

Si le pseudonyme de votre cible est très commun sur Internet, il ne vous mènera probablement pas bien loin (par exemple « squall » ou « blackninja ») car des milliers de personnes utilisent aussi ce pseudo.

En revanche si votre cible se surnomme « Alfacroco45 », vous aurez plus de chance de retrouver sa piste grâce à Google.combien de personnes utilisent exactement ce pseudonyme sur Terre ? Probablement une seule.

Sur Google, pensez à utiliser l'astuce des guillemets pour faire une recherche exacte sur le pseudonyme. Recherchez donc "alfacroco45" et pas seulement alfacroco45, au risque de vous retrouver avec des résultats bidons (par exemple le site d'Alfa Romeo).

Vérifiez aussi que cette personne n'a pas, par hasard, des comptes sur les principaux réseaux sociaux associés à son pseudonyme. Rendez-vous sur :

facebook.com/alfacroco45
twitter.com/alfacroco45
pinterest.com/alfacroco45
vine. co/alfacroco45
instagram.com/alfacroco45
…

Le site *Checkusernames.com* vous permet de tester un pseudonyme sur plus de 300 sites célèbres en quelques secondes. Il est à ranger dans votre boite à outils du parfait *doxer*.

Tester des pseudonymes automatiquement
www.pandore.it/acu

Ce que vous devez retenir

Un pseudonyme est une identité informelle et officieuse. Du coup, il n'existe aucun annuaire des pseudos qui pourrait vous être utile.

Utilisez en priorité *Checkusernames.com* et bien évidemment Google dans vos recherches.

6. Que faire avec une photo ou un avatar ?

On sous-estime souvent la richesse d'une simple photo trouvée sur Internet ou sur un ordinateur. Vous allez découvrir deux méthodes d'extraction d'informations à partir d'une simple image. Ces méthodes pourront vous permettre de remonter jusqu'à la personne qui a pris la photo initialement !

I) L'extraction d'EXIF

Les données EXIF sont des informations associées à des fichiers images par l'appareil photo d'un utilisateur.

Si vous disposez d'un iPhone ou d'un smartphone Android, il y a fort à parier que votre application Appareil Photo ajoute automatiquement des données EXIF à toutes vos photos à votre insu.

Ces données EXIF contiennent généralement :

- Les coordonnées GPS de l'endroit où a été prise la photo ;
- Les informations sur l'auteur de la photo ;
- L'heure et la date de prise de la photo ;

Ce sont donc des informations extrêmement riches. Pour savoir si une photo contient des EXIF et surtout pour accéder à ces EXIF, utilisez simplement un service web comme Verexif qui est totalement gratuit.

Accéder à Verexif :
www.pandore.it/aver

Il vous suffit d'*uploader* votre photo sur le site et il vous indiquera immédiatement les données EXIF associées.

Pour information, un pirate informatique s'est fait coincer par la police à cause des données EXIF d'une photo qu'il avait mise en ligne pour narguer les autorités… l'histoire est marrante (et navrante) !

Un pirate arrêté à cause… des seins de sa copine !
www.pandore.it/asc

Si le photographe désactive l'intégration des EXIF sur son appareil avant la prise, vous ne pourrez jamais y avoir accès.

II) La recherche inversée

Il y a encore 2-3 ans, la recherche inversée d'images n'était pas si efficace. Et pour cause, Google ne s'y était pas encore mis !

Depuis 2011, Google propose en plus de son célèbre moteur de recherche d'images, un moteur de recherche d'images… inversé !

En clair : vous lui soumettez une image, il vous indique tous les sites web qu'il connaît qui utilisent cette image (ou une image très similaire dans le pire des cas).

Accéder à la recherche d'image inversée Google : www.pandore.it/aig

Une fois sur le moteur de recherche d'images Google, cliquez sur le petit appareil photo à l'intérieur du champ de recherche et sélectionnez l'image à analyser.

Même si l'image est partiellement modifiée (filtre sépia, filtre noir et blanc, etc.) Google la retrouvera sans problème.

Cette méthode permet entre autres :

- De remonter au site qui a publié la photo en premier ;
- De se rendre compte qu'une photo de profil est utilisé sur 200 sites différents (et donc qu'il s'agit d'une fausse photo de profil) ;
- De trouver des sites sur lesquels est inscrit votre cible, s'il s'agit d'une photo qu'elle utilise fréquemment comme photo de profil.

Ce que vous devez retenir

Il n'existe que deux manières d'exploiter une image aujourd'hui : la recherche inversée et l'extraction d'EXIF.

Pensez à vérifier les données EXIF de toutes les images que vous pouvez analyser dans votre *doxing* : certains logiciels de traitement photo ajoutent des EXIF intéressantes sur les images.

Vous remarquerez sûrement que chaque méthode de recherche a ses propres limites. C'est pour cette raison qu'il ne faut négliger aucune information.

7. Que faire avec une simple adresse e-mail ?

Vous allez dire que je manque d'originalité, mais commencez donc par une recherche Google sur cette adresse e-mail ! Vous pourriez trouver des informations très intéressantes sur votre cible (loisir, communauté d'intérêt, messages sur des forums, annonce Leboncoin, etc.).

I) Utiliser un tracking link

Premier réflexe après votre recherche Google : le *tracking link* bien sûr ! Profitez de ce super outil pour pister votre cible à son insu.comme d'habitude avec votre *tracking link*, il vous faudra une bonne dose d'imagination pour envoyer un e-mail à la fois subtil et efficace, qui incitera le destinataire à cliquer sur votre lien espion.

Les méthodes d'hameçonnage les plus efficaces ne sont pas forcément très morales ni très légales, je préfère vous laisser réfléchir un peu par vous-même. Conseil d'ami : n'hésitez pas à vous aider de la partie du livre sur la création d'identité factice.

II) Facebook et la recherche par e-mail

En tapant une adresse e-mail dans le moteur de recherche Facebook, vous pourrez voir sortir le profil de son propriétaire. À deux conditions :

- Que son compte Facebook soit associé à cette adresse e-mail ;
- Qu'il n'ait pas décoché la case « permettre de me retrouver avec mon adresse e-mail » ;

C'est une piste comme une autre, à ne pas négliger malgré son côté assez hasardeux.

III) Twitter et la recherche par e-mail

Pour Twitter c'est un peu différent : si vous avez envie de retrouver un utilisateur du site *via* son adresse e-mail, il faudra ruser. Voici la méthode :

1. Créez une adresse e-mail Gmail ou Yahoo Mail bidon, c'est gratuit et très rapide ;
2. Sur cette adresse bidon, ajoutez comme seul contact dans votre carnet d'adresse l'e-mail de la personne que vous souhaitez retrouver sur Twitter ;
3. Rendez-vous ensuite sur votre compte Twitter et cliquez sur « retrouver mes amis ». Twitter vous demandera alors de renseigner vos identifiants e-mail pour accéder à votre carnet d'adresses.

Twitter va pouvoir fouiller dans votre carnet d'adresses… qui ne contient qu'une seule adresse mail : celle de votre cible. Si celle-ci a associé son e-mail à un compte Twitter, son pseudonyme s'affichera immédiatement.

IV) J'ai oublié mon mot de passe

Une adresse e-mail se compose vulgairement de deux parties : avant le signe arobase se trouve l'identifiant, après le signe arobase se trouve le fournisseur de service.

Par exemple : charlie@gmail.com. « charlie » est l'identifiant de ma boite mail, « gmail.com » est le fournisseur de la boite mail.

Identifiez le fournisseur de l'e-mail de votre cible et rendez-vous sur son site. Si l'adresse e-mail est fournie par un des gros géants habituels (@yahoo.com, @gmail.com, @orange.fr, etc.) c'est très facile. Si vous remarquez cependant que le fournisseur est un site complètement inconnu qui n'a rien à voir avec un fournisseur d'adresses e-mail, passez directement à la méthode 5 ci-dessous.

Une fois sur le site du fournisseur (www.gmail.com si l'e-mail de votre cible termine par @gmail.com par exemple), cherchez le lien « j'ai oublié mon mot de passe » ou « je n'arrive pas à me connecter à mon compte » sur la page de connexion.

Cette procédure, que vous connaissez sûrement, permet de récupérer le mot de passe de votre boite mail lorsque vous l'avez oublié.

Nous allons exploiter une petite faille de cette procédure pour en savoir un peu plus sur notre cible. Démarrez la procédure de récupération de mot de passe et entrez l'e-mail de votre cible lorsque le site vous le demande.

À cette étape de la procédure, on vous proposera plusieurs moyens pour récupérer le mot de passe. Soit par SMS, soit par e-mail si le titulaire du compte a spécifié un mail de secours lors de son inscription.

Si vous testez cette méthode sur gmail.com, vous remarquerez que Gmail fournit les premières et les dernières lettres de l'e-mail de secours associée au compte dont vous souhaitez récupérer le mot de passe. Idem pour le téléphone. Certains sites, moins scrupuleux, donnent carrément l'e-mail de secours complète.

En clair, Gmail affichera un message semblable à celui-ci :

> Choisissez la méthode que vous préférez pour réinitialiser votre mot de passe :
>
> Par e-mail, sur votre adresse de secours : ch********ro@o*****e.fr
>
> Par SMS, au 06 21 ** ** **

Ces informations sont extrêmement précieuses. Si vous aviez une idée un peu floue de l'identité de la personne derrière cette adresse e-mail, ces indications pourraient confirmer vos doutes. Vérifiez dans votre répertoire téléphonique si aucun numéro de téléphone ne commence par « 06 21 » par exemple.

V) La redirection mail

Cette méthode n'est valable que dans le cas où l'adresse e-mail que vous pistez n'est pas fournie par un fournisseur d'e-mails classique.

Par exemple, les auteurs de l'Institut Pandore (l'entreprise qui édite ce livre) disposent tous d'une adresse e-mail du type : prenom@auteur. institut-pandore.com.

Vous remarquez que cette adresse mail n'est ni proposée par Yahoo, ni par Gmail… mais par « auteur. institut-pandore.com » ! Comment cela est-il possible ?

Moyennant une dizaine d'euros, il est possible d'acheter des adresses e-mails personnalisées. Autrement dit, vous pouvez vous-même créer votre propre adresse e-mail « trucbidule@ce-que-vous-voulez.com ». C'est ce qu'a fait l'Institut Pandore pour proposer de jolies adresses à ses auteurs.

Dans certains cas, il est possible de savoir qui se cache derrière ces adresses e-mails un peu opaques. En d'autres termes : lorsque j'envoie un e-mail à « machin@truc-bizarre.com », comment savoir qui reçoit réellement mon message ?

L'explication étant un peu longue et technique, il a été préférable de la déplacer sur le blog du livre. Vous l'avez bien compris : cette technique ne vous sera utile que dans le cas où

la personne que vous cherchez à *doxer* n'utilise pas une boite e-mail traditionnelle (Gmail, Yahoo, etc.).

Pistez une adresse e-mail anonyme
pour connaître son propriétaire
www.pandore.it/ape

8. Que faire avec un nom et un prénom ?

Le problème lorsqu'on ne dispose que d'un nom et d'un prénom, c'est qu'on ne possède aucun moyen évident de prendre contact avec la personne.

Première étape… est-ce la peine de vraiment en parler ? Il s'agit bien entendu de faire quelques recherches sur Google et sur Facebook. Peut-être qu'un résultat pertinent apparaîtra et vous permettra de poursuivre votre enquête tranquillement.

Deuxième étape : utiliser *Checkusernames.com* dont j'ai parlé plus haut en testant le pseudonyme « {non}{prenom} ». Par exemple « charliechaplin » ou « chaplincharlie ».

Dernière chance : faire des recherches manuelles plus poussées. C'est ce que nous allons voir tout de suite.

I) Les réseaux sociaux auxquels on ne pense pas toujours

Lorsqu'on fait une recherche de personne sur un nom et un prénom, on pense immédiatement à Facebook et Google. Mais avez-vous pensé à chercher sur les sites suivants :

- Copains d'avant : pour retrouver une personne de plus de 30 ans ;
- LinkedIn et Viadeo : pour retrouver une personne grâce à ses informations professionnelles ;
- Pinterest, Ask. fm, Instagram : population assez hétéroclite.

Certains réseaux sociaux peu connus en France sont massivement utilisés dans d'autres pays. Je pense par exemple à VK qui n'est autre que le « Facebook russe », à Weibo le twitter chinois, ou encore Orkut principalement utilisé par les Brésiliens.

On pourrait penser que Google fait **forcément** remonter ces sites dans ses résultats de recherche, mais en pratique ce n'est pas le cas. Il est donc parfois plus intéressant de chercher manuellement.

II) Les méta moteurs de recherche

Il existe ce qu'on appelle des méta-moteurs de recherche. Ces méta-moteurs ne font que chercher à votre place sur plusieurs autres moteurs de recherche en même temps. Le plus connu de ces méta-moteurs est probablement *pipl.com*, spécialisé dans la recherche de personnes.

Tapez-y le nom de quelqu'un et le méta-moteur ira faire des recherches sur Facebook, Google, LinkedIn et bien d'autres sites sociaux à votre place. Tous les résultats seront affichés sur une seule et unique page. En plus de rassembler les résultats sur une même page, les recherches effectuées à votre place sont optimisées.

Essayez toujours *pipl.com* si vos recherches manuelles n'ont rien donné, vous pourriez être surpris du résultat ! Le site fait parfois remonter des informations enfouies profondément dans Google.

Accéder à Pipl
www.pandore.it/apipl

Il existe des dizaines de méta-moteurs dédiés à la recherche de personnes. Chacun d'entre eux a tendance à faire remonter des informations assez uniques. Je vous recommande de tous les essayer si votre enquête piétine. En voici deux autres, très efficaces :

- Yatedo : http://yatedo.com/
- Webmii : http://webmii.com/

Dans l'éventualité où une requête sur le patronyme de votre cible ne retourne aucun résultat concluant, vous allez devoir utiliser le générateur d'adresses e-mails.

III) Le générateur d'e-mails

Je vais être honnête : quand on en arrive là, c'est qu'on a essayé tout le reste.

Il s'agit d'un outil que j'ai conçu assez récemment et qui m'a permis de retrouver la trace de trois personnes. Ça marche, mais c'est très aléatoire.

> *Accéder au générateur d'e-mails :*
> *www.pandore.it/amg*

Le principe est simple. Il consiste à envoyer des e-mails à toutes les adresses potentielles de votre cible. Au lieu d'imaginer toutes ces adresses vous-même, j'ai créé un petit générateur d'e-mails qui vous mâchera le travail.

Vous donnez le prénom et le nom de votre cible au générateur et il va automatiquement vous lister les adresses e-mails potentielles de cette personne.

Exemple : vous proposez « jean dupont » au générateur d'adresses. Il vous suggérera automatiquement des dizaines d'adresses e-mails comme jean.dupont@gmail.com, dupontjean@gmail.com, jean.dupont@orange.fr, jeandupont@orange.fr, etc.

En soi, ces e-mails ne vous serviront pas à grand–chose. Parmi les dizaines d'e-mails que le générateur vous proposera bêtement, beaucoup n'appartiendront à personne.

Vous allez faire un premier tri en utilisant le site *Verify-Email.org*. L'inscription est gratuite et ne prend que quelques secondes.

Accéder au site VerifyEmail :
www.pandore.it/ave

Une fois inscrit, cliquez sur le bouton « Bulk Verifier ». Copiez-collez toutes les adresses e-mails proposées par le générateur dans le formulaire du site et cliquez sur « verify ».

Attendez patiemment. Toutes les adresses que vous avez données et qui sont effectivement utilisées par quelqu'un s'afficheront en vert. Il s'agit d'un premier tri très utile.

Il ne vous reste plus qu'une chose à faire : envoyer des e-mails en masse aux adresses qu'il vous reste. Parmi ces adresses se trouve peut-être l'adresse e-mail de votre cible.

N'oubliez pas le *tracking link*. Il est extrêmement utile dans cette situation pour savoir si les personnes à qui vous avez envoyé un e-mail à l'aveuglette l'ont lu et ont cliqué sur le lien à l'intérieur.

Cette technique équivaut à envoyer des bouteilles à la mer et à attendre une réponse. Parfois ça marche, parfois non.

Ce que vous devez retenir

Partir uniquement d'un nom et d'un prénom demande beaucoup d'astuces et de persévérance, d'autant plus si votre cible ne développe pas sa présence sur Internet sous sa véritable identité.

Lors de vos recherches, pensez à associer le nom et le prénom de votre cible avec une ville où elle pourrait habiter (« jean dupont marseille ») ou une entreprise où elle pourrait travailler. Un mot-clef en plus dans une recherche Google change **complètement** la donne, surtout lorsqu'il s'agit de l'associer à un patronyme.

9. Que faire avec un site Internet ?

En France, les éditeurs de sites web ont l'obligation de faire figurer le nom et l'adresse du responsable de publication quelque part sur leurs pages. Le responsable de publication est la personne qui représente légalement le site aux yeux de la loi.

Il est toutefois possible de créer son site sous couvert d'anonymat à condition de transmettre toutes ses informations de contact à son hébergeur, qui sera lui-même

obligé de les transmettre à la justice en cas de demande d'un juge.

Les informations sur le propriétaire d'un site sont pratiquement toujours indiquées sur une page « Mentions Légales » que vous trouverez en fouillant un peu.

Si le créateur du site a décidé de ne pas divulguer son identité dans ses mentions légales, vous pourrez toujours effectuer un « Who Is » sur son nom de domaine. Pour faire simple, un *Who Is* est un service gratuit qui interroge l'organisme en charge des noms de domaine sur Internet.

Lorsque vous achetez un nom de domaine, c'est-à-dire une adresse de site personnelle (par exemple « www.jean-michel-dupont.com »), vous passez par un prestataire spécialisé. C'est ce prestataire que va interroger le *Who Is*.

Pour utiliser ce fameux *Who Is*, vous pouvez utiliser le site gratuit Whois.net. Il en existe des milliers d'autres qui proposent exactement la même chose.

Faire un whois
www.pandore.it/awh

En tapant l'adresse d'un site dans le formulaire de Whois.net, vous obtiendrez une seconde plus tard toutes les informations disponibles sur le propriétaire du domaine.

Il est toutefois possible d'anonymiser ces informations sans aucun problème, voire d'indiquer de fausses informations.

I) Ce que vous devez retenir

Le *Who Is* est un bon moyen d'obtenir des informations sur le propriétaire d'un site si celui-ci n'a pas mis en ligne de mentions légales.

Cependant la confiance que vous devez accorder à ce fameux *Who Is* est toute relative : il est facile de le truquer, voire de le masquer.

Conclusion

Vous l'avez compris : la recherche de personnes sur Internet est quelque chose de très empirique. Les astuces et les méthodes décrites plus haut doivent être adaptées à votre situation et aux informations que vous possédez.

Google est l'outil le plus puissant dont nous disposons actuellement, il est primordial d'en connaître les méandres et les subtilités.

Avoir une « culture internet » vous aidera aussi beaucoup à être plus débrouillard dans vos recherches. Je ne suis pas sûr que ce soit quelque chose qui s'apprenne théoriquement en lisant un livre. On devient débrouillard en utilisant son ordinateur, de la même manière qu'on devient bon cuisinier en cuisinant.

La prochaine partie du livre est consacrée à la création d'une fausse identité sur Internet. *Doxer* sous votre véritable identité serait en effet une grossière erreur.

Comment se créer une fausse identité sur Internet ?

Cette partie sera brève et factuelle. Pour jouer au détective sur le web, il est souvent nécessaire de recourir à de fausses identités.

Créer une fausse identité ne veut pas dire usurper une identité, **bien au contraire**. Il s'agit de créer une fausse identité de A à Z qui ne portera préjudice à personne.

Vous allez découvrir ici quelques trucs et astuces pour optimiser vos fausses identités et ne pas vous prendre les pieds dans le tapis.

1. Anonymiser votre navigation

Ne vous y fiez pas : la célèbre « navigation privée » de Google Chrome ou de Firefox n'a rien d'anonymisant.

Pour limiter les traces que vous laissez derrière vous en surfant, je vous invite à découvrir le dernier chapitre du livre qui traite cela bien en détails (en particulier la sous-partie sur le *spoofing IP* et celle sur les cookies).

2. Des fausses coordonnées

I) Une fausse adresse email

Un faux profil implique nécessairement de fausses coordonnées. Créer une boite e-mail ne prend quelques

secondes et ne coûte rien. Privilégiez Gmail et Yahoo Mail qui n'éveillent aucun soupçon.

II) Un faux compte Facebook

Même chose que pour la boite mail : n'hésitez pas à créer de faux comptes Facebook pour être à l'aise lors de vos séances enquêtes.

Il est possible de créer plusieurs comptes Facebook depuis la même connexion Internet sans aucun problème. À partir d'une certaine limite (six comptes environ), Facebook vous obligera à lui donner un numéro de téléphone unique pour vérifier votre identité. Le point suivant pourra vous être utile si vous en arrivez là.

III) Un faux numéro de téléphone

Plusieurs entreprises vous permettent de disposer de numéros de téléphone virtuels. Ces numéros sont virtuels parce qu'ils ne font que rediriger les appels et les SMS vers votre vrai numéro.

Grâce à eux, vous pourrez camoufler votre numéro de téléphone personnel dernière un numéro virtuel jetable. C'est très utile pour vous inscrire sur des sites qui demandent une confirmation par SMS par exemple.

Découvrez une liste de fournisseurs de numéros virtuels sur le blog du livre :

Obtenir un numéro virtuel
www.pandore.it/anv

Comptez 1 € par mois en souscrivant à l'offre la plus low-cost du marché.

C'est très utile si vous baroudez beaucoup sur Internet. Cela vous permet de changer de numéro gratuitement, en deux clics, et surtout de ne jamais donner votre vrai numéro. En dehors de l'anonymat, c'est surtout une bonne manière d'éviter la publicité.

IV) Une fausse photo de profil

Le site *Uifaces .com* propose des photos d'utilisateurs libres de droit. Vous pouvez prendre n'importe laquelle de ces photos pour crédibiliser votre faux profil. C'est légal.

Cerise sur le gâteau : le site n'est pas assez référencé par Google pour que l'on puisse faire une recherche inversée sur votre photo et retomber sur *UIfaces.com*.

Accéder au site UIFaces, rubrique authorized
www.pandore.it/aui

3. Comment bien utiliser vos fausses identités ?

Si vous utilisez le navigateur Firefox, Internet Explorer ou Opéra au quotidien, je vous conseille d'installer un autre navigateur sur votre ordinateur. Utilisez votre navigateur habituel pour votre identité principale et un autre navigateur pour gérer votre fausse identité. Cela vous évitera de vous mélanger les pinceaux.

Si vous utilisez Google Chrome, vous avez de la chance ! Ce navigateur propose une gestion des multi-identités fabuleuse.

Rendez-vous dans les options de Chrome, cherchez « Gérer les identités » et ajoutez une nouvelle identité.

Une fois cette identité créée, un nouveau menu apparaîtra dans Google Chrome : le menu « Utilisateurs ». Vous y trouverez votre profil utilisateur habituel ainsi que votre nouvelle identité fraîchement créée.

Vous pourrez ouvrir chacune de vos identités dans une fenêtre séparée de Google Chrome. Et chaque identité pourra être connectée à un compte Facebook différent, un compte Gmail différent, un compte Twitter différent… Bref, c'est pour moi le meilleur moyen de gérer des multi-comptes.

Ce que vous devez retenir

Par pitié, n'usurpez pas l'identité d'autres personnes sur Internet. D'une part c'est lâche, d'autre part cela vous sera infiniment préjudiciable dans un futur proche.

Faites jouer votre imagination pour créer vos identités factices. Le site Fakenamegenerator.com pourra vous aider : il génère à votre place un profil complet en seulement 1 clic.

Accéder au Fake Name Generator
www.pandore.it/afk

Manipulation sociale et *cold-reading* virtuel

J'ai l'honneur d'inviter Félix Boussa, auteur et mentaliste, à co-écrire cette partie du livre à mes côtés. Avant d'entrer dans le vif du sujet, je me permets de vous présenter brièvement Félix si vous ne le connaissez pas encore.

Il est auteur et mentaliste passionné depuis une quinzaine d'années. Il a fondé entre autre apprendre-a-manipuler.com, Sixième Sens et le Labo des Mentalistes. Ces trois sites sont devenus au fils des années des piliers du mentalisme dans la sphère francophone.

Passionné par la psychologie sociale et plus particulièrement par la manipulation et les mécanismes d'influence, il était la personne la plus apte à diriger cette partie de l'ouvrage.

1. Les bases du *profiling* sur Internet

Sur Internet comme dans la vie réelle, vous pouvez facilement analyser la personnalité de vos interlocuteurs et les associer à un « profil type » qui leur correspond. Si vous vous êtes déjà intéressé au mentalisme, il s'agit en quelque sorte d'un *cold-reading* virtuel. On appelle aussi ça le profilage (« profiling » en anglais).

Le profilage consiste à analyser un individu par différents moyens et à le placer dans une case sociale pour mieux le cerner. Nous disposons chacun de nos propres cases sociales

en fonction de nos convictions, de nos rencontres et de nos expériences.

Voyez le profilage comme un dessin. Plus vous apprenez à connaître une personne, plus le dessin que vous ferez d'elle sera proche de la réalité. Plus votre instinct de profiler sera développé, plus votre dessin sera réaliste. Malgré cela, votre analyse sera toujours un brouillon : « profiler quelqu'un » ne veut absolument pas dire « définir quelqu'un ». Il est facile de tomber dans l'excès en catégorisant trop vite et trop mal toutes les personnes que l'on rencontre. Je reviendrai sur cela plus tard.

I) Critères de profiling et stéréotypes

Dans la vie non-virtuelle, c'est-à-dire en dehors d'Internet, vous profilerez vos interlocuteurs en fonction de leur gestuelle, de leur look, de leur façon de parler. Mais sur Internet, comment faire ? À moins de discuter par webcams, vous ne pouvez observer ni le look, ni la gestuelle, ni même entendre la voix de vos correspondants.

En discutant avec un parfait inconnu sur Facebook par exemple, vous aurez accès tout au mieux à quelques photos de vacances ou de soirées. Dans ce cas précis votre profilage pourra se baser sur son look, ses occupations ou ses fréquentations.

Dans le cas contraire, sans avoir accès à la moindre photo, comment définir le groupe social auquel appartient un individu ? Il existe heureusement quelques solutions alternatives propres à la vie virtuelle.

Sans aucun moyen de voir ou d'entendre votre interlocuteur, vous devrez vous concentrer sur le seul élément d'apparence dont vous disposez : sa syntaxe.

La syntaxe d'un individu sur Internet est définie principalement par trois composantes :

- La qualité de son orthographe ;
- L'utilisation de smileys ;
- L'utilisation de certains mots connotés.

Il existe d'autres métriques qui seront abordées dans le chapitre consacré à la stylométrie. Contentons–nous pour l'instant de ces trois indicateurs.

Voici deux exemples de groupes sociaux virtuels que je retrouve fréquemment sur mes sites, associés à leurs particularités syntaxiques :

1. Le quarantenaire, ou plus âgé, un peu perdu avec un clavier entre les mains. Sa syntaxe est facile à reconnaître :
    - Beaucoup de signes de ponctuation à la fin de ses phrases (« bonjour !!!!!!! », « ah bon ????? ») ;
    - Étourderies syntaxiques à cause d'une méconnaissance du clavier (des « ; » à la place des « . » par exemple) ;
    - Pratiquement aucune apostrophe ni aucun accent, assez difficiles à atteindre sur un clavier.

2. Le (la) jeune adolescent(e) un peu « kikoolol » très à l'aise avec un ordinateur et qui discute régulièrement avec ses amis ou même avec des inconnus. Sa syntaxe est reconnaissable grâce à :
    - Une utilisation parfois intensive des smileys (^^, x), xD, :D, :)) ;
    - Un vocabulaire jeune, comme à l'oral ;
    - Des fautes d'orthographe type SMS ou simplement dues à la rapidité de frappe sur le clavier ;

Les groupes sociaux reposent sur des stéréotypes, il s'agit donc d'une vision grossière et brouillonne de la réalité. Le travail d'un *profiler* consiste justement à affiner constamment ses analyses, en faisant des rencontres et en remettant en question chacune de ses analyses.

Lorsque vous discutez avec un inconnu sur Internet, il est important, pour ne pas dire fondamental, de rapidement déterminer le groupe social auquel il appartient. Encore une fois, il n'y a pas de « bonne réponse » : vous avez vos groupes, vos stéréotypes, et j'ai les miens. Et devinez quoi ? Ils sont probablement différents.

Nous n'avons pas fait les mêmes rencontres, nous n'avons pas les mêmes opinions politiques et sociologiques, nous n'avons pas la même expérience de la vie. Autant de différences qui vont altérer le résultat de nos analyses.

L'idée clef derrière le concept de profilage est d'être capable de catégoriser rapidement vos interlocuteurs pour deviner leurs traits de personnalités, les sujets de discussions qui les feront

vibrer, les discussions qu'ils apprécieront moins, les détails sur lesquels ils aiment être flattés, etc.

Grâce à ce genre d'analyses, vous saurez instinctivement qu'un individu appartenant à tel groupe social apprécie particulièrement telle chose et déteste particulièrement telle autre chose . C'est extrêmement pratique pour aborder un individu sur Internet. Cela vous permet de lancer une conversation intéressante sans vous prendre la tête.

Exemple : un individu appartenant à votre groupe « trentenaire, jeune cadre, jeune parent » aimera probablement parler de ses enfants, peut-être de sa carrière si elle est réussie. Un individu appartenant au groupe social « militant UMP » aura horreur des idées socialistes.

Posées à l'écrit, ces affirmations semblent simplistes voire dangereuses tellement elles raccourcissent la pensée humaine et la vie en société. À cette remarque, je répondrais deux choses.

Tout d'abord, c'est le principe même de la sociologie que de mécaniser le fonctionnement humain. Il est convenu que tout ce que raconte la psychologie sociale n'a pas valeur de règle immuable et que chacun peut s'imaginer en dehors des théories existantes. À mon sens, il serait tout de même présomptueux de penser que l'on échappe, nous ou notre entourage proche, aux grandes généralités sociologiques. Même les grands excentriques (auto)proclamés rentrent parfaitement dans les cases auxquels ils essaient d'échapper. À force de vouloir nager à contre-courant, on s'enferme dans le stéréotype qu'on voulait fuir.

Deuxièmement , faites attention à ne pas vous enfermer dans une grille de stéréotypes péjoratifs et malhonnêtes. Restez objectif lorsque vous décortiquez votre interlocuteur. Vous avez le droit d'être dans l'erreur et vous le serez souvent. Cependant, ne tombez pas dans la calomnie ou dans le racisme au sens large.

Pour résumer le principe du profilage virtuel en quelques mots :

1. Analysez votre interlocuteur grâce à sa syntaxe (smileys, orthographe, vocabulaire). Le reste du chapitre détaillera la méthodologie à adopter.
2. Définissez un groupe social qui lui correspond, en fonction de sa syntaxe et de tous les autres éléments dont vous disposez pour vous aider (une photo de profil ou un pseudonyme peuvent aider) ;
3. Adaptez votre conversation et votre façon de communiquer en fonction du groupe social auquel appartient votre interlocuteur. Nous verrons plus en détails comme cela se passe en pratique.

Un dernier aspect du profilage mérite d'être précisé avant de passer à la suite : votre « brouillon psychologique » doit s'affiner constamment au fil du temps. Ne restez pas enfermé dans l'analyse que vous avez faite d'entrée de jeu. Ne restez pas bloqué sur votre première impression. Faites évoluer le profil de votre interlocuteur petit à petit, grâce aux informations que vous apprenez de lui.

Voyez ça comme une enquête policière. Lorsqu'un policier enquête sur un meurtre et qu'il soupçonne le meurtrier, il ne

doit pas se forcer à faire coïncider les preuves qu'il trouve avec son hypothèse. Les preuves doivent confirmer sa suspicion, pas l'inverse. C'est la même chose pour le *profiling*.

II) Comment créer vos propres cases sociales ?

Vous construirez votre échiquier social sur Internet de la même manière que vous le construirez dans votre vie non-virtuelle. C'est-à-dire en faisant des rencontres et en observant les gens autour de vous.

Sur Internet, il est facile d'observer passivement des groupes sociaux tellement le web est une sorte de « zoo gratuit ».

Voici des idées prêtes à l'emploi qui vous permettront d'observer des inconnus directement dans leurs groupes sociaux respectifs :

1. Lire les commentaires sous les articles des grands quotidiens nationaux (*Le Monde, Figaro, Libération*, etc.). Faites quelques recherches pour connaître l'orientation politique de chaque journal, cela vous permettra d'observer le comportement des individus en fonction de leurs bords politiques. Les commentateurs des journaux de droite sont rarement des électeurs de gauche et vice-versa.

2. Suivre des communautés Facebook éloignées de vos goûts personnels. Suivez par exemple la communauté de Matt Pokora, du PSG ou des collectionneurs de papillons. Les pages Facebook (ou équivalent sur d'autres sites) offrent un terrain de jeu incroyable aux profilers.

3. Vous inscrire sur des forums thématiques (forums de jeux-vidéo, forum de cuisine, etc.) et analyser, de temps en temps, les discussions les plus populaires.

Il n'y a pas de mystère : le *profiling* virtuel se développe en fréquentant Internet. Ne cherchez pas de livre ou de formation à ce sujet, cela n'existe pas. Chacun d'entre nous doit apprendre à analyser les individus qu'il rencontre à sa manière. Selon ses convictions. Selon son expérience.

III) Ce que vous devez retenir

Le *profiling* consiste à cerner rapidement les gens , grâce à des observations bien senties et un certain sens de la déduction.

Les jugements que nous portons sur les autres doivent rester personnels. Jugez à votre manière, établissez vos propres groupes sociaux. Attention à ne pas tomber dans le piège de la calomnie ou de la discrimination en généralisant vos observations à outrance.

Dans la partie suivante, nous allons mettre en pratique nos techniques de *profiling* à l'usage de la séduction – au sens large – et de la manipulation sociale. Vous allez apprendre à influencer quelqu'un derrière votre écran, à devenir proche de lui et à analyser son comportement.

2. Les bases de la manipulation en ligne

I) Apprendre à manipuler c'est malsain, non ?

Si vous ne vous êtes jamais intéressé à l'art de la manipulation, l'idée même « d'apprendre à manipuler » pourrait vous paraître extrêmement malsaine.

Laissez-moi vous montrer que c'est tout l'inverse. La manipulation telle que je l'enseigne dans mes formations consiste avant tout à analyser nos relations sociales pour les améliorer. Pour les optimiser. Tout cela, grâce à l'étude de la psychologie.

Il n'est écrit nulle part que la manipulation implique le mensonge, la trahison ou des comportements toxiques. Cette vision très malsaine a toujours été mise en avant dans les médias : fraudes, sectes, mensonges politiques.
Heureusement, la manipulation peut être éthique… et même positive !

Nos relations sociales sont quotidiennement influencées et manipulées par des milliers de facteurs qui nous échappent : les émotions et les croyances, les nôtres et celles des autres, des biais psychologiques et sociologiques. Vous pouvez passer votre vie sans chercher à comprendre tout cela : « les choses sont comme elles sont. Les gens sont ce qu'ils sont et je fais avec ».

Mais vous pouvez au contraire chercher à creuser : « pourquoi les gens agissent de cette manière ? », « pourquoi est-ce que je pense cela depuis toujours ? ». La manipulation, celle que

j'enseigne, permet de comprendre les processus sociaux qui nous entourent au quotidien.

Une fois la théorie acquise, on peut s'en servir pour se protéger des manipulateurs. On peut aussi s'en servir pour manipuler son entourage gentiment (par exemple se faire servir un café sans bouger le petit doigt) ou dans un objectif plus humaniste (inciter un ami à suivre un régime ou l'aider à reprendre sa vie en main).

Ceux qui manipulent pour faire le mal autour d'eux n'ont pas besoin d'apprendre quoi que ce soit dans des livres. Ils agissent naturellement. La manipulation émotionnelle toxique ne s'apprend pas.

Apprendre la manipulation ne consiste donc pas à devenir une ordure. C'est le contraire : il s'agit de décortiquer nos relations sociales au quotidien pour en tirer le meilleur. Pour nous, et pour les autres.

Si le sujet vous intéresse, vous en apprendrez davantage sur mon site. Avancer dans la vie sans connaître les mécanismes sociaux qui agissent sur vous équivaut à marcher les yeux bandés. Selon moi, apprendre la manipulation – je dis bien « apprendre » et pas forcément l'utiliser – est quelque chose d'absolument fondamental.

Accéder au site de Félix Boussa
www.apprendre-a-manipuler.com

II) La clef de la manipulation : l'ego

Si vous ne deviez retenir qu'un seul concept lié à la manipulation sociale, ça serait l'ego.

L'ego est la partie de l'esprit la plus exploitable pour le manipulateur. On peut détruire quelqu'un en brisant son ego ou au contraire obtenir sa confiance en flattant son ego.

Vous allez découvrir plus bas quelques techniques de manipulation par l'ego à l'usage du web et des messageries virtuelles (tchat, e-mail, SMS, etc.).

Je tiens à préciser que ce chapitre n'est pas exhaustif. La manipulation sociale est une discipline extrêmement vaste. Dans la suite de cet ouvrage, je vais détailler les principales transpositions psychologiques du réel au virtuel. Sachez qu'il existe une infinité de techniques d'influence et de manipulation, aussi bien dans l'espace réel que dans l'espace numérique.

III) Pourquoi le doxing et la manipulation sont étroitement liés ?

En tant que *doxer* ou détective du web, vous aurez probablement besoin de vous rapprocher de vos interlocuteurs rapidement sans éveiller les soupçons. C'est souvent le cas lorsque l'on cherche à obtenir des informations, à briser un secret ou à deviner l'identité d'un anonyme.

Prenons une situation précise comme nous l'avons fait dans le reste de cet ouvrage. Cette situation ne vous concernera peut-être pas mais cela n'a aucune importance. Elle nous servira avant tout de prétexte pédagogique.

Depuis le boom des smartphones, les applications « anti-vol » font fureur.

Ces applications vous permettent d'espionner l'utilisation de votre propre téléphone portable depuis votre ordinateur si quelqu'un vous le vole. Il ne s'agit ni plus ni moins que d'un mouchard que vous installez sur votre propre téléphone pour le surveiller en cas de problème.

Sur les forums, il est fréquent de lire des histoires du style : « on m'a volé mon téléphone et j'ai accès à tous les SMS, les photos, les e-mails et les identifiants Facebook de mon voleur. Que faire ? ».

À ce propos, un site génial a vu le jour. Il est tenu par un jeune homme qui s'est fait voler son téléphone. Jusque là, rien d'intéressant. Mais voilà : le voleur s'est fait piéger par une application anti-vol. Résultat, toutes les photos qu'il prend depuis le téléphone volé sont envoyées au propriétaire légitime… qui les expose sur son blog personnel. Jour après jour.

Life of a stranger who stole my phone
www.pandore.it/assf

Dans cette situation où vous espionnez l'utilisation de votre propre téléphone à distance suite à un vol, il est primordial d'agir intelligemment et sans brusquer les choses, surtout si vous arrivez à obtenir les coordonnées de votre voleur.

Dans la majorité des cas, les (mauvais) voleurs se connectent à leurs comptes Facebook, à leurs comptes Twitter ou à leurs

comptes e-mail juste après avoir volé le téléphone. Dans ce cas de figure, l'application de sécurisation que vous aviez installée au préalable vous enverra toutes les activités du voleur en temps réel. Aussi bien les messages qu'il écrit, que les photos qu'il prend. Sans oublier sa position GPS.

Vous vous retrouvez avec l'e-mail ou le profil Facebook de votre voleur. Que faire ? Quoi lui dire ? Comment l'aborder ?

Dans la suite du livre, nous allons apprendre à devenir rapidement proche de quelqu'un sur Internet en utilisant des biais psychologiques simples. Le vol de votre téléphone sera finalement le fil conducteur du chapitre.

IV) Quelles différences entre la manipulation classique et la manipulation virtuelle ?

Deux grandes différences jouent en notre faveur. D'une part, parler ou mentir à quelqu'un derrière notre écran est moins angoissant que lors d'un face à face réel. D'autre part, nous pourrons prendre tout notre temps pour réfléchir à nos réponses.

La seule différence qui nous désavantage par rapport à une discussion réelle est le manque de *feedbacks* (comprendre « de retours »). Sans avoir la personne en face de nous, on ne peut pas savoir si elle est contente, triste, angoissée ou si elle nous ment. Nous n'avons accès à aucun des indices habituels (langage du corps, son de la voix, etc.).

nous allons tout de même nous débrouiller pour exploiter quelques failles humaines. Même sans *feedbacks*.

3. Technique #1 : la synchronisation syntaxique

La synchronisation syntaxique est une technique de PNL bien connue. La PNL (programmation neuro-linguistique) est une discipline vaste et très critiquable qui vise à améliorer son bien-être et sa compréhension du monde grâce à des outils psychologiques et des théories neurologiques.

Revenons à la synchronisation. Il s'agit de calquer, le plus discrètement possible, la gestuelle et le vocabulaire de votre interlocuteur pendant une conversation pour qu'il s'identifie à vous inconsciemment et vous apprécie davantage.

Cette technique est utile dans de nombreuses situations : un rendez-vous amoureux, une négociation, une discussion à cœur ouvert pour remonter le moral d'un ami. Il y a quelques années, j'avais remarqué que Vladimir Poutine utilisait la synchronisation avec Obama, c'était très fin de sa part et très impressionnant à observer. Malheureusement, je suis incapable de remettre la main sur cet extrait vidéo.

Lorsque Obama remettait son nœud de cravate, Poutine en faisait autant. Lorsque Obama tournait la tête, Poutine tournait aussi la tête, etc.

Si vous voulez en savoir plus sur la synchronisation, je vous recommande cet article de *Sixième Sens*.

Apprendre la synchronisation PNL
www.pandore.it/aasp

Revenons-en à Internet.comment adapter la synchronisation gestuelle et vocale classique pendant une discussion sur un tchat, par SMS ou par e-mail ? Réponse : en se synchronisant sur la syntaxe de votre interlocuteur.

Il parle en SMS ? Parlez en SMS. Il écrit parfaitement bien ? Écrivez parfaitement bien. L'étape du *profiling* (voir la partie précédente) devrait vous aider à bien cerner les éléments distinctifs de sa syntaxe.

Ne pas synchroniser votre syntaxe sur celle de votre interlocuteur revient à arriver en costume cravate à une soirée pyjama. Vous créerez une rupture immédiate en agissant trop différemment.

Voici quelques pistes à explorer dans votre synchronisation. Tout n'est pas bon à prendre pour toutes vos futures conversations, à vous de faire le tri et de vous synchroniser sur ce qui semble le plus important pour la personne à qui vous parlez.

I) Les smileys (:-), :-(, :-D, etc.)

Les plus de 40 ans qui n'ont pas évolué avec l'informatique ne les utilisent pas beaucoup.

Au contraire, les utilisateurs habitués à Internet les utilisent régulièrement… voire à outrance. Il s'agit d'un moyen tellement ingénieux de faire passer des émotions par l'écran qu'il est dommage de s'en passer.

1. Si votre interlocuteur utilise majoritairement <u>un seul smiley</u>, faites comme lui ;

2. Si votre interlocuteur met un « nez » à ses smileys, faites la même chose :-) (le nez est le tiret qui sépare les yeux de la bouche) ;
3. Si votre interlocuteur n'utilise aucun smiley, n'utilisez aucun smiley.

II) La ponctuation

Votre interlocuteur utilisera peut-être des virgules, des points, des points de suspension… encore une fois le conseil est simple : calquez-vous sur lui.

S'il termine toutes ses phrases par un point, faites de même. S'il n'utilise aucune virgule, n'en utilisez pas non plus.

III) La longueur de ses phrases

Un autre élément de synchronisation à prendre en compte est le rythme des phrases. Par e-mail, certaines personnes écrivent des paragraphes de 20 lignes sans un seul retour à la ligne. Au contraire, d'autres aèrent régulièrement leurs messages.

Sur une messagerie instantanée, certains utilisateurs envoient une phrase par message. D'autres préfèrent envoyer plusieurs phrases par message.

Suivez le rythme de votre interlocuteur et recopiez-le.

IV) L'orthographe

Cela va vous sembler affreux si vous avez tendance à accorder une grande importance à l'orthographe… mais comme pour le reste, il est important de se synchroniser sur la qualité de

l'orthographe de votre interlocuteur. S'il écrit en SMS, mettez-vous à son niveau. S'il écrit bien, forcez-vous à bien écrire.

Écrire en bon français face à une personne qui écrit en langage SMS créera automatiquement une sorte de décalage social.

Imaginez un rappeur gangsta (« yo, mec ! ») qui discute avec un bourgeois du XVII^{e} siècle (« bonjour monseigneur. »). L'écart linguistique creuse un fossé qui semble insurmontable entre les deux hommes. Dans une moindre mesure, s'adapter au niveau orthographique de votre interlocuteur équivaut à éviter une situation de rupture sociale.

V) Quels autres détails faut-il prendre en compte ?

Il y en a beaucoup d'autres : le vocabulaire, la vitesse de frappe et la vitesse de réponse si vous discutez *via* une messagerie instantanée, l'utilisation des majuscules en début de phrase, les mots internet utilisés (« lol », « mdr », « wtf », etc.).

Fixez-vous au moins cinq contraintes de synchronisation pour être efficace. Autrement dit : après avoir analysé la syntaxe de votre interlocuteur, obligez-vous à vous synchroniser sur au moins cinq éléments différents. Cela me semble être le minimum recommandé pour être cohérent.

4. Technique #2 : Exploiter une conviction forte

Après avoir réussi à vous synchroniser sur votre interlocuteur, une bonne manière de vous rapprocher de lui consiste à exploiter l'une de ses convictions les plus fortes. C'est à dire

trouver quelque chose qu'il défend ou quelque chose qu'il déteste, pour vous mettre de son côté de manière complètement artificielle.

Tout le monde a des convictions à propos de choses et d'autres (politiques, écologie, philosophie d'un art quelconque, trait de personnalités, etc.). Il s'agit de trouver celle qui fera vraiment vibrer votre interlocuteur.

L'idée de cette technique consiste à orienter la discussion vers un sujet « sensible ». Il s'agit d'un sujet qui va captiver la personne à qui vous parlez. Un sujet qui fera en sorte qu'elle n'ait pas envie de vous supprimer de ses contacts, de fermer la conversation ou de vous ignorer.

Pour cela, il faudra faire preuve d'un peu de psychologie. Pour ma part, je cherche à découvrir ce que revendique être mon interlocuteur, ce qui le rend fier dans la vie. En d'autres termes, j'essaie de trouver ce qu'il répondrait instinctivement à la question suivante : « Qui es-tu, en deux mots ? ».

À cette question, certains répondraient par exemple instinctivement « je suis un passionné de foot et un bon joueur de foot ». Ils le clameraient haut et fort parce qu'ils en sont fiers, parce qu'ils vivent à travers cette passion, parce qu'ils respirent football, ils s'habillent football, parlent football. Bref, *football everywhere*.

À n'en pas douter, le fait qu'ils vivent à travers cette passion implique qu'ils ont des convictions liées à ce sujet. Ces convictions vont par exemple se traduire par une équipe préférée ou par des considérations plus philosophiques sur le sujet. Ils auront un avis sur le salaire des footballeurs, sur le comportement des joueurs dans les médias, etc.

En creusant dans cette direction, vous pourrez facilement trouver un appât pour tenir la discussion avec votre interlocuteur et le mettre dans votre poche. En quelque sorte, il s'agit de lancer un débat ou une discussion fertile qui fera forcément mouche.

Deux cas de figure malheureux peuvent se produire.

Premièrement, votre interlocuteur vit à travers une passion dont vous ne connaissez absolument rien. Dans ce cas, difficile de lancer une conversation sur le sujet, à moins de faire quelques recherches improvisées sur Google en simultané et faire semblant de savoir de quoi vous parlez. C'est tout à fait possible, mais ça demande une certaine agilité d'esprit. Une autre solution consiste simplement à creuser dans une autre direction et trouver une seconde passion, peut-être moins prenante, mais qui vous permettra d'être plus efficace.

Deuxième cas de figure problématique : votre interlocuteur semble n'avoir aucune passion. C'est assez fréquent, beaucoup de gens n'ont aucune passion clairement identifiable.

Lorsque cela arrive, je vous conseille d'orienter votre discussion autour de grands sujets sociétaux qui font forcément réagir les gens :

- Les derniers scandales people ;
- Le Front National ;
- La dernière série que tout le monde aime.

Bref, des sujets passe-partout ou un peu provoc. Il s'agit là de savoir mener une conversation naturellement et ce n'est malheureusement pas le sujet de ce livre. À vous de faire

preuve de suffisamment de psychologie pour intéresser votre interlocuteur. La technique des convictions a beau être efficace en théorie, vous n'allez pas entamer la discussion avec quelqu'un comme cela : « bonjour, tu trouves pas que le PSG est une équipe absolument nulle ? ».

Il faut toujours broder, faire preuve d'empathie et d'astuce pour amener la discussion là où vous voulez qu'elle aille.

5. Technique #3 : La méthode Columbo

Le célèbre détective Columbo est un manipulateur hors du commun : derrière ses airs de benêt se cache un grand génie. Sa stratégie du « profil bas » est sa marque de fabrique et c'est probablement ce qui le rend si efficace dans ses enquêtes. Les méchants ne se méfient jamais de lui. Lorsqu'ils comprennent que Columbo est loin d'être stupide, il est souvent trop tard pour eux et le détective a déjà résolu l'affaire, preuves à l'appui.

Vous devez garder tout cela en tête : pour manipuler quelqu'un et l'amener à dire (ou à faire) ce que vous voulez, il n'est pas nécessaire d'être quelqu'un d'important, d'intelligent, de beau ou de charismatique.

Il y a quelques années, j'ai appelé le standard d'une entreprise concurrente à la mienne en me faisant passer pour un étudiant qui recherchait des informations pour sa thèse. En posant quelques questions très naïves, j'ai obtenu des renseignements confidentiels sur l'entreprise en question. C'était l'objectif de mon coup de fil, j'ai eu la chance de tomber sur un employé pas très avisé au téléphone.

En me faisant passer pour un étudiant naïf, j'ai en quelque sorte désactivé les systèmes de surveillance de mon interlocuteur.

Cette technique, appliquée d'une manière ou d'une autre, pourra vous être extrêmement utile pour aborder vos cibles sur Internet. Ne cherchez pas toujours à leur ressembler ou à les impressionner. La technique inverse peut être extrêmement efficace.

Endormez la vigilance de votre interlocuteur, faites lui penser qu'il n'a rien à craindre de vous. Si votre stratagème fonctionne, il sera rapidement gonflé d'orgueil et de confiance.

Vous voulez obtenir des aveux ou des informations confidentielles ? Les personnes dotées d'un ego démesuré sont généralement très bavardes lorsqu'il s'agit de parler d'elles puisqu'elles adorent ça.

Dans son livre *Les 48 lois du pouvoir,* Robert Greene explique comment Galilée a su saisir une opportunité professionnelle importante en mettant en valeur ses interlocuteurs (une riche famille de mécènes) au lieu de se mettre lui-même en avant (loi n°1).

- Certains animaux utilisent cette technique du profil bas pour capturer leurs proies ;
- Les joueurs de poker professionnels utilisent cette technique lorsqu'ils bluffent ;
- Les commerciaux rusés qui veulent des informations sur des clients utilisent cette technique ;

- Les manipulateurs qui veulent infiltrer un groupe d'inconnus utilisent cette technique.

6. Technique #4 : Développez votre charisme sur Internet

Dans la mesure où vous n'essaierez pas de vous synchroniser à l'écrit sur votre interlocuteur en recopiant ses mimiques typographiques, il existe quelques trucs pour développer votre charisme sur Internet.

Avoir du charisme, c'est donner envie aux gens de vous écouter, de vous croire, de vous suivre. Le charisme fonctionne donc aussi sur Internet. Il existe des moyens simples pour rendre vos écrits plus percutants, plus intéressants. Bref, plus charismatiques.

I) L'orthographe

Je ne vais pas m'étendre sur ce point : les « gen ki fon dé faut d'ortograf » ne sont pas crédibles sur Internet. Ils énervent parce qu'ils manquent cruellement de respect à leurs interlocuteurs. Personne n'a envie de les lire.

Si vous voulez être pris au sérieux, concentrez-vous là-dessus. On a tous le droit de faire des fautes en écrivant, ce n'est pas le problème. Mais respectez le minimum légal en matière d'orthographe et de typo pour rester crédible.

II) La longueur des phrases

Ce point est primordial. Si vous essayez de convaincre à l'écrit, réduisez absolument la taille de vos phrases. On ne peut pas convaincre rapidement et efficacement en écrivant des phrases à rallonge parce qu'on perd trop facilement le lecteur et un lecteur qui se perd dans une phrase, c'est un lecteur qui ne vous écoute plus, donc aucune chance d'influencer quelqu'un qui ne vous lit plus, ça parait logique alors faites gaffe et relisez bien vos phrases et si vous les trouvez trop longues, coupez-les avec un point, une virgule ou que sais-je, on a beaucoup de choix grâce à la richesse de langue française ! Vous voyez ce que je veux dire ?

Préférez des phrases courtes. Efficaces. Imaginez qu'une voix off lit votre texte. Ces voix lisent toujours des phrases percutantes très courtes. C'est un peu dans cet esprit qu'il faut écrire un argumentaire.

III) L'utilisation des parenthèses

Ne mettez jamais des choses importantes entre parenthèses. Beaucoup de gens zappent le contenu entre parenthèses. Normal : des parenthèses indiquent un contenu facultatif. Votre message doit avoir le même sens, avec ou sans le contenu entre parenthèses.

J'évite d'utiliser des parenthèses dans mes mails importants parce qu'elles ont tendance à casser l'attention de mon lecteur. S'il était concentré et qu'il lit un contenu mis entre parenthèses, j'ai peur qu'il relâche son attention (« ah, c'est entre parenthèses donc je m'en fiche ») et qu'il n'arrive pas à se reconcentrer correctement par la suite. En clair, les

parenthèses cassent le rythme de lecture. Plus on casse le rythme de lecture, plus on risque de perdre le lecteur (qui a plein d'autres choses à faire que de nous lire).

IV) Les premiers mots d'une phrase

La meilleure solution pour donner envie d'être lu, c'est d'avoir des débuts de phrases percutants. C'est comme dans la vraie vie. Quand quelqu'un commence toutes ses phrases par « ben » ou par « heu », on a envie de le zapper.

Sur Internet, évitez de commencer vos phrases par une conjonction de coordination (mais, ou, et, donc, or, ni, car). Ces petits mots cassent le rythme de lecture. Privilégiez des débuts de phrases qui ont du punch. Le mieux ? Commencer une phrase par « vous » (ou « tu ») pour que votre lecteur se sente immédiatement concerné.

V) Utilisez la forme active et des tournures de phrases simples

Beaucoup de gens écrivent des lettres de motivation avec des tournures complètement alambiquées. Pour casser un rythme de lecture, il n'y a pas mieux que de commencer une phrase par un adverbe :

« Ayant de grandes compétences dans le développement de produits, je… ». C'est pénible à lire. La phrase commence à l'envers, et cette virgule… grr !

« J'ai de grandes compétences dans le développement de produits. » : ça va droit au but, on n'en demande pas plus. Pas de ponctuation inutile, un rythme soutenu et efficace.

préférez la forme active à la forme passive :

« N'ayant pas eu le temps aujourd'hui, le dossier du client XYZ n'a pas pu être clôturé ». Pénible à lire.

« Je n'ai pas eu le temps de clôturer le dossier du client XYZ aujourd'hui ». Encore une fois, c'est efficace. Les gens ne demandent rien d'autre que de l'efficacité, ils se moquent de vos envolées lyriques.

VI) L'habit ne fait pas le moine

Cette assertion est déjà complètement fausse dans la vie réelle. L'apparence est notre premier critère de jugement (qu'il soit acerbe ou pas). Sur Internet c'est la même chose : si votre texte ne donne pas envie d'être lu, personne ne le lira. Un texte lisible est un texte aéré, avec plusieurs paragraphes et pourquoi pas avec des images et des sous-titres au milieu si vous rédigez un document complet.

Autre chose : dans certains mails, je mets en gras les mots-clefs importants. Le but, c'est de pouvoir relire le mail **uniquement** en lisant les mots en gras.comme ça si le lecteur est pressé, il lit les mots en gras et a tout compris au message. Si les mots en gras sont percutants, il aura envie de lire en détail ce que je lui ai envoyé.

L'autre raison d'utiliser du gras, c'est d'ajouter des points d'accroche visuels à votre texte. Un texte sans aucune accroche visuelle est difficile à lire sur un écran. En rajoutant quelques parties importantes en gras (une par paragraphe en moyenne), vous offrez des points d'accroche visuels à vos lecteurs. Ils auront plus facilement envie de se plonger dans votre texte.

VII) Relire oui, mais pas n'importe quand

Si l'envoi de votre message peut attendre, alors relisez-le le lendemain. Pas avant. Une nuit de sommeil remettra vos émotions et vos idées à zéro. Si vous l'écrivez un matin à 10h, ne faites pas une relecture le soir à 19h. Attendez **vraiment** le lendemain matin, c'est important.

Pensez aussi à relire à haute voix et pas seulement dans votre tête. En lisant à haute voix, vous vous surprendrez à dire des choses qui ne sont pas écrites telles quelles dans votre texte. Cela veut dire que la version écrite ne vous convient pas et qu'instinctivement, votre cerveau a remanié la phrase en la lisant. Ce phénomène ne survient pas en lisant de tête.

VIII) Le cœur du message ? Dans le « P.-S. ».

Si vous envoyez un long mail et qu'au milieu du blabla vous avez besoin d'insister sur quelque chose de très important, mettez-le en post-scriptum.

> Cher Monsieur,
>
> blabla…
>
> Cordialement,
> John Doe
>
> P.-S. : j'attends une réponse dans la semaine pour le devis que je vous ai envoyé.

Le P.-S. est clairement l'élément le plus important d'un e-mail. Étrange à première vue, on pourrait penser qu'il s'agit plutôt

d'un élément rajouté après coup, sans grande importance. Et bien non : vous devez lui accorder sa chance. Il est un puissant levier d'influence. Si votre mail est long et plein d'informations, c'est le P.-S. dont vos lecteurs se souviendront le plus. Et il est même probable que ce soit la première chose à laquelle ils répondent dans leur message de retour. Essayez si vous ne me croyez pas !

Conclusion

Ce chapitre sur la manipulation Internet s'arrête là. Faisons un petit récapitulatif de tout ce que vous y avez découvert :

1. Il est important de profiler ses interlocuteurs pour bien les cerner. Pour cela, fiez-vous à tous les indices qui s'offrent à vous : syntaxe, photos de profil, pseudonyme, etc. ;

2. Profiler vos interlocuteurs vous aidera à optimiser vos relations en abordant des sujets de conversation plus percutants ou en mettant en avant vos ressemblances avec eux par exemple ;

3. Il existe énormément de techniques pour manipuler quelqu'un par écran interposé. Voici les trois principales que vous devez retenir : manipuler son ego, se synchroniser sur lui, soigner votre apparence virtuelle.

N'oubliez pas : il n'existe pas de « vie réelle » et de « vie non-réelle ». La vie sur Internet est bien réelle. Elle est simplement virtuelle. Cela implique que toutes les théories psychologiques qui s'appliquent à la vie en dehors d'Internet s'appliquent aussi

sur Internet. À vous d'imaginer des applications intelligentes lorsque vous en aurez besoin.

Si le sujet vous intéresse, pensez à visiter les deux sites web de Félix Boussa. Ils regorgent d'informations sur la psychologie sociale, la manipulation et le mentalisme.

Apprendre à manipuler.com
www.apprendre-a-manipuler.com

Le magazine Sixième Sens
www.sixiemesens-lemag.fr

Étude de la stylométrie

1. Introduction

La stylométrie est un mélange de linguistique et de statistique. Ce procédé permet d'identifier l'auteur d'un texte en analysant le contenu des phrases, les expressions ou même la ponctuation du texte en question.

La stylométrie se base sur des dizaines de métriques bien précises pour décortiquer un document :

- L'emploi de certains temps ;
- L'emploi des majuscules ;
- L'emploi de certains acronymes ;
- Des fautes d'orthographe récurrentes ;
- La ponctuation ;
- L'utilisation de smileys (sur Internet uniquement) ;
- Les formulations des phrases ;
- Les « mots de connexion » entre les phrases ;
- L'utilisation de mots rares.

En analysant plusieurs documents A et B d'un auteur préalablement connu, il est possible de procéder à une étude stylométrique afin de savoir si un document C a été écrit par ce même auteur ou non. La police criminelle utilise fréquemment la stylométrie dans ses enquêtes, notamment lorsqu'il s'agit de retrouver l'auteur d'une lettre de menace ou de chantage.

Les chercheurs en histoire ou en littérature font aussi usage de la stylométrie pour retrouver les auteurs de textes orphelins. Par exemple en 1987, deux chercheurs ont ainsi réussi à attribuer la paternité d'un poème à Shakespeare grâce à une étude stylométrique.

Il ne faut pas confondre la graphologie avec la stylométrie. La graphologie est une théorie empiriste sans fondement scientifique qui consiste à déterminer le profil émotionnel et psychologique d'un individu en analysant la forme de son écriture manuscrite ou sa signature. La stylométrie consiste à analyser la syntaxe, l'orthographe, la ponctuation et le vocabulaire d'un texte afin de reconnaître son auteur.

2. Quand utiliser la stylométrie au quotidien ?

Voici quelques situations prises au hasard qui pourront vous arriver (ou qui vous sont peut-être déjà arrivées), et dans lesquelles la stylométrie vous rendra service. Chaque situation est à adapter à votre propre expérience, bien entendu.

1. Un collègue de travail ou un voisin vous a laissé un mot anonyme, vous aimeriez le démasquer ;
2. Une personne louche, *a priori* sous une fausse identité, vous contacte par Internet. Vous suspectez un ami de vouloir vous piéger ;
3. Vous cherchez à analyser l'écriture d'un proche à travers ses messages pour décrypter son état émotionnel ;

4. Au travail, vous avez souvent affaire à la boite mail institutionnelle d'un partenaire. Plusieurs personnes l'utilisent et répondent aux messages sans signer, vous aimeriez deviner facilement qui se cache derrière chaque message ;

5. Repérer les escrocs sur Internet en exploitant leurs faiblesses linguistiques lorsqu'il s'agit d'étrangers. Pratique pour éviter les escrocs de la Côte d'Ivoire par exemple, qui agissent en toute impunité sur Leboncoin, Facebook et dans nos boites e-mails ;

6. Vous souhaitez aller plus loin dans le *profiling* virtuel en décodant plus en profondeur la stylométrie des messages de vos interlocuteurs.

Par la suite, j'illustrerai une étude stylométrique dans le cadre de la situation 2. C'est-à-dire un de vos anciens collègues qui cherchent à vous piéger en vous contactant sous une fausse identité.

3. La stylométrie et l'informatique

Il est aujourd'hui inconcevable qu'un professionnel ayant besoin d'étudier la stylométrie d'un texte s'amuse à le faire à la main. Cela consisterait à compter manuellement les mots, les lettres, les accents, à noter l'usage de chaque signe de ponctuation, la fréquence d'utilisation de tel ou tel temps, de telle ou telle conjonction, etc. Quel travail ingrat, quand on sait de quoi est capable un ordinateur !

Il existe un logiciel de référence dans le domaine de la stylométrie informatisée : j'ai nommé JGAAP. Il est gratuit,

open-source et compatible Linux, Windows et OS/X (des fois on peut dire merci à Java).

Télécharger JGAAP
www.pandore.it/ajg

JGAAP n'est pas très compliqué à utiliser, vous trouverez d'ailleurs un guide de prise en main très bien fait sur le site officiel des développeurs. Il faudra tout de même prendre une petite heure pour bien cerner le logiciel, peut-être un peu plus si vous n'avez aucune notion en mathématique.

JGAAP vous demande trois choses :

- Quelques textes qu'il va apprendre et dont vous connaissez les auteurs au préalable ;
- Un ou plusieurs documents dont vous ne connaissez pas l'auteur ;
- Quelques réglages pour procéder à l'analyse des textes orphelins.

Lorsque vous lui aurez donné tout cela à manger, il vous dira si les textes orphelins appartiennent ou non à l'un des auteurs connus que vous lui avez proposé au départ.

Dans la suite du chapitre, nous n'allons pas utiliser JGAAP ou un autre logiciel du même genre. Nous ferons nos analyses stylométriques à la main, sans prendre en compte des statistiques complexes comme le fait JGAAP.

Vous avez déjà découvert quelques critères stylométriques dans le chapitre précédent grâce au *profiling* virtuel. Allons un peu plus loin.

4. Les métriques de base de la stylométrie

Vous connaissez déjà quelques métriques utilisables pour vous synchroniser avec votre interlocuteur. Je reprendrai brièvement ces métriques pour les replacer dans le cadre de la stylométrie avant d'en expliquer de nouvelles.

Ayez bien en tête cela tout au long du chapitre : la stylométrie permet de retrouver l'auteur d'un texte orphelin facilement, à condition d'émettre une hypothèse sur l'identité de cet auteur. Vous devrez comparer le texte ou les messages orphelins avec les écrits d'une tierce personne que vous suspectez d'être l'auteur. En d'autres termes, la stylométrie n'est pas un moyen magique de connaître l'auteur d'un texte. Il s'agit uniquement de vérifier qu'un texte appartient bien à telle ou telle personne.

I) Les smileys

Les smileys sont des éléments stylométriques que vous exploiterez principalement sur Internet. Une même personne a tendance à toujours utiliser la même gamme de smileys lorsqu'elle participe sur un forum ou lorsqu'elle discute *via* une messagerie instantanée. Pas grand-chose à dire sur ce point, l'étude stylométrique des smileys est triviale.

II) La ponctuation

L'étude de la ponctuation est extrêmement intéressante. Il existe de nombreux points à analyser. En voici une liste non exhaustive :

- Fréquence d'utilisation des virgules ;
- Surabondance des signes de ponctuation (« !!!!!! » ou « ???? ») ;
- Fréquence d'utilisation des points-virgules (caractère assez peu utilisé qui distingue facilement un auteur d'un autre) ;
- Utilisation originale des espaces typographiques autour des signes de ponctuation. Par exemple : « pardon ? » au lieu de « pardon ? » ou « ok . » au lieu de « ok. ».

III) La typographie et l'aspect général du texte

Là encore vous pourrez observer un grand nombre de détails :

- L'utilisation des majuscules ;
- L'utilisation de guillemets simples et doubles, de cédilles, d'accents… ;
- L'aération du texte en paragraphe ainsi que les sauts de ligne (simples ou double) ;
- La présentation générale du texte (listes à puces fréquente ou non, citations fréquentes ou non) ;
- Utilisation de styles de police comme : gras, souligné, italique et fréquence d'utilisation de ces styles.

IV) L'orthographe et la conjugaison

Beaucoup de choses à voir ici :

- L'emploi de certains temps en particulier. Certaines personnes parlent plus au présent qu'au futur par exemple ;
- Les abréviations sur certains mots (« qq » au lieu de « quelques », « cmb » pour « combien », etc.) ;
- Les fautes d'orthographes récurrentes. Ne pas confondre les gens qui massacrent le français et ceux qui font quelques fautes occasionnelles en s'appliquant du mieux qu'ils peuvent. Chez ces derniers, les fautes sont plus facilement exploitables, puisqu'elles sont plus rares et plus ciblées.

V) Le vocabulaire

Pour terminer, il est possible d'analyser un texte en exploitant des éléments propres au vocabulaire de l'auteur :

- Les mêmes mots qui commencent fréquemment ses phrases ;
- L'emploi de certains acronymes et la manière de les écrire (« SNCF » ou « S. N.C. F » par exemple) ;
- Les mots de connexion entre les phrases ;
- L'utilisation de mots « rares ».

5. Cas pratique d'une étude stylométrique réelle

Prenons une situation de harcèlement concrète.

Vous recevez une invitation Facebook d'une certaine « Charlotte Bidule » qui souhaite devenir votre amie. Vous trouvez son profil louche : peu de photos, peu d'interactivités naturelles avec d'autres amis. Vous suspectez rapidement Martin, un ancien collègue avec qui vous avez perdu contact en de mauvais termes il y a 3 mois.

À l'époque, Martin vous avait raconté qu'il s'amusait à créer de faux comptes Facebook pour harceler et se moquer des gens qu'il n'appréciait pas par pure vengeance.

Cette situation peut vous paraître grotesque si vous n'avez jamais entendu parler du « stalking » (« harcèlement » en français). Le *stalking* sur Internet est extrêmement repandu, surtout chez les adolescents.

Le principe est simple : Bob crée un faux compte Facebook soit pour insulter Alice et la harceler violemment, soit pour la séduire et lui briser le cœur en l'humiliant.

Détruits, plusieurs centaines d'adolescents (recensés par les médias) se sont suicidés à cause de cette pratique. Il n'est donc pas idiot de chercher à s'armer. Pour nous, pour nos enfants, et pour notre entourage.

Le canular qui tourne mal
www.pandore.it/acqt

Revenons à notre cas pratique : comment profiter de la stylométrie pour savoir si votre collègue Martin se cache effectivement derrière ce compte plus que louche qui vous a ajouté récemment ?

I) Première étape : faire parler Charlotte

Discutez avec la personne et reportez-vous aux métriques que je vous ai présentées précédemment. Repérez les grandes particularités de son style d'écriture en répertoriant chaque métrique dans un document texte ou un fichier Excel :

- Point-virgule : jamais utilisé ;
- Majuscule en début de phrase : rare ;
- Point en fin de phrase : très fréquent ;

Ainsi de suite avec les autres mesures stylométriques.

II) Deuxième étape : repérer les incohérences

Certains harceleurs rusés se forceront à déformer leur stylométrie naturelle pour donner un caractère particulier à leur(s) personnage(s). Par exemple : en écrivant en SMS, ou avec plein de smileys.

Dans ce cas précis où votre *stalker* s'amuse à changer son écriture, vous pourrez remarquer assez rapidement de grosses incohérences stylométriques. À moins d'avoir étudié la stylométrie comme vous le faites aujourd'hui, peu de gens sont capables de dissimuler instinctivement leur véritable façon d'écrire pendant une discussion un peu longue.

Une incohérence stylométrique consiste par exemple à écrire tantôt en SMS, tantôt en bon français. Sans régularité. Changer sa manière d'écrire demande un réel effort intellectuel que peu de gens sont capables à faire jusqu'au bout.

Mettre des majuscules ou de la ponctuation devient rapidement un réflexe lorsque l'on est habitué à soigner son langage sur Internet. Un mauvais harceleur fera peut-être l'effort de saboter son français au départ mais faites-moi confiance : il reprendra rapidement ses bonnes habitudes en mettant des majuscules en début de phrases et en utilisant une ponctuation cohérente.

Cette deuxième étape vous permettra de savoir si la personne qui vous parle joue un rôle, ou non.

III) Troisième étape : comparer Martin et Charlotte

Une fois votre étude terminée, il est temps de comparer vos résultats avec une étude stylométrique sur l'écriture de Martin.

Cherchez un document, un e-mail ou un message quelconque que Martin vous aurait envoyé à l'époque et comparez vos résultats avec ceux de votre étude sur « Charlotte Bidule ».

Dans une grande majorité des cas, le résultat est assez net :

- Soit les résultats de vos études stylométriques sont très proches ;
- Soit les résultats de vos études stylométriques sont très différentes.

En stylométrie, il est assez rare de se retrouver nez-à-nez avec des résultats mitigés lorsqu'on étudie manuellement les auteurs.

Afin d'affiner votre conclusion sur Charlotte et Martin, je vous propose de découvrir trois erreurs très classiques que commettent les stylographes débutants.

6. Trois erreurs à ne pas commettre lors d'une étude stylométrique

I) Considérer tous les types de messages exploités comme équivalents

En clair, comparer l'écriture d'un SMS avec l'écriture d'un e-mail n'est absolument pas pertinent. Même une personne habituée à soigner son français sur un clavier peut se laisser tenter par quelques raccourcis linguistiques lorsqu'elle utilise un téléphone (en utilisant moins de ponctuation, moins de majuscules, etc.).

II) Donner le même poids à tous vos observations

Certaines métriques sont plus importantes que d'autres. Par exemple beaucoup d'internautes oublient l'espace avant un point d'exclamation. Si deux de vos interlocuteurs oublient de mettre un espace avant un signe de ponctuation double, cela ne veut pas dire qu'il s'agit de la même personne.

En revanche, une même faute d'orthographe rare (par exemple écrire « bonjours ») fréquemment employée par deux identités

virtuelles différentes est un signal assez fort dans le cadre d'une étude stylométrique.

III) Faire de la graphologie

Étudier l'écriture d'une personne ne vous permet pas de deviner ses traits de personnalité comme le prétend la graphologie. Dans un contexte bien particulier, la stylométrie permet de « cold-reader » vos interlocuteurs comme Félix vous l'a expliqué en détails dans le chapitre précédent.

En revanche, des phrases courtes et sèches n'impliquent pas que votre interlocuteur soit quelqu'un de sévère ou de méchant dans la vie. Des phrases pleines de fautes n'impliquent pas que votre interlocuteur soit quelqu'un de stupide. Enfin, ce n'est pas parce que votre interlocuteur saute beaucoup de lignes et écrit souvent en majuscules qu'il faut automatiquement diagnostiquer un complexe d'infériorité… contrairement à ce que prétendent les graphologues.

Ce qu'il faut retenir de la stylométrie

Il existe deux types d'études stylométriques :

L'étude informatisée, qui se base sur des probabilités et des statistiques assez complexes. Ce type d'étude est menée par ordinateur, généralement par les policiers et par les historiens. Des logiciels gratuits vous permettent de vous amuser vous aussi !

L'étude manuelle, qui se base sur l'observation des caractéristiques de l'écriture d'un individu. C'est celle que vous serez amené à faire régulièrement lorsque vous enquêterez sur quelqu'un.

La stylométrie vous aidera non seulement dans vos futures enquêtes, mais elle est aussi un excellent moyen d'améliorer vos compétences en *cold-reading* virtuel et en synchronisation.

Enfin, vos connaissances en stylométrie vous permettront de devenir plus facilement anonyme sur Internet. C'est ce que nous allons voir très en détails dans le chapitre suivant.

Sources :

- Contribution de la métrique à la stylométrie : http://www.pandore.it/acst par Valérie Beaudouin et François Yvon (consulté le 5 juin 2014).
- La stylométrie et son application en OSINT : http://www.pandore.it/asfa par Félix Aimé (consulté le 5 juin 2014).

Comment se protéger du *doxing* ?

1. Introduction

Après avoir étudié le *doxing*, le social engineering et la stylométrie, vous connaissez les principaux moyens de pénétrer dans la sphère numérique d'un individu. Vous connaissez les pièges et quelques leviers, mais vous ne savez pas forcément vous en protéger personnellement.

Le fait d'apprendre à attaquer n'a rien de malsain. Selon moi, c'est un axe pédagogique plus efficace que la « prévention à papa » qui vous répète ce que vous n'avez pas le droit de faire sur le web.

Soyons clair : la protection de la vie privée et la contre-manipulation s'apprennent par l'expérience. Les enfants qui font du vélo dans la rue commencent à faire plus attention à partir du jour où ils se sont pris une bonne gamelle. Pour le *doxing* c'est la même chose : les internautes qui font attention sont ceux qui ont déjà été piégés. Ce chapitre vous servira à prendre une longueur d'avance et, je l'espère, à éviter vos premières gamelles.

Malheureusement, il y aura toujours quelqu'un de plus malin que vous qui arrivera à exploiter une faille à laquelle ni vous ni moi n'avons pensé. Restez vigilant. Pas paranoïaque, juste vigilant. N'oubliez pas que tout ce que vous apprendrez ici ou ailleurs ne sera jamais suffisant.

À ceux qui s'offusqueraient des conseils qui suivront : l'anonymat sur Internet peut servir à nuire, j'en ai bien

conscience. Malheureusement, ceux qui cherchent à devenir invisible pour harceler, pirater ou faire le mal sur Internet n'ont pas attendu la sortie de ce livre. N'importe quel bidouilleur du dimanche connaît les procédés d'anonymisation. Il n'y a rien d'illégal ou de secret dans ce que vous découvrirez. C'est avant tout du bon sens, associé à quelques explications techniques.

D'autre part, il est naïf de penser que toutes ces techniques suffiraient à éviter la justice dans le cas d'un délit. L'affaire PRISM de la NSA nous a appris quelque chose à ce sujet : les renseignements intérieurs (et extérieurs) ont une longueur d'avance sur nous depuis des années.

Maintenant que les choses sont claires, commençons.

2. Sécurisez votre connexion Internet

Dans le premier chapitre du livre, vous avez découvert le *tracking link*. Cet outil permet de connaître entre autres l'adresse IP d'un internaute sans difficulté. Cette adresse IP permet ensuite d'obtenir la localisation géographique précise de l'individu et d'autres informations moins percutantes.

Très pratique quand c'est vous qui en profitez… mais inversement, comment vous en protéger ? Autrement dit, comment camoufler votre adresse IP pour éviter de vous faire pister et géolocaliser à votre insu ?

Il existe principalement quatre méthodes qui permettent de changer votre adresse IP pour surfer plus anonymement. Cerise sur le gâteau : certaines de ces méthodes permettent aussi de sécuriser votre connexion Internet.

Cette partie étant assez technique, j'ai préféré la déporter sur le blog du livre. Vous y trouverez des explications claires et illustrées.

Comment devenir (réellement) anonyme sur Internet ?
www.pandore.it/acda

3. Cacher votre *user-agent*

Rappelez-vous le premier chapitre : l e *user-agent* donne beaucoup d'infos sur vous. Il est possible de connaître votre navigateur et votre système d'exploitation avec précision.

Un pirate pourrait se servir de ses informations pour lancer une attaque sur votre machine s'il découvrait par exemple que vous utilisez un système d'exploitation non mis à jour, ou un navigateur obsolète.

Dans une autre situation, un bon *doxer* pourrait tracer votre portrait électronique comme nous l'avons vu précédemment.

Il existe des extensions de navigateurs très simples à installer et à utiliser pour cacher votre *user-agent*. Tout est détaillé dans cet article du blog :

Comment changer et camoufler votre user-agent ?
http://www.pandore.it/acua

4. Éviter le *tracking* par cookies

Les cookies sont des petits fichiers que les sites web peuvent déposer sur votre ordinateur vous enregistrer des informations à votre sujet. Ils sont massivement utilisés pour cibler la publicité qui s'affiche sur votre écran à longueur de temps.

Les navigateurs récents disposent tous d'un mode « navigation anonyme » ou « navigation privée » qui permet de ne pas garder les cookies sur votre ordinateur lorsqu'un site en dépose.

Pour surfer en navigation privée, cherchez dans le menu principal de votre navigateur, vous trouverez vite. Une nouvelle fenêtre s'ouvrira avec une petite icône bien particulière (souvent un masque ou une personne masquée). Tous les sites que vous ouvrirez dans cette nouvelle fenêtre pourront enregistrer des cookies sur votre ordinateur mais ceux-ci seront automatiquement détruits lorsque vous fermerez la fenêtre. De quoi être tranquille !

Si vous désirez bloquer les cookies *ad vitam æternam*, vous pouvez bidouiller les réglages de votre navigateur et décocher la case « autoriser les cookies ». Cette manipulation peut toutefois empêcher certains sites de fonctionner, car les cookies ne servent pas seulement à vous inonder de publicités. Ils servent aussi à améliorer votre expérience sur le web, sans que vous ne vous en rendiez compte.

5. Évitez de donner votre adresse e-mail

Donnez votre e-mail à des sites (ou des personnes) un peu louches peut devenir gênant. Si vous avez envie de garder votre e-mail personnel propre et à l'abri des spammeurs et autres hurluberlus du web, il existe deux solutions.

Le site yopmail.com permet de créer en un clic n'importe quelle boite mail du type « machin. truc@yopmail.com » et de voir les courriers qui ont été envoyés à cette adresse.

Lorsque vous vous inscrivez sur un site louche (ou même lorsqu'on vous oblige à donner votre e-mail dans la vie réelle), mettez n'importe quelle adresse qui termine par « @yopmail.com » et allez relever votre courrier sur le site de Yopmail.

Cette méthode cependant a deux défauts.

Yopmail et ses concurrents sont souvent bardés de pub et la navigation sur leurs sites est parfois pénible et assez lente. Pour palier à cela, vous pouvez utiliser SpamGourmet.com qui permet de créer des e-mails poubelles qui redirigent vers votre e-mail personnel classique. Ces redirections poubelles s'autodétruisent au bout d'un moment, ce qui évite aux spammeurs de pouvoir continuer à vous spammer.

Le second problème de Yopmail réside dans le fait que les adresses jetables commencent à être massivement bannies par la majorité des sites web. Il est de plus en plus difficile de s'inscrire avec ce type d'adresse.

Il existe alors une deuxième méthode, plus sûre, plus pratique, plus efficace. Elle demande un peu de débrouillardise. Vous la trouverez expliquée sur le blog.

Créez votre propre "fournisseur de mails"
pour survivre sur Internet
www.pandore.it/acfe

6. Fausser l'étude stylométrique

C'est souvent à cette étape que les apprentis « anonymes » se font avoir : la stylométrie. Ils ne cherchent pas à camoufler leur écriture et se font démasquer assez facilement par des proches ou des internautes qui les connaissent sous leur vraie identité.

En étudiant la stylométrie, vous avez découvert des métriques un peu obscures que vous ne suspectiez probablement pas.

Lorsque vous souhaiterez devenir anonyme, il sera désormais primordial d'y repenser et de jouer avec ces nouveaux concepts lorsque vous écrirez un message :

- Mettez des espaces au hasard autour des virgules ;
- Oubliez des majuscules ;
- Faites des fautes récurrentes sur la conjugaison d'un temps (toujours le même) ou sur une règle de grammaire ;
- Utilisez des smileys exotiques.

Relisez bien le chapitre sur la stylométrie et essayez de jouer avec un maximum de métriques de manière cohérente. Ne

cherchez pas à en faire trop ou vous risquerez de perdre en cohérence rapidement.

Ne partez pas du principe que les gens sont trop bêtes pour analyser la stylométrie. Au contraire, partez toujours du principe que les personnes avec qui vous parlez ont lu ce livre.

7. « Googlez » régulièrement votre nom et nettoyez les résultats

Le *doxing* se pratique naturellement sur Google à l'heure où j'écris ces lignes. Il est donc tout naturel de vérifier régulièrement ce que Google sort à votre sujet.

Tapez votre nom, votre nom avec votre ville, votre pseudonyme principal et ouvrez dans plusieurs onglets séparés tous les résultats qui semblent vous concerner.

Vous serez parfois surpris de voir apparaître en première page les résultats d'un de vos profils privés sur un site de streaming de musique, sur un site de jeux-vidéos, sur un forum de discussion ou que sais-je encore.

Pour faire supprimer un résultat des recherches Google, vous avez deux solutions :

1. Soit vous supprimez le contenu à la source, c'est à dire directement en traitant avec le site web qui publie vos informations ;
2. Soit vous demandez à Googler de supprimer le résultat de son index. Dans ce cas, il faut que le résultat en question viole certaines règles en matière de vie privée.

Détaillons chacune des deux situations plus en profondeur.

I) Méthode 1 : supprimer le contenu à la source

La CNIL (Commission Nationale Internet et Liberté) est chargée, en France, de garantir le respect des droits et de la vie privée des internautes Français. Cette CNIL, loin d'être l'organe le plus efficace et le plus pro-actif de notre État, a tout de même donné naissance à quelque chose de sympa : la loi « informatique et liberté » de 1978.

Cette loi permet entre autres à chaque internaute français de demander la modification, l'obtention ou la suppression d'une partie ou de l'intégralité de ses données personnelles numériques stockées par une entreprise qui opère sur le territoire français.

Avant d'en arriver à invoquer cette loi, je vous conseille de fouiller dans la documentation du site en question ou dans vos paramètres pour trouver un lien « supprimer mon compte ». Une option « rendre mon profil privé » est une alternative intéressante.

S'il s'avère que le site ne vous offre pas la possibilité de supprimer votre compte vous-même, cherchez un moyen de les contacter et invoquez cette fameuse loi 1978. Vous trouverez un modèle type de courrier à envoyer (par voie postale ou par e-mail selon les dispositions de l'entreprise) sur le blog officiel du livre :

Comment porter plainte à la CNIL quand on se moque de vous ?
www.pandore.it/acnil

Si l'entreprise en question refuse de supprimer le contenu du site, vous pouvez envoyer une mise en demeure à la CNIL pour qu'ils fassent pression de leur côté. À titre personnel, je n'ai eu aucune expérience concluante en demandant de l'aide à la CNIL. Peut-être un simple manque de chance ?

Une fois le contenu réellement supprimé du site qui pose problème, attendez une ou deux semaines avant de le voir disparaître des résultats Google, sinon plus dans le pire des cas.

II) Méthode 2 : demander à Google de supprimer le résultat

Google accepte volontiers de supprimer des résultats de son index de recherche à conditions que ces résultats fassent mentions des types d'informations suivants :

- Numéros d'identification nationaux ;
- Numéros de comptes bancaires ;
- Numéros de cartes de paiement ;
- Images de votre signature manuscrite (celle que vous faites sur vos chèques par exemple).

En dehors de ces quatre situations, Google refusera de faire supprimer une page qui vous concerne de ses résultats.

Vous avez peut-être déjà compris la ruse : faire apparaître, si possible, une de ces quatre informations sur la page que vous souhaitez faire disparaître de Google.

Prenons une situation concrète : en tapant votre nom dans Google, s'affiche votre profil sur le site « passion-armes-a-feu.com ». Rien ne vous interdit d'être passionné par les armes. Simplement, il est compréhensible que vous ne souhaitiez pas afficher l'information publiquement sur votre page de recherche Google.

Disons aussi que le site *passion-armes-a-feu.com* n'est plus maintenu par personne. Le webmaster est parti, plus personne ne répond à vos e-mails demandant la suppression de votre profil. Malgré tout, vous pouvez vous connecter sur votre compte *passion-armes-a-feu.com* et modifier vos informations.

L'astuce consiste à rendre publique votre signature manuscrite (par le biais d'une photo de profil par exemple) ou votre numéro de sécurité sociale sur la page que vous souhaitez faire disparaître de Google.

Entendons-nous : Google n'ira pas (et ne pourra pas) vérifier que la signature ou le numéro de sécu qui s'affichent sur votre profil public de *passion-armes-a-feu.com* vous appartiennent réellement. Vous devez **absolument** mettre en ligne une **fausse** signature et un **faux** numéro de sécurité sociale. Il en va de votre sécurité. Diffuser votre vrai numéro de sécurité sociale est aussi grave que diffuser votre numéro de carte bancaire (voire plus grave). N'hésitez pas à utiliser le site *FakeNameGenerator* présenté précédemment pour trouver un numéro de sécurité sociale fictif et inutilisé. Pour la signature,

tapez « signature » dans Google Image et prenez-en une au hasard.

Choisissez seulement l'une ou l'autre des astuces : soit le numéro de sécu, soit la signature. Pas les deux en même temps. Le personnel de Google chargé de répondre à votre demande trouverait sûrement cela louche.

Lorsque c'est fait, vous pouvez signaler la page à Google en passant par leur formulaire de contact :

Suppression d'un résultat Google, procédure 1
www.pandore.it/aggs

Ils répondent généralement en 72 heures. La suppression du résultat de recherche sera prise en compte d'ici une bonne semaine à compter du jour où ils ont confirmé votre demande.

Cette technique a beau être sournoise, elle a toujours fonctionné lorsque j'en ai eu besoin. Adaptez cette faille à vos besoins : comme d'habitude, l'exemple du livre n'est probablement pas exactement la situation exacte que vous rencontrerez.

Bon à savoir

Quelques jours avant la sortie de ce livre, Google a mis en ligne un formulaire de demande de suppression de résultat de recherche au titre de la législation européenne. Autrement dit, ils se sont fait taper sur les doigts par l'Europe et ont été obligé de proposer un outil accessible à Monsieur Tout-le-monde.

Vous pourrez désormais demander la suppression d'un résultat de recherche en utilisant ce formulaire :

Suppression d'un résultat Google, procédure 2
www.pandore.it/agge

N'ayant pas encore eu de retour sur l'efficacité de cette procédure, l'explication précédente reste de mise.

Je conclurai ce chapitre avec quelques notions de bon sens que beaucoup de gens ignorent… ou oublient.

8. Les trois pièges des réseaux sociaux, qui vous rendent vulnérable bêtement

I) Ne donnez pas votre nom de famille

J'ai commencé à utiliser un ordinateur dès mes 4 ans, grâce à un père très aux faits de la technologie et une mère convaincue – peut-être un peu malgré elle – du bénéfice que cela pouvait procurer à un enfant.

Cela étant, elle me rabâchait sans cesse une chose : « ne donne jamais ton nom de famille lorsque tu discutes avec des inconnus sur Internet ». J'ai suivi ce conseil assidûment, même à l'âge adulte. Les quelques digressions que je me suis permis me sont toujours retombées dessus alors je me suis fait une raison : donner son nom « à Internet » est une erreur que l'on regrette toujours un moment ou à un autre.

Lorsque vous écrivez un commentaire sur une actualité Facebook ou sur le statut public d'un ami par exemple, sachez que Google l'indexe. Cela veut dire que votre commentaire peut ressortir sur la première page des résultats concernant votre nom.

Nos idées, notre maturité : tout cela évolue au fil du temps. D'une année à l'autre. Si aujourd'hui vous assumez ce que vous dîtes sur Facebook, êtes-vous certain de l'assumer tout aussi bien dans un an ? Dans deux ans ?

Faisons plutôt le raisonnement inverse : assumez-vous encore **tout** ce que vous avez publié, dit ou fait sur le web ces quatre dernières années ?

Pour éviter ce genre de réflexions, il suffit de ne pas donner votre nom de famille sur Internet.

Si vous vous appelez « Jean-Marc Durantille », indiquez plutôt le nom « Drntll » (en supprimant les voyelles) pour permettre à vos proches de vous reconnaître, mais pour éviter à Google et à Facebook d'associer n'importe quoi à votre identité réelle. Cette suggestion vaut aussi bien pour votre blog personnel, les commentaires que vous publiez sur des sites d'information, sur des forums ou des blogs.

II) Faites l'effort de configurer vos profils

Ce conseil va sembler évident et laconique, mais prenez le temps de bidouiller les réglages de confidentialité sur chaque compte que vous créez sur le web (Facebook et Google en priorité). Ces réglages changent pratiquement tous les mois. Pour éviter de rendre mon explication obsolète, vous trouverez

les explications détaillées sur le blog du livre. Elles seront mises à jour régulièrement :

> *Configurer votre Facebook pour ne laisser fuir aucune information privée (réellement)*
> *www.pandore.it/afbk*

III) Vous êtes votre unique source de problèmes

Ce conseil tient en une phrase : on ne trouve sur Internet que ce que des internautes ont bien voulu y laisser.

Concernant vos informations personnelles, il est rare qu'une personne s'obstine délibérément à faire fuiter vos données personnelles sans votre accord. La meilleure façon d'éviter tout problème consiste donc à ne pas les publier vous-même.

Vous n'avez pas envie que votre âge soit disponible ? Ne donnez pas votre date de naissance.

Vous avez peur de mal régler la confidentialité de vos albums photo ? Ne publiez pas vos photos sur Facebook, envoyez-les par e-mail ou sur un site plus respectueux de votre vie privée.

Facebook est un monstre qui grossit parce que les gens lui donnent à manger. Dans quelques années, je suis persuadé que l'on apparentera la relation des utilisateurs à Facebook à une sorte de syndrome de Stockholm déguisé.

La manière la plus simple de ne jamais donner vos informations personnelles sur Internet est de vous créer un « faux profil » et de vous y tenir. Concrètement, mettez-vous en tête qu'à chaque fois qu'un site vous demandera votre date

de naissance, vous mettrez « 1er janvier 1970 ». Mettez-vous aussi en tête qu'à chaque fois qu'un site vous demandera votre ville, vous choisirez « Paris ». Et ainsi de suite.

À part les sites de e-commerces qui vous demandent votre adresse de livraison et quelques rares exceptions hors e-commerce, très peu d'entreprises commerciales ont besoin de votre véritable adresse postale, de votre numéro de téléphone et de votre nom de famille. Ne vous sentez jamais obligé de tout donner.

Ce qu'il faut retenir

Les proxies et les VPN peuvent vous protéger efficacement des attaques les plus basiques. Cependant, il n'existe qu'une seule manière de vous protéger du *doxing* et de la manipulation : agir intelligemment.

Il est surtout question de changer d'état d'esprit : partez du principe que publier des informations personnelles sur Internet est une erreur grave. Avant de publier quoi que ce soit, posez-vous ces trois questions :

En serais-je toujours fier dans 3 ans ?

Que penseraient respectivement mon chef, ma mère et mon meilleur ami de ce que je viens de publier s'ils tombaient dessus ?

Qu'aurais-je pensé de ce je viens de publier si je l'avais lu venant de la part d'un inconnu ?

Les réponses à ces trois questions sont sans ambiguïté : faites cet effort. Votre « vous dans le futur » vous le revaudra forcément.

Conclusion

C'est ainsi que se termine cette « version 1 » du livre. Elle a été écrite dans le même état d'esprit que l'on fabrique un logiciel informatique : elle évoluera, version après version, pour vous apporter régulièrement de nouvelles fonctionnalités et de nouvelles connaissances.

Personne ne saurait être exhaustif sur la question du *doxing*, du *hot-reading* et du *social-engineering*. Les capacités que vous développerez sur ces trois sujets passionnants dépendront entièrement de votre vécu (passé et futur), de vos ambitions et de vos fréquentations.

Les outils et les astuces que vous avez découvert tout au long de votre lecture ne sont que des pistes, des chemins déjà tracés pour vous aider à avancer plus rapidement. Dans ce domaine, il est de votre devoir de découvrir de nouvelles routes. D'inventer de nouvelles méthodes. De mettre au point de nouvelles ruses et de nouveaux outils.

Je reste à votre disposition sur le blog (jesaisquivousetes.com) et par e-mail (charles. cohle@auteur. institut-pandore.com), pour répondre à toutes vos questions.

Merci d'avoir participé à l'aventure en achetant ou en piratant ce livre.

Très bonne continuation,
Charles Cohle

Prix de vente : 10€ (numérique)
Dépôt légal : juin 2014
Achevé d'imprimer aux États-Unis
pour le compte de l'Institut Pandore