La fraude immobilière sur internet

Analyse de sites des petites annonces

Anne-Sophie Sandor

Note de recherche no. 20

Université de Montréal

Chaire de recherche du Canada en Sécurité et Technologie

Ce travail a été réalisé dans la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'automne 2014), offert aux étudiants de la Maîtrise en Criminologie sous la direction du Professeur Benoît Dupont.

La Chaire de recherche du Canada en sécurité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers.

Anne-Sophie Sandor
anne-sophie.sandor@umontreal.ca

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.benoitdupont.net

Table des matières

Résumé

La fraude immobilière sur internet via les sites de petites annonces revêt une importance toute particulière qui passe pourtant parfois inaperçue. En effet, si la littérature s'intéressant à la fraude de manière générale est extrêmement florissante, aucune recherche n'étudie spécifiquement sa dimension relative aux arnaques immobilières. Pourtant, un nombre considérable de citoyens se font duper chaque année en envoyant de l'argent par mandat-cash via des organismes légaux, sérieux et populaires tels que Money Gram ou Western Union, pour un bien qu'ils n'obtiendront pas. Cette étude exploratoire cherche à mettre en avant le script de ce type de fraude en examinant étape par étape son fonctionnement grâce à un échange de courriels avec un échantillon de fraudeurs. L'objectif est de comprendre à chaque étape du script les éléments cognitifs ou motivationnels qui ont pu pousser la victime à agir et poser des actes, et ce afin d'avoir une vue globale de ce type de fraude et permettant d'élargir notre connaissance sur le sujet.

1. Introduction Théorique

Afin de comprendre l'enjeu de la recherche, il est nécessaire de procéder dans un premier temps à un travail de définition de la fraude avant de l'étudier dans un contexte de cybercriminalité. Nous procédons ensuite au recensement des divers facteurs de risque de victimisation face à ce type de délinquance avant de mettre en place le cadre théorique des scripts.

i. Définition de la fraude

La fraude est une infraction qui n'est pas nouvelle, faisant sans cesse parler d'elle dans bien des domaines. Traditionnellement définie comme le fait d'amener une personne, au moyen d'une supercherie ou d'un mensonge à se départir d'un bien, la fraude se distingue du vol. Si le voleur dépossède sa victime à son insu, le plus souvent en lui subtilisant son bien, le fraudeur, plus astucieux, influe sur l'esprit de la dupe pour l'amener à se déposséder elle-même[1]. Il s'agit donc d'un acte accompli dans l'illégalité, dans le but de tromper délibérément, de soutirer de l'argent ou encore de falsifier des documents en portant atteinte aux droits ou aux intérêts d'autrui. Trois éléments sont généralement mis en avant dans de tels cas : un élément intentionnel, une volonté de dissimulation et enfin un mode opératoire (Le Maux et al, 2013). Par ailleurs, fraude et arnaque sont étroitement liées et tendent même à se confondre lorsque l'on parle de fraude immobilière via les sites de petites annonces. D'un point de vue global, l'infraction de ruse se caractérise par deux traits essentiels : le mensonge et l'usurpation. Le mensonge est de l'essence même des infractions de ruse car c'est lui qui permet de les distinguer des infractions de violence (Gassin, 2009). Et si avec l'apparition d'internet un phénomène de déplacement des infractions a pu être observé, la fraude n'y a pas échappé. En effet, l'explosion de l'utilisation des technologies de l'information et du commercer électronique a engendré une croissance significative des transactions en ligne. La révolution technologique a par la même entrainé l'apparition de la cybercriminalité (Kelci, 2007), dont la fraude fait aujourd'hui partie.

[1] Définition classique de la fraude par l'arrêt anglais Re London 1 Globe Finance Co (1903).

ii. La fraude dans un contexte de cybercriminalité

La fraude s'est développée sur internet en prenant une ampleur considérable. L'évolution des libertés individuelles et la croissance des échanges économiques sur le web ont créé les conditions idéales pour le développement des activités criminelles dans le monde virtuel. Comme le relève Kapersky (2008) la cybercriminalité, basée sur une condition d'anonymat, est désormais devenue l'une des formes d'exploitation économique les plus profitables avec un minimum de risques. Selon Joël Rivière (2008), la cybercriminalité désigne l'ensemble des infractions commises où intervient l'usage de moyen informatique. C'est donc la transposition dans la sphère informatique de méthodes issues de la criminalité traditionnelle, telle la fraude. Ainsi, la cybercriminalité fait appel à des moyens techniques nouveaux, issus de la généralisation des nouvelles technologies de l'information et de la communication (NTIC) et de leur ubiquité dans nos sociétés modernes (Rivière & Lucas, 2008). Il paraît important de relever que depuis les années 1980, les escroqueries aux particuliers et aux entreprises sont un champ d'activité sans limite. Les secteurs les plus ciblés sont les services financiers et commerciaux en ligne et les réseaux sociaux, sources primaires pour le vol d'argent et d'informations financières, confidentielles ou propriétaires (« phishing »). Les techniques de fraude se retrouvent surtout dans l'installation et la distribution invisibles des dispositifs malveillants et le sabotage des programmes de sécurité. Dans ce contexte, la naïveté des internautes reste cruciale. La nécessité de combattre cette criminalité induit un effort commun entre les services policiers et la société civile afin de sensibiliser les consommateurs (Kaspersky, 2008). Ainsi, certaines formes d'escroqueries, à l'image de la fraude nigériane, des annonces de gains mirobolants, des loteries fictives sont désormais très connues, mais d'autres arnaques restent encore à étudier. C'est par exemple le cas de la fraude immobilière sur internet via les sites de petites annonces. Il s'agit d'une forme de cybercriminalité d'une importance non négligeable qui attire dans ses filets de nombreuses personnes quotidiennement. La littérature s'intéressant à la fraude informatique met davantage l'accent sur l'usurpation d'adresse IP, le Hameçonnage et l'envoie de « Pourriel » ou encore les programmes malveillants sans tellement prendre en considération cette problématique plus précise. Pourtant, il existe sur des sites très populaires au Canada tel que Kijiji ou Craigslist un nombre indéfinissable d' « arnaques immobilières », et chaque année de nombreuses personnes se font duper en transférant de l'argent via Money Gram ou Western Union après un échange de courriels avec le « faux propriétaire » sans jamais voir la couleur du bien. Mais comme le souligne le site Kijiji: « *N'oubliez pas que si ça paraît être trop beau pour être vrai, c'est probablement le cas* »

iii. Les facteurs de risque de victimisation liés à la fraude par avance de fonds

La fraude sur internet via les sites de petites annonces peut être définie comme appartenant au type de fraude par avance de fonds puisque la victime paie l'escroc sans obtenir le bien pour lequel le transfert d'argent a eu lieu. Différentes questions se posent alors quant aux risques de victimisation et au comportement cognitif des victimes faisant qu'elles se laissent piéger.
Dans leur étude, Trahan, Marquant et Mullings (2005) affirment que simplement connaître les caractéristiques démographiques et socio-économiques d'une victime de fraude par avance de fond ne suffit pas à comprendre pourquoi les gens répondent. Il apparaît donc que l'explication

de la victimisation ne peut pas se faire uniquement avec les seules informations démographiques. Ils affirment en effet que des preuves sont nécessaires sur la manière dont les délinquants manipulent les victimes pour former une relation de confiance propice à l'extraction des fonds. Ils mettent alors en avant que les personnes qui passent de longues heures sur internet sont plus à risque de devenir la cible des nombreux délinquants, en vertu de la théorie des activités routinières de Cohen et Felson (1979). De plus, les auteurs mettent en exergue le manque de self-control comme élément déterminant. Gottfredson et Hirschi (1990) affirment que les individus dotés d'un faible self-control ont tendance à agir pour leur propre intérêt sans considération pour les conséquences à long terme. Holtfreter, reisig et Pratt (2008) ont en effet montré que les gens qui avaient un faible self-control avaient plus tendances à être victime de fraude.

D'autres études décrivent que la victimisation peut s'expliquer par les jugements cognitifs (décisions d'erreurs) et les motivations que les fraudeurs utilisent pour manipuler la victime en utilisation des stratégies de persuasion et tromperie (Office of fair trading, 2006). Différentes stratégies psychologiques associées à la fraude ont été regroupées selon qu'elles soient liées à la source (la motivation et les plans des délinquants), le milieu (la forme de la communication frauduleuse), le message (les stratégies utilisées pour persuader les victimes potentielles à saisir dans la fraude) ou le destinataire (les caractéristiques qui font des victimes vulnérables). Pour toutes ces stratégies, les fraudeurs ont un avantage dans la mesure où ils utilisent des e-mails ou encore des sites qui confirment la validité de la fraude. D'autres éléments ont été identifiés comme le fait pour la victime de ne pas être capable de gérer ses réponses émotionnelles aux messages frauduleux.

Quant à Langerderfer et Shimp (2001), ils relèvent deux possibilité pour expliquer la victimisation : d'une part la victime de fraude a évalué le risque d'escroquerie mais n'est pas parvenue à reconnaître les indices qui pourraient l'alerter sur la véritable nature de l'opération ou d'autre part, la victime n'a pas bien évalué l'offre et a agit sans considérer la possibilité qu'il pouvait s'agir d'une fraude.

Enfin, on peut également relever la « theory of déception » de Johnson et al (2001) qui définit la duperie comme une interaction cognitive entre deux parties : la cible et l'escroc. Ce dernier manipule l'environnement de la cible afin d'induire une mauvaise représentation cognitive et par conséquent le comportement souhaité.

Ainsi, de nombreux facteurs peuvent être pris en considération afin d'expliquer le pourquoi du fonctionnement de la fraude, notamment dans les réponses cognitives transmises par les victimes.

iv. Le cadre théorique de la recherche : les scripts

La commission d'un crime implique un nombre de choix et de décisions pris à chaque stade de l'acte criminel : la préparation, le choix de la cible, la commission de l'acte, la fuite ou encore les répercussions. Ainsi, afin de comprendre étape par étape le processus de passage à l'acte derrière le crime, Cornish (1994) a mis en exergue la notion de script, permettant aux personnes travaillant dans le domaine de la prévention du crime un cadre théorique clair applicable à l'étude du processus de passage à l'acte. Comme le relève Genest (2013), en appliquant la

perspective des scripts au crime, Cornish (1994) a développé un cadre procédural permettant d'identifier la séquence complète d'actions adoptées avant, pendant et après la commission du crime. L'utilisation de cette notion a été utilisée pour comprendre divers phénomènes tels les crimes contre la propriété comme le vol (Cornish, 1998), la falsification de chèques (Lacoste et Tremblay, 2003), la production de drogues synthétiques (Chiu et al, 2011), ou encore la revente de véhicules volés (Morselli et Roy, 2008; Tremblay et al., 2001). Développée il y a vingt ans, la notion de script est encore utilisée par les criminologues et a servi récemment pour étudier différentes formes de crimes violents tels les crimes contre les employés et les usagers de transport en commun (Smith et Cornish, 2006), les agressions sexuelles sur des mineurs (Leclerc et al., 2011) ou même les infractions sexuelles en série par des étrangers (Beauregard et al., 2007). Genest (2013) explique qu'afin de mieux comprendre ce que sont les scripts, il faut d'abord comprendre le concept de schéma. Un schéma est une structure cognitive servant à organiser les représentations des comportements et expériences passées. Selon Leclerc (2014), cette structure est composée d'hypothèses et d'attentes relatives à l'environnement social qui guident une personne dans l'interprétation de ses expériences futures. Il affirme donc qu'un script est un schéma d'évènements, soit une structure de connaissances qui organise les séquences d'action à adopter dans un contexte particulier. Selon Shank et Abelson (1977), chaque personne possède un répertoire de séquences comportementales archivées dans la mémoire et qui est prête à être activé inconsciemment. Ils illustrent le concept avec la notion du « restaurant script » qui organise la connaissance sur ce que le client doit faire dans un restaurant par séquence d'action : entrer dans le restaurant, attendre d'être placé, prendre connaissance du menu, commander, manger, demander l'addition, payer et sortir du restaurant. Lorsqu'appliqués aux crimes, les scripts représentent donc la séquence complète d'actions adoptées avant, pendant et après la commission de l'acte (Genest, 2013). Appliqué à la fraude sur internet via les sites de petites annonces, la notion de script permet de mettre en avant les différentes étapes utilisées par le fraudeur à travers l'évolution de ses courriels afin d'entrainer sa cible dans une erreur de jugement jusqu'à ce qu'elle fasse ce qu'il souhaite.

v. Objectif de la recherche

Nous savons que la fraude sur internet via les sites de petites annonces fait chaque année un nombre important de victimes et rapporte des sommes non négligeables aux fraudeurs. Contrairement à ce que nous pensions, cette dimension de la fraude semble avoir été laissée à l'écart par les criminologues. En effet, si la fraude n'est pas un phénomène nouveau et a été étudiée dans de très nombreuses dimensions, la littérature sur notre sujet est presque inexistante. Pourtant, étudier ce type de fraude aiderait à mettre en place des politiques de prévention visant à réduire son impact et à protéger en amont les personnes susceptibles de se faire arnaquer. Ainsi, comprendre le script de la fraude par les sites de petites annonces permettrait d'augmenter notre connaissance sur le sujet pour non seulement mieux les contrer, mais également la prévenir.

2. Méthodologie

Nous avons en premier lieu pris connaissance de la littérature sur le sujet de la fraude d'une manière relativement générale afin d'avoir une vision globale du phénomène. Nos recherches ont porté notamment sur les facteurs de risque liés à ce type de victimisation. Par ailleurs, en

cherchant de la littérature plus précise relative à la fraude sur internet, nous nous sommes aperçu que celle se rapportant spécifiquement à la fraude immobilière via les sites de petites annonces était presque inexistante. Ainsi, nous nous plaçons dans une démarche exploratoire au vu du peu d'informations dont nous disposons et afin de mettre en lumière le fonctionnement de la fraude. Pour ce faire, nous avons pris le parti de prendre directement contact avec des fraudeurs en nous faisant passer pour d'éventuels locataires.

Premièrement, il s'agissait d'éplucher les sites de petites annonces afin de repérer celles qui pouvaient être frauduleuses. En effet, lorsque les photos sont trop belles et le prix très attractif, cela peut d'ores et déjà éveiller notre curiosité. Toutefois, nous avons remarqué qu'il n'était pas toujours si facile de distinguer les annonces sérieuses des annonces frauduleuses. Nous avons également remarqué que le numéro de téléphone n'était majoritairement pas présent et laissait place à une adresse courriel.

La seconde démarche consistait en l'envoie d'un message aux soi-disant propriétaires afin d'affirmer notre intérêt pour leur bien et demander un éventuel rendez-vous. Notre échantillon se compose alors de quatre contacts dont la première approche s'est faite grâce au site Kijiji. La taille de notre échantillon s'explique par le fait que contrairement à ce que nous pensions de prime abord, il n'existe pas tant d'annonces frauduleuses. Il semble qu'une annonce puisse faire plusieurs victimes ; les annonces ne se renouvèlent donc pas si souvent. De plus, pour une meilleure compréhension et visibilité, nous avons décidé de nommer les contacts de délinquant n°1 à délinquant n°4.

Enfin, nous avons procédé à un échange de courriels avec les quatre adresses mails que nous avions pu obtenir. Nous avons observé une moyenne de cinq courriels de la part de chaque fraudeur amenant chacun différents éléments.

Notre objectif étant de comprendre le fonctionnement de la fraude, le but de la recherche était de créer le script de celle-ci en observant étape par étape les informations qui étaient transmises. Afin de comprendre pourquoi les personnes répondent aux messages jusqu'à transférer l'argent, nous lions chaque étape du script à des éléments de la psychologie de la victime permettant d'expliquer les erreurs de jugement.

Notre méthodologie comporte des limites évidentes dans la mesure où notre échantillon est relativement restreint et que nous n'avons pas pu avoir des informations sur les fraudeurs. À la fin des échanges concernant le bien, nous avons essayé, en vain, de prendre contact avec eux afin de leur poser différentes questions qui nous auraient permis d'étoffer notre recherche. Aussi, nous ne sommes pas en mesure de savoir combien de personnes différentes se cachent derrière une adresse mail ou même si une seule personne se cache derrière plusieurs. Toutefois, la mise en place de script suivant les différents échanges de courriels permet de comprendre étape par étape le fonctionnement global de ce type de fraude.

3. Étude du script de la fraude immobilière sur internet via les sites de petites annonces

Étant donné non seulement qu'il s'agit d'une recherche exploratoire et que nous souhaitons mettre en lumière le script de la fraude, nous lions évidemment analyse et discussion des résultats.

Le script de la fraude immobilière sur internet via les sites de petites annonces peut alors être analysé en six étapes principales : le fraudeur laisse venir la victime à lui grâce à l'annonce (1) puis répond à son courriel enclenchant le contact et demandant des informations (2). Il renforce le processus cognitif avec de nouveaux éléments (3) avant d'ajouter la personne sur Skype (4). Vient alors la demande de dépôt par mandat-Cash (5) suivi d'une explication insistante sur le fonctionnement de ce type de transfert d'argent (6).

Etape 1 : Laisser la victime venir

Dans leur ouvrage, Blanchard et Fortin (2013) mettent en avant deux éléments essentiels dans la fraude sur internet, à savoir « rejoindre l'utilisateur » et « déployer le baratin ». En comparaison avec d'autres crimes, la fraude requiert un degré de coopération de la part des victimes. Une fraude ou une arnaque ne peut fonctionner sans que la victime ne prenne des actions positives (Modic & Lea, 2013). De plus, si le courriel était la meilleure façon de joindre les victimes dans les débuts d'internet, cette méthode à diminué dès l'apparition des sites de petites annonces en ligne qui offraient une plateforme plus directe et un auditoire plus attentif (Blanchard & Fortin, 2013). En effet, l'individu cherchant un bien immobilier lira à coup sur l'offre proposée par un éventuel fraudeur. Le fraudeur rejoint la victime de manière extrêmement subtile et astucieuse puisqu'il met en place un stratagème faisant que c'est la victime elle-même qui va aller vers lui. Il met en ligne une annonce sur un site légal et populaire avec une description précise du bien et de fausses photos. Aucun numéro de téléphone n'est donné, il est seulement possible de contacter la personne via courriel, ce que fait donc celui ou celle intéressé-e par le bien en demandant davantage d'informations ou en souhaitant un rendez-vous. L'arnaque ne peut donc fonctionner que si la victime s'implique. À ce stade, il est encore difficile de détecter la fraude. Avec cette première étape, le processus est amorcé et le fraudeur n'a plus qu'à « déployer son baratin ».

Etape 2 : La prise de contact

Dans notre échantillon, les quatre fraudeurs ont agit de manière identique dans la réponse faisant suite à notre première prise de contact.
Le courriel est accompagné de photographies supplémentaires du bien immobilier et contient un résumé des caractéristiques de celui-ci.

> *J'ai pris bonne note de votre courriel. Il s'agit d'un Studio meublé à proximité de toutes commerces et commodités. Le Studio est très propre comme sur les photos ce dernier était occupé par ma fille. Le Loyer est de 495$ avec les charges inclus (Chauffage, eau chaude, électricité, Internet haute vitesse et wifi, téléphone, câble TV, 5 Électro, Stationnement etc.).(Délinquant n°1)*

Après la description suit un argumentaire sur la raison de la location du studio à un prix aussi attractif. Dans 50% de notre échantillon, l'explication était quasi-identique alors qu'elle variait

quelque peu dans l'autre moitié. Toutefois, dans 100% des courriels, le fraudeur dit se trouver à chaque fois en France et ne souhaite pas laisser le studio inoccupé.

> *La raison de cette éventuelle location est de ne pas laisser le Studio vide et non entretenu vu que ma fille qui occupait le Studio vient de me rejoindre à Paris (FRANCE) dans le cadre de ces études pour une durée de 5 Ans. (Délinquant n°2)*

Ou encore

> *J'ai déménagé actuellement pour Bourgogne (FRANCE) compte tenu de mon travail et à cause de ma famille qui y vit là bas et n'ayant pas envie de laisser mon studio inoccupé, j'ai décidé de le mettre en location à $ 460 (charges comprises, chauffage, eau chaude et eau froide). (Délinquant n°4)*

Notons que dans le courriel du délinquant n°4, de nombreuses erreurs peuvent être relevées comme le fait que le correspondant se trouve désormais *« à Bourgogne (FRANCE) »* et que le studio est *« situé près de la plage »*. Si la région Bourgogne existe, aucune ville ne porte cette appellation en France. De même, le studio semble être à la fois en plein cœur de l'île de Montréal mais à côté de la plage.

En fin de courriel, le correspondant amorce l'idée d'une visite et prétend qu'il va se déplacer de France spécialement pour procéder à celle-ci. L'emménagement peut se faire quand on le souhaite, peu importe la durée du bail mais il faudra donner une garantie d'une « *mois de caution (qui sera remboursable à la fin du bail ou prise en compte pour le dernier mois de loyer) » (délinquant n°1, 2 et 3).*

Enfin, dans 100% des réponses, le fraudeur demande des informations personnelles comme le nom, prénom, âge, numéro de téléphone, nationalité, nombre de personnes dans le studio, durée du bail, profession, la situation maritale, l'adresse actuelle ou encore le revenu mensuel approximatif.

La structure du courriel se résume à un paragraphe unique sans saut de ligne ni alinéa, sans aucune mise en page et comportant de nombreuses fautes d'orthographes et de syntaxe malgré un style qui se veut soutenu. Mais différents éléments pourraient déjà à ce stade réduire les capacités cognitives de la victime tel le « time principle» (University of Exeter, 2009). En étant sous une pression temporelle pour faire un choix important, la personne va utiliser des stratégies différentes pour prendre des décisions. Les arnaqueurs utilisent cette pression et dirigent leur cible vers des stratégies impliquant moins de raisonnement (Stajano & Wilson, 2009). Or, en parlant de logement, il est fort probable que l'échéance temporelle soit restreinte impliquant alors moins de temps pour le raisonnement. De plus, les individus vont davantage avoir tendance à répondre positivement à une offre s'ils pensent qu'il s'agit d'une bonne offre, rare ou même unique (Kolkes, Martin & Gupta, 1993 ; Kramer & Caroll, 2009 ; Surri, Kohli, & Monroe, 2007). Par exemple, Lynn (1989) a démontré que les œuvres d'arts et le vin sont perçus comme ayant plus de valeur si le client pense qu'il y a une forte demande pour eux. Il semble en être de même pour l'immobilier puisque de nombreuses personnes peuvent vouloir le même bien, mais une seule l'obtiendra. Il faut donc répondre vite et avec intérêt.

Etape 3 : renforcement du processus cognitif

Le courriel précédent de chaque correspondait demandait une réponse comportant notamment les renseignements personnels. Suite à cela, le fraudeur répond dans un second courriel où il est question de la durée du bail ou encore du jour de la visite.

> *Re !*
> *Je vous remercie pour le vif intérêt que vous portez à notre logement et je confirme qu'après lecture de vos informations nous sommes d'accord de vous accorder la visite et espérant que vous soyez notre nouveau locataire. La durée de bail souhaitée vous sera accordée. Le jour de la visite je serai en possession du titre de propriété et du contrat de bail enfin que vous prenez note et que vous allez signer si notre logement vous convient après la visite, et comme je vous l'ai expliqué dans mon premier mail, je suis en déplacement en Europe et je serai disponible pour venir à Montréal, donc la visite peut se faire entre Mercredi & Dimanche .La visite sera programmée selon votre disponibilité. J'espère que cela vous convient? Vous deviez être en possession : Le versement du dépôt d'un mois de loyer + 1 Mois de caution (Remboursable à la fin du bail ou prise en compte pour le dernier mois de loyer).Veillez me faire parvenir Votre date effective pour la visite afin que nous puissions nous en conformer pour la suite et vous expliquez comment ça se déroulera. Merci de me dire si vous aviez Skype afin qu'on puisse discuter de tous autres détails , Si oui donnez moi vos identifiants afin que je puisse vous ajoutez. (Délinquant n°2)*

Dans trois quarts de l'échantillon, le courriel était presque identique alors que pour le dernier quart (délinquant n°4), il semblait davantage personnalisé (il adressait le message à notre nom) et plus aéré. Mais dans 100% des cas la réponse fut extrêmement rapide. Encore une fois, on peut facilement observer ici une syntaxe peu convaincante et des fautes d'orthographes très présentes. Le délinquant semble manipuler la victime pour former une relation de confiance propice à l'extraction des fonds (Ross & Smith, 2011). En lisant qu'un accord a été trouvé sur la durée du bail ou encore que la visite sera programmée selon ses disponibilités, la victime est alors rassurée. Cela peut également être mis en lien avec un manque de self-control. Les personnes répondant aux arnaqueurs ont tendance à moins savoir gérer leurs émotions (Langenderfer & Shimp, 2001). Egalement, les escroqueries sont souvent personnalisées pour créer l'impression que l'offre est unique au destinataire et les escrocs soulignent parfois l'urgence d'une réponse afin de réduire la motivation de la victime potentielle à étudier le contenu de l'arnaque (University of Exeter, 2009). Or, non seulement les réponses rapides du délinquant incitent la victime à répondre rapidement mais le fait qu'il s'adresse directement à cette dernière par l'utilisation de la première personne du pluriel, ou encore qu'il lui propose une visite en fonction de ses propres disponibilités font penser à un message personnalisé alors qu'il semble au contraire être un schéma repris de manière identique, ou presque, pour chaque cible.

Etape 4 : L'ajout Skype

Dans trois quarts des échanges (délinquant n°1, 2 et 3), le courriel se clôturait par une demande d'ajout Skype. Aussi, nous avons transmis notre identifiant et un mail nous revenait nous informant que l'ajout avait été réalisé et qu'il fallait donc accepter ce nouveau contact. Il apparaît clairement que le fraudeur continue à travailler la relation de confiance en utilisant Skype et en faisant croire à la victime qu'un échange visuel serait possible pour obtenir des

informations. Si nous avons accepté les trois identifiants, nous n'avons finalement pu échanger avec aucun, et nous ne recevions aucune réponse par rapport à un éventuel rendez-vous via ce système. L'Université of Exeter School of Psychology (2009), relève l'excès de confiance comme processus cognitif pouvant amener à une erreur de jugement. Cela fausse alors la prise de décision et la recherche d'information (Fischer et al, 2008). De plus, selon la même étude (University of Exeter school of psychology, 2009), les gens ont tendance à apprécier les gens qui les apprécient. Or la demande d'ajout Skype suggère au destinataire qu'il est apprécié en tant que futur locataire. Malheureusement, les choses et les gens ne sont pas toujours ce qu'ils semblent être et les arnaqueurs savent comment manipuler pour faire croire qu'ils sont quelqu'un d'autre (Stajano & Wilson, 2009).

Etape 5 : La demande de dépôt Money Gram

Avant cette étape, il n'était pas explicitement question de transfert d'argent. Le délinquant se contentait de mettre la victime en confiance. Ce nouveau courriel, confirmant la date de la visite, amorce la question du dépôt par mandat cash. Le fraudeur prend soin de justifier l'utilisation d'un tel procédé en faisant en sorte d'apitoyer la victime sur le fait qu'il se déplace de très loin, voire même de la faire culpabiliser.

> *J'ai déjà eu des intéressés malhonnêtes et je me déplace de France simplement pour la visite. (Délinquant n°3)*

Ou encore

> *Car je me déplace de loin et ne veut pas venir pour rien, en plus je souhaite vous réserver mon studio. (Délinquant n°4).*

Enfin, le fonctionnement de Money Gram prend une place importante dans le corps du mail.

> *En ce qui concerne le Money Gram c'est très simple il vous suffira d'aller à succursale et de demander à faire un dépôt, au guichet on vous remettra une Fiche à remplir avec vos coordonnées ainsi que mes coordonnées et ensuite le montant. Après ils vous donneront un reçu imprimé sur lequel il y a un **CODE** encore appelé **NUMÉRO DE RÉFÉRENCE** qui sert de base au retrait de l'argent que vous aurez à déposer chez eux alors comprenez donc qu'un dépôt chez **Money Gram** n'a aucun engagement financier et tant que vous ne remettrez pas le **CODE (NUMÉRO DE RÉFÉRENCE) , Personne à part vous ne pourra toucher à votre argent que vous aurez a déposé à la Money Gram** comme garantie enfin de me prouver votre intérêt.*
>
> *Donc après avoir effectué le dépôt vous garderez sur vous le reçu avec lequel vous viendrez au rendez-vous avec tous vos dossiers. Après la visite si l'appartement vous convenait, on signe le bail et la remise des clés aura lieu sur place ainsi donc vous me laissez le reçu **MoneyGram** pour que je puisse me rendre à une agence pour effectué le retrait. (Délinquant n'°2)*

Une fois encore, le délinquant renforce la relation de confiance en prenant soin d'expliquer le fonctionnement du système et en affirmant que tant que le code, ou numéro de référence (dont la répétition est importante) n'est pas transmis, l'argent ne peut être retiré.

Une fois encore, les courriels des différents correspondants sont extrêmement ressemblants et dans un post-scriptum écrit en gras, le fraudeur cherche une nouvelle fois à rassurer puisque

« une fois sur place, [il] sera en possession avec le titre de propriété que nous pourrions vérifier auprès de la régie avant tout signature du contrat de bail ». (Délinquant n°1)
Dans ce courriel, l'écriture semble encore plus pressante que dans les précédents et le correspondant insiste fort sur la légitimité du fonctionnement de l'accord et sur le fait qu'il détient un véritable titre de propriété.

À ce stade, s'ils n'étaient pas encore apparus, les doutes concernant une éventuelle fraude peuvent voir le jour. Cependant, les personnes ont tendance à apprécier la cohérence non seulement dans leur propre comportement mais également dans le comportement et les réactions des autres (Festinger, 1957; 1964; Frey, 1986). La cohérence apparaît ici dans l'échange progressif des mails et cette cohérence donne un sentiment de contrôle (University of Exeter, 2009). Même si le fond des messages n'apparaît pas comme très cohérent au vu de la structure et des nombreuses fautes, c'est l'enchainement de ceux-ci, suivant un fil conducteur clair qui donne une impression de cohérence. Il s'agit donc d'un prédicteur important de réponse à une offre frauduleuse. Cela peut également se traduire par le besoin d'honorer des engagements pris précédemment (Cialdini & Goldstein, 2004), comme le fait d'avoir déjà répondu à plusieurs courriels et de savoir que le « propriétaire » se déplace d'Europe pour nous faire visiter. Par ailleurs, si un doute avait pu survenir, les études relèvent une préférence pour l'information de confirmation. Lors d'une prise de décision, les gens vont avoir tendance à chercher de l'information qui confirme leur hypothèse initiale plutôt que de l'information qui pourrait révéler qu'ils ont tort (Festinger, 1957; Frey, 1986; Wason, 1966). Ayant déjà pris du temps et s'étant impliqué dans le processus, le futur locataire espère avoir raison même si différents éléments pourraient l'amener à penser qu'il a tort.

Etape 6 : Insistance sur le transfert d'argent
Nous avons laissé l'un de nos contacts sans réponse pendant quelques jours afin d'observer sa réaction et il nous a relancé en nous pressant de faire le dépôt si nous voulions être sûre de pouvoir visiter l'appartement.

> *Le dépôt postal via le service MONEYGRAM doit être fait avant la visite du studio.*
> *Cela va me permettre de vous réserver le studio et de remplir le contrat de bail en votre nom.*
> *Alors si vous êtes vraiment intéressé, merci de me faire part de votre mail pour que je vous envoie l'adresse pour le dépôt de garantie des $ 920. (Délinquant n°4).*

Par la suite, il nous a donné une adresse à laquelle le dépôt devait être fait qui n'existe pas (Puisque Bourgogne n'est pas une ville de France), avant de s'impatienter pour *« obtenir une preuve que le dépôt est vraiment fait »*.

Mais dans le reste de l'échantillon, il s'agissait ici de la dernière étape, du dernier courriel que nous avions reçu. À ce stade, le fraudeur explique une fois encore le fonctionnement du dépôt par Mandat Cash (accompagné de l'adresse à laquelle le dépôt doit être fait) afin de renforcer le processus cognitif.

> *En ce qui concerne le dépôt MoneyGram , il sera retiré qu'après que vous m'ayez communiqué Le CODE qui est le NUMÉRO DE RÉFÉRENCE .Le dépôt dont la*

> *caution (remboursable le jour de votre sortir ou servira simplement de Deuxième mois pour le loyer)+ le Premier loyer (qui sera prise en compte après avoir emménager dans l'appartement).Votre premier loyer comptera après votre entré dans l'appart. Tout sera notifié sur le contrat que je vous ferez signé. Le dépôt MoneyGram n'est pas compliqué. Quand vous y effectué un envoie, C'est ce CODE qui permettra au bénéficiaire de rentrer en possession de l'argent qui lui à été envoyé.Donc, après envoie , sur votre reçu du dépôt le CODE de Sécurité sera le NUMÉRO DE RÉFÉRENCE pour le retrait de l'argent et vous me le remettrai après signature du Bail. Aussi, votre garantie est que, après avoir effectué le dépôt, vous aviez la possibilité d'annuler si vous n'êtes plus d'accord pour prendre l'appartement. Il vous suffira de vous rendre toujours où vous aviez effectué l'envoie et avec votre reçu, vous annulez le dépôt et vous récupérer votre argent. C'est sécuritaire tant que vous ne donnez pas le CODE (NUMÉRO DE RÉFÉRENCE) au bénéficiaire .Donc pour être que c'est fait vous allez prendre une photo du reçu en prenant soin de cacher le CODE puis me l'envoyer par courriel. (Délinquant n°2)*

La répétition du mot « Code », qui plus est écrit en lettre majuscule, cherche à rassurer la victime qui a désormais tendance à croire son correspondant, et est donc persuadée qu'effectivement si le code est caché, l'argent ne pourra pas être retiré. Il est également précisé que nous pourrons revenir sur notre décision si le bien ne nous plait pas. Malheureusement, si la victime procède au transfert, elle ne verra plus la couleur de son argent et ne verra personne à l'heure du rendez-vous. À partir de ce moment-là, plus aucun contact avec le fraudeur n'est possible et si l'argent a été transféré l'arnaque est terminée (avec succès).

4. Forces et limites de l'étude

Nous sommes conscients que notre étude comporte des biais qu'il était difficile d'éviter dans un premier temps. En premier lieu, au vu du temps dont nous disposions, il en résulte que notre échantillon est assez réduit. De plus, nous ne sommes pas en mesure de savoir si derrière nos quatre contacts se cachent quatre personnes différentes. En effet, si le délinquant n°4 se distinguait des trois autres non pas par la substance mais par la forme de ses courriels, nous ne pouvons affirmer que les délinquants n°1, 2 et 3 soient des personnes différentes. Egalement, nous n'avons pas pu communiquer avec les fraudeurs autrement qu'en se faisant passer pour de potentiels locataires, puisque, malgré les précautions prises, nous n'avons reçu aucune réponse lorsque nous avons souhaité leur poser des questions plus scientifiques. Toutefois, notre élaboration du script permet de comprendre le fonctionnement de la fraude étape par étape. En tant que recherche exploratoire, cette dimension de la fraude n'avait pas encore été étudiée en profondeur et mettre en avant le schéma de celle-ci permet d'avoir une vue globale de son fonctionnement permettant alors de mettre en place des mesures pour l'éviter.

5. Conclusion

« Il est beaucoup plus facile de voler quelqu'un que vous ne pouvez ni voir, ni toucher, ni connaître » relève Eugène Kapersky (2008) concernant le cybercrime. Pour lui, il s'agit d'un

métier comme un autre, une forme d'exploitation économique qui répond aux mêmes critères de gestion traditionnelle tels la rentabilité ou la gestion des risques.

Aussi, Internet n'est pas à l'origine d'une véritable révolution de la fraude en ligne mais constitue plutôt un support pour celle-ci permettant l'emploi d'anciennes méthodes dans un contexte renouvelé (Blanchard & Fortin, 2013), comme on peut le voir avec la fraude en ligne et plus spécifiquement celle se rattachant aux arnaques via les sites de petites annonces sur internet. Les besoins et les désirs rendent les personnes vulnérables, et en sachant ce que l'on souhaite, les arnaqueurs savent comment manipuler (Stajano & Wilson, 2009). Si une personne répond à une annonce immobilière en ligne, c'est qu'elle souhaite trouver un logement. Il devient alors aisé pour le délinquant, par différents procédés, de faire en sorte que sa victime lui réponde. De plus, il existe une situation de déséquilibre entre l'auteur et la victime qui conditionne l'infraction et c'est l'exploitation abusive de cette situation par l'agent au détriment de la victime qui crée la fraude (Gassin, 2009).

La réponse aux arnaques impliquent un processus à la fois cognitif et motivationnel (University of Exeter, 2009), et à travers l'échange de courriels, le locataire potentiellement intéressé se laisse manipuler jusqu'à transférer l'argent sans voir la couleur du bien qu'il convoitait. En étudiant le script de ce type de fraude, on s'aperçoit à quel point le processus cognitif peut-être altéré et on comprend mieux pourquoi les personnes répondent, malgré des indices frauduleux. Il est donc intéressant de mettre en exergue le fonctionnement de la fraude afin de pouvoir agir en amont, grâce à de la prévention primaire ou secondaire. Différents éléments doivent être pris en considération par la personne répondant à l'annonce à l'image du rapport qualité prix du bien mais plus encore dès la réception du premier message.

Enfin, notons que la fraude est une activité à faible risque, comparé aux chances de réussite, et une activité rentable (Kapersky, 2008). Bien que certaines personnes vont déceler l'arnaque avant même d'envoyer un message, d'autres y répondront. Et même si seulement un pourcentage réduit de personnes visionnant l'annonce y répond et finit par transférer de l'argent, cela reste extrêmement rentable et les risques pour les fraudeurs de se faire arrêter sont infimes, puisqu'ils agissent souvent à partir d'un autre pays, cela causant des problèmes de juridiction.

Afin de pouvoir mettre en place des politiques en prévention, des recherches futures devraient d'abord s'attarder à étudier plus en profondeur l'organisation de ces fraudeurs afin d'en comprendre toutes les dimensions, et de se rendre compte à quel point cette activité est rentable. S'intéresser aux comportements de la victime pourrait également être un atout.

Références

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, JF.(2007). Script Analysis of the Hunting Process of Serial Sex Offenders. *Criminal Justice and Behavior,* 34(8), 1069- 1084.

Blanchard, F., & Fortin, F. (2013). *nouveaux habits de la vieille fraude : une vision « écosystémique » des fraudeurs, de leurs instruments et de leurs victimes, Cybercriminalité : Entre inconduite et crime organisé*. presses interPolytechnique. 237-258.

Chiu, Y., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of Drug Manufacturing in Clandestine Laboratories, *Bristish Journal of Criminology*,51, 55-374.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends : A routine activity approach, *American sociological review*, 44, 588-608.

Cornish, D. B. (1994). The Procedural Analysis of Offending and its Relevance for Situational Prevention. In Clarke, R. V., Crime Prevention Studies, Criminal Justice Press, (3), 1-249.

Cornish, D. B. (1998). Regulating Lifestyles: A Rational Choice Perspective. Papier présenté au 7e "Séminaire international sur la criminology environnementale et l'analyse du crime, Barcelone.

Gassin. R., (2009). Essai de théorie générale de la ruse en criminologie, Aix Marseille : Presses universitaires.

Genest, I., (2013). La perspective des scripts appliquée aux homicides et implications pour les enquêtes criminelles, mémoire de l'université de Montréal.

Festinger, L (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Festinger, L. (1964). *Conflict, decision and dissonance*. Stanford CA: Stanford University Press.

Fischer, P., Greitemeyer, T., & Frey, D. (2008). Self-regulation and selective exposure: The impact of depleted self-regulation resources on confirmatory information processing. *Journal of Personality and Social Psychology*, *94*, 382- 395.

Frey, D. (1986). Recent research on selective exposure to information. In L. Berkowitz (Eds.), *Advances in experimental social psychology*, pp. 41-80. San Diego, CA: Academic Press.

Gottfredson, M., & Hirschi, T .(1990). A général theory of crime, Stanford Universy Press.

Holtfreter, K., Reisig MD & Pratt, TC. (2008). low self-control, routine activities and fraud victimization, *criminology*, 46(6), 189-220.

Johnson, P. E., S. Grazioli., K. Jamal., & G. Berryman. (2001). Detecting Deception: Adversarial Problem Solving.

Kaspersky E,.(2008). Défis de la cybercriminalité, *sécurité globale*, 6, 19-28.

Kelci, S. (2007). fraude et autres infractions semblables et Internet, *Lex Electronica*, 12(1).

Kramer, T., & Carroll, R. (2009). The effect of incidental out-of-stock options on préférences. *Marketing letters*, 20(2), 197-208.

Lacoste, J., & Tremblay, P. (2003). Crime and Innovation : A Script Analysis of Patterns in Check Forgery. In : Smith, M., & Cornish, D. B. : *Crime Prevention Studies, Theory for Practice in Situational Crime Prevention*, 16, New York : Criminal Justice Press.

Langenderfer,J., & Shimp, T.A. (2001). consumer vulnerability to scams, swindles, and Fraud : A new theory of viscera Influences on Persuasion. *Psychology & Marketing*, 18(7), 763-783.

Leclerc, B., Wortley, R., & Smallbone, S. (2011). Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency*, 48, 209-237.

Leclerc, B. (2014). New developments in script analysis for situational crime prevention: moving beyond offender scripts. In B. Leclerc et R. Wortley (eds.), *Cognition and crime: offender decision making and script analyses* (pp. 221-236).

Le Maux J., & al. (2013). De la fraude en gestion à la gestion de la fraude, une revue de littérature. *revue française de gestion*, 231, 73-85.

Modic, D., & Lea, S. E. (2013). Scam Compliance and the Psychology of Persuasion. *Journal of Applied Social Psychology*.

Office of fair trading, (2006), Research on impact of Mass marketed scams. London : OFT
Rivière., J & Lucas., D. (2008). Criminalité et internet, une arnaque à bon marché. *Sécurité globale*, 4(6), 67-82.

Ross S., & Smith, R.G. (2011). Risk factors for advance fee fraud victimisation. *Trends & issues in crime and criminal jsutice*, 420.

Schank, R. C., & Abelson, R. P. (1977). *Scripts, Plans, Goals and Understanding*. Lawrence Erlbaum Associates, Hillsdale, New Jersey.

Stajano, F., Wilson, P. (2009). Understanding scam victims : seven principles for systems security, technical report of University of Cambridge, n°754

Smith, M. J., & Cornish, D. B. (2006). Secure and Tranquil Travel: Preventing Crime and Disorder on Public Transport. United Kingdom: University College London, Jill Dando Institute of Crime Science.

Suri, R., Kohli, C., & Monroe, K, (2007), the effect of perceived scarcity on consumers' processinf of price information, *journal of the Academy of Marketing Sciences*, 35(1), 89-100.

Trahan, A., Marquart, J.W., & Mulings, J. (2005). Fraud and the American dream : Toward an understanding of fraud vicitmisation. *Déviant behaviour*, 26, 601-620.

Tremblay, P., Talon, B., & Hurley, D. (2001). Body Switching and Related Adaptations in the Resale of Stolen Vehicles. Script Elaborations and Aggregate Crime Learning Curves. *The British Journal of Criminology*, 41(4), 561-579.

University of Exeter School of Psychology (2009). *The psychology of scams: Provoking and committing errors of judgement*, Office of Fair Trading: Londres.

Wason, P. C. (1966). Reasoning. In B. M. Foss (Eds.), *New Horizons in Psychology I*, pp. 135-151. Harmondsworth: Penguin.