Université de Montréal

La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière

Par

Cameron Coutu

École de criminologie

Faculté des Arts et des Sciences

Mémoire présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention du grade de Maîtrise ès sciences (M.Sc) en criminologie

Août 2019

Université de Montréal
École de criminologie, Faculté des arts et des sciences

Ce mémoire intitulé

La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière

Présenté par
Cameron Coutu

A été évalué par un jury composé des personnes suivantes

Francis Fortin
Président-rapporteur

Benoit Dupont
Directeur de recherche

Marc Ouimet
Membre du jury

Résumé

La recherche menée dans le cadre de ce mémoire s'intéresse à la prévention des cybercrimes. De façon plus précise, l'étude avait pour objectif d'évaluer les effets perçus d'une campagne de prévention des cybercrimes réalisée par une institution financière canadienne. Une attention particulière a été accordée aux perceptions des personnes en lien avec leur sentiment de sécurité. Après la fin de la campagne (qui a eu lieu en octobre 2018), 1452 clients francophones (831 hommes et 521 femmes) ont répondu au sondage par l'entremise d'un panel web disponible en ligne. Les résultats indiquent que la campagne de prévention a été bien perçue pour une majorité des répondants (75%), en particulier chez les participants plus âgés (55 ans et plus). Les analyses ont aussi révélé que le genre n'était pas un facteur associé significativement aux réponses des répondants. De façon générale, les participants ont estimé que la campagne avait contribué à augmenter leur sentiment de sécurité, cependant, on constate que la campagne a manqué de visibilité car seulement un faible pourcentage d'individus se souvient l'avoir vue avant de répondre au sondage. Il en ressort néanmoins que la plupart des répondants sondés ont démontré de l'intérêt à recevoir plus d'informations sur la cybercriminalité et les moyens de s'en protéger. Dans le futur, il serait utile de mener des campagnes de prévention plus ciblées afin de mieux atteindre les objectifs poursuivis. La discussion fait état de plusieurs autres recommandations qui prennent appui sur les résultats obtenus et sur l'analyse de la documentation consultée.

Mots clés : cybercrimes, campagnes de prévention, sécurité, sentiment de sécurité, institution financière

Abstract

The purpose of this study was to evaluate the impact of a prevention campaign about cybercrimes that was run by a Canadian financial institution. More specifically, we examined how participants/clients perceived the financial institution's initiative to inform them about cybercrimes. The study also explored whether or not the campaign had the desired effect, which was to reinforce their sense of security. This campaign took place on October 2018 and 1,452 adults (831 males and 521 females) participated in the online web survey. The results indicated that the prevention campaign had been positively perceived by most of the respondents (75%), especially among older individuals (55 y/o and over). Further analysis has shown no gender differences in participants' responses. In general, participants felt that the campaign has increased their sense of safety; however, they also noted that the campaign lacked visibility and only a low percentage of individuals had seen it prior to the completion of the survey. Nonetheless, most participants have expressed an interest in receiving more information on cybercrime and how to take actions on protecting one's self. In the future, it would be advisable to conduct targeted prevention campaigns in order to better achieve its objectives. Discussion also includes recommendations based on the results and the review of the literature.

Keywords: cybercrimes, prevention campaigns, security, sense of safety, financial institution

Table des matières

Liste des tableaux

Liste des annexes

Remerciements

Je tiens à remercier mon directeur de recherche, le professeur Benoit Dupont pour ses judicieux conseils et pour son soutien tout au long de mes études de maitrise. Je le remercie très sincèrement d'avoir cru en moi et d'avoir accepté de diriger mon mémoire. Je le remercie également de m'avoir fait profiter de son expertise et de ses vastes connaissances dans le domaine de la cybercriminalité.
Je remercie l'institution financière qui m'a accueilli comme stagiaire et qui a accepté que j'utilise une partie de leurs données pour la réalisation de mon mémoire. Cette expérience de travail fut très enrichissante pour moi.
J'ai réalisé mes études de maitrise dans un contexte très difficile alors que ma mère a été très longuement hospitalisée dans une unité de soins intensifs. Sa détermination à affronter la maladie et le soutien indéfectible que lui a apporté mon père ont été pour moi une formidable source d'inspiration. Malgré ces moments difficiles, j'ai pu bénéficier en tout temps de leur appui et de leurs encouragements. Il me fait plaisir de leur témoigner toute mon admiration et leur rendre hommage en réalisant ce travail de recherche.

Introduction

De façon générale, la présente recherche s'intéresse à la cybercriminalité et aux stratégies de prévention de ce type de crime. Au cours des deux dernières décennies, la navigation sur Internet et l'utilisation de tous les services en ligne à partir d'appareils informatiques ou de communication sont devenues des activités très courantes et répandues au niveau planétaire, avec pour conséquence que de plus en plus de personnes sont victimes d'arnaqueurs (pour des fraudes informatiques, des vols d'identité ou de renseignements personnels, etc.). Au fil des ans, on constate également que les moyens utilisés par les malfaiteurs sont de plus en plus sophistiqués et ingénieux (Jagatic et al., 2005). Certaines enquêtes de victimisation de la cybercriminalité ont effectivement démontré que la prévalence de ces crimes n'est pas négligeable et en hausse constante. Pour bien mettre en contexte le sujet principal de ce mémoire, une définition de ce que l'on entend par cybercriminalité sera proposée et un portrait de l'étendu de ce phénomène sera dressé à partir des données provenant d'enquêtes de victimisation. La section suivante traitera des impacts de ce type de crime tant pour les personnes que les institutions et les milieux de travail. Dans la section suivante, il sera question des résultats d'études qui ont cherché à identifier les facteurs (notamment les caractéristiques individuelles) et les conditions qui augmentent le risque d'être victime de cybercrimes.

Le phénomène des cybercrimes est préoccupant car il prend de l'ampleur et les conséquences adverses pour les individus, les industries, l'économie et les gouvernements sont de plus en plus considérables et coûteux. Même si de nombreux moyens technologiques ont été développés ces dernières années pour enrayer ce type de crime (par exemple, les logiciels de détection, l'encryptage de données, etc.), force est de constater que ces seuls moyens ne sont pas infaillibles et qu'ils demeurent insuffisants pour prévenir tous les types de cybercrimes. Les modèles théoriques émanant des travaux en criminologie ont, depuis longtemps, guidé le développement des programmes de prévention qui se sont souvent avérés efficaces pour réduire l'occurrence des crimes du « monde réel », tels que les agressions physiques ou sexuelles, le vol d'argent ou de biens personnels, les fraudes commerciales, etc. Par contre, certains experts pensent que les approches préventives traditionnelles (par exemple, celles issues de la criminologie environnementale) peuvent plus difficilement convenir aux crimes commis dans le cyberespace en raison des particularités de ceux-ci et des conditions dans lesquelles ils sont commis (Brown, 2006). En effet, dans le cas des crimes se produisant dans le monde réel, les contrevenants agissent dans un contexte (un lieu de l'espace physique) bien délimité et il est possible d'agir sur cet espace

pour rehausser la sécurité, rendre plus difficile l'accès aux gains et aménager les lieux de manière à dissuader ou compliquer la commission du crime (comme c'est le cas avec la prévention situationnelle). Les études criminologiques ont également réussi à amasser au fil des ans de très nombreuses données sur les caractéristiques des contrevenants (pour à peu près tous les types de crimes), sur leur histoire de vie, sur leurs motivations ainsi que sur les facteurs « prédisposants ». De telles données ont été très utiles pour concevoir des mesures de prévention adaptées à ces réalités (par exemple, en concevant des interventions préventives visant à soutenir l'apprentissage de comportements socialement adaptés ou de protection chez les groupes à risque). Compte tenu de l'importance de toutes ces données théoriques, la recension des écrits abordera sommairement les modèles théoriques développés dans le domaine de la criminologie ayant guidé la conception des mesures préventives des crimes commis dans le monde physique (par opposition au monde virtuel). Une attention particulière sera accordée aux travaux réalisés en criminologie environnementale. Des exemples de programmes et autres initiatives de prévention seront aussi décrits brièvement et leur efficacité sera discutée.

Les cybercrimes ont comme particularité d'être largement répandus : toute la population, tous les lieux de travail, les commerces et toutes les institutions (scolaires, financières, gouvernementales, etc.) disposant d'un ordinateur et utilisant Internet peuvent être touchés ou pris pour cible. Pour cette raison, la prévention de la cybercriminalité peut être plus largement partagée entre les agences gouvernementales de la sécurité publique (pour protéger le public en général), les organisations privées qui souhaitent protéger leur clientèle ou leurs employés de la fraude ou des vols d'identité ou de renseignements personnels (par exemple, les compagnies d'assurances, les banques et les grandes corporations financières) et les individus eux-mêmes. Même si les études plus récentes en cybersécurité arrivent à nous renseigner un peu mieux sur les modes opératoires des cybercriminels et sur les conditions qui favorisent les crimes commis dans l'univers virtuel, il demeure difficile, faute de connaissances suffisantes, de mettre en place des dispositifs préventifs efficaces ciblant les cybercriminels. Dans ce contexte, un des moyens de prévention à la disposition des individus, des décideurs et des chefs d'entreprise est de miser sur l'éducation et la sensibilisation du public ou des employés (par la transmission d'informations, de conseils sur les façons de se protéger et d'assurer sa sécurité). L'idée de mieux informer le public et les clients des risques potentiels liés à l'utilisation des nouvelles technologies (navigation Internet, achats en ligne, utilisation de la messagerie électronique, etc.) est devenue une nécessité. Augmenter les

connaissances au sujet des stratégies de protection constitue en effet un objectif de prévention louable dans la mesure où cela responsabilise les usagers et leur permet de mettre en place une variété de moyens éprouvés et de favoriser l'adoption de comportements sécuritaires qui réduisent les risques d'être victimes (par exemple, en faisant preuve de prudence face à des sollicitations douteuses, en protégeant ses données personnelles, en changeant régulièrement de mot de passe, etc.).

L'idée de bien informer le public semble bien répondre à un besoin réel. À preuve, une majorité des Canadiens ne se sentent pas aptes à bien se protéger en ligne (seulement 44% ont dit savoir se protéger des cybermenaces) (Accenture, 2017). Cela augmente leur préoccupation et ces derniers souhaiteraient être mieux informés et outillés pour bien assurer leur sécurité en ligne. Ainsi, 78% des personnes sondées par Accenture (2017) ont répondu qu'elles souhaitaient que les gouvernements et agences de sécurité publique les éduquent davantage sur les meilleures méthodes de prévention pour leurs données personnelles en ligne.

Afin de répondre à ce besoin, différents organismes et institutions de plusieurs pays ont décidé d'élaborer et de lancer des campagnes d'information et de sensibilisation pour prévenir la cybercriminalité. Le gouvernement du Canada ne fait pas exception et a développé une campagne de prévention (*Get Cyber Safe*) qui se tient durant le mois d'octobre (*Cyber Security Awareness Month*). Cette campagne de prévention a pour but d'aider les Canadiens à être plus sécuritaires en ligne en les informant des différentes « petites actions » qu'ils peuvent entreprendre pour se protéger. Chaque semaine porte sur un thème différent en matière de sécurité (e.g., la valeur des données que l'on partage en ligne pour les cybercriminels). Une campagne similaire, développée suite à un effort combiné de la part du département de sécurité intérieure et le *National Cyber Security Alliance* (NCSA) existe aux États-Unis (CIS, 2019). Maintenant, le Royaume-Uni, l'Australie et la Nouvelle-Zélande font également leur propre campagne de prévention durant le mois d'octobre.

Si l'idée de bien informer le public en matière de cybersécurité fait consensus, on s'interroge maintenant sur les meilleures stratégies pour atteindre les objectifs de prévention. Certains experts ont proposé de s'inspirer des modèles théoriques développés dans le domaine de la santé publique qui, depuis longtemps, est largement impliqué dans le développement de mesures préventives populationnelles. Un parallèle peut en effet être établi entre les mesures préventives socio-sanitaires (protection contre les maladies, adoption de saines habitudes de vie) et les mesures

de protection contre les cybercrimes (protection contre les virus informatiques, les cyberattaques, etc.). Un modèle retient particulièrement l'attention : le *Health Belief Model* (HBM) (Rosenstock, Strecher, & Becker, 1994). Ce modèle s'intéresse plus spécifiquement aux représentations et aux croyances des individus en lien avec leur sentiment d'auto-efficacité et de sécurité. Ce modèle a été retenu car il permet d'expliquer les mécanismes qui agissent sur la motivation des personnes à se protéger. Ce modèle peut guider le développement de stratégies de prévention de la cybercriminalité pouvant être efficaces en augmentant le sentiment de sécurité et d'auto-efficacité des individus. La dernière partie de la recension des écrits abordera donc de façon plus détaillée le sujet de la prévention dans le contexte de la cybercriminalité. Le modèle théorique HBM sera décrit et sa pertinence sera justifiée dans l'élaboration des mesures de prévention. Les caractéristiques et les effets de certaines campagnes de prévention populationnelles seront aussi traités dans cette section. Enfin, le chapitre de la recension des écrits sera suivi par la présentation des questions de recherche (Chapitre 2).

Le projet de mémoire porte plus spécifiquement sur la prévention des cyberfraudes dans le contexte des institutions financières (IF). Une IF canadienne a décidé de lancer une campagne de prévention dont le but était de sensibiliser ses clients à la cybercriminalité. Plus précisément, trois objectifs étaient poursuivis : (1) mesurer l'intérêt des clients à être informés sur les sujets se rapportant à la cybercriminalité ; (2) proposer des stratégies de protection (au moyen d'affiches et d'articles en ligne) et, (3) évaluer l'impact de la campagne sur le sentiment de sécurité des clients. De plus, l'IF souhaitait obtenir un aperçu du point de vue de la clientèle au sujet de la campagne, peu de temps après que celle-ci ait pris fin. De nombreux utilisateurs ne se sentent pas concernés lorsqu'il s'agit de cybercrimes et pensent qu'il revient à leur institution financière de régler le problème. En informant les clients, on souhaite augmenter leurs connaissances et, par le fait même, leur donner les outils nécessaires afin qu'ils adoptent des comportements plus sécuritaires.

L'objectif principal de ce projet de mémoire, tel que défini au chapitre 2, est d'évaluer comment les participants ont perçu la campagne de prévention qui leur a été proposée. De façon plus précise, deux sous-objectifs sont poursuivis : 1) évaluer dans quelle mesure les répondants se souviennent des messages préventifs (de l'affichage et de la campagne) et analyser ce qu'ils ont retenu de ceux-ci (ce qu'ils pensent de cette initiative, de son utilité) ; et 2) évaluer quels sont les effets perçus (de la campagne et de l'affichage) par les répondants sur leur sentiment de sécurité envers l'IF. Un objectif secondaire est d'évaluer si ces effets varient en fonction de certaines

caractéristiques individuelles possiblement déterminantes (le genre, l'âge, le niveau d'épargne et l'intérêt pour les sujets relatifs à la protection informatique).

Le troisième chapitre traite de la méthode utilisée alors que le quatrième chapitre s'attarde à la présentation des résultats. Le dernier chapitre du mémoire (chapitre 5) présente une discussion et une analyse critique des résultats et propose quelques recommandations découlant des résultats obtenus et de l'analyse de la documentation scientifique consultée.

Chapitre 1 : Recension de la littérature

1.1. La cybercriminalité : définition et prévalence

Maras (2017) définit la cybercriminalité comme la commission d'un crime, c'est-à-dire un acte qui viole une ou des lois existantes, par l'entremise de la technologie (avec l'utilisation d'Internet, d'un ordinateur). De plus, d'après cette auteure on pourrait classifier les cybercrimes en six catégories distinctes : *cyberintrusion* et cybervandalisme ; cybervol (*cybertheft*) ; cybercrimes interpersonnels ; cyberdéviance et cybercrime d'ordre public ; cybercrime organisé ; et le cybercrime politique.

La *cyberintrusion* est le fait d'accéder à des systèmes informatiques ou des appareils numériques sans autorisation. Les fraudeurs peuvent alors décider d'interrompre l'accès à un site ou encore de voler des informations confidentielles. Quant au cybervandalisme, c'est lorsqu'un individu dégrade ou modifie le contenu d'un site web par exemple. Le cybervol est l'action de voler de l'argent ou des informations personnelles, médicales ou financières. On pense alors aux escrocs qui usurpent l'identité d'un individu afin de commettre une fraude. Ensuite, il y a les cybercrimes interpersonnels. Ces derniers sont des crimes commis contre un individu en particulier. L'auteur du crime est en communication et peut avoir une relation réelle ou imaginée avec la victime. Cela inclut les crimes du type *cyberbullying*. La cyberdéviance fait référence à l'utilisation de la technologie dans le but de commettre un acte qui va à l'encontre des normes sociales. Cela peut être légal (e.g., fétichisme des pieds) ou illégal (e.g., pornographie juvénile) et varier selon les lois locales. Le cybercrime d'ordre public est un acte illégal qui défie les normes, les valeurs et les coutumes à l'aide de la technologie. Par exemple, il y a des sites de jeux en ligne dont la légalité varie d'un pays à l'autre. Le crime organisé en ligne est un type de crime qui est fait par de nombreux individus qui se coordonnent afin de commettre des crimes en ligne. Le type de crime peut être varié (par exemple, un groupe criminalisé qui met au point un système pour escroquer des commerçants). Finalement, les cybercrimes politiques sont les crimes commis par des individus qui cherchent à faire avancer une cause politique ou encore dont l'objectif est politique (par exemple, les fraudes électorales en ligne) (Maras, 2017).

Les cybercrimes sont de plus en plus nombreux et les coûts reliés à ceux-ci deviennent plus élevés tant pour les individus que pour les organisations (commerciales et financières) et les gouvernements (de Bruijn & Janssen, 2017). D'après Wall (2008), il y aurait trois différentes générations de cybercrimes qui auraient évoluées au fil des années. La première génération comprend les crimes dits traditionnels, c'est-à-dire ceux qui existaient avant l'avènement de

l'informatique mais pour lesquels l'ordinateur et Internet facilitent le processus d'organisation (par exemple, le vol). La deuxième génération serait aussi basée sur les crimes traditionnels, mais pour lesquels la technologie a accru les opportunités criminelles (par exemple, les criminels ont maintenant un bassin de victimes potentielles beaucoup plus grand pour faire de la fraude). Ensuite, il y a la troisième génération qui, elle, n'existe que grâce à l'apparition du réseau Internet (par exemple, les virus informatiques).

Bien que les cyberincidents soient plus fréquents que dans le passé, le nombre de cybercrimes qui sont rapportés à la police n'a pas augmenté autant que l'on aurait pu s'y attendre (McGuire & Dowling, 2013). Les experts s'entendent pour dire qu'il est difficile de connaitre précisément le nombre de cybercrimes qui ont été perpétrés durant une année dans une population donnée, notamment parce qu'une minorité de crimes est rapportée aux autorités policières (Cross, Richards, & Smith, 2016; Deevy, Luchich, & Beals, 2012). De plus, les statistiques policières peuvent être influencées par la culture et la loi des pays (classification, définition, comptabilisation) (van Dijk, Mayhew, & Killias, 1990). Malgré tout, des sondages d'envergure ont été réalisés ces dernières années dans le but d'avoir une estimation la plus précise possible du phénomène des cyberfraudes. Par exemple, un sondage national a été réalisé par l'institut de la statistique, le *Crime Survey of England and Wales* (CSEW, 2019). Ce sondage de victimisation représentatif au Royaume-Uni a permis de constater que les cybercrimes représentent près de la moitié de tous les crimes recensés dans ce pays. Près d'une personne sur dix serait victime de cyberfraude, ce qui représenterait autour de 3,8 millions de cas. De ce nombre, on remarque que plus de 85% des cas n'ont pas été rapportés à la police (CSEW, 2019).

D'autres sondages réalisés en Europe confirment la prévalence élevée des crimes perpétrés en ligne. Reep-van den Bergh et Junger (2018) ont analysé les résultats de neuf sondages européens et ont constaté que deux types de cybercrimes obtiennent des taux de prévalence particulièrement élevés : le piratage informatique (de 1% à 6% des répondants selon les sondages) et la victimisation par logiciels malveillants (2% à 15%). Selon la même étude, la prévalence des fraudes liées aux achats en ligne oscillerait entre 1 et 3 % alors que les fraudes en lien avec les transactions bancaires et les paiements en ligne auraient un taux de 1 à 2%. Un des problèmes cependant avec les sondages est qu'il n'y a pas de questions standardisées par rapport aux cybercrimes. Ainsi, les sondages n'utilisent pas les mêmes termes ce qui rend difficile l'obtention d'un taux précis de cybercrimes. Par exemple, dans un sondage réalisé par le *National Computer Security Survey* (NCSS), on a

utilisé le terme *Computer virus* pour représenter différentes formes de logiciels malveillants (e.g., ver informatique et cheval de Troie) alors que d'autres sondages sont plus précis dans la désignation du type de virus (Maras, 2017).

Aux États-Unis, il existe le *National Incident-Based Reporting System* (NIBRS) qui permet de collecter des données par rapport aux incidents informatiques qui se produisent. Ainsi, lorsqu'une personne en autorité arrête un individu, elle peut indiquer si un ordinateur était impliqué d'une quelconque façon dans le crime. Par contre, cela n'indique pas quel type d'offense a été commis (Maras, 2017). Comme source officielle, on retrouve également le *Uniform Crime Reporting Program* (UCR Program) aux États-Unis. C'est un programme volontaire auquel les différentes forces de l'ordre peuvent décider de prendre part ou non. De plus, lorsqu'il y a plusieurs crimes de commis, seule l'infraction la plus grave va être rapportée (la loi de la hiérarchie). Il y a également un problème quant à la classification puisqu'on regroupe les différents types de cybercrimes ensemble, sans discernement (Maras, 2017).

Le Bureau des statistiques judiciaires aux États-Unis a également mis en place le *National Crime Victimization Survey* (NCVS) qui sonde la population deux fois par année. Comme pour tout sondage auto-révélé, il est cependant possible que les victimes sur-rapportent ou sous-rapportent les crimes qu'ils ont subis puisque les données rapportées ne font pas l'objet de vérification (Maras, 2017).

En Australie, l'organisme Scamwatch recense les crimes rapportés par la population au *Australian Competition and Consumer Commission* (sur le site web et au téléphone). Les données sont mises à jour mensuellement. L'hameçonnage serait le crime le plus souvent rapporté (13,5% des rapports en 2018). Le groupe d'âge qui aurait le plus rapporté de crimes est celui de 65 ans et plus (14,6% des rapports), suivi par le groupe d'âge de 25 à 34 ans (11,8% des rapports). Tout crime confondu, il y aurait eu 177 517 rapports durant cette année et les sommes perdues s'élèveraient à plus de 107 millions AUD. Les crimes ayant le plus fait perdre d'argent aux individus seraient les fraudes d'investissement. Les hommes auraient perdu plus d'argent que les femmes durant cette même période (plus de 56 millions AUD contre 48 millions AUD) ; cependant, les femmes ont davantage rapporté leur victimisation (53,1% des rapports contre 44,9% chez les hommes) (Scamwatch, 2019).

Au Canada, en 2009, l'Enquête sociale générale (ESG) sur la victimisation a été menée auprès des Canadiens de 15 ans ou plus (Statistique Canada, 2011). L'ESG a permis de recueillir

pour la première fois auprès des Canadiens de l'information sur leurs perceptions et leurs expériences en ce qui concerne la victimisation sur Internet, notamment le cyberbullying, la fraude bancaire par Internet, et les problèmes concernant les achats sur Internet. Les résultats démontrent que 7% des internautes de 18 ans et plus ont rapporté qu'ils avaient été victimes de cyberbullying ou de menaces. La forme de cyberbullying (qui inclut toutes formes de menaces selon l'enquête) la plus souvent mentionnée était le fait de recevoir des courriels ou des messages agressifs (ce type d'incident ayant été signalé par 73 % des victimes). La deuxième forme d'intimidation la plus fréquente concernait le fait d'être la cible de commentaires haineux (55 % des victimes). Enfin, moins de 1 victime sur 10 (8 %) a indiqué que quelqu'un avait envoyé des courriels menaçants en son nom. En ce qui concerne les fraudes bancaires, l'enquête révèle que 4% des personnes interrogées déclarent en avoir été victimes. Le pourcentage de victimes serait moins élevé chez les francophones (25% de moins que chez les anglophones). De façon intéressante, l'ESG a aussi démontré que ce type de crime constitue une source de préoccupation élevée parmi la population d'internautes canadiens (64% des personnes consultées). Enfin, en ce qui concerne les achats en ligne, 14% des personnes rapportent avoir rencontré des problèmes avec ce type d'activité dans les 12 mois précédant l'enquête (Statistique Canada, 2009).

Les coûts reliés à ce type de crime sont considérables et en croissance. Par exemple, pour les industries canadiennes, on estime qu'une somme de 14 milliards CAD aurait été dépensée au total sur une année en lien avec les incidents de cybersécurité (prévention, détection et recouvrement) (Statistique Canada, 2018a). Les sommes varient selon la taille de l'entreprise : les plus grandes entreprises auraient dépensé en moyenne 948 000$, tandis que les petites entreprises, 46 000$ (Statistique Canada, 2018a). On estime à 11.7 millions USD, la somme par établissement que les industries et grandes institutions financières américaines ont dû débourser en 2017 pour se protéger contre les cybercrimes (Ponemon, 2017).

D'après Statistique Canada (2018a), seulement 10% des entreprises qui ont subi une cyberattaque ont rapporté l'incident à la police en 2017. Ce très faible pourcentage peut s'expliquer soit par une résolution du conflit à l'interne (pour 53% des compagnies), soit une résolution à l'aide de consultants ou contracteurs en technologie informatique (35%) ou encore parce que l'impact était considéré trop mineur pour être rapporté à la police (29%) (Statistique Canada, 2018a). Certains sondages confirment qu'un très faible taux de crime est rapporté à la police, comme c'est le cas au Royaume-Uni : on estime qu'environ 120 à 150 cas sont rapportés par

rapport à 1 million de fraudes (Wall, 2007). En général, les gens perçoivent ces incidents comme étant trop futiles ou préfèrent que cela soit réglé à l'interne, en particulier lorsqu'il s'agit d'incident subvenant dans le contexte du travail. De la même façon, lorsqu'il s'agit d'une fraude bancaire, cela serait assez commun que les clients préfèrent informer seulement leur institution financière afin que celle-ci règle la situation, plutôt que d'avoir recours à la police (Wall, 2008).

Fafinski et Minassian (2009) ont avancé que cela pourrait être dû aux inquiétudes des individus et des institutions à l'effet que cela nuise à leur réputation. Selon ces mêmes auteurs, les cas de fraudes ou de cyberattaques rapportés par le public ou les institutions (financières ou commerciales) restent très faibles, soit 1% et 2% respectivement. Tandis que les crimes « traditionnels » sont rapportés beaucoup plus fréquemment, soit à 31% (Statistique Canada, 2018b). Il y a diverses explications possibles du très faible taux de cybercrimes rapporté par la population : manque d'information quant aux personnes à contacter pour rapporter le crime ; une attitude insouciante (avoir l'impression que c'est un crime qui ne vaut pas la peine d'être rapporté) ; ne pas croire que la police puisse agir et, finalement, ne pas être conscient d'avoir été victime d'un cybercrime (e.g., l'installation d'un logiciel malveillant) (Holt & Bossler, 2016; Maras, 2017). En effet, les conséquences liées à une cyberattaque ne sont pas toujours visibles pour les victimes (Wall, 2008).

La représentation que se font le public des cyberattaques pourrait être influencée par les sources d'information qu'ils consultent (Heath & Gilbert, 1996; Jackson, 2011; Riek, Bohme, & Moore, 2016; Wahlberg & Sjoberg, 2000). En effet, les journaux et les médias télévisés rapportent quasi exclusivement les cybercrimes de grande ampleur. De plus, grâce à Internet, les nouvelles se propagent maintenant très rapidement sans nécessairement qu'il n'y ait de vérifications de la véracité des faits (Brunton-Smith, 2017). Les reportages ou articles de journaux font souvent mention de l'importance de se protéger des cyberattaques ou des fraudes ; cependant, le public est rarement informé de façon claire et adéquate quant aux moyens efficaces de le faire (Shillair et al., 2015). Cela peut être une source d'angoisse pour certains utilisateurs qui redoutent les changements technologiques.

1.2. Conséquences des cybercrimes et facteurs de risque

1.2.1. Conséquences sur les individus, l'économie et les institutions

Les conséquences reliées aux cybercrimes sont variables et de diverses natures (financières, psychologiques, relationnelles, etc.) (Al-Ali, Nimrat, & Benzaid; 2018, Button, Lewis, & Tapley, 2014). Il y a divers facteurs (tels que l'âge, le genre et le revenu du ménage) qui ont une influence sur la manière dont les conséquences de la victimisation sont perçues (Keown, 2010; Walklate, 2007). Les individus qui sont victimes de cybercrimes peuvent souffrir d'anxiété, d'un trouble de stress post-traumatique ou d'un trouble de stress aigu et subir des pertes financières (Kirwan, 2011). Les pertes financières peuvent varier de façon significative ; dans les pires cas, cela peut mener certains individus à se retrouver à la rue (Cross, Richards, & Smith, 2016). Parmi les facteurs aggravants, Cross, Smith et Richards (2014) soulignent le fait que les autorités manquent souvent de considération envers les victimes qu'elles considèrent responsables de ne pas s'être suffisamment informées sur les moyens de protection. De plus, les victimes sont blâmées sous prétexte qu'elles se sont mises elles-mêmes dans cette position en étant négligentes (Button, Tapley, & Lewis 2013). Les victimes peuvent également être affectées psychologiquement et émotionnellement et ressentir de la colère (envers elles-mêmes ou l'arnaqueur) ou éprouver de la tristesse (Cross, et al., 2016; Henson, Reyns, & Fisher, 2016).

Les victimes qui ont répondu à des courriers électroniques frauduleux vont même jusqu'à être perçues comme des personnes « cupides et naïves » puisqu'elles souhaitaient obtenir des gains facilement (e.g., fraude nigérienne où on fait miroiter à la victime d'importantes sommes d'argent). Les victimes elles-mêmes vont tenir des propos qui blâment les individus qui sont tombés dans le piège en ayant répondu à ce type de fraude … tout en se dissociant elles-mêmes de ce discours (Cross, 2013). Un autre élément qui vient nuire à la perception qu'ont les individus envers la victime est que, même si cette dernière rapporte le crime à la police, si celui qui a perpétré le crime se trouve dans un autre pays (ce qui n'est pas rare), la victime est alors laissée à elle-même puisque les autorités de son pays vont déléguer la responsabilité à celles du pays concerné (qui est libre ou non d'y donner suite). Dans les cas plus extrêmes, certaines personnes vont avoir des pensées suicidaires ou même aller jusqu'à se suicider à la suite d'une telle fraude (Button et al., 2014; Cross et al., 2014). Pour certains individus, les conséquences de la fraude vont se faire ressentir sur de nombreuses années (e.g., la perte financière initiale peut mener à d'autres pertes plus importantes, telles que la perte de sa maison ou de son automobile) (Ganzini, McFarland, & Bloom, 1990). De

plus, les cybercrimes peuvent avoir un impact sur les activités quotidiennes des victimes en les privant de certains privilèges (par exemple, ne pas pouvoir retirer de l'argent avec leur carte bancaire dans l'attente de la nouvelle carte).

Maintenant que l'Internet est accessible à une plus grande proportion de la population, de meilleures méthodes de sécurité sont nécessaires afin de minimiser le nombre de victimes. En effet, la proximité ou le contact direct avec la victime n'est plus nécessaire dans la perpétration d'un crime. Il est maintenant possible pour les fraudeurs d'obtenir de l'information et causer des dommages financiers à des individus qui vivent sur un autre continent. Il n'y a donc plus de limites quant à l'étendue des victimes potentielles. De nos jours, la plupart des citoyens canadiens ont entendu parler des cybercrimes par l'entremise de différentes sources d'information (reportages, articles de journaux et campagnes de prévention), maintenant que ce type de crime est devenu un problème de plus en plus répandu. Toutefois, plusieurs chercheurs notent que la perception du public au sujet des fraudeurs (hackers) et de leur façon de procéder est parfois inexacte (Wall, 2008; Wash & Rader, 2015). La perception qu'entretient la population au sujet de la fraude informatique est principalement basée sur ce qu'elle voit et entend aux bulletins de nouvelles ou dans les médias. Plus récemment, Internet et les réseaux sociaux agissent comme une source d'information additionnelle pour certains individus. Or, bien que l'information soit transmise plus rapidement qu'avant, les nouvelles propagées ne sont pas toujours véridiques et cela peut créer de fausses nouvelles. Les portraits qui sont dépeints dans les films abordant la cybercriminalité est également peu représentative de la réalité (Wall, 2008). Néanmoins, comme déjà mentionné, il existe toujours un stigma autour des victimes de crimes informatiques.

Parmi les autres conséquences possibles que peuvent avoir les cybercrimes, on retrouve les conséquences économiques et institutionnelles. Ces dernières peuvent affecter tant les individus ou les entreprises et les gouvernements (Choo, 2011). Pour les compagnies, celles-ci peuvent être victimes de vols de données ou encore avoir une perte de propriété intellectuelle, ce qui pourrait résulter en une diminution de compétitivité avec les autres compagnies dans le même domaine d'activité. Pour les institutions (financières, gouvernementales, etc.), les conséquences peuvent prendre la forme de pertes de profit, de perturbations dans les services offerts et une désaffection de la clientèle.

1.2.2. Variables individuelles associées au risque de victimisation des cybercrimes : l'effet de l'âge, du genre, de la personnalité et du statut socioéconomique

Des chercheurs ont tenté de déterminer si certains facteurs associés aux caractéristiques des personnes ont un effet sur leur risque de cybervictimisation. Les résultats de leurs études se sont souvent avérés mixtes et peu concluants (Maras, 2017). Par exemple, il y a des études qui n'ont pas trouvé de différence entre les hommes et les femmes quant aux risques d'être victime d'un cybercrime (Ngo & Paternoster, 2011), tandis que d'autres ont constaté que le genre avait une importance. Ainsi, Reyns (2013) a trouvé que les hommes seraient plus à risque d'être victimes d'un vol d'identité en ligne que les femmes. Pour ce qui est du *cyberbullying*, les victimes seraient principalement des femmes (près de 60%; Li, 2007). D'autres études ont également démontré que les femmes ont plus d'inquiétude face à leur confidentialité en ligne (Hoy & Milne, 2010). En d'autres mots, elles voient leurs actions en ligne comme étant plus à risque que les participants masculins. Or cette inquiétude ferait également en sorte que ces dernières ont plus tendance à suivre avec attention les recommandations de sécurité que les hommes (Herath & Rao, 2009).

Cependant, les femmes ont moins tendance à faire les mises à jour des logiciels, ce qui peut les mettre en danger et elles sont plus nombreuses à adopter des mots de passe moins sécuritaires (Gratian et al., 2018). Leurs intentions en matière de sécurité seraient inférieures à ceux des hommes. Cela vient contredire une étude précédente d'Ifinedo (2012) qui avait trouvé que les hommes avaient de plus basses intentions de conformité en ce qui a trait à la sécurité. Un plus grand nombre d'hommes jugerait qu'ils sont aptes à bien se protéger par eux-mêmes sur Internet. De plus, lorsqu'on a demandé à un groupe de participants de juger de leur niveau de compétence, on a remarqué que les hommes avaient tendance à se qualifier comme étant plus compétents que les femmes. Or, parmi ceux qui se sont jugés comme étant compétents, on a remarqué que leurs actions ou notions de compétence variaient entres les participants. Ainsi, il n'y avait pas une grande différence entre les utilisateurs « moyens » et les utilisateurs « avancés » au plan de leurs connaissances des moyens de protection. Les utilisateurs avancés n'appliquaient pas toujours des moyens sécuritaires car plusieurs considéraient ces options comme non-pratiques et contraignantes (Ifinedo, 2012). En fait, d'après l'étude de Cain et collègues (2018), ceux qui se sont décrits comme experts en cybersécurité ont rapporté avoir des habitudes moins sécuritaires et avaient moins de connaissances en termes de cyberhygiène que les autres répondants à leur étude. Un fait surprenant cependant est que, pour les courriels d'hameçonnage, bien que les femmes soient plus préoccupées

par les potentiels de risques, ces dernières étaient plus susceptibles de succomber aux courriels d'hameçonnage que les hommes (54,7% contre 49%) (Sheng et al., 2010). Dans le cas de cette étude, les chercheurs attribueraient la différence au fait que les femmes qui ont participé à cette étude avaient moins de formation technique et de connaissances techniques que les hommes de la même étude. La différence entre le degré de conscience d'information sécuritaire (*Information Security Awareness* – ISA) entre les hommes et les femmes était cependant minime.

Pour ce qui est de l'âge, les plus jeunes auraient plus tendance à partager leurs mots de passe, ce qui est une pratique risquée (Gratian et al., 2018; Whitty et al., 2015). Les logiciels anti-espions seraient plus utilisés par les personnes plus âgées que les jeunes, ce qui ferait en sorte que ces derniers ont plus souvent des appareils infectés par des logiciels malveillants (Cain, Edwards, & Still, 2018). Il semblerait que les utilisateurs les plus âgés (plus de 50 ans) seraient ceux qui seraient le moins aptes à prévenir et éviter des accidents de cybersécurité suivi par les plus jeunes (en bas de 21 ans) (Koyuncu & Pusatli, 2019). Certaines études obtiennent des résultats contradictoires en ce qui concerne l'effet de l'âge en tant que prédicteur des vols d'identité en ligne. L'étude de Pratt, Holtfreter et Reisig (2010) n'a pas trouvé de différence significative entre les groupes d'âge, tandis que l'étude de Reyns (2013) a démontré que les plus jeunes étaient moins susceptibles d'être victimes d'un vol d'identité en ligne. Ainsi, il semblerait qu'il n'y ait pas de profil évident de « victime typique » pour les cybercrimes (notamment en ce qui concerne l'âge et le genre). Il apparait nécessaire de tenir en compte du type de crime commis (par exemple, le *cyberbullying* est beaucoup plus courant chez les adolescents que les autres groupes d'âge, bien qu'il ne faille pas négliger qu'il y ait également des victimes adultes et des enfants ; Kowalski & Giumetti, 2017) afin d'établir plus clairement si certaines caractéristiques propres aux victimes varient selon la nature des cybercrimes.

Par ailleurs, certains traits de personnalité pourraient prédisposer les individus à adhérer ou non à des comportements sécuritaires qui seraient en phase avec leurs intentions en matière de sécurité – ces traits seraient : le niveau de conscience (*conscientiousness*) et l'agréabilité qui font partie du modèle de personnalité des cinq dimensions (*Big Five*) en psychologie (Shropshire, Warkentin, & Sharma, 2015). Donc, les personnes qui présenteraient ces deux traits de personnalité auraient davantage tendance à se conformer aux mesures de sécurité (réduisant ainsi leur risque d'être victimes). Pour leur part, les individus ayant un niveau d'extraversion élevé seraient plus susceptibles de succomber aux courriels d'hameçonnage (Lawson et al., 2017). Une

étude faite par McBride et collègues (2012) est venue confirmée que les traits de personnalité influencent la manière dont les individus réagissent lorsqu'on leur présente le même scénario sur la sécurité. Ainsi, pour convaincre les utilisateurs à adopter des mesures de sécurité le plus efficacement possible, il faudrait adapter l'approche utilisée selon l'individu plutôt que d'utiliser un protocole générique.

Cette même étude de McBride et collègues (2012) a permis d'apporter des nuances quant à l'influence des traits de personnalité sur l'attitude des individus par rapport à la cybersécurité. Par exemple, un haut niveau d'agréabilité n'est pas à lui seul suffisant pour déterminer si un individu va être enclin à respecter les consignes de sécurité. Lors de leur étude, en plus des traits de personnalité, des facteurs situationnels ont été considérés soit : 1) l'auto-efficacité – la confiance perçue dans ses habiletés à se conformer aux politiques de cybersécurité; 2) la certitude d'une punition – la probabilité perçue d'être puni si on enfreint les politiques de cybersécurité; 3) la sévérité de la sanction – la sévérité de la peine encourue si on contrevient aux politiques de cybersécurité; 4) la vulnérabilité à la menace – le risque perçu qu'il y aura une conséquence négative si on viole les politiques de cybersécurité; 5) la sévérité de la menace – la gravité perçue des risques si on transgresse les politiques de cybersécurité; 6) l'efficacité de la réponse – l'efficacité perçue des mesures de cybersécurité; 7) le coût de la réponse – les conséquences négatives perçues si on adhère aux politiques de cybersécurité; 8) le réalisme – les probabilités qu'un des scénarios présentés dans l'étude puisse se produire au travail. Ainsi, un individu qui a un haut niveau d'agréabilité mais qui estime qu'il a peu de risques d'être puni (certitude d'une punition) sera plus susceptible de déroger des protocoles de cybersécurité (McBride, Carter, & Warkentin, 2012). Il en est également ressorti que les individus présentant un faible niveau d'auto-efficacité avaient plus tendance à ne pas respecter les politiques de cybersécurité. Lorsque les individus percevaient soit un niveau de certitude de punition ou de sévérité de punition faible, cela influençait également les probabilités que l'individu enfreigne les mesures de cybersécurité.

Un autre exemple connu est la recherche menée par Cellar, Nelson, Yorke et Bauer (2001) où la relation entre la personnalité et l'intention d'adopter un logiciel de sécurité basé sur le Web a été explorée. Ces derniers ont mis en évidence une relation significative inverse entre les variables « conscience » et « agrément » ainsi que le nombre total d'incidents (liés à la sécurité) survenus au travail. Cela suggère que les personnes les plus consciencieuses et ayant le plus tendance à respecter les règles sont moins susceptibles d'être impliquées dans une situation problématique au travail,

notamment au niveau cyber-sécurité (Cellar et al., 2001). Ce résultat a été corroboré par Organ et Paine (1999) qui ont démontré le même lien sans que les individus ne sachent que leurs comportements étaient surveillés.

En plus des variables associées à l'âge, au genre et à la personnalité, le statut socioéconomique des personnes peut aussi constituer un facteur d'influence à prendre en considération. En effet, Brennan et Dauvergne (2010) ont démontré que les statistiques en lien avec les crimes déclarés au Canada varient en fonction des conditions socioéconomiques des personnes (les individus les mieux nantis pouvant être moins à risque d'être victimes de certains crimes). Dans la même veine, certaines études en victimologie ont établi un lien entre le statut social (associé au niveau de revenu) des individus est la crainte d'être victime d'un cybercrime (Virtanen, 2017).

1.2.3. Les conditions favorables aux cybercrimes et la vulnérabilité des utilisateurs

Les attaques en sécurité informatique sont classifiées en trois catégories : physique, syntaxique et sémantique (Downs, Holbrook, & Cranor, 2006). En résumé, les attaques physiques vont s'en prendre à l'infrastructure physique de l'ordinateur et de son réseau, tandis que les attaques syntaxiques se font grâce à des virus, un ver informatique ou encore un cheval de Troie. Ainsi, on s'introduit dans l'ordinateur de la victime par l'entremise d'un logiciel. La troisième catégorie, quant à elle, vise à induire l'humain en erreur. On utilise des subterfuges pour lui faire croire quelque chose de faux ou de frauduleux. Par exemple, les attaques d'hameçonnage qui fonctionnent reposent sur la mauvaise identification de sites non légitimes perçus comme étant légitimes par la victime (Wu, 2006).

Une attention particulière sera accordée à cette dernière catégorie pour illustrer comment l'individu peut, par inadvertance, favoriser sa propre victimisation en laissant un fraudeur (hacker) exploiter ses vulnérabilités cognitives. Pour ce faire, l'utilisation de messages avec une bonne qualité visuelle et un contenu vraisemblable sont nécessaires. D'autres facteurs de nature psychologique ou humaine peuvent également contribuer à influencer le comportement des usagers. Par exemple, les techniques de persuasion ont fait l'objet de nombreuses études en marketing et en psychologie sociale. Afin de mieux comprendre comment la persuasion opère, Petty et Cacioppo (1986) ont développé un modèle de fonctionnement cognitif divisé en deux voies de traitement de l'information : la voie centrale et la voie périphérique. La voie centrale requiert un certain effort cognitif et les arguments sont soigneusement considérés par l'individu. Il faut

donc que l'information soit bien élaborée afin de convaincre l'individu d'adopter un comportement sécuritaire ou de protection. À l'inverse, la voie périphérique requiert peu d'effort cognitif pour traiter l'information, ce qui en fait la voie préférentielle pour les fraudeurs qui souhaitent influencer l'individu. Le système cognitif tente de minimiser les efforts en utilisant des stratégies plutôt que toutes les données disponibles (Besnard & Arief, 2004).

Plusieurs études ont tenté de comprendre pourquoi les gens succombent aux courriels d'hameçonnage. Après avoir analysé les courriels frauduleux de plusieurs usagers, Ferreira et Lenzini (2015) ont identifié des points communs à ceux qui étaient plus enclins à fonctionner (i.e. provoquer le clic sur le lien frauduleux). Par exemple, elles notent que la richesse de l'information (sentiment d'une présence sociale) est un élément clé pour une attaque réussite. Les gens sont deux fois plus susceptibles de se laisser prendre par un courriel contenant de l'information riche. En analysant et classifiant les différents courriels d'hameçonnage, les auteures en sont arrivées à la conclusion que la paire de principes la plus commune regroupait l'autorité (e.g., intimer la personne à cliquer ici) et la distraction (e.g., par l'utilisation d'un logo attrayant). La création d'un sens d'urgence a également été prouvée utile comme technique d'hameçonnage (Tavakoli & Yaacob, 2018). L'utilisation de signaux d'urgence fait en sorte que les gens négligent les « bons » signaux qui leur permettraient de détecter que le courriel est frauduleux (erreurs de grammaire ou d'orthographe, piètre qualité du logo, etc.) (Vishwanath et al., 2011).

Dès qu'il y a un élément qui éveille des soupçons de la part de l'utilisateur, ce dernier procède à un traitement systématique (l'individu va alors examiner les détails avec attention avant de prendre une décision) plutôt qu'un traitement dit « heuristique » (se servir des raccourcis mentaux tels l'utilisation une règle générale basée sur l'expérience antérieure plutôt que la théorie) (Vishwanath, Harrison, & Ng, 2018). C'est pourquoi les fraudeurs ont maintenant raffiné leurs techniques et il peut être plus ardu pour les individus avec peu de connaissances en cybersécurité de déceler les éléments trompeurs. À titre d'exemple, l'utilisation d'un protocole SSL (*Secure Sockets Layer*) qui affiche un cadenas dans la barre URL pour laisser croire que le lien est sécurisé (Tavakoli & Yaacob, 2018). Il faut donc s'assurer de bien vérifier la fiabilité de l'émetteur du certificat SSL. En plus de la façon dont le cerveau humain traite l'information, il faudrait également prendre en compte les comportements automatisés (Vishwanath et al., 2018). Ces derniers, bien qu'ils aient pour but de faciliter les actions quotidiennes, peuvent nuire lorsqu'il est

question de sécurité. Ces actions sont faites systématiquement sans que l'individu prenne réellement conscience de ce qu'il est en train de faire (LaRose, 2010).

D'après Benenson (2016), 78% des gens affirment être conscients des risques qu'il peut y avoir en cliquant des liens inconnus dans un courriel ; cependant, plusieurs d'entre eux vont tout de même cliquer sur ces liens, malgré les risques anticipés. Cela constitue un réel problème puisqu'il est estimé qu'un courriel sur 131 contient un logiciel malveillant (Symantec, 2017). Une étude de Ngo et Paternoster (2011) a d'ailleurs démontré, à partir d'un échantillon composé d'étudiants, que les compétences en informatique n'étaient pas un facteur de prédiction significatif de la victimisation de l'hameçonnage.

Il semblerait qu'une grande partie des utilisateurs tentent d'éviter d'avoir à prendre des décisions lorsqu'il s'agit de la sécurité puisqu'ils ne se sentiraient pas aptes à bien maintenir le niveau de sécurité nécessaire (Wash, 2010). Les utilisateurs délègueraient la responsabilité à une entité qu'ils perçoivent comme plus compétente qu'eux en matière de sécurité (par exemple, leur institution financière). Inversement, on constate que les individus ayant une perception d'auto-efficacité élevée tendent à utiliser plus de logiciels de sécurité (Rhee, Kim, & Ryu, 2009). Ceux-ci ont également tendance à faire des copies de sauvegardes plus régulièrement et à utiliser des mots de passe forts. De plus, les utilisateurs avec un score élevé en auto-efficacité sont davantage déterminés dans leur intention à poursuivre leurs efforts en matière de sécurité. L'auto-efficacité semble donc être un élément clé important pouvant aider à déterminer les pratiques de sécurité d'un individu. L'auto-efficacité servirait également à motiver un individu à exercer un effort continu pour maintenir son niveau de protection. Par contre, la perception d'auto-efficacité peut changer positivement comme négativement au gré des expériences vécues. Par exemple, être victime d'un virus ou d'une cyberfraude pourrait avoir pour effet de diminuer de façon significative le sentiment d'auto-efficacité d'une personne. Cela pourrait créer chez celle-ci créerait un état émotionnel négatif tel que l'anxiété ou le stress (Rhee et al., 2009).

Il est possible d'avoir conscience des comportements sécuritaires à adopter et d'en faire fi (Rhee, Ryu, & Kim, 2012). Par exemple, Whitty et ses collègues (2015) ont trouvé que connaître les bonnes pratiques de cybersécurité n'est pas suffisant pour changer ses habitudes problématiques (par exemple, partager son mot de passe). C'est pourquoi certains chercheurs se sont questionnés sur la relation entre les intentions de l'individu et son comportement. Par exemple, Bagozzi (2007) a trouvé un faible lien entre les intentions de l'individu et l'adoption de

ses comportements en matière de sécurité. D'après les études actuelles, les intentions sont mises en action seulement environ 50% du temps (Sheeran & Webb, 2016). Comme déjà mentionné, même lorsque les individus savent qu'il est important d'être sécuritaires et se disent motivés à l'être, ils vont mettre la sécurité de côté lorsqu'il y a conflit de priorité entre fonctionnalité et sécurité (Albrechtsen, 2007). On cherche à atteindre un niveau de performance qu'on estime acceptable plutôt qu'optimal (Simon, 1957). D'après Sheeran et Orbell (2000), il est plus probable qu'un individu réussisse à modifier un comportement basé sur ses propres croyances que lorsque celui-ci agit afin de se conformer aux normes sociales. Ainsi, il y aurait des facteurs additionnels liés à la personnalité des individus qui pourraient modérer le lien entre les intentions d'agir et l'usage des comportements appropriés. Il faut donc faire preuve de prudence lorsqu'on questionne les personnes à propos de leurs intentions puisque leurs comportements peuvent ne pas coïncider.

Quant aux actions qu'ils entreprennent pour se protéger, 89% des utilisateurs affirment avoir un logiciel anti-virus sur leur ordinateur. Cependant, parmi ces gens, très peu comprennent vraiment comment ces outils informatiques fonctionnent et comment bien les configurer (Furnell et al., 2007). De plus, lorsqu'un message de sécurité intervient avec la tâche que l'individu est en train de réaliser, celui-ci va avoir tendance à l'ignorer ou encore à le contourner afin de continuer ses actions (Pfleeger & Caputo, 2012). Cela signifie que même si un site a été identifié comme potentiellement malveillant, l'individu va tout de même vouloir y accéder si cela s'inscrit dans la tâche qui est en cours. Le même processus est applicable pour le changement de mot de passe. Les utilisateurs ont tendance à reporter le moment où ils vont devoir le modifier de façon intentionnelle (Belanger et al., 2011).

Ainsi, on remarque que l'utilisateur est le maillon faible dans la chaîne de sécurité (Gratian et al., 2018; Herley, 2009; Schneier, 2000), puisque les systèmes d'information restent vulnérables si l'humain décide de ne pas mettre en pratique les mesures de sécurité. Un des problèmes expliquant cela serait que, malgré tous les efforts déployés pour transmettre l'information et sensibiliser les utilisateurs d'Internet à se conformer aux règles de sécurité, on utilise souvent une approche qui met l'accent sur les données factuelles plutôt que d'adapter l'approche à l'audience que l'on souhaite rejoindre (Stewart & Lacey, 2012). Il faut donc bien comprendre le « modèle mental » du public cible pour contrer les cybercrimes (cet aspect sera développé plus en détail dans la section portant sur la prévention des cybercrimes). Le modèle mental réfère à la manière de raisonner d'un individu (Morgan et al., 2002). Ce dernier est basé sur ses croyances, la force de

ces croyances et les liens entre ces croyances ; cela explique comment l'utilisateur en vient à faire des choix qu'il perçoit comme rationnels (son modèle de décision) (Wash, 2010). C'est également en exploitant les modèles mentaux que les fraudeurs réussissent à faire les cyberattaques de type sémantique.

Wash (2010) a identifié des modèles de décision qui permettent d'expliquer pourquoi les utilisateurs ignorent les recommandations de sécurité des experts. Par exemple, il y a le modèle où les hackers sont perçus comme attaquant seulement les « gros poissons ». Ainsi, ils s'en prendraient majoritairement aux gens riches et puissants. Les utilisateurs qui ont cette croyance ne se sentiraient pas à risque puisqu'ils ne se considèrent pas comme étant assez importants (ou assez nantis) pour qu'un individu décide de s'en prendre à leur ordinateur (Wash, 2010).

Un autre motif a été invoqué par Herley (2009) pour expliquer la vulnérabilité des utilisateurs d'Internet aux crimes en ligne. Cet auteur avance l'idée voulant que les individus perçoivent davantage d'inconvénients à appliquer les mesures de sécurité que de gains potentiels. Cette hypothèse dite « économique » suppose que lorsque vient le temps d'établir le ratio coûts/bénéfices, les utilisateurs prennent en compte le temps et l'effort (coûts) qu'ils doivent dépenser pour mettre en place les conseils de sécurité. En contrepartie, les bénéfices sont plus intangibles ou moins évidents puisque les utilisateurs ne percevront aucun changement si les mesures prises leur ont permis d'éviter les conséquences négatives d'une attaque (ils peuvent aussi se dire que la probabilité d'être victime est assez infime et que cela ne vaut pas la peine de se mobiliser au plan de la sécurité).

Une autre raison permettant d'expliquer la vulnérabilité des personnes au cybercrimes est que, lorsqu'il est question de risque, la prise de décision est souvent irrationnelle et non conforme aux options proposées par les experts (Wash, 2010). Cela pourrait être dû au phénomène de la rationalité limitée d'Herbert Simon qui explique pourquoi des individus qui semblent logiques prennent parfois des décisions irrationnelles d'un point de vue extérieur (Simon, 1957). Selon cette notion de rationalité limitée, il y aurait trois grandes limitations qui amèneraient les individus à être irrationnels : 1) la focalisation sur la satisfaction (*satisficing) :* les individus apprennent à être contents de résultats satisfaisants plutôt qu'optimaux, ce qui diminuent leur intérêt à tenter de trouver la meilleure solution possible; 2) les individus sont limités par leurs habiletés (et comment ils perçoivent leurs habiletés), ainsi un individu qui perçoit l'installation de logiciels anti-virus comme étant hors de sa portée ne le fera pas, et 3) les individus basent leurs décisions en fonction

des limites de temps et ressources lorsqu'ils doivent consacrer pour faire des tâches – ils se servent de procédés « heuristiques ». L'étude d'Albrechtsen (2007) sur la perception des utilisateurs sur la sécurité de l'information en est arrivée à une conclusion semblable. Lorsqu'il y a un conflit d'intérêt entre les tâches à effectuer (tâches primaires) et la sécurité (tâches secondaires), les individus ont favorisé la complétion de leurs tâches primaires (Pfleeger, Sasse, & Furnham, 2014). La rationalité limitée fournit une explication sur la raison qui pousserait les utilisateurs à choisir l'option qui semble la moins sécuritaire parmi les options qui pourraient être appliquées – l'humain a tendance à privilégier l'option qui est la moins limitative et la plus facile à appliquer pour répondre à ses besoins.

Lorsqu'il est question de sécurité informatique, seule une minorité d'individus (quatre utilisateurs sur dix) se sent apte à comprendre et à accorder le temps requis pour la sécurité (Furnell et al., 2007). Pour la majorité des répondants, il y a divers obstacles ou barrières perçus qui les empêchent de comprendre les mesures de sécurité ou encore de les mettre en application. Ce sujet sera développé davantage dans la section réservée à la présentation des effets des campagnes de prévention de la cybercriminalité.

Avant d'aborder plus spécifiquement les stratégies préventives adaptées à la cybercriminalité, il convient de décrire les approches et les modèles développés dans le domaine plus général de la criminologie en lien avec la prévention du crime.

1.3. La prévention en criminologie

1.3.1. Les approches en matière de prévention du crime

La prévention peut se définir comme l'ensemble des dispositions prises pour prévenir un danger, un risque ou un mal (Dictionnaire Larousse, 2019). En criminologie, la prévention réfère à tout moyen ou stratégie visant à réduire la probabilité qu'un crime soit perpétré. Les moyens de prévention peuvent être utilisés par un individu (en adoptant des mesures de sécurité personnelles telle que verrouiller les portières de sa voiture), par un groupe de citoyens (par exemple, des résidents qui se mobilisent pour assurer la surveillance de leur quartier), par les autorités policières (par exemple, des patrouilleurs qui donnent des conseils à des propriétaires sur la façon de se protéger contre les vols), par des établissements scolaires, commerciaux ou financiers (par exemple, avec l'embauche d'un agent de sécurité) et par les gouvernements (par exemple, en suggérant des mesures de protection du public au moyen de campagnes d'information). La prévention peut aussi être définie en fonction de la nature des crimes : prévention contre les

agressions ou crimes contre les personnes ; prévention des crimes concernant l'intégrité des lieux et les possessions (vandalisme, vols d'objets), la prévention du non-respect des lois et des règlements (par exemple, les affiches incitant les conducteurs à réduire leur vitesse) et prévention des fraudes ou crimes de nature financière (détournement de fonds, blanchiment d'argent), etc. Enfin, la prévention peut aussi être examinée sous l'angle des moyens utilisés pour réduire les dangers ou les risque de criminalité : les moyens technologiques (systèmes d'alarme, logiciel anti-virus), les moyens humains (présence policière, agent de sécurité) et les stratégies informatives ou de communication (affichage, messages télévisés, etc.).

De façon générale, on distingue trois grandes approches préventives adaptées au domaine de la criminologie : la prévention primaire, secondaire et tertiaire (Mackey, 2013). Ces approches ont initialement été développées dans le domaine de la santé mais on peut attribuer leur adaptation à la criminologie à Brantingham et Faust (1976). Ces types de prévention ont en commun de chercher à réduire l'incidence ou la prévalence de certains phénomènes criminologiques. La prévention primaire a habituellement comme but de rejoindre toute la population en général pour diminuer les risques qu'un crime ne soit commis. Ainsi, l'accent est mis sur l'anticipation, bien avant qu'un crime n'ait eu lieu. Par exemple, le gouvernement qui souhaite contrer les vols de voiture pourrait lance une campagne de prévention en utilisant différents moyens pour rejoindre l'ensemble de la population (télévision, journaux, affichage, etc.). D'après Brantingham et Faust (1976), ce type de prévention serait la plus prometteuse des trois puisque l'on agit avant qu'il y ait de la criminalité.

La prévention secondaire, quant à elle, vise une population plus ciblée : ceux qui sont à hauts risques de devenir des délinquants. Ces derniers sont en présence de plusieurs facteurs de risques mais ils ne sont pas encore considérés comme des délinquants chroniques (Mackey, 2013). Cette approche vise à renforcer les facteurs de résilience et à réduire les facteurs de risque (Shader, 2003). Par exemple, l'instauration d'un programme préscolaire dans un milieu défavorisé pour favoriser l'apprentissage de comportements prosociaux (Regoli, Hewitt, & DeLisi, 2010). Certains experts critiquent toutefois ce type de prévention puisqu'elle risque d'entraîner une forme « d'étiquetage » des groupes visés (une forme de labelling) pouvant créer des prophéties auto-réalisatrices (Gilling, 1997). Finalement, il y a la prévention tertiaire qui tente de prévenir qu'un délinquant qui est déjà sous le contrôle du système de justice ne commette d'autres crimes (Mackey, 2013). Ce type de prévention mise principalement sur la réhabilitation, en plus de cibler

les facteurs de risque et de protection. Par contre, certains ont questionné l'efficacité de certains programmes de ce type, tel *Scared Straight* (1978). Finckenauer, Gavin, Hovland et Storvoll (1999) ont évalué l'impact qu'a eu ce programme sur les jeunes délinquants. Ils en ont conclu que celui-ci n'a pas eu l'effet escompté ; le programme aurait même nui (effets iatrogènes) puisque le groupe contrôle (11%) a moins récidivé que le groupe expérimental (41%) après la fin du programme, six mois plus tard. D'autres études sont arrivées à des résultats similaires démontrant que les programmes de sensibilisation visant les contrevenants mineurs ne sont pas efficaces dans la dissuasion de la criminalité (Klenowski, Bell, & Dodson, 2010; Petrosino, Turpin-Petrosino, & Buehler, 2003).

Outre la classification des types de prévention (primaire, secondaire et tertiaire), il est possible d'étudier la prévention en criminologie sous l'angle des approches ou modèles théoriques ayant guidé le développement des stratégies préventives. Les approches les plus importantes élaborées dans le domaine de la criminologie sont décrites ici.

La prévention situationnelle (*Situational Crime Prevention*) est une approche qui cible les opportunités criminelles et émane des efforts de prévention déployés par le *Home Office Research Unit* dans les années 1970 (Clarke, 2005). Le programme initial cherchait à identifier les caractéristiques des délinquants qui ont tendance à récidiver. Par la suite, le programme a également considéré les écarts de conduite lors de l'institutionnalisation. Cela a amené le *Home Office* à voir la délinquance comme étant une réponse à l'environnement. Ainsi est venue l'idée de réduire la criminalité en bloquant ou réduisant les opportunités criminelles. Le *Home Office* a ensuite publié les résultats de cette recherche dans « *Crime as Opportunity* » (Mayhew et al., 1976). Les résultats découlant de ces travaux ont inspiré Clarke (1980) et ont mené à l'élaboration du concept de prévention situationnelle. Avec cette approche, on cherche à prévenir les crimes en : (1) introduisant des changements à l'environnement afin de rendre les opportunités criminelles moins attrayantes ; (2) en réduisant les « récompenses » (gains potentiels) ; (3) en augmentant l'effort nécessaire perçu pour réussir ; (3) en augmentant la perception du risque encouru ; (4) en réduisant les provocations, et (5) en enlevant les excuses. En tout, Clarke a établi cinq catégories générales de moyens (mentionnées plus haut) comprenant 25 techniques pour réduire les crimes. L'objectif principal de cette approche de prévention est d'enlever les opportunités criminelles (Clarke, 2010).

Cette approche ne tente pas d'expliquer les causes du crime mais bien de prévenir celui-ci. Les trois composantes principales sont celles-ci : on cible une forme de crime spécifique, on introduit un changement dans l'environnement qui se veut le plus permanent possible, ce qui vient par la suite rendre la tâche plus difficile au délinquant ou encore lui offre un gain (une récompense) moins grand qu'auparavant (Clarke, 2010). Si on applique cette approche aux cybercrimes par exemple, il serait possible de proposer l'utilisation d'un mot de passe fort, ce qui augmenterait l'effort nécessaire perçu par le criminel opportuniste (Chavez, 2018). Il est en effet beaucoup plus facile de modifier les éléments qui constituent la situation (tel qu'ajouter un code de sécurité sur son téléphone cellulaire) que d'essayer de changer les intentions d'un individu qui a décidé de commettre un crime.

La plupart des théories sur le contrôle du crime mette l'accent sur le criminel afin de réduire le taux de crime (Clarke, 1997). La prévention situationnelle, à l'inverse des autres, se penche avant tout sur les mesures à prendre afin de réduire le risque d'être victime d'un crime. Le gouvernement ainsi que les institutions ont un rôle à jouer dans l'aménagement des espaces (secteurs d'activités) et des bâtiments qui pourraient être propices à des actes criminels. L'Angleterre et les Pays-Bas sont de bons exemples puisque ces pays ont intégré des aspects de la prévention situationnelle dans leur politique gouvernementale de prévention du crime. Ainsi, le contrôle du crime est maintenant considéré comme une responsabilité partagée dans tous les secteurs de la société, et non plus comme la responsabilité exclusive du gouvernement (Garland, 1996). Il faut évidemment trouver un juste milieu entre la protection des citoyens et la liberté individuelle de ces derniers. C'est d'ailleurs pourquoi il y a autant de réticence par rapport à l'adoption de cette approche en prévention par les différents États. Par exemple, les membres du gouvernement issus de la droite conservatrice aux États-Unis sont nombreux à percevoir ce type de prévention comme une atteinte à la liberté et à la vie privée des citoyens respectueux de la loi (Bright, 1992).

Une autre théorie communément employée en prévention en criminologie et dérivée de la prévention situationnelle est la Routine Activity Theory (RAT). Celle-ci a été conceptualisée par Cohen et Felson (1979) et tente d'expliquer la criminalité en se basant sur les actions des individus (victimes comme délinquants). Selon ces auteurs, trois facteurs viendraient faciliter la commission d'un crime : la présence d'une victime potentielle, la présence d'un ou d'une personne délinquante motivée à commettre un crime et l'absence de gardes compétents (mesures de surveillance et de

contrôle efficaces). Ainsi, un manque de surveillance combinée avec un délinquant motivé en présence d'une cible potentielle seraient les conditions propices à la commission d'un crime. D'après ce modèle, les opportunités criminelles peuvent être manipulées en jouant avec les différents facteurs. Bien évidemment, il est essentiel d'avoir un criminel cherchant une opportunité criminelle afin que le crime soit commis. Par exemple, si on augmente la surveillance d'un lieu de façon directe ou indirecte (Felson, 2002), les opportunités criminelles diminuent. Cette théorie s'est avérée utile pour comprendre pourquoi il y a eu une augmentation des vols de domiciles dans les années 1960. En effet, durant cette décennie, il a été établi qu'il y avait de moins en moins de femmes au foyer, ce qui faisait en sorte que les maisons étaient davantage laissées sans surveillance (avec les biens plus facilement à disposition), ce qui augmentaient les opportunités criminelles des cambrioleurs (Lab, 2010).

Contrairement à la RAT, la *Lifestyle Perspective* (Hindelang, Gottfredson, & Garofalo, 1978) met davantage l'accent sur les victimes et leurs choix. Ainsi, le style de vie et les comportements d'un individu pourrait avoir un impact sur les risques de victimisation. Par exemple, si un individu décide de fréquenter des lieux dangereux régulièrement, ils augmentent ses chances d'être victime d'un acte criminel.

Parmi les théories souvent utilisées pour guider les efforts de prévention, on retrouve le *Rational Choice Theory (RCT)* qui est également une théorie qui cible l'environnement en criminologie. Cette théorie, élaborée au 18^{e} siècle, sous-entend que les êtres humains agissent en fonction de leurs propres intérêts (Wright, 2009). Ce concept a également été mis de l'avant par Jeremy Bentham qui l'a appelé *utilitarianisme*. C'est cependant Clarke et Cornish (1985) qui l'ont développée telle que nous la connaissons aujourd'hui. Les théoriciens associés à cette approche croient que l'individu décide de par lui-même de commettre ou non un acte criminel en se basant sur le calcul qu'il fait des gains par rapport aux pertes potentielles (Mackey, 2013). Ainsi, ce modèle s'approche de la théorie de la dissuasion (*deterrence theory*) qui avance que l'éventualité d'une menace de punition est une condition susceptible d'entrainer le désistement de l'acte criminel (Pratt, Cullen, Blevins, Daigle, & Madensen, 2006). Selon ce même modèle théorique, il y a trois conditions nécessaires afin de s'assurer qu'un individu ne commette pas de crime : la punition doit être rapide (*swift*), assurée et sévère (en proportion avec l'acte). On peut diviser les moyens de dissuasion en deux formes : générale et spécifique. La première souhaite prévenir le crime dans la population générale grâce aux diverses lois, tandis que la seconde a comme objectif

de dissuader les individus ayant déjà commis des crimes d'enfreindre la loi de nouveau (Mackey, 2013).

La *Crime Pattern Theory* (Brantingham & Brantingham, 1993) vient compléter l'ensemble des trois principales théories de l'environnement en criminologie (avec le RAT et le RCT). Cette dernière stipule qu'il est possible de discerner des schémas (ou patterns) de comportements criminels. En d'autres mots, il y aurait des moments et des lieux qui seraient plus propices à la criminalité et il est judicieux de connaitre ces données (sur ces schémas criminels) pour être en mesure de réduire les risques que le crime soit commis. Ainsi, si on arrive à comprendre quand et où les crimes sont plus probables de survenir, on peut intervenir et prévenir leur apparition.

Issues de la prévention par l'aménagement du milieu, deux autres approches ont été élaborées, celles-ci étant de type prévention primaire. Elles ont également été influencées par les RCT et RAT (Robinson, 1996). Il s'agit des approches du « *crime prevention through environmental design* » ou CPTED par C. Ray Jeffery (1971) et du « *defensible space* » par Oscar Newman (1972). Ces théories sont toutes maintenant classifiées comme faisant parties de la catégorie CPTED. Les travaux d'Elizabeth Wood (1961) et Jane Jacobs (1961), entres autres, ont influencé la création de l'approche de l'espace défendable (Kitchen & Schneider, 2001; Robinson, 1996). Pour Wood (1961), il était important que les adolescents aient un endroit où aller afin de prévenir les actes de criminalité (pouvant être commis sous prétexte de ne pas avoir de lieux ou de choses à faire). Elle prônait aussi l'importance d'avoir des lieux de loisirs bien en vue afin d'améliorer leur accessibilité et ainsi prévenir le crime (Armitage, 2013). Jacobs (1961) a introduit le concept de « yeux sur la rue » (*eyes on the street*) qui propose que d'avoir le plus de circulation piétonnière possible amène plus de surveillance et améliore ainsi la sécurité des rues de la ville.

Le terme CPTED, qui est toujours utilisé aujourd'hui, a été introduit par Jeffery (1971). Ce dernier a démontré de l'intérêt dans les travaux de Wood et postulait que les individus étaient sensibles à leur environnement et les stimuli environnementaux. Ainsi, l'utilisation de techniques modifiant l'environnement pourrait diminuer les stimuli amenant à la commission de crimes et entraîner des réponses aversives de la part des délinquants en même temps (Gilling, 1997). Jeffery n'a cependant pas été précis quant aux techniques qui devraient être utilisées afin d'en arriver aux résultats souhaités.

L'approche de « l'espace défendable » a été créée par un architecte et repose donc sur l'architecture des bâtiments. Newman a proposé quatre notions clés : 1) la territorialité – la sous-

division des bâtiments et environs pour repousser les intrus de pénétrer et encourager les résidents à défendre leur zone, 2) la surveillance naturelle – aménager les édifices afin de permettre une surveillance, c'est-à-dire avoir des bâtiments peu élevés par exemple, 3) l'image et l'apparence – si on ne prend pas soin d'un bâtiment et qu'on laisse les graffitis cela va encourager le vandalisme; en le gardant propre, on renforce le sentiment d'appartenance et, 4) le milieu – le secteur où est situé l'édifice est également important (Mayhew, 1979). Parmi ces quatre aspects, Newman met particulièrement l'accent sur la division du territoire des zones résidentielles et l'amélioration des opportunités de surveillance afin de prévenir le crime.

Une autre théorie qui a été élaborée dans les années 1980 visant à prévenir la criminalité est la théorie de la fenêtre brisée par Wilson et Kelling (1982) – celle-ci a été développée à partir de la notion d'image de Newman. Cette théorie prône que lorsqu'il y a des signes de désordre social et physique (par exemple une fenêtre brisée), cela va mener à plus de désordre et contribuer à la criminalité puisque les délinquants vont percevoir le quartier comme ayant peu de contrôle social. Les traces visibles de désordre vont attirer d'autres délinquants (Mackey, 2013). De plus, ils ont remarqué que cela est relié à la peur du crime (Grohe, 2011). La peur du crime combinée avec une perception de crime élevé amènent les citoyens d'un quartier à être moins satisfaits (Hipp, 2010) et, par le fait même, à s'investir moins dans leur quartier (Skogan, 1990). Cela mène aussi à l'exil des individus ayant un meilleur statut socio-économique (ne laissant sur place que les plus démunis qui ne peuvent partir). Cet exode contribue à alimenter le sentiment de peur de la population qui reste dans le quartier maintenant appauvri (Grohe, 2011). La méthode pour remédier à ce problème serait d'avoir des membres de l'autorité qui maintiennent l'ordre en employant une tolérance zéro. Ainsi, si on répare immédiatement lorsqu'il y a des dommages (pour préserver une image d'ordre) cela ferait en sorte que le quartier ne serait pas perçu comme étant sous l'emprise d'un faible contrôle social (Mackey, 2013).

Les mesures de prévention du crime qui cherchent à limiter le nombre de victimes visent tout particulièrement à modifier les attitudes, les connaissances et les comportements de la population en générale. Ces mesures peuvent aussi servir à sensibiliser le public aux conséquences de leurs mauvaises habitudes ou comportements à risque (Self-Brown et al., 2008). Les deux sections qui suivent présentent respectivement les approches institutionnelles de la prévention du crime et les caractéristiques des campagnes visant à prévenir la criminalité.

1.3.2. Approches institutionnelles des programmes de prévention du crime

Dans le but d'assumer leurs responsabilités vis-à-vis leur population en matière de protection et de sécurité publique, plusieurs États se sont dotés d'organismes ayant pour mandat d'étudier, de développer et de mettre en pratique des moyens de prévention des crimes. Les premières institutions en prévention du crime ont commencé à être instaurées en Europe dans les années 1970. Cela a été un processus graduel comportant des stratégies, des politiques et des programmes en matière de prévention de crimes par le gouvernement (Sansfaçon & Waller, 2001). C'est au Danemark en 1971 qu'a été créé le premier Conseil national officiel en prévention du crime. Cependant, c'est en France qu'a réellement débuté l'engouement pour le développement des Conseils de prévention du crime locaux en 1982 avec la création du *Conseil national de la prévention du crime* (CNPC). Peu de temps après, d'autres pays ont suivi le pas. En 1998, le gouvernement d'Angleterre et du Pays de Galles a lancé un nouveau programme visant à prévenir le crime : le *Crime Reduction Programme* (CRP) (Dhiri et al., 2001). Celui-ci était différent des programmes employés dans le passé puisqu'il était basé sur une approche fondée sur des données probantes. C'était la première fois que le gouvernement de tous pays confondus investissait une somme aussi considérable pour un programme de prévention du crime. Auparavant, on tentait de composer avec les effets des crimes une fois que ceux-ci étaient survenus. La différence majeure était que, cette fois, on voulait réduire les crimes en ciblant leurs causes. Le programme CRP proposait des stratégies testées à adopter afin de réduire le taux de crimes. À titre d'exemple, l'accent était mis sur les familles, enfants et écoles qui ont des facteurs de risques élevés en lien avec la délinquance (e.g., statut socioéconomique faible) (Day & Wanklyn, 2012). Ainsi, on travaillait en collaboration avec ces milieux pour tenter de réduire les risques. Ce programme s'est avéré efficace et a été prolongé en 1999. Par la suite, cette approche a également été intégrée à divers programmes reliés tels le programme sur la violence domestique et violence contre les femmes. Le Canada, quant à lui, a vu son premier programme national officiel de prévention du crime instauré en 1994 et 1998 (Sansfaçon & Waller, 2001).

Outre les organismes gouvernementaux dédiés à la prévention institutionnelle à grande échelle, on retrouve également des programmes de prévention du crime plus ciblés (financés par des ministères, des fondations privées) qui visent plus particulièrement les familles (e.g., Elmira Prenatal/Early Infancy Project - PEIP; Olds et al., 1997), les milieux scolaires (e.g., Montreal Longitudinal-Experimental Study; Tremblay et al., 1992) et les communautés (e.g., *The New York*

Boys Club; Thrasher, 1936). Ceux-ci ne sont pas décrits ici puisque ce type de programme a comme principal objectif de prévenir la délinquance juvénile. Ces programmes proposent des mesures pour agir sur l'environnement des jeunes qui grandissent dans les milieux à risque et précarisés sur le plan socio-économique (par exemple, en renforçant l'encadrement et la supervision des jeunes, en leur proposant des activités dirigées, etc.). En outre, ce type de programme de prévention s'applique davantage aux crimes traditionnels.

1.3.3. Les campagnes de prévention du crime : quelques exemples

Étant donné la nature de ce projet de mémoire, une attention particulière est accordée aux campagnes de prévention du crime ciblant différents publics. Les campagnes de prévention sont souvent utilisées par les ministères ou organismes gouvernementaux dans le but de promouvoir de saines habitudes de vie et l'amélioration de la santé publique. On a regroupé en quatre grandes catégories les types de publicités utilisés dans ce type de campagnes, selon le public cible, la portée géographique de la campagne et le type de message (spécifique ou général). On retrouve donc : a) les campagnes incitant le public à être prudent (*Strategies encouraging public action regarding safety*) où on prône l'importance de la sécurité et l'évitement de comportements augmentant le risque de victimisation, tout en sensibilisant le public quant aux risques (avec des statistiques de victimisation par exemple) ; b) les campagnes à stratégies informatives (*Informant strategies*) qui visent à encourager le public à coopérer avec les autorités dans le but d'appréhender les criminels ; c) les campagnes ciblant les délinquants (*Offender-targeted strategies*) qui cherchent à dissuader les criminels de commettre des crimes en les informant qu'ils sont à risques ; et finalement, d) les campagnes promouvant les interventions en prévention (*Crime prevention intervention publicity*) dont le but est d'informer la population locale qu'il y a des agences ou des organismes dont le rôle est de réduire les taux de crimes (Bowers & Johnson, 2005). À titre d'exemple, on retrouve la campagne de prévention *Taking A Bite Out of Crime* qui a débuté à la fin des années 1970 et qui mettait en scène un personnage animé sous la forme d'un chien (« *McGruff* ») qui prodiguait des conseils de sécurité à la population (*Strategies encouraging public action regarding safety*). La campagne avait quatre objectifs principaux : a) modifier l'opinion du public envers le crime et le système de justice (offrir une vision plus réaliste de la criminalité); b) tenter de responsabiliser les citoyens par rapport aux crimes et à sa prévention; c) encourager la population à être plus coopérative avec le système de justice pour combattre le crime; et d) améliorer les efforts de prévention du crime déjà existants (Lab, 2010). Cette campagne de prévention a fait l'objet de

deux évaluations successives afin de déterminer son efficacité.

La première évaluation fût réalisée par O'Keefe et Mendelsohn (1984) avec 1200 participants de 1979 à 1981. Ils ont trouvé qu'environ 50% des répondants sondés avaient vu la campagne et de ce nombre, seulement 3% étaient en mesure de se rappeler les campagnes publicitaires sans aide. Parmi les répondants plus âgés, seulement 33% se rappelaient l'avoir vue. Pour ce qui est du message retenu, près de 90% des individus étaient capables de décrire des suggestions spécifiques de la campagne (il y en avait 25 au total, e.g., verrouiller ses portes) et 22% ont déclaré avoir appris quelque chose de nouveau. De plus, plus de la moitié des répondants ont dit se sentir plus responsables de la prévention du crime et un quart auraient commencé à incorporer les suggestions recommandées dans la campagne. Plus négativement, 22% ont également rapporté ressentir une plus grande peur d'être victime de crime suite à la visualisation de la campagne. Ceci est bien évidemment un résultat allant à l'encontre des attentes. Le niveau d'intérêt des personnes sondées à propos du contenu de la campagne était plus élevé lorsque ces dernières étaient déjà intéressées par la prévention du crime. L'opinion des hommes par rapport à la prévention du crime a changée plus que celle des femmes suite à la campagne. Cependant, ce sont les femmes et les mieux nantis (ceux qui se sentent le plus menacés) qui ont le plus augmenté leurs comportements coopératifs (e.g., informer la police si on est témoin d'un crime). Par contre, ce changement n'a pas eu d'impact sur leurs connaissances, efficacité et compétence en matière de prévention. De plus, cette campagne n'a pas changé la perception des individus par rapport aux taux de criminalité ou leur sentiment de sécurité la nuit.

La seconde évaluation a été réalisée en 1992 par O'Keefe et collègues (1996). Cette fois, parmi les personnes sondées, 80% ont révélé avoir vu la campagne. La campagne avait surtout rejoint les plus jeunes, les hommes (6% de plus que les femmes), les personnes ayant déjà été victime d'un crime et ceux ayant un niveau de scolarité plus élevé (i.e. ceux détenant au minimum un diplôme d'étude secondaire). L'étude a aussi démontré que peu de variables socio-démographiques étaient associées au succès de la campagne (les répondants ayant rapporté avoir appris de cette campagne ne se distinguaient pas de ceux pour qui la campagne n'a pas eu d'impacts).

Même si cette campagne de prévention s'est avérée somme toute fructueuse, elle n'a pas réussi à rejoindre les groupes les plus vulnérables, ceux qui auraient le plus à gagner de modifier

leurs comportements afin de réduire leurs risques de victimisation. Ceux pour qui la campagne a eu le plus de succès sont les groupes d'individus qui sont traditionnellement les moins vulnérables aux crimes et ceux qui ont déjà à cœur d'assurer leur sécurité (donc qui prennent déjà des précautions). De plus, un des objectifs étaient de changer l'opinion du public envers le crime et le sentiment de peur. Or, bien que de nombreux individus ont rapporté avoir modifié leurs comportements suite à la campagne, leur perception par rapport aux crimes n'a pas changée (O'Keefe & Mendelsohn, 1984).

Comme autre exemple, on retrouve le programme de prévention *Crime Stoppers.* Ce programme fût implanté en 1976 et est maintenant appliqué dans de nombreux pays (Crime Stoppers International, 2018). Cette initiative est basée sur la coopération du public avec les autorités policières (*Informant strategies*). On cherche ici à sensibiliser la population à l'importance de signaler toute infraction ou comportement suspect en échange d'une récompense (petite somme d'argent). Les taux de succès de ce programme est difficile à évaluer en ce qui a trait à la réduction de la peur de la criminalité et de la baisse du taux de crime et de victimisation (Rosenbaum, Lurigio, & Lavrakas, 1989). Par exemple, en Australie, la police a recensé en 2002 près de 140 000 appels (Challinger, 2003) et de ce nombre, seulement 2% des appels ont mené à des arrestations.

Par la suite, il y a le *Boston gun project* qui visait à réduire le trafic d'armes à feu et le taux d'homicides chez les jeunes (Kennedy, Braga & Piehl, 2001). Cette campagne de prévention s'adressait aux membres de gang de rue et utilisait des stratégies dissuasives (*Offender-targeted strategies*) telles la tolérance zéro pour les comportements violents. En plus des affiches indiquant les conséquences auxquelles ils pourraient faire face s'ils se faisaient arrêter, des rencontres structurées avec des membres de gang ainsi que des assemblées dans les écoles ont eu lieu afin de leur transmettre le message. Suite à la campagne, le taux d'homicides chez les jeunes a diminué de 63% et il y a eu une baisse de 32% d'appels concernant des coups de feu. Ainsi, la campagne a été considérée comme efficace à la réduction du taux de criminalité.

Concernant la catégorie de programmes de prévention du crime misant sur les publicités, Bowers et Johnson (2003) ont examiné les données de 21 initiatives visant à réduire le cambriolage en Angleterre. Ils ont trouvé que les campagnes de prévention qui ont été les plus efficaces étaient celles pour lesquelles il y avait le plus de publicité. Ainsi, plus les campagnes duraient longtemps

et avaient de la visibilité, plus elles avaient un haut taux de succès. Cependant, si la campagne est menée de façon trop constante, il y a des risques que cela fasse de la surexposition et que les individus se lassent de la voir. Ainsi, il est plutôt recommandé de la faire en « rafale » (Riley & Mayhew, 1980)

Pour ce qui est des campagnes de prévention en cybercriminalité, le gouvernement du Canada a lancé plusieurs campagnes contre la fraude (Agence du revenu du Canada, 2019; Bureau de la concurrence Canada, 2018). Ces campagnes incluent des affiches contenant des conseils de prévention. À titre d'exemple, l'Agence du revenu du Canada incite le public à la prudence et mentionne sur ses affiches qu'elle ne demandera jamais d'information financière par email. Le Bureau de la concurrence Canada, quant à lui, offre des services et des renseignements concernant la fraude. Il y a également un jeu-questionnaire afin de tester ses connaissances sur le sujet. Ce département organise aussi un Forum sur la prévention de la fraude qui a pour but de combattre la fraude. Ce même Forum procède au lancement d'une campagne de sensibilisation durant le mois de mars.

Aux États-Unis, la U.S. Bank (2019) fournit également sur son site web des conseils et des suggestions à suivre pour se protéger. Les sujets abordés sont : la prévention de la fraude, le vol d'identité, la protection de son ordinateur et les médias sociaux. Les documents disponibles sont simples et faciles à comprendre : des étapes sont listées sur les moyens à prendre pour minimiser ses risques d'être victime de fraude. Au Royaume-Uni, on retrouve une campagne de prévention lancée contre la fraude par l'organisme *Financial Fraud Action* UK (2019). Cette campagne est une initiative de l'industrie des services de paiement au Royaume-Uni. Elle vise plus particulièrement les banques et compagnies qui émettent des cartes de crédit ou de débit mais a également des conseils pour les clients. Leur campagne inclut des affiches et des pamphlets avec de l'information et une liste de points à se rappeler afin d'éviter d'être victime de fraudeurs.

En Australie, le gouvernement a lancé la campagne *Scamwatch* sous la direction de l'*Australian Competition and Consumer Commission* (ACCC). Le site traite de divers types de sollicitations malveillantes (scams) tels que les faux organismes de charité, les organismes frauduleux qui offrent des possibilités d'investissements, etc. Il est possible pour les individus de rapporter une fraude (scam) sur ce même site. Une liste de ressources en ligne est également disponible pour ceux qui cherchent à en connaître davantage (Scamwatch, 2019).

À Singapore, le *National Crime Prevention Council* (NCPC) a lancé *Scam Alert Singapore* (2018). Le site comprend une multitude de « scams » existants, des témoignages d'individus ayant été victime, des ressources (affiches, vidéos, blogues) et un quiz interactif. Les affiches incluent des tactiques employées par des fraudeurs. Elles sont disponibles en anglais et en mandarin.

Les résultats des diverses campagnes de prévention en criminalité varient énormément (Lab, 2010). Un des problèmes avec les campagnes de prévention (surtout celle visant le public en général) serait que les décideurs/concepteurs tentent de rejoindre le plus d'individus possibles et, de ce fait, utilisent des messages trop diffus ou des généralisations ; cela aurait donc pour effet de diminuer l'efficacité du message transmis. Pour cette raison, Sacco et Trotman (1990) ont suggéré de repenser les campagnes de manière à ce que les messages transmis portent davantage sur des objectifs plus réalistes et mieux ciblés, en proposant au public des attitudes et des comportements plus spécifiques que généraux.

1.4. Cybercriminalité et prévention

1.4.1. Modèles traditionnels de prévention et cybercriminalité

Il peut être utile de se référer aux différentes théories explicatives de la criminalité pour établir les fondements des stratégies préventives. Parmi les théories les plus souvent citées en criminologie, on retrouve la théorie de l'apprentissage (Akers, 1998), la théorie générale du crime (Gottfredson & Hirschi, 1990), la théorie générale de la tension (*General Strain Theory*; Agnew, 1992) et la neutralisation (Sykes & Matza, 1957). Toutes ces théories ont en commun de proposer des postulats ou des explications sur les processus et les conditions requises permettant de comprendre pourquoi un individu commet un crime. On tente ainsi d'expliquer les raisons qui motivent ou mènent à la criminalité. La théorie générale du crime de Gottfredson et Hirschi (1990) a également été appliquée afin de tester l'hypothèse selon laquelle les caractéristiques des victimes viendraient influencer leurs risques de victimisation, en mettant l'accent sur le faible niveau de contrôle de soi (Holt, Bossler & Seigfried-Spellar, 2015). Cependant, ce type de théorie cible plus les risques de victimisation d'un individu que l'incitation à la prévention, comme c'est le cas dans le présent mémoire. Il est d'ailleurs reproché aux théories traditionnelles en criminologie de ne pas avoir incorporé le développement rapide de l'Internet et les cybercrimes (Jahankhani, 2013). Comme exception, on retrouve la théorie développée par Jaishankar (2008) qui s'intitule *Space Transition Theory* et qui porte spécifiquement sur les cybercrimes. Cette théorie propose différents

postulats sur la transition des comportements (de conformité et de non-conformité) des individus du monde physique réel au monde virtuel du cyberespace. Par exemple, il est suggéré que les personnes qui répriment des comportements criminels dans les situations réelles (monde physique) en raison de leur statut ou position sociale peuvent plus facilement s'autoriser à commettre des cybercrimes dans le monde virtuel plus anonyme. Le fait d'avoir une identité flexible, de profiter d'un pouvoir d'action anonyme et de pouvoir agir dans un environnement ayant peu de facteurs de dissuasion constitueraient également des conditions favorisant l'exécution des crimes en ligne. Cette théorie est utile pour comprendre les motivations et les rationnels sous-jacents aux comportements des cybercriminels ; toutefois, elle s'avère peu pertinente pour le développement des mesures de prévention populationnelles visant la protection du public et la réduction des risques de victimisation de la cybercriminalité.

Comme déjà mentionné, la plupart des approches de prévention en criminologie ont comme objectif de dissuader la perpétration des crimes : on cherche essentiellement à réduire le nombre de crimes commis et le nombre de délinquants (Hirschi, 1986). Or, lorsqu'il s'agit de prévention des cybercrimes, il pourrait être plus souhaitable d'avoir recours à des modèles théoriques provenant de d'autres domaines (par exemple, la santé publique) puisque la population ciblée est plus difficilement le délinquant lui-même et son environnement (réseau Internet partagé) mais plutôt les victimes potentielles. Puisque le criminel est, dans bien des cas, inaccessible et inconnu (le fraudeur en ligne peut opérer en secret et à l'insu de tous, n'importe où sur la planète en autant qu'il a un accès internet), il est plus facile de concentrer les efforts pour protéger les victimes potentielles. Ainsi donc, avec ce type d'approche, on tente moins d'empêcher la commission d'un crime en intervenant sur le délinquant ou l'environnement physique (car celui-ci est virtuel) mais plutôt en encourageant les individus qui pourraient devenir des victimes à être proactifs en les incitant à prendre les précautions nécessaires pour se protéger.

Bien que les différentes théories en prévention de la criminalité puissent s'avérer pertinentes pour identifier certains moyens de protection du public, d'aucuns affirment que la cybercriminalité est un phénomène suffisamment différent de la criminalité dite « traditionnelle », ce qui confirmerait l'idée voulant que d'autres approches théoriques non traditionnelles en prévention pourraient être nécessaires (Brown, 2006). Par exemple, les victimes de crimes économiques (*white collar crimes*) sont en général plus âgées, ont un meilleur statut socio-économique et sont plus souvent des femmes (comparativement aux victimes de crimes violents) (Ganzini et al., 1990).

Ainsi, les efforts de prévention ne viseront pas nécessairement les mêmes individus. À cet égard, on constate qu'il y a souvent de l'appréhension face à la création de stratégies à employer pour prévenir les cybercrimes. Plus précisément, deux barrières sont identifiées : (1) la présence de craintes à propos de la technologie due aux représentations sensationnalistes qu'en font les médias et, (2) d'un point de vue académique, il y a encore des lacunes quant aux connaissances des différents types de cybercrimes, incluant ceux mentionnés dans les médias (Downing, 2013). Les diverses façons de définir les cybercrimes pourraient empêcher un consensus permettant de cerner la meilleure méthode à employer pour la prévention de la cybercriminalité (Gordon & Ford, 2006; Reyns, Henson, & Fisher, 2014). En effet, il en ressort qu'un des problèmes dans l'étude et la prévention des crimes reliés à Internet est un manque de définition faisant consensus. Par exemple, le *cyberbullying* est défini comme une répétition d'actions de harcèlement (Patchin & Hinduja, 2006; Smith et al., 2008; Vandebosch & Van Cleemput, 2008) ; cependant, cette définition s'applique difficilement dans le cas d'une séquence vidéo humiliante propagée à d'autres personnes – dans un tel cas, il n'est pas clair qui répète le harcèlement : l'envoyeur initial ou ceux qui le partagent par la suite (Grigg, 2010).

1.4.2. Modèles théoriques de prévention adaptés à la cybercriminalité

Un premier modèle théorique qui a été considéré se nomme le Modèle d'acceptation de technologie - TAM (*Technology Acceptance Model*). Le modèle TAM est souvent utilisé comme référence dans le cadre d'études en cybersécurité puisqu'il s'intéresse particulièrement aux éléments qui motivent les individus à utiliser des technologies de sécurité et ainsi qu'aux facteurs qui favorisent l'utilisation des nouvelles technologies au quotidien (ce qui les rend plus acceptables aux yeux des utilisateurs). Cette théorie a été élaborée dans les années 1980 alors qu'on tentait de comprendre pourquoi des travailleurs ne voulaient pas adhérer aux nouvelles technologies auxquelles ils avaient accès (Davis, 1989). Ces technologies étant utiles à l'utilisateur d'une quelconque façon en lui apportant des résultats concrets. Lorsqu'il est question de cybersécurité, on vise la protection dont le but principal est d'éviter les conséquences négatives et qui procure peu de résultats tangibles pour l'utilisateur (Conklin, 2006). Dans le contexte de la présente étude, ce modèle est jugé moins pertinent car on ne cherche pas à comprendre pourquoi certaines personnes voudraient utiliser ou non la nouvelle technologie disponible. On cherche plutôt à comprendre les perceptions des membres et clients par rapport à la cybercriminalité. La présente recension vise également à documenter les approches de prévention les plus prometteuses pour

renforcer le sentiment de sécurité des utilisateurs. Dans ce contexte, d'autres modèles théoriques apparaissent plus adaptés et utiles.

Un autre modèle souvent mentionné dans le domaine de la prévention des cybercrimes est le *Protection Motivation Theory*. Cette théorie propose que l'adoption des mesures de protection par un individu dépend de son estimation de la menace (sévérité perçue et susceptibilité perçue) et de son estimation en sa capacité à s'y adapter et à y faire face (efficacité de la réponse et auto-efficacité). Ces deux derniers processus cognitifs seraient stimulés en présence d'une menace, ce qui serait déclencherait des comportements protectifs dans le but de réduire cette dernière (Doane et al., 2016). Ici encore, ce modèle apparait quelque peu limité puisqu'il se centre exclusivement sur les variables motivationnelles. Toutefois, certains de ses postulats sont intégrés au modèle HBM (notamment le rôle crucial de la perception des menaces) présenté dans la sous-section suivante.

Le principal cadre théorique en lien avec la prévention de la cybercriminalité retenu pour le présent projet de mémoire a pour nom le Modèle des croyances relatives à la santé ((*Health Belief Model* - HBM). Ce modèle s'avère particulièrement utile dans le contexte de la prédiction des comportements préventifs en cybersécurité (Claar, 2011; Davidson & Sillence, 2010; Dodel & Mesch, 2017; Ng, Kankanhalli, & Xu, 2009). Bien que ce cadre théorique ait initialement été développé dans le domaine de la santé (notamment en santé publique), il est maintenant reconnu qu'il est pertinent de transposer les fondements de cette théorie dans domaine de la cybercriminalité. En effet, au même titre que les saines habitudes de vie et les comportements de santé, les pratiques de sécurité peuvent elles-aussi être vues comme des comportements à promouvoir dans le but de prévenir un incident (Ng et al., 2009).

Un parallèle peut ainsi être établi entre le domaine de la santé et celui de la cybersécurité puisque chacun cherche à identifier et favoriser la mise en œuvre d'actions préventives visant à réduire le risque avant que ne surviennent des problèmes potentiels chez les individus (Claar & Johnson, 2010; Lee, Larose, & Rifon, 2008). Dans les deux cas, il y a une probabilité que la personne ne prenne pas conscience des bénéfices qu'elle pourra retirer suite à l'adoption des nouveaux comportements (de santé ou de sécurité) ; en effet, l'application des actions préventives n'entraine pas toujours de rétroaction positive chez l'individu (ou ne sont pas toujours perceptibles). Il est donc beaucoup plus difficile de faire adopter le comportement désiré puisqu'il n'y a pas de renforcement positif immédiat. Il se peut d'ailleurs que la personne ne se sente jamais

concernée si elle décide de faire fi des recommandations ou des actions proposées. Un autre parallèle pouvant être fait entre le domaine de la santé et celui de la cybercriminalité est que les comportements adoptés par l'individu (en matière de santé et de sécurité) ne sont pas uniquement motivés par un rationnel ou par des faits objectifs. Il existe plusieurs autres éléments qui vont venir influencer et moduler le comportement de l'individu et l'amener à se conduire comme il le fait (par exemple, si la personne considère qu'il y a trop d'inconvénients à se protéger contre certaines maladies ou les cyberattaques, elle pourra maintenir ses comportements habituels sans subir l'influence des mesures préventives).

De plus, le modèle théorique HBM gagne en popularité et plusieurs études ont démontré qu'il était valide pour comprendre les processus mentaux (croyances, biais et représentations) qui agissent dans l'adoption de comportements préventifs. Ce modèle théorique stipule qu'il y a deux principaux déterminants des comportements de santé : 1) les perceptions de menaces et 2) les attentes perçues par rapport au comportement à adopter (Rosenstock, 1974; Rosenstock, Strecher, & Becker, 1994). La première notion regroupe deux ensembles de perceptions : la susceptibilité perçue face au risque et la sévérité perçue quant aux conséquences de ces menaces. Ces perceptions sont basées sur les croyances des individus et non sur les faits objectifs. La susceptibilité perçue est basée sur les croyances de l'individu à propos du risque qu'il encoure d'être affecté par le problème. La susceptibilité perçue peut varier énormément d'un individu à un autre. Par exemple, si une personne a déjà été victime dans le passé d'une cyberattaque, il y a de fortes chances que sa susceptibilité perçue soit plus élevée que celle d'un individu n'ayant jamais été attaqué.

Une étude de Öğütçü et collègues (2016) a démontré que lorsqu'un individu perçoit des menaces, son comportement va devenir plus protectif. De plus, si un individu a des connaissances sur le sujet ou s'il a été sensibilisé par un proche qui a vécu une cyberattaque, ce dernier peut être plus enclin à se croire susceptible. Ainsi, dans le cas de la cybercriminalité il s'agirait par exemple de la probabilité estimée par l'individu qu'un virus vienne infecter son ordinateur. La notion de menace perçue appliquée à la cybersécurité pourrait prendre la forme de la question suivante : « Quelles sont mes risques d'être victime d'une fraude ? ». La sévérité perçue quant à elle, réfère plutôt à la gravité de l'impact que pourrait avoir l'incident s'il venait à se produire. On peut alors penser, par exemple, aux probabilités qu'un virus informatique encrypte l'information de l'ordinateur et que l'utilisateur n'y ait plus accès sauf s'il accepte de débourser une somme d'argent

(rançongiciel). La sévérité peut être influencée par le type d'emploi que l'individu occupe. Si, par exemple, ce dernier manipule des informations confidentielles, il pourrait y avoir des conséquences graves sur sa situation au travail et il pourrait perdre son emploi s'il ne prend pas les précautions nécessaires pour contrer la menace à la sécurité.

Le deuxième facteur principal du modèle HBM regroupe : les bénéfices perçus ainsi que les barrières perçues par l'utilisateur. D'après Ng et ses collègues (2009), les bénéfices perçus sont l'un des facteurs déterminants quant aux comportements sécuritaires qu'un utilisateur va adopter sur Internet. Les deux autres facteurs seraient la susceptibilité perçue et l'auto-efficacité (voir plus loin). De façon plus précise, les bénéfices perçus font en sorte que l'individu qui pose des gestes de prévention perçoit ces derniers comme étant des moyens efficaces de protection contre les cyberattaques. Dans le domaine de la cybersécurité, comme déjà mentionné, il peut parfois être difficile pour les gens de percevoir les bénéfices puisqu'ils ne sont pas immédiats ou visibles. En effet, en se protégeant, on prévient une situation fâcheuse ; cependant, il n'y a pas de récompenses concrètes pour l'utilisateur (West, 2008). L'individu doit alors se fier aux bénéfices qu'il perçoit (ou imagine s'il n'avait rien fait), bien que ceux-ci ne soient pas tangibles et qu'il ne peut pas objectivement les percevoir. Si l'on transpose ce principe dans cette étude, les bénéfices pourraient être de se sentir plus en sécurité face à une fraude potentielle lorsqu'on prend les précautions nécessaires (e.g., s'assurer de la provenance du message).

Les barrières perçues sont les éléments qui feraient en sorte que cela encoure des coûts à l'utilisateur. Encore une fois, les coûts dépendent des individus puisqu'il s'agit de leur perception. Les barrières peuvent être différentes selon ce que l'individu veut mettre en place afin de se protéger. Les barrières ne sont pas nécessairement reliées aux connaissances de l'individu ou encore à la susceptibilité perçue, car même si l'individu sait qu'il encourt un risque, il se peut qu'il décide de ne pas les mettre en place en particulier s'il a l'impression que l'application des mesures de protection est un fardeau additionnel pour lui (comme déjà vu dans la section des facteurs de vulnérabilité). Par exemple, il faut que les gens prennent régulièrement le temps de faire les mises à jour de sécurité suggérées afin d'être bien protégés. Comme barrière, il pourrait y avoir un sentiment de ralentissement dans la productivité puisqu'il faut bien prendre le temps de s'assurer du contenu des pièces jointes avant de les ouvrir par exemple.

D'autres concepts ont été apportés par la suite afin de mieux compléter le modèle théorique : les signaux à l'action et l'auto-efficacité. Les signaux à l'action sont composés de

signaux internes et externes. Il s'agit de signaux qui rappellent à l'utilisateur qu'il faut prendre des précautions. Ils déclenchent une réaction chez l'utilisateur. Les signaux vont varier selon les individus. Comme signal interne, il y a par exemple la victimisation antérieure. Ainsi, si un utilisateur a été victime dans le passé d'une cyberattaque, il peut se rappeler l'événement et cela peut agir comme un signe qu'il faut renforcer la sécurité de son ordinateur afin d'éviter d'être de nouveau victime. Tandis que pour les signaux externes, on réfère souvent aux campagnes de prévention qui servent de rappel aux gens, comme c'est le cas pour la présente étude. Ce ne sont pas des signaux qui vont avoir la même efficacité pour tout le monde puisqu'il faut y porter attention. L'auto-efficacité est basée sur la confiance qu'à un individu en ses propres compétences (Dodel & Mesch, 2017). Ce dernier va être plus enclin à vouloir relever des défis ou encore à mieux se protéger car il se sent apte à le faire. Par exemple, lorsqu'un individu perçoit qu'il est capable de bien se protéger car il a les connaissances et outils nécessaires pour y arriver.

La présente recherche étudiera différentes questions en lien avec certaines des composantes de ce cadre théorique, dans le contexte d'une campagne de prévention de la cybercriminalité menée par une institution financière. De façon plus spécifique, les questions relatives au sentiment de sécurité des utilisateurs feront l'objet d'une attention particulière.

1.4.3. Les stratégies préventives en cybercriminalité : les campagnes de prévention

Afin de rejoindre le plus de personnes possibles, les campagnes sociétales implantées à grande échelle utilisent divers moyens pour communiquer leurs messages à la population : des affiches posées dans des lieux publics, des messages télévisés ou diffusés à la radio ou des vidéo annonces placées dans des sites Internet (Bertrand et al., 2006). Ces campagnes de prévention sociétale peuvent s'avérer très coûteuses et certains chercheurs s'interrogent sur leur efficacité et les bénéfices réels que la population en retire (rapport coût-bénéfice). En effet, les résultats des effets des campagnes de prévention universelle, notamment en santé publique, révèlent que celles-ci souvent très coûteuses et n'obtiennent pas tous les effets escomptés (Bertrand et al., 2006).

En contrepartie, d'autres études ont montré que les campagnes de prévention universelle (tous domaines confondus) donnent parfois des résultats positifs pour le public ciblé lorsque certaines conditions sont rencontrées (Bauman et al., 2001; Self-Brown et al., 2008). Par exemple, un des ingrédients clés du succès de ces campagnes de prévention est d'instaurer une phase de maintien ou de rappel à moyen et à plus long terme (Mitchell, Aley, & Eastwood, 1992). La population a besoin que le message soit réitéré afin de rappeler à leur mémoire les risques ainsi

que les comportements préventifs à adopter. Une campagne implantée à un seul moment (*one-off campaign*) ne sera pas aussi efficace que si les organisateurs prévoient différentes phases de rappel qui reprend ou adresse le même message en insistant sur l'importance du problème (Casswell & Duignan, 1989). De plus, la façon de transmettre le message constitue aussi un facteur de succès déterminant qui doit être pris en considération. Ainsi, il a été démontré que le contenu du message et la stratégie employée pour le transmettre doivent être adaptés aux besoins et aux caractéristiques du public cible (Schmid et al., 2008). Par exemple, un message s'adressant à des intervenants formés (par exemple des professionnels de la santé) pourra comporter plus de contenu technique ou des allusions à leurs réalités de travail alors qu'un message s'adressant à des parents issus de différents milieux pourra miser davantage sur leurs expériences de vie à la maison (Schmid et al., 2008).

Comme déjà mentionné, on retrouve dans le domaine de la protection du public des mesures de prévention prises par les gouvernements dans le but de réduire la fréquence de certains crimes. Ces dernières années, avec l'augmentation de la popularité d'Internet, quelques mesures de prévention ont été implantées dans le but de mieux protéger les usagers des crimes commis en ligne. Par exemple, en 2010, le Gouvernement fédéral canadien, sur la base de la Stratégie nationale de cybersécurité, a lancé l'initiative « Pensez cybersécurité » (*Get cyber safe*) (Public Safety Canada, 2015). À ce jour, cette stratégie a ciblé différentes problématiques en lien avec l'utilisation d'Internet : le *cyberbullying*, la sécurité des réseaux Wi-Fi, l'importance de faire des copies de sureté de ses documents, la protection des données personnelles et la protection contre les sollicitations malveillantes (scams) (Get Cyber Safe, 2017). Les États-Unis ont aussi développé leur propre campagne nationale de prévention de la cybercriminalité nommée « *Stop.Think.Connect* » (Department of Homeland Security, 2017). Le but de cette politique nationale est de sensibilité la population aux risques potentiels de l'utilisation d'Internet. Cette campagne, tout comme celle au Canada, vise aussi à éveiller les consciences (*sense of awareness*), à informer le public des moyens à leur disposition pour se protéger et à encourager l'adoption de comportements sécuritaires.

Comme mentionné précédemment, il existe trois types de campagnes de prévention lorsqu'il s'agit de la criminalité : celles qui définissent le problème, celles qui ont pour but de dissuader les criminels, et celles qui ont pour but d'éduquer les utilisateurs quant aux façons de réduire les risques (Sacco & Trotman, 1990). La troisième alternative est la plus fréquemment

employée et c'est également celle qui a ciblée dans le cadre de ce mémoire. En se servant de cette méthode, on cherche à inciter le public visé à adopter des comportements plus sécuritaires en leur fournissant des instructions ou conseils sur leur manière d'agir. De plus, une campagne de prévention efficace doit s'assurer que le public cible ait une bonne exposition aux contenus de la campagne (Sacco & Silverman, 1981) et que les thèmes de la campagne soit perçus comme évidents (Star & Hughes, 1950; Mendelsohn, 1973).

1.4.4. Cybercriminalité, prévention et institution financière : le rôle déterminant du sentiment de sécurité

La cybercriminalité qui cible les institutions financières et leurs clients est un domaine d'étude qui prend de l'ampleur et les connaissances en lien avec ce type de crime demeurent encore aujourd'hui relativement peu nombreuses. Les cyberfraudes (et les moyens de les prévenir) ont beaucoup été étudiées en mettant l'accent sur les aspects technologiques ou informatiques (virus informatique vs logiciel antivirus, logiciels malveillants, etc.). Dans ce mémoire, une attention particulière est accordée à la prévention des cybercrimes sous l'angle des victimes potentielles (usagers Internet adultes), à leurs caractéristiques personnelles et aux moyens pouvant être utilisés pour prévenir de tels crimes. L'analyse des données de recherche disponibles a permis d'identifier certains constats en lien avec ce sujet.

Les recherches ont montré qu'il y a lieu d'augmenter et de mieux cibler les efforts de prévention pour réduire ce type de crime. Or, on remarque que les mesures de prévention et de sensibilisation du public sont relativement peu nombreuses et celles existantes ont rarement fait l'objet d'une évaluation ou ont été peu fructueuses (Bada, Sasse, & Nurse, 2015). On peut peut-être attribuer cet insuccès au fait que les mesures de prévention ne sont pas suffisamment arrimées aux besoins des usagers et à leur niveau de compréhension ou d'évaluation des risques encourus. Par exemple, il y a eu des campagnes de sensibilisation afin de dissuader les individus de pirater du contenu en ligne (films, jeux vidéos, etc.). Ces campagnes de prévention ont légèrement réduite le piratage pour une courte période de temps ; cependant elles n'ont pas eu d'effet sur le taux de piratage de façon continue (Bachmann, 2007).

Les recherches évaluatives effectuées tant en criminologie qu'en santé publique ont démontré que les campagnes de prévention sont plus efficaces quand elles ciblent adéquatement les besoins du public cible et qu'elles transmettent un message clair qui favorise une réelle prise de conscience. Rares sont les mesures préventives qui prennent en considération le point de vue

des usagers (leurs perceptions, leurs croyances) ou leurs connaissances des moyens à leur disposition pour se protéger. Comme déjà vu, nombreux sont les auteurs consultés qui suggèrent de transposer le modèle conceptuel des croyances en santé (*Health Belief Model*) au contexte de la prévention en cybercriminalité.

Ainsi donc, une piste prometteuse consiste à mieux documenter les opinions et les représentations des usagers afin de comprendre leurs croyances en ce qui concerne leur sécurité informatique et les moyens mis à leur disposition. Il apparait particulièrement pertinent d'évaluer dans quelle mesure les usagers se sentent en sécurité et quel est leur niveau de confiance envers leurs institutions financières en matière de protection (de leurs renseignements personnels et de leur capacité à les protéger dans le contexte des transactions financières effectuées en ligne). De fait, le survol de la littérature scientifique a permis de constater qu'il existe très peu de données sur les représentations des utilisateurs d'Internet en lien avec leur sentiment de sécurité et de confiance.

En définitive, un des aspects qui semblent particulièrement peu considérés dans les recherches actuelles est ce que retiennent les usagers des messages transmis lors des campagnes de prévention (sur les stratégies de protection à leur disposition) et comment ils perçoivent ces stratégies (sont-elles à leur portée ? répondent-elles à leurs besoins et sont-elles jugées utiles ? les clients changent-ils leur perception de l'institution suite à la campagne ? etc.). Ces questions sont centrales pour le présent projet de mémoire.

Dans le contexte des transactions financières en ligne, le sentiment de sécurité découle de la perception que va avoir un individu quant à son évaluation du risque que ses informations personnelles soient bien gérées (Kim, Chung, & Lee, 2011). La confiance, quant à elle, peut être définie comme étant le sentiment de sécurité et la disposition qu'à la personne de dépendre de quelqu'un d'autre. Le sentiment de confiance serait négativement influencé par la perception de risques, cette dernière étant basée sur l'incertitude à propos du futur (Cheung & Lee, 2000). Donc, lorsqu'il y a un sentiment de confiance, les risques estimés sont réduits ou perçus comme négligeables. Il y aurait également une différence entre les hommes et les femmes quant à la perception des risques. Les femmes auraient tendance à prendre davantage en considération les pertes possibles associées aux risques (Midha, 2012). Or, Tversky et Kahneman (1989) ont démontré que lorsque les individus ne perçoivent pas la même valeur aux pertes et aux gains, une plus grande importance serait accordée aux pertes. Cela pourrait expliquer pourquoi les femmes

sont plus préoccupées que les hommes à propos de leur sécurité informatique dans le cadre d'achats en ligne (Garbarino & Strahilevitz, 2004). Les personnes âgées ont également moins tendance à utiliser Internet ; les femmes âgées étant celles avec le moins connaissances quant aux risques de sécurité sur Internet (Grimes et al., 2010). Cela peut laisser entendre que l'âge et le genre sont deux facteurs qui influencent comment les individus perçoivent et utilisent Internet (Downing, 2013).

Le sentiment de sécurité est étroitement lié à la confiance. Un individu est plus enclin à faire confiance lorsqu'il se sent en sécurité. L'inverse est également vrai. En général, dans la plupart des situations, les femmes se sentent moins en sécurité que les hommes (Delbosc & Currie, 2012; Quine & Morrell, 2008; Grohe, 2011). En effet, ces dernières percevraient un plus grand risque dans plusieurs domaines (financier, médical, et environnemental) (Garbarino & Strahilevitz, 2004). Cela pourrait également s'appliquer dans les situations de navigation en ligne. Une étude sur le « magasinage en ligne » a démontré que les femmes étaient moins portées à vouloir faire des achats en ligne en l'absence de recommandations d'une personne de confiance qu'elles connaissent (Garbarino & Strahilevitz, 2004). Elles auraient également moins tendance à faire confiance aux vendeurs en ligne que les hommes (Midha, 2012). Un facteur pouvant influencer le sentiment de sécurité serait les expériences de victimisation (Keown, 2010). D'après une étude par Button et collègues (2009), 74,5% des victimes auraient reporté avoir modifié leurs comportements suite à un incident de victimisation en ligne relié à une fraude. Cela les aurait incités à devenir plus vigilants et aurait également eu un effet sur leur capacité à faire confiance.

Cependant, il semblerait que les victimes de cybercrimes ont tendance à être de nouveau victime par la suite. Par exemple, Reyns et Henson (2016) ont proposé des moyens pour réduire le risque de victimisation relié au vol d'identité en ligne (e.g., changement de mots de passe, installation d'un logiciel antivirus et élimination des courriels provenant de destinataires inconnus). Il semblerait que les stratégies employées dans le cadre de leur étude n'ont pas été efficaces pour diminuer les risques d'être de nouveau « victimisé ». Il se pourrait que ce soit dû aux comportements illégaux (ou risqués) des victimes elles-mêmes (par exemple si elles décident de télécharger du contenu piraté en ligne, se mettant ainsi à risque). Il semblerait également que les victimes de cybercrimes font davantage preuve de crédulité que les non-victimes. En effet, dans les crimes plus traditionnels où une proximité physique avec la victime est nécessaire, le délinquant va « sélectionner » (désigner) sa victime. Or, dans les crimes comme la « fraude nigériane » où le

même message frauduleux est envoyé à des milliers d'individus, c'est la victime qui décide d'y répondre. Ainsi, la victime aurait des prédispositions à être victime à répétition puisqu'elle aurait plus tendance à croire et à faire confiance facilement (Pease, Ignatans & Batty, 2018). Une victimisation répétée peut également survenir lorsque le délinquant a eu une expérience fructueuse avec la victime la première fois. Cela va l'amener à retenter un autre crime auprès de cette même victime (Gill & Pease, 1998). Un des facteurs favorisant une seconde victimisation par le délinquant serait que le crime n'ait pas été rapporté aux autorités la première fois. Ainsi, le criminel sait qu'il a peu de chances de se faire attraper puisque la victime a eu une faible réaction/réponse (Farrell, Phillips & Pease, 1995). On peut facilement appliquer cela aux cybercrimes où le nombre de crimes rapportés à la police est très bas.

Ainsi donc, le contexte des cybercrimes est différent de celui des crimes traditionnels pour lesquels les moyens d'autoprotection (tels qu'éviter les lieux dangereux, verrouiller les portes de leur maison) permettent d'éviter ou de réduire sensiblement les risques de victimisation (Farrell & Pease, 2006). Comme mentionné, beaucoup de personnes ont un biais d'optimisme qui fait en sorte qu'elles se perçoivent comme moins à risque que les autres (Campbell et al., 2007; Pfleeger & Caputo, 2012; Rhee et al., 2012; West, 2008) ou, encore, elles sont biaisées dans leur perception du risque véritable (Redmill, 2002). Les organisations *America Online* (AOL) et *National Cyber Security Alliance* (NCSA) (2005) ont sondé des utilisateurs aux États-Unis à propos de leurs habitudes et leur perception de risque en ligne. L'une des questions portait sur les virus : on demandait aux répondants à quel point ils estimaient que leur ordinateur était à l'abri des virus. Une grande majorité (79%) a répondu qu'ils trouvaient que leur ordinateur était plus en sécurité (*very safe, somewhat safe*) qu'en danger (*not very safe, not at all safe*). Les résultats étaient très similaires pour les questions concernant les menaces en ligne et les hackers. C'est aussi pourquoi la plupart des participants (68%) conservaient des données de nature sensible sur leur ordinateur (e.g., leurs informations financières). Un autre sondage réalisé au Canada révèle que le groupe d'individus qui est le plus satisfait de sa sécurité personnelle sont les jeunes âgés de 15 à 24 ans et ce, même si leur taux de victimisation pour les crimes en général est plus élevé que pour les canadiens plus âgés (Brennan, 2011).

Lorsqu'un individu est victime d'un crime, il va avoir plus tendance à recourir à des mesures de prévention afin de prévenir la répétition du crime. Les victimes sont également moins sujettes à être satisfaites de leur sécurité. Les expériences indirectes reliées à un crime pourraient

également venir influencer le sentiment de sécurité des personnes (Brennan, 2011). Cependant, de façon surprenante, la victimisation n'a pas changé les habitudes de cyberhygiène des individus (Cain et al., 2018). Les femmes, les personnes âgées et les pauvres se percevraient comme plus vulnérables à la victimisation (Grohe, 2011).

La section qui suit présente les questions de recherche retenues pour le présent mémoire et qui découlent de la documentation scientifique recensée.

Chapitre 2 : Problématique

Considérant tous les efforts consentis à la prévention des cybercrimes, il est primordial de se questionner sur l'efficacité des mesures employées pour réduire leur prévalence. En effet, la cybercriminalité est un phénomène en croissance et il est nécessaire de bien documenter dans quelle mesure les stratégies préventives atteignent leurs cibles. Les conséquences adverses reliées aux cybercrimes sont considérables et il est important d'informer et de sensibiliser adéquatement la population à ce phénomène afin d'assurer efficacement leur protection et d'augmenter le sentiment de sécurité des individus.

La présente recherche s'inscrit dans le contexte d'une consultation (par sondage) menée par une institution financière canadienne immédiatement après la fin d'une campagne de prévention des cybercrimes. Le projet de mémoire porte sur une partie des données recueillies auprès de clients adultes québécois inscrits à un panel web. Les objectifs de recherche spécifiques à la présente recherche sont les suivants :

1) Quelle est la perception générale des répondants à propos de la campagne de prévention. De façon plus précise, les éléments suivants seront examinés : Combien de répondants se souviennent d'avoir vu les affiches de campagne ? Combien se souviennent avoir consulté la section du site dédiée à la campagne ? Combien trouvent utiles les conseils énoncés dans la campagne ? Quel est le niveau d'intérêt des répondants pour les différents thèmes de la campagne ? Quel est le principal message retenu par les répondants à propos de l'affichage de la campagne ?
2) La deuxième question de recherche se rapporte aux effets perçus de la campagne chez les répondants. De façon plus précise, on examinera dans quelle mesure la campagne a eu un effet sur leur sentiment de sécurité et si celle-ci a amélioré leur perception de l'institution financière. Un sous-objectif sera de déterminer si les effets perçus sur le sentiment de sécurité varient en fonction des caractéristiques des répondants. Quatre variables individuelles potentiellement déterminantes seront prises en considération : le genre, l'âge, le niveau de revenu et le niveau d'intérêt envers les sujets ciblés.

L'analyse des données permettra de tirer certaines conclusions en lien avec les retombées de la campagne de prévention en cybersécurité et, potentiellement, de dégager des recommandations susceptibles de bonifier l'élaboration et la mise en application de nouvelles mesures de prévention.

Chapitre 3 : Méthodologie

3.1. Participants

Les participants sont des clients adultes d'une institution financière canadienne recrutés sur le territoire québécois. Ces personnes ont donné leur accord pour faire partie d'une liste de clients que l'institution consulte régulièrement afin de recueillir des données sur leurs opinions, leur niveau de satisfaction, etc. Ces consultations en ligne ont pour but d'améliorer la qualité des services offerts et de mieux répondre aux attentes de la clientèle. Ainsi, une invitation à remplir un sondage a été envoyée aux clients ayant accepté de faire partie d'un panel web. Ceux-ci ont été invités à répondre aux questions de façon volontaire. Le sondage a été rempli par 1468 participants. De ce nombre, 16 d'entre eux ont été exclus, soit parce qu'ils n'habitaient pas au Québec (n=14), soit en raison d'un trop grand nombre de données manquantes (n=2). L'échantillon final se compose donc de 1452 participants francophones (831 hommes et 521 femmes) âgés entre 18 à 94 ans (moyenne de 53,7 ans et écart type de 14,8). Il n'était pas exigé que les répondants aient vu l'affichage ou les messages de la campagne de prévention au préalable pour être autorisés à répondre au sondage (voir plus loin pour les détails concernant la campagne de prévention). En outre, pour faire partie du panel web, il n'y avait pas d'autres conditions que celles d'être un client adulte de l'institution financière, être capable de lire le français et être résident canadien (pour les fins de la présente étude seuls les participants provenant du Québec ont été sélectionnés).
Les critères d'inclusion à notre étude sont donc les suivants :

1) avoir 18 ans ou plus ;
2) être client de l'institution financière
3) résider au Québec ;
4) être capable de lire le français

Les caractéristiques personnelles des répondants (au plan de l'âge, du sexe et du niveau d'épargne) sont présentées dans le Tableau 1.

On constate que l'échantillon est majoritairement constitué d'hommes alors que la population est divisée plus également en deux. Cette différence étonne puisque dans la majorité des sondages, il y a habituellement un taux de réponses plus élevés chez les femmes (Curtin, Presser, & Singer, 2000; Goyder, Warriner, & Miller; 2002). De plus, les plus jeunes ont également tendance à participer plus souvent dans les sondages que les plus âgés (Moore & Tarnai, 2002). Cela pourrait être dû au fait que les études en sciences sociales ont souvent recourt à des échantillons de commodité, soit la population étudiante qui est majoritairement constituée de femmes et de jeunes.

De plus, nos répondants sont pour la plupart plus âgés que la population générale. L'échantillon est aussi composé de répondants assez bien nantis puisque 51,7% d'entre eux ont un niveau d'épargne supérieur à 50,000$ (cette donnée n'est pas disponible pour la population générale puisque les statistiques sont uniquement disponibles pour le revenu annuel moyen).

Tableau I: Caractéristiques sociodémographiques de l'échantillon vs population québécoise

	Population totale (%)	Échantillon (%)
Genre		
Homme	49,7	57,2
Femme	50,3	42,8
Âge		
18-34 ans	25,9	13,7
35-44 ans	16,5	16,6
45-54 ans	16,2	14,3
55-64 ans	18,2	27,3
65 ans ou plus	23,2	28,1
Niveaux d'épargne ($)		
0-999	n.d.	8,3%
1,000-9,999	n.d.	16,7%
10,000-49,999	n.d.	23,3%
50,000 ou plus	n.d.	51,7%

3.2. Méthode de collecte de données

Les données ont été collectées par une firme de sondage employée par l'institution financière. Deux équipes travaillant pour l'institution ont aussi été mises à contribution, notamment dans l'élaboration et la validation des questions.

Les questions pour le sondage ont été élaborées à l'été 2018 dans le but d'intégrer les données à un indicateur sur le sentiment de sécurité des clients. L'auteur de ce mémoire a participé à ce travail d'élaboration du questionnaire. L'équipe cherchait à savoir si la campagne de

prévention, qui existe depuis maintenant quelques années, était efficace pour transmettre ses messages et, aussi, si cela renforçait ou non le sentiment de sécurité des clients. Ainsi, les questions ont été créées avec l'indicateur en tête, puis ont été transmises à l'équipe de marketing qui en a fait une validation et les a adaptées afin qu'ils correspondent mieux aux types de questions qui sont habituellement posées dans ce genre de consultation auprès de la clientèle.

Le questionnaire s'intéressait principalement à deux aspects de la campagne de prévention, soit comment l'affichage a été perçu par les répondants et comment la campagne, de façon plus générale, a été perçue. La campagne de prévention a duré un mois (octobre 2018) et était essentiellement numérique, c'est-à-dire accessible en ligne. Le thème principal de la campagne de prévention était la cyberhygiène. La cyberhygiène, similairement à l'hygiène personnelle, consiste à être proactif afin d'éviter des problèmes dans le futur (tels avoir des virus informatique). Il est nécessaire d'utiliser les bons outils (e.g., un logiciel anti-virus) pour y arriver et savoir bien s'en servir afin qu'ils soient efficaces (e.g., faire les mises à jour lorsqu'il y en a). Aussi, il faut qu'on intègre ces pratiques à notre routine quotidienne, comme l'hygiène personnelle (Norton, 2019). Les deux principaux volets ou types de contenus inclus dans la campagne étaient : (1) une affiche proposant des comportements sécuritaires à adopter au quotidien (visible notamment sur les écrans dans les succursales) et, (2) de courts articles sur la sécurité en ligne (abordant divers sujets tels que l'hameçonnage, le vol d'identité et la prévention de la fraude). Il était donc possible pour les clients d'avoir eu accès au contenu de la campagne à leur domicile (sur le site web de l'institution financière) et/ou en succursale, ou, encore, de ne pas avoir pris connaissance de ces contenus.

À partir des questions du sondage, la direction de l'institution souhaitait déterminer si la campagne de prévention avait eu l'effet escompté, c'est-à-dire, est-ce que le message transmis est bien compris et est-ce que les conseils proposés en regard des comportements sécuritaires ont été mis en pratique par les clients. On voulait aussi déterminer si les répondants ont de l'intérêt pour le thème de la campagne de prévention. Un des objectifs poursuivis à plus long terme était que l'information recueillie permettrait d'améliorer l'efficacité des prochaines campagnes de prévention en matière de sécurité.

Un fichier comportant uniquement les réponses aux questions du sondage nous a été transmis après avoir obtenu les autorisations requises de la part d'un membre de la direction (le fichier ne contenait aucun renseignement personnel permettant d'identifier les répondants). Comme déjà mentionné, le panel web est disponible uniquement aux clients qui acceptent d'en faire partie et

de répondre volontairement aux sondages. Dans le cas de la présente étude, le questionnaire comprenait 17 questions dont 13 à choix multiples et quatre questions ouvertes. La durée moyenne pour remplir le sondage a été estimée à six minutes. Il a été administré en français et la collecte de données s'est effectuée du 29 octobre au 6 novembre 2018.

Un panel web est une méthode appropriée pour constituer un échantillon représentatif de la clientèle. Cela est important pour s'assurer que tous les groupes de la société soient représentés au sein de l'échantillon (et éviter la sous-représentation ou la surreprésentation de certains groupes lors de sondage). Le panel web est une méthode alternative aux méthodes d'échantillonnage de commodité (par exemple lorsqu'on a recourt aux étudiants universitaires qui sont souvent peu représentatifs de la population générale) ou encore le « crowdsourcing », qui implique un aspect de collaboration entre une compagnie et le public dans le but de créer ou d'améliorer un produit (Redmiles et al., 2017). Ainsi, les panels webs sont habituellement créés par des compagnies ou des organismes qui souhaitent recruter des participants à grande échelle grâce à divers moyens (e.g., à partir de listes de diffusion). Dans le cas présent, l'institution financière affiche la possibilité à ses clients qui le désirent de s'inscrire pour faire partie du panel web. Les participants ne sont pas rémunérés après chaque participation ; cependant, en participant ils courent la chance de gagner un prix suite à un tirage au sort. Grâce à ce type de méthode, il est possible de cibler le type de répondants voulu selon l'étude ou le sujet. Il est donc intéressant d'utiliser cette méthode si l'on souhaite rejoindre un groupe de répondants en particulier (e.g., âge, genre, provenance, etc.). Aussi, certains chercheurs ont voulu savoir si les personnes qui participent à un sondage « en ligne » ont tendance à fournir des réponses plus détaillées aux questions ouvertes que celles qui répondent à un sondage en format papier (Kiesler & Sproull, 1986; Schaefer & Dillman, 1998). Ceux-ci ont trouvé que c'était le cas puisque les participants peuvent rectifier leurs erreurs de façon plus aisée que s'ils répondent par écrit (Baer, 1988). Les résultats sont également transmis de façon beaucoup plus rapide puisqu'une fois que les participants soumettent leur sondage, les résultats sont automatiquement compilés dans un ordinateur. Il n'est donc plus nécessaire de saisir les données manuellement à partir de copies-papier. Cela facilite l'analyse des données par la suite en plus de réduire le coût relié aux sondages traditionnels (Andrews, Nonnecke & Preece, 2003; McPeake, Bateson & O'Neill, 2014).

Dans la présente étude, nous avons ciblé principalement des participants qui résidaient dans la province du Québec (un sous-échantillon plus marginal de personnes résidant en Ontario a été

exclu ; n< 5%) et qui parlaient le français (le questionnaire était seulement accessible dans cette langue). Évidemment, il y a aussi des inconvénients à ce type de sondage. Ainsi, ce ne sont pas tous les participants éligibles qui acceptent de répondre au sondage qu'on leur envoie. Il y a un haut taux de non-réponse ce qui fait en sorte qu'on ne peut pas toujours généraliser les résultats à l'ensemble de la population par la suite.

Comme mentionné, la campagne de prévention a été menée par l'institution financière auprès de ses clients en octobre 2018. La direction a choisi de sonder les clients peu de temps après la fin de la compagne (fin octobre et début novembre 2018) afin de maximiser les chances que les répondants se souviennent des messages transmis par l'affichage et la campagne. Le questionnaire se divise en différentes catégories de questions, soit : les questions en lien avec l'affichage de la campagne de prévention (4 questions) ; l'intérêt des répondants à recevoir de l'information sur comment se protéger (leurs appareils, leurs comptes bancaires, et leur identité – 3 questions). Quatre questions ouvertes (sans choix de réponses) ont été proposées afin de permettre aux répondants de donner leur opinion sur des sujets relatifs à la campagne de prévention (notamment sur les aspects qu'ils ont apprécié de la campagne) et aussi afin d'évaluer ce qui a été retenu de la campagne et ce qui pourrait être fait pour améliorer son efficacité. Une dernière question (à choix multiples) demande aux répondants d'évaluer si leur sentiment de sécurité a augmenté, resté inchangé ou diminué suite à la campagne. Dans le questionnaire, on incitait également les répondants à aller visiter le site web ainsi que les sections comprenant les articles sur la sécurité pour ceux qui ne l'avaient jamais vu auparavant. Aussi, cela pouvait également servir de rappel pour ceux qui l'avaient déjà consulté. Enfin, on demandait aux répondants de regarder l'affichage de la campagne et de donner leur avis sur la signification des messages transmis lors de la campagne.

3.3. Procédure et méthode d'analyse

Les répondants ont pu accéder au questionnaire en ligne en se connectant à l'aide de leur nom d'utilisateur et mot de passe. Le sondage était accessible entre le 29 octobre et le 6 novembre 2018. Les participants ont été sollicités grâce au panel web qui leur donne également accès à d'autres sondages sur divers thèmes.

Le logiciel SPSS (version 26) a été utilisé afin de faire l'analyse des données quantitatives et de répondre aux questions de l'étude. À l'aide du logiciel, nous avons pu procéder à la

vérification des données, retirer les données manquantes, analyser les données descriptives et effectuer les tests statistiques requis.

La première question de recherche visait à décrire comment l'affichage/campagne ont été perçus (de façon générale) par les répondants (en rapport avec la visibilité, l'appréciation, l'utilité et les sujets d'intérêt). Pour ce faire, pour chacune des questions quantitatives ciblées du sondage, on a établi le pourcentage de répondants ayant fourni chaque choix de réponse possible. Une question qualitative a aussi fait l'objet d'une analyse : *Globalement, que retenez-vous du message transmis par l'institution financière* ? La procédure d'analyse de cette question est décrite plus loin.

Pour la deuxième question de recherche, des analyses descriptives ont également été effectuées pour évaluer les effets perçus de l'affichage et de la campagne (sur leur opinion envers l'institution et sur le sentiment de sécurité). Le nombre et le pourcentage de répondants ayant fourni les réponses à chaque question sont rapportés. On a ensuite effectué des analyses de chi-carré (Chi-2) pour déterminer l'existence de liens significatifs entre les variables à l'étude (pour déterminer si les caractéristiques individuelles sont reliées aux réponses). Le test chi-carré est indiqué ici car les variables sont de type catégoriel. Il s'agit d'un test statistique non paramétrique qui peut être utilisé pour comparer des fréquences (observées et attendues) exprimées en proportions, pourcentages ou probabilités. Il est recommandé d'appliquer le test de chi-carré à des variables nominales et ordinales qui comportent un nombre limité de catégories ou de niveaux (ce qui est le cas dans cette étude). Grâce au chi-carré, il est possible de déterminer si la différence entre deux distributions de fréquences est due à l'erreur d'échantillonnage ou bien s'il y a réellement une différence significative (rejet de l'hypothèse nulle avec une probabilité d'erreur inférieure à 5%).

Outre les questions à choix de réponse du sondage, les répondants ont été invités à répondre à quelques questions ouvertes dans le but d'avoir leur opinion sur des aspects précis de la campagne. Pour ce mémoire, une question qualitative a fait l'objet d'une analyse : Globalement que retenez-vous du message que veut transmettre l'institution financière ? La technique d'analyse utilisée ici est : l'analyse inductive générale (Thomas, 2006). Cette dernière est bien adaptée pour l'analyse de données pour des recherches exploratoires où il y a encore peu de littérature existante. Elle consiste à passer du spécifique (e.g., les participants parlent de leur propre expérience par rapport à un sujet) au général, afin de pouvoir appliquer ce qui en ressort dans divers contextes.

Pour commencer l'analyse inductive, il faut d'abord identifier ce qui nous intéresse de façon spécifique. Puis, on doit relire les données brutes à plusieurs reprises afin de se familiariser avec les réponses et tenter d'en ressortir les thèmes émergents tout en gardant un esprit ouvert et ne pas tenter de trouver un certain type de résultat. On procède alors à la codification des données afin de diminuer la quantité d'informations à analyser. La codification étant un des éléments clés de l'analyse qualitative (Morse & Richards, 2013). Il faut donc « étiqueter » les énoncés rédigés par les participants (dans le cas de cette étude) pour créer des catégories. Une fois cette étape finie, il est important de raffiner davantage en reliant les catégories similaires entre-elles ou redondantes. Ainsi, les catégories préliminaires, qui étaient plus spécifiques, vont devenir plus générales et ce sont ces catégories que nous allons conserver pour la codification finale (Thomas, 2006). On commence alors à voir émerger les idées principales qui émanent des diverses réponses des répondants.

Chapitre 4 : Résultats

4.1. Résultats en lien avec la perception générale de l'affichage et de la campagne

Le tableau 2 présente le pourcentage et le nombre de participants ayant répondu aux questions générales du sondage (en lien avec la visibilité de l'affichage, l'appréciation, et l'utilité de la campagne et l'intérêt des répondants envers les sujets de sécurité).

Les réponses au sondage indiquent qu'un pourcentage relativement faible de participants se souvient avoir vu l'affichage (18%). Un pourcentage encore plus faible (15%) a rapporté avoir consulté les articles de la campagne de prévention sur le site de l'IF. Un examen plus attentif des caractéristiques des répondants qui se souviennent de l'affichage et qui rapportent avoir consulté les articles nous permet de constater que ce sont, en grande majorité, les personnes les plus âgées de l'échantillon (environ les 2/3 de ces répondants ont 55 ans et plus).

Ainsi, le nombre de participants qui rapporte n'avoir vu ni l'affichage, ni les articles de la campagne est très élevé (82%). Toutefois, une très forte majorité de personnes sondées ont apprécié recevoir des conseils sur la sécurité (93%) et trouvé ces conseils utiles (81%). En ce qui concerne l'intérêt des répondants pour les différents sujets reliés à la sécurité, on constate que ceux abordant la protection du compte bancaire et la protection de l'identité suscitent le plus d'intérêt (près de 80% pour les deux sujets). Le thème de la protection des appareils rejoint l'intérêt d'un peu moins de participants (61,5%).

Tableau II: Pourcentage et nombre de participants ayant répondu aux questions principales du sondage (visibilité, appréciation, utilité et intérêt)

Principales questions sur la perception de l'affichage/campagne et choix de réponse	Nombre et pourcentage de répondants % (n)
Vous souvenez-vous d'avoir vu l'affichage ?	
Oui	18,4% (268)
Non	86,1% (1188)
Avez-vous déjà accédé à la section (conseils de sécurité) du site ?	
Oui	15,5% (225)
Non	84,5% (1231)
J'apprécie que l'IF informe ses clients sur la sécurité ?	
En accord	93,3% (1355)
En désaccord	3,1% (45)
Ne sais pas	3,8% (56)
Quel est le niveau d'utilité perçue des conseils de sécurité ?	
Utile	81% (1180)
Inutile	13,7% (199)
Ne sais pas	5,3% (77)
Quel est votre intérêt à recevoir des conseils sur les sujets suivants ?	
a) La protection de vos appareils :	
Beaucoup	61,5% (896)
Un peu/pas	37,1% (540)
Ne sais pas	1,4% (20)
b) La protection de votre compte bancaire :	
Beaucoup	78,6% (1145)
Un peu/pas	20,5% (298)
Ne sais pas	0,9% (13)
c) La protection de votre identité :	
Beaucoup	79,1% (1152)
Un peu/pas	20,2% (294)
Ne sais pas	0,7% (10)

4.2. Analyse qualitative

La première lecture des réponses fournies a permis de dégager les constats suivants : la très grande majorité des réponses comportaient peu de mots (courts énoncés de 6 mots ou moins) ; les répondants ont utilisé des termes assez semblables (synonymes) ; un nombre non négligeable de répondants ont critiqué le libellé de la question plutôt que d'y répondre et plusieurs autres ont inscrit une réponse qui n'avait pas de lien évident avec la question. Une première catégorisation des réponses a permis d'élaborer la grille de codification des données des participants. Cette catégorisation a été élaborée en dégageant des thèmes émergeants mutuellement exclusifs à partir des réponses recueillies (principal message retenu de la campagne). Au total, sept grandes catégories ont été identifiées : 1) la campagne avait comme thème principal la prudence/sécurité des clients **au sens général**. Cela regroupe toutes les expressions en lien avec cette thématique sans toutefois faire allusion à un moyen de protection spécifique (par exemple, « *il faut être prudent* », « *la vigilance d'impose* », « *il faut être sécuritaire* », etc.) ; 2) la campagne portait sur la prudence/sécurité mais le répondant rapportait **de façon plus spécifique** un conseil ou un moyen de protection qu'il avait retenu (par exemple, « *il faut changer régulièrement notre mot de passe* », « *s'assurer d'avoir un bon logiciel anti-virus* », etc.) ; 3) la campagne de prévention a démontré que l'institution financière se préoccupe de la sécurité (par exemple, « *l'institution souhaite que ses clients soient bien protégés* », « *l'institution met tout en œuvre pour assurer notre sécurité* », etc.) ; 4) la campagne portait sur les dangers d'utiliser Internet (par exemple, « lorsqu'on navigue sur Internet, on est vulnérable », « il y a des risques à faire des transactions en ligne », etc.) ; 5) le thème de la campagne de prévention n'était pas clair (par exemple, « je n'ai pas compris le sens ») ; 6) autre réponse : la réponse fournie était ambiguë, non pertinente et ne permettait pas d'être classée parmi les autres catégories, et 7) rien ou indifférence : le répondant a mentionné que la campagne l'avait laissé indifférent ou qu'il n'avait rien retenu en particulier.

La seconde étape a consisté à codifier chaque réponse à l'aide de la grille de codification. Deux codeurs ont fait cet exercice (l'auteur de ce mémoire et un autre étudiant de deuxième cycle). La comparaison des codifications a permis de constater un niveau de concordance très élevé, le nombre de désaccord étant marginal (<2%, 26 désaccords). Les deux codeurs ont ensuite examiné les désaccords afin de s'entendre sur le code à attribuer.

Tableau III: Codification des réponses : ce que les répondants ont retenu de la campagne

Catégories	**Échantillon total** **% (n)**	**Hommes** **% (n)**	**Femmes** **% (n)**
Prudence/sécurité (général)	64,5% (932)	61,3 % (514)	66,3% (418)
Prudence/sécurité (spécifique)	4,4% (65)	3,7% (31)	5,4% (34)
Préoccupations de l'institution financière	3,7% (55)	4,4% (37)	2,9% (18)
Dangers reliés à Internet	0,5% (7)	0,4% (3)	0,6% (4)
Campagne n'était pas claire	5,7% (83)	6% (50)	5,2% (33)
Autres	8,3% (122)	8,7% (73)	7,8% (49)
Rien ou indifférence	5,6% (82)	5,6% (47)	5,6% (35)
Non répondu	8,3% (122)	9,9% (83)	6,2% (39)
Total	100% (1468)	100% (838)	100% (630)
($\chi 2(5)= 6,31$; p=0,28, n.s.)			

Le tableau 3 présente les pourcentages de répondants pour chaque catégorie de la grille de codification en fonction du sexe du répondant. Ces données permettent de constater que la majorité des répondants (près des 2/3) ont retenu le message « général » visé par la campagne : il est nécessaire de faire preuve de sécurité, de prudence et d'être vigilant en ligne. L'absence de réponse et les réponses non pertinentes (autres) obtiennent le deuxième pourcentage le plus élevé (8,3%). Ensuite, de façon moins importante (3,7% des répondants) ont fait référence à l'institution financière. Ceux-ci ont perçu la campagne de prévention comme une démonstration que l'institution financière se soucie de la sécurité de ses clients et qu'elle y accorde de l'importance (e.g., « la sécurité est une priorité chez cette institution financière »). La quatrième catégorie qui portait sur les « dangers » est celle qui a obtenu le taux d'occurrence le plus faible (0,5%, n=7). Elle regroupe les participants qui ont seulement fait mention des risques liés à l'utilisation de l'Internet sans évoquer la sécurité. La septième catégorie (5,6%) a été codée lorsque les participants ont répondu que la campagne les avait laissés indifférents ou, encore, qu'il n'avait retenu rien en particulier de la campagne. On constate que les hommes et les femmes ont fourni des réponses dans des proportions assez similaires pour chaque catégorie. L'analyse de Chi-2 (sans la catégorie « dangers reliés à Internet » qui contient des cellules < 5) confirme l'absence de

différence significative dans les réponses qualitatives des répondants (principal message retenu) selon le genre ($\chi 2(5)= 6,31$; $p=0,28$, n.s.).

Le tableau 4 présente les pourcentages de répondants pour chaque catégorie codifiée en fonction des groupes d'âge. L'analyse de Chi-2 (sans la catégorie « dangers reliés à Internet » qui contient des cellules < 5) révèle une différence significative dans les réponses qualitatives des répondants (principal message retenu) selon le groupe d'âge ($\chi 2(5)= 33,26$; $p=0,03$) : les répondants plus âgés (65 ans et plus) sont, en proportion, moins nombreux à percevoir un message « général » de sécurité à la campagne (inférieur à 58% alors que ce pourcentage dépasse 63% pour les autres sous-groupes d'âge). En contrepartie, les répondants plus âgés sont un peu plus nombreux à attribuer un message de sécurité plus précis à la campagne (comme si les personnes de cette catégorie d'âge avaient retenu un ou des moyens spécifiques de la campagne). Ce sous-groupe se démarque aussi pour la catégorie des dangers perçus. Enfin, les répondants plus âgés ont été le plus nombreux à n'avoir rien retenu de particulier de la campagne ou en être indifférents (8,3% comparativement à moins de 6,2% pour les autres sous-groupes).

Tableau IV: Codification des réponses qualitatives selon l'âge des répondants

Catégories	Groupes d'âges				
	18 à 34 ans	**35 à 44 ans**	**45 à 54 ans**	**55 à 64 ans**	**65 ans ou plus**
	% (n)	**% (n)**	**% (n)**	**% (n)**	**% (n)**
Prudence/sécurité (général)	66,7% (134)	69,3% (169)	66% (140)	63,1% (253)	57,6% (236)
Prudence/sécurité (spécifique)	5% (10)	2,5% (6)	3,8% (8)	4,5% (18)	5,6% (23)
Institution financière	5,5% (11)	4,1% (10)	3,3% (7)	3,7% (15)	2,9% (12)
Dangers reliés à Internet	0% (0)	0,4% (1)	0,5% (1)	0,2% (1)	1% (4)
Campagne n'était pas claire	4,5% (9)	2,5% (6)	4,7% (10)	7,5% (30)	6,8% (28)
Autres	7,5% (15)	9,4% (23)	9,4% (20)	7% (28)	8,8% (36)
Rien ou indifférence	2% (4)	3,3% (8)	6,1% (13)	5,7% (23)	8,3% (34)
Non répondu	9% (18)	8,6% (21)	6,1% (13)	8,2% (33)	9% (37)
Total $(\chi 2(5)= 33,26; p=0,03)$	100% (201)	100% (244)	100% (212)	100% (401)	100% (410)

4.3. Résultats en lien avec les effets perçus de la campagne de prévention

Les sections qui suivent présentent les analyses effectuées en lien avec la deuxième question de recherche : les effets perçus de la campagne sur le sentiment de sécurité et l'opinion des répondants à l'égard de l'institution financière. Le tableau 5 rapporte le pourcentage de répondants pour chaque catégorie de réponse liée aux deux questions retenues.

Tableau V: Effets perçus de l'affichage/campagne sur l'opinion des répondants envers l'institution financière et le sentiment de sécurité

Questions en lien avec les effets perçus de l'affichage/campagne	% (n)
Améliore l'opinion que j'ai de l'institution ?	
En accord	67,5% (980)
En désaccord	17,9% (260)
Ne sais pas	14,6% (212)
A eu un impact sur votre sentiment de sécurité envers IF?	
En accord	66,5% (966)
En désaccord	22,5% (327)
Ne sais pas	11,0% (159)
Quel impact sur votre sentiment de sécurité envers IF ?	
Augmenté	48,9% (710)
Diminué	0,5% (7)
Ni augmenté, ni diminué	48,5% (704)
Ne sais pas	2,1% (31)

Globalement, l'affichage a été perçu de façon plus positive que la campagne de prévention. Pour 66,5% des répondants, l'affichage a contribué à améliorer leur opinion et a eu un impact sur leur sentiment de sécurité envers l'institution financière. En ce qui a trait à la campagne de prévention, les impacts étaient plus négligeables. En effet, on constate que pour 48,5% des répondants cela a augmenté leur sentiment de sécurité, cependant pour la même

proportion de répondants cette campagne n'a rien changé. Ainsi, leur sentiment de sécurité est resté le même. Cela laisse donc sous-entendre que l'affichage a été perçu comme plus efficace que la portion site web de la campagne de prévention pour augmenter la sécurité.

Sur les 717 personnes ayant répondu que la campagne a eu un effet (710 effet positif perçu et 7 effet négatif perçu), la presque la totalité (99%) ont estimé que celui-ci était positif. Seulement sept répondants ont répondu que leur sentiment de sécurité avait diminué suite à la campagne de prévention.

4.3.1. Relation entre le genre des répondants et les effets perçus des mesures sur leur sentiment de sécurité

Le tableau 6 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon le genre.

Les analyses de Chi-2 révèlent que le genre du répondant n'est pas associé à leur réponse en lien avec l'effet perçu de l'affichage ($\chi 2(1)= 0,01$; $p= 0,99$, n.s.), ni à celle reliée à l'effet de la campagne ($\chi 2(1)= 1,88$; $p=0,17$, n.s.). En d'autres mots, il n'y a pas de différence significative selon le sexe des répondants sur les deux mesures. On remarque qu'une proportion plus élevée de répondants (autant masculin que féminin) affirme que l'affichage a eu un impact sur leur sentiment de sécurité envers l'institution. Par contre en ce qui concerne les effets de la campagne, une proportion assez équivalente de répondants a répondu que celle-ci n'avait eu aucun effet comparé à ceux qui ont estimé qu'il y avait une augmentation de leur sentiment de sécurité.

Tableau VI: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment de sécurité envers l'institution, selon le genre

Effet perçu sur le sentiment de sécurité envers l'institution	Genre du répondant	
	Masculin	**Féminin**
	% (n)	**% (n)**
Affichage a eu un effet sur le sentiment		
En désaccord	25,3% (187)	25,3% (140)
En accord	74,7% (552)	74,7% (414)
($\chi2(1)= 0,01$; $p= 0,99$, n.s.)		
Campagne a eu un effet		
En désaccord	48% (393)	51,7% (311)
En accord	52% (426)	48,3% (291)
($\chi2(1)= 1,88$; $p=0,17$, n.s.)		

4.3.2. Relation entre le groupe d'âge des répondants et les effets perçus des mesures sur leur sentiment de sécurité

Le tableau 7 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon le groupe d'âge. Les analyses de Chi-2 révèlent qu'il existe une différence significative entre les groupes d'âge en lien avec l'effet perçu de l'affichage ($\chi2(4) = 14,8$; $p < 0,05$) et avec l'effet perçu de la campagne ($\chi2(4) = 62,76$; $p < 0,0001$).

Une proportion plus élevée des répondants ayant plus de 55 ans affirme que l'affichage et la campagne de prévention ont eu un impact sur leur sentiment de sécurité envers l'institution. En ce qui concerne l'affichage, 75% des répondants sont d'accord pour dire que celui-ci a contribué à augmenter leur sentiment de sécurité. Les clients ayant moins de 55 ans sont moins nombreux, en proportion à être d'accord avec l'affirmation (70%). Ce pourcentage s'élève à 76,3% chez les 55-64 ans et il est de 80,8% chez les répondants les plus âgés (65 ans et plus).

L'effet perçu de la campagne sur le sentiment de sécurité est plus faible que celui relié à l'affichage. En effet, seulement 50% des clients (échantillon total) ont répondu que la

campagne avait augmenté leur sentiment de sécurité. Cependant, le même effet lié à l'âge est observé que pour celui de l'affichage : plus les répondants sont âgés, plus ils tendent à répondre que la campagne a augmenté leur sentiment de sécurité (les pourcentages sont inférieurs à 45% pour les groupes âgés de moins de 55 ans ; il s'élève à 55% chez les 55-64 ans et atteint 63% chez les 65 ans et plus).

Tableau VII: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment de sécurité envers l'institution, selon le groupe d'âge

Effet perçu sur le sentiment de sécurité envers l'institution	**Groupe d'âge du répondant**				
	18 à 34 ans	**35 à 44 ans**	**45 à 54 ans**	**55 à 64 ans**	**65 ans ou plus**
	% (n)	**% (n)**	**% (n)**	**% (n)**	**% (n)**
Affichage a eu un effet sur le sentiment?					
En désaccord	29,7% (54)	30,7% (67)	29,7% (54)	23,7% (82)	19,2% (70)
En accord	70,3% (128)	69,3% (151)	70,3% (128)	76,3% (264)	80,8% (295)
(χ2(4)= 14,8; p < 0,05)					
Campagne a eu un effet sur le sentiment?					
En désaccord	60,3% (120)	63,4% (151)	57,3% (114)	44,9% (172)	36,6% (147)
En accord	39,7% (79)	36,6% (87)	42,7% (85)	55,1% (211)	63,4% (255)
(χ2(4)= 62,76; p < 0,0001)					

4.3.3. Relation entre le niveau d'épargne des répondants et les effets perçus de l'affichage et de la campagne sur leur sentiment de sécurité

Le tableau 8 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon l'épargne.

En ce qui concerne l'effet perçu de l'affichage, 75% des répondants estiment que celui-ci a eu un effet bénéfique sur leur sentiment de sécurité. Ce pourcentage est assez équivalent pour tous les groupes d'épargne, du plus petit au plus grand. Ces résultats indiquent que quel

que soit le niveau d'épargne du répondant, cela n'a pas eu un effet significatif sur la perception de l'effet de l'affichage.

En ce qui concerne l'effet de la campagne sur le sentiment de sécurité, on remarque que celui-ci est perçu comme étant plus faible (50%) que celui de l'affichage (75%) – par contre, on constate que l'effet perçu de la campagne varie selon l'épargne des répondants, à la faveur des plus nantis. En effet, on remarque qu'une majorité de gros épargnants (50000$ et plus) ont rapporté que la campagne de prévention a eu un impact sur leur sentiment de sécurité. Pour les trois autres groupes d'épargnants, une proportion plus faible de répondants (inférieure à 47%) ont jugé que la campagne leur avait été bénéfique pour leur sentiment de sécurité.

Les analyses de Chi-2 confirment que le niveau d'épargne du répondant n'est pas associé à leur réponse en lien avec l'effet perçu de l'affichage ($\chi2(3)= 3,84$; $p = 0,28$); en revanche, un lien significatif est obtenu entre le niveau d'épargne et l'effet perçu de la campagne ($\chi2(3)= 10,28$; $p < 0,05$).

Tableau VIII: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment de sécurité envers l'institution, selon l'épargne

Effet perçu sur le sentiment de sécurité envers l'institution	**Épargne du répondant**			
	0$ à 999$	**1 000 à 9 999$**	**10 000$ à 49 999$**	**50 000$ ou plus**
	% (n)	**% (n)**	**% (n)**	**% (n)**
Affichage a eu un effet sur le sentiment				
En désaccord	22,4% (n=24)	30,4% (n=66)	24,3% (n=73)	24,6% (n=164)
En accord	77,6% (n=83)	69.6% (n=151)	75,7% (n=228)	75,4% (n=504)
($\chi2(3)= 3,84$; $p = 0,28$)				
Campagne a eu un effet				
En désaccord	53,4% (n=62)	54,4% (n=129)	53,8% (n=179)	45,4% (n=334)
En accord	46,6% (n=54)	45,6% (n=108)	46,2% (n=154)	54,6% (n=401)
($\chi2(3)= 10,28$; $p < 0,05$)				

4.3.4. Relation entre l'intérêt des répondants dans la protection de leurs appareils et les effets perçus de l'affichage et de la campagne sur leur sentiment de sécurité

Le tableau 9 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon l'intérêt dans la protection de leurs appareils. Les analyses de Chi-2 révèlent que l'intérêt du répondant (pour la protection des appareils) est associé à leur réponse en lien avec l'effet perçu de l'affichage ($\chi2(1) = 83,31$; $p < 0,001$) et encore davantage à celle reliée à l'effet de la campagne ($\chi2(1) = 186,13$; $p < 0,0001$). Ces résultats indiquent que les répondants ayant un plus grand intérêt dans la protection de leurs appareils ont également été plus nombreux à rapporter un effet plus positif de l'affichage (83%) et de la campagne (65%) que ceux ayant moins d'intérêt envers la protection de leurs appareils (60% et 26% respectivement pour l'affichage et la campagne).

Pour 99,0% des répondants sur lesquels la campagne a eu un effet, c'était un effet positif. Seulement sept répondants sur les 716 ont vu leur sentiment de sécurité diminuer suite à la campagne de prévention.

4.3.5. Relation entre l'intérêt des répondants dans la protection de leurs comptes bancaires et les effets perçus de l'affichage et de la campagne sur leur sentiment de sécurité

Le tableau 10 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon l'intérêt dans la protection de leurs comptes bancaires.

Les analyses de Chi-2 révèlent que l'intérêt du répondant est associé à leur réponse en lien avec l'effet perçu de l'affichage ($\chi2(1) = 68,1$; $p < 0,001$) et à celle reliée à l'effet de la campagne ($\chi2(1) = 118,55$; $p < 0,0001$). Ces résultats indiquent que les répondants ayant un plus grand intérêt dans la protection de leurs comptes bancaires ont également perçu un effet plus positif de l'affichage (80%) et de la campagne (58%) que ceux ayant moins d'intérêt envers la protection de leurs comptes bancaires (55% et 21% respectivement pour l'affichage et la campagne).

Tableau IX: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment de sécurité envers l'institution, selon l'intérêt dans la protection de leurs appareils.

Effet perçu sur le sentiment de sécurité envers l'institution	**Protection de vos appareils**	
	Pas/peu d'intérêt	**Beaucoup d'intérêt**
	% (n)	**% (n)**
Affichage a eu un effet sur le sentiment		
En désaccord	40,2% (183)	17,1% (142)
En accord	59,8% (272)	82,9% (689)
($\chi 2(1) = 83{,}31$; $p < 0{,}001$)		
Campagne a eu un effet		
En désaccord	72,8% (382)	35,2% (311)
En accord	27,2% (143)	64,8% (573)
($\chi 2(1) = 186{,}13$; $p < 0{,}0001$)		

Tableau X: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment envers l'institution, selon l'intérêt dans la protection de leurs comptes bancaires

Effet perçu sur le sentiment de sécurité envers l'institution	**Protection de vos comptes bancaires (Q10BR)**	
	Pas/peu d'intérêt	**Beaucoup d'intérêt**
	% (n)	**% (n)**
Affichage a eu un effet sur le sentiment		
En désaccord	45,1% (116)	20,2% (208)
En accord	54,9% (141)	79,8% (823)
($\chi2(1)= 68,1$; $p < 0,001$)		
Campagne a eu un effet		
En désaccord	77,9% (225)	42,0% (472)
En accord	22,1% (64)	58% (653)
($\chi2(1)= 118,55$; $p < 0,0001$)		

4.3.6. Relation entre l'intérêt des répondants dans la protection de leur identité et les effets perçus de l'affichage et de la campagne sur leur sentiment de sécurité

Le tableau 11 présente la proportion de participants ayant perçu ou non un effet de l'affichage et de la campagne de prévention sur le sentiment de sécurité envers l'institution, selon l'intérêt dans la protection de leur identité.

Les analyses de Chi-2 révèlent que l'intérêt du répondant est associé à leur réponse en lien avec l'effet perçu de l'affichage ($\chi2(1) = 82,01$; $p < 0,001$) et à celle reliée à l'effet de la campagne ($\chi2(1) = 109,4$; $p < 0,0001$). Ces résultats indiquent que les répondants ayant un plus grand intérêt dans la protection de leur identité ont également été plus nombreux à rapporter un effet positif de l'affichage (80%) et de la campagne (57%) que ceux ayant moins d'intérêt envers la protection de leur identité (53% et 22% respectivement pour l'affichage et la campagne).

Tableau XI: Pourcentage et nombre de participants ayant perçu ou non un effet de l'affichage et de la campagne sur leur sentiment de sécurité envers l'institution, selon l'intérêt dans la protection de leurs identités

Effet perçu sur le sentiment de sécurité envers l'institution	**Protection de votre identité**	
	Pas/peu d'intérêt	**Beaucoup d'intérêt**
	% (n)	**% (n)**
Affichage a eu un effet sur le sentiment?		
En désaccord	47,4% (120)	19,8% (206)
En accord	52,6% (133)	80,2% (832)
($\chi2(1) = 82,01$; $p < 0,001$)		
Campagne a eu un effet sur le sentiment?		
En désaccord	77% (221)	42,4% (480)
En accord	23% (66)	57,6% (651)
($\chi2(1) = 109,4$; $p < 0,0001$)		

Chapitre 5 : Discussion

5.1. Interprétation des résultats

Le présent mémoire poursuivait deux objectifs principaux. Le premier était d'évaluer, à partir des résultats d'un sondage de type panel web, comment les clients d'une institution financière ont perçu les conseils de sécurité proposés lors d'une campagne de prévention. De façon plus précise, on a cherché à déterminer le nombre de répondants qui se souviennent avoir vu/consulté les messages préventifs (affichage et campagne) et à évaluer dans quelle mesure l'information transmise était perçue utile pour eux. Le niveau d'appréciation des clients concernant l'initiative de prévention de leur institution et le message qu'ils ont retenu de l'affichage ont aussi été étudiés. Le deuxième objectif était d'évaluer les effets perçus de la campagne sur le sentiment de sécurité des clients répondants. On a aussi cherché à savoir dans quelle mesure les clients ont perçu que la campagne de prévention avait un effet sur l'image qu'ils ont de leur institution financière. Enfin, des analyses ont été effectuées afin de déterminer si les effets perçus étaient liés à certaines caractéristiques individuelles des clients (le genre, le groupe d'âge, le niveau d'épargne et leur intérêt à être mieux informés au sujet des moyens de protection de différents cybercrimes).

Les premiers résultats laissent entrevoir que la campagne de prévention n'a atteint que partiellement sa cible en ce qui concerne sa visibilité et pour susciter l'intérêt des clients (à en connaitre davantage sur le sujet). En effet, moins d'un répondant sur cinq (18%) se souvient d'avoir vu les messages préventifs et un nombre encore plus faible rapporte avoir consulté les articles les informant des mesures de sécurité à leur disposition (15%). Comme la consultation a été effectuée quelques temps après la fin de la campagne, on ne peut que difficilement attribuer ce faible résultat à un oubli. Une explication plus probable serait que l'affichage n'a tout simplement pas retenu l'attention des clients. Le public est inondé d'information de toutes sortes (sur Internet mais aussi dans les médias et dans les nombreux affichages installés dans les lieux publics et commerciaux) et il est possible que les messages de la campagne soient passés inaperçus ou n'aient pas été suffisamment visibles pour qu'une majorité de clients s'en souviennent (peut-être parce que le message ne se démarquait pas suffisamment des autres informations disponibles). À ce sujet, une étude réalisée par van Dijk et Steinmetz (1981) sur le succès des campagnes de prévention en criminologie a trouvé que seulement 9% des répondants se souvenaient avoir vu les affiches – cette faible proportion va dans le même sens que le résultat

obtenu ici. Une seconde hypothèse serait que les clients consultés se sentent peu concernés ou interpellés par les messages transmis. Dans ce cas, ça ne serait pas la visibilité des messages qui seraient en cause mais plutôt l'intérêt des personnes. Il se peut en effet que l'attention d'une grande proportion des répondants n'a pas été orientée vers les messages de la campagne (suffisamment pour s'en souvenir) parce qu'ils ne se sentaient pas concernés ou avaient l'impression qu'ils ne s'adressaient pas à eux. En effet, des recherches ont démontré que les campagnes de prévention sont plus efficaces lorsqu'elles portent sur des problèmes « locaux spécifiques » (Bowers & Johnson, 2003). À l'appui de cela, l'étude menée par Verril et Bentley (2003, citée par Bowers & Johnson, 2005) indique que plus du deux tiers des répondants ont rapporté qu'ils ne portaient pas attention au message préventif lorsque celui-ci était trop général par rapport à la prévention du crime – nos résultats semblent indiquer que ce fut peut-être le cas ici.

De façon intéressante, les analyses révèlent que ce sont les répondants appartenant aux groupes d'âge plus élevés (55 ans et plus) qui rapportent se souvenir davantage de l'affichage et avoir consulté les articles qui leur étaient destinés (les 2/3 des personnes ayant répondu positivement à ces premières questions font partie de ces groupes d'âge). On peut donc supposer que la campagne a davantage suscité l'intérêt des personnes plus âgées faisant partie de leur clientèle (en répondant à leur besoin d'être informés). Les études réalisées en victimologie ont démontré qu'avec l'âge, la prise de risque diminue chez les adultes alors que la crainte d'être victimisé augmente (Williams, McShane, & Akers, 2000). Ainsi, les résultats obtenus semblent confirmer que les personnes plus âgées de notre échantillon sont plus prudentes et se montrent plus motivées à faire le nécessaire pour se renseigner sur les moyens de protection. Les personnes plus jeunes sont davantage familières avec les outils et le maniement informatique (qu'ils ont connu depuis leur jeune âge) et font peut-être preuve de plus d'insouciance face à leur protection. En revanche, les personnes plus âgées sont peut-être davantage conscientes des risques et des limites de leurs capacités à assurer leur sécurité. Une recension effectuée par Gourbesville (2007) sur les dangers d'Internet confirme que les plus jeunes sont plus confiants que leurs ainés et donc plus vulnérables face aux risques de l'utilisation du Web. Si on applique cette conclusion au contexte de la campagne, il n'est pas étonnant que les répondants les plus jeunes se souviennent peu des messages préventifs.

Les répondants ont été très nombreux à répondre que les conseils de sécurité de la campagne étaient utiles (81%) et que l'initiative de l'IF d'informer ses clients était très appréciée (93%). De tels résultats sont encourageants et soutiennent la pertinence de la campagne de prévention. Toutefois, on ne peut laisser de côté la possibilité qu'un biais de désirabilité sociale ait influencé les réponses des participants. Ce type de biais est souvent présent dans les enquêtes de satisfaction et il est fréquent que les répondants surévaluent les éléments positifs de la consultation (leur niveau d'appréciation, l'utilité des mesures proposées) pour « transmettre un message positif » (Steenkamp, De Jong, & Baumgartner, 2010).

D'autres réponses sont obtenues en lien avec l'intérêt des répondants en ce qui concerne trois sujets (ou thèmes) spécifiques se rapportant à la cybersécurité : la protection des appareils, la protection de l'identité et la protection des données bancaires ; les trois sujets sont perçus comme suscitant de l'intérêt chez une majorité de répondants. Cependant, ils ont été plus nombreux à manifester de l'intérêt pour les deux derniers types de protection (à plus de 80%) comparativement au sujet de la protection des appareils (62%). De tels résultats laissent entendre que la transmission d'informations ou de conseils plus explicites sur les moyens de protection des données bancaires et de l'identité pourrait répondre davantage aux besoins d'une majorité des clients adultes. Ces sujets sont sans doute jugés plus importants et intéressants du fait que le manque de protection (en lien avec l'identité et les données personnelles) est plus susceptible d'entrainer de graves conséquences. En comparaison, la protection des appareils est jugée un peu moins intéressante, possiblement parce que les personnes estiment être en mesure d'exercer eux-mêmes des mesures de protection. Il se peut aussi que les conséquences associées à un manque de protection des appareils soient perçues comme moins graves. Les réponses fournies sur les questions se rapportant à l'intérêt des personnes pour les sujets de protection semblent contredire les réponses en lien avec leurs souvenirs. En effet, on aurait pu s'attendre que si l'intérêt est présent chez les clients, ceux-ci devraient porter davantage attention aux messages transmis et s'en souvenir, Dans ce cas, ou bien les messages n'étaient pas si visibles ou bien l'intérêt n'est pas aussi élevé que rapporté.

Enfin, une analyse qualitative a été réalisée dans le but de catégoriser les réponses des répondants en lien avec le message qu'ils ont retenu de l'affichage (à noter qu'un rappel de l'affichage a été effectué durant la consultation). Cette analyse a permis de dégager une diversité de « points du vue » émergents concernant ce qui a été retenu des conseils de prévention. Sans

trop de surprise, l'analyse a mis en évidence que les répondants (64%) ont bien identifié (sans plus) le thème général de la campagne : l'importance de se protéger et d'applique des mesures de sécurité. Dans une proportion moindre, les participants ont identifié des mesures de protection spécifiques ou ont retenu que l'IF avait un souci de protéger sa clientèle. Une minorité de répondants ont soumis des réponses plus négatives (le message de la campagne n'était pas clair) ou aucun message particulier n'a été retenu (ou indifférence). Les autres catégories de réponses étaient plus marginales. Le faible pourcentage de répondants désintéressés, indifférents ou n'ayant rien retenu de particulier appuie l'idée voulant que la clientèle a été sensible au thème central de la campagne de prévention.

Une analyse plus détaillée des réponses permet d'établir qu'il y a peu de distinctions en fonction du genre des répondants. Par contre, le sous-groupe des répondants plus âgés (55 ans et plus) est plus nombreux à avoir retenu comme message un moyen de protection précis. Ici encore, la variable « groupe d'âge » ressort comme étant un facteur d'importance en lien avec la perception de la campagne et du message retenu. Ce résultat n'est toutefois pas étonnant puisque ce sont les répondants plus âgés qui rapportent se souvenir davantage de l'affichage et d'avoir consulté la documentation. Pour cette raison, les personnes plus âgées interrogées sont en mesure de fournir une réponse plus précise sur le message préventif transmis.

Les résultats obtenus en lien avec la perception des effets de l'affichage et de la campagne vont globalement dans le sens des objectifs poursuivis : plus des deux tiers des participants au sondage (68%) rapportent que l'affichage a contribué à améliorer l'opinion qu'ils avaient de leur IF. Une proportion équivalente de répondants (67%) a révélé que l'affichage avait eu un impact sur leur sentiment de sécurité envers l'IF. Une proportion plus faible de répondants (49%) a répondu que la campagne avait contribué à augmenter leur sentiment de sécurité envers leur IF et une même proportion ont rapporté que la campagne n'avait ni augmenté, ni diminué leur sentiment de sécurité. Les résultats de l'effet de l'affichage vont dans le sens attendu : il est en effet prévisible que les initiatives prises par l'institution pour informer leurs clients (en fournissant des conseils affichés) sont de nature à améliorer leur perception et à rehausser leur sentiment de sécurité envers cette dernière.

Les effets perçus de la campagne sur le sentiment de sécurité sont moins évidents. Deux raisons peuvent expliquer cette proportion plus faible : 1) il est possiblement moins clair pour les personnes interrogées de savoir à quoi réfère la campagne de façon très précise (seulement

15% de l'échantillon total ont révélé avoir accédé aux documents et autres informations de la campagne); à l'inverse, l'affichage est plus facilement identifiable car les répondants ont eu droit à un rappel durant la passation du questionnaire ; 2) le libellé de la question se rapportant à la campagne était quelque peu différent de celui en lien avec les effets de l'affichage (dans le premier cas, on demandait si la campagne avait augmenté, diminué ou eu aucun effet sur le sentiment de sécurité alors que dans le deuxième cas, on leur demandait le niveau d'accord avec une affirmation). Ces deux raisons combinées peuvent peut-être expliquer les résultats plus mitigés se rapportant à l'effet de la campagne.

Les analyses statistiques effectuées pour déterminer s'il y avait un lien entre les caractéristiques des répondants et les effets perçus sur le sentiment de sécurité ont produit quelques résultats intéressants. En résumé, des liens significatifs ont été obtenus pour trois des quatre variables prises en compte : le groupe d'âge, le niveau d'épargne et l'intérêt pour la protection (appareil, fraude bancaire et vol d'identité). Seule la variable genre n'est pas liée significativement aux réponses obtenues. On aurait pu s'attendre à ce que les répondants de sexe féminin rapportent un effet plus grand de la campagne sur leur sentiment de sécurité car certaines études révèlent qu'elles sont plus nombreuses que les hommes à être préoccupées de leur protection contre les cybercrimes. Une campagne de prévention offrant différents moyens pour mieux les protéger aurait pu répondre à un plus grand besoin chez les femmes. Les résultats obtenus ne confirment pas cette hypothèse et démontrent plutôt qu'une proportion assez semblable des répondants des deux genres rapporte que l'affichage et la campagne ont contribué à augmenter leur sentiment de sécurité envers l'IF.

Les tests statistiques démontrent que les personnes plus âgées de l'échantillon, ayant un plus haut niveau d'épargne et ayant un intérêt élevé pour les sujets traitant de la protection se démarquent significativement des autres groupes de répondants en ce qui concerne l'effet perçu positif de la campagne et de l'affichage sur leur sentiment de sécurité envers l'IF. La variable qui apparait la plus importante ici est le groupe d'âge ; en effet, les répondants les plus âgés sont ceux qui ont un plus haut niveau d'épargne et ce sont également les personnes qui affichent un plus haut niveau d'intérêt envers les moyens de protection. Ces trois caractéristiques ne sont pas indépendantes les unes des autres. Ici encore, il apparait logique que ce sous-groupe plus âgé se distingue des autres en rapportant plus d'effet positif de la campagne sur le sentiment de sécurité : ils sont plus nombreux à se souvenir de la campagne, à avoir retenu un message

préventif spécifique et précis et à avoir consulté les documents de la campagne. De tels résultats permettent d'avancer que la campagne a davantage répondu à un besoin chez ce sous-groupe de clients et qu'elle a davantage atteint sa cible chez eux que chez les autres groupes de répondants.

5.2. Résultats obtenus et modèle théorique

Les résultats se rapportant à l'effet de la campagne sur le sentiment de sécurité semblent confirmer la pertinence du modèle théorique central (HBM) retenu dans ce mémoire sur les croyances des personnes ciblées. Le fait que la majorité des personnes associent la présentation des mesures préventives de la campagne à un plus grand sentiment de sécurité va dans le sens de l'atteinte d'un objectif important de toute campagne de prévention. Comme déjà vu, les croyances des personnes sont déterminantes pour l'adoption des comportements de sécurité (davantage que les faits objectifs ou la simple présentation de données statistiques) – dans le cas présent, on peut penser que cette perception plus positive envers l'institution pourra contribuer, ultérieurement, à une plus grande ouverture face à l'utilisation des outils ou stratégies de protection proposées par celle-ci. Il est logique de penser que les personnes qui sont les plus sensibles aux risques potentiels de fraudes seront particulièrement motivées à s'informer sur les mesures de protection et, éventuellement, mettre en pratique les conseils transmis. Dans la présente étude, il a été possible d'établir un lien entre un élément de motivation (l'importance accordée par les répondants aux sujets abordés) et l'augmentation perçue de leur sentiment de sécurité. Malheureusement, les données recueillies ne permettent pas de savoir quels sont les participants qui ont effectivement mis en pratique les mesures proposées et si ces personnes sont celles qui avaient des croyances particulières quant à leur évaluation du risque (pour véritablement valider les postulats du modèle théorique).

5.3. Recommandations découlant des résultats obtenus et de l'analyse de la documentation

Les recommandations proposées ici, au nombre de dix, découlent en partie des résultats obtenus dans ce mémoire et en partie suite à l'analyse des conclusions émanant des recherches recensées sur les campagnes de prévention.

Premièrement, pour qu'une campagne soit considérée comme efficace, il est nécessaire qu'elle soit vue par le plus de personnes possibles pour que ces dernières retiennent les messages transmis. Dans le cas présent, seule une faible proportion des clients se souvient avoir vu des affiches et de la campagne (et un nombre encore plus faible rapporte avoir consulté les

documents de la campagne). Il faudrait donc augmenter la visibilité et l'intensité des messages préventifs en diversifiant les canaux de diffusion et en utilisant d'autres médias (que l'affichage et le site). Il pourrait être utile de prolonger la durée de la campagne pour assurer une meilleure visibilité. Le manque de visibilité a pu possiblement biaiser ou invalider quelque peu les résultats du sondage (puisqu'un rappel a été nécessaire). Par contre, il y a un risque à une trop grande visibilité : celle-ci risque en effet de provoquer ce que les experts appellent une « fatigue de sécurité » (*security fatigue*) (O'Donnell, 2019). À trop entendre et se faire répéter les mêmes messages, il y a une perte d'intérêt et d'attention importante qui est notée. Un « bon dosage » de l'intensité et de la fréquence de l'exposition aux messages préventifs semble la clé.

Deuxièmement, en plus de la visibilité, il serait recommandé de mieux évaluer les besoins de la clientèle et leurs attentes concernant la sécurité en ligne. Ces données permettraient ensuite de bien arrimer les messages de la campagne aux besoins réels exprimés. Dans la présente étude, il a été constaté que la campagne semblait mieux répondre aux besoins des clients plus âgés. La campagne a entrainé moins d'effets perçus positifs chez les clients plus jeunes et il apparait nécessaire de s'interroger pourquoi il en est ainsi. Une enquête préalable sur les connaissances des usagers en matière de cybersécurité pourrait apporter un éclairage intéressant en ce sens.

Troisièmement, l'étude a révélé que l'affichage et la campagne ont eu un effet (perçu) positif sur le sentiment de sécurité envers l'IF pour une nette majorité de répondants. Ce résultat constitue une retombée importante car il laisse entendre que la campagne a été utile pour renforcer l'image des clients envers leur institution bancaire. Les résultats indiquent aussi qu'il y a un lien entre la perception de l'effet positif et le niveau d'intérêt pour les sujets relatifs à la protection. Ce dernier résultat est particulièrement intéressant car il semble démontrer que plus il y a de l'intérêt pour le sujet abordé en campagne, plus celle-ci contribue à augmenter le sentiment de sécurité. Cela laisse aussi supposer que si on arrive à définir les messages préventifs en fonction de ce qui intéresse réellement les clients (au sujet de la sécurité personnelle), cela pourrait contribuer à ce qu'ils développent une confiance accrue envers leur institution et à se sentir mieux protégés.

Quatrièmement, la campagne de prévention de l'IF a utilisé des moyens simples et « classiques » (affichage, documents en ligne) et l'information transmise était présentée de façon assez conventionnelle (série de trucs ou conseils pour se protéger, articles). Les sujets

abordés étaient aussi assez généraux et diversifiés (sur la fraude bancaire, le vol d'identité, la protection des appareils, etc.). Certaines études ont démontré que les campagnes ayant un message trop général, trop varié ou trop diffus avaient moins de succès. Une piste prometteuse serait de mieux utiliser et mettre à profit les connaissances en marketing afin d'innover dans les moyens utilisés pour attirer l'attention du client, pour maintenir son intérêt et pour transmettre l'information. Par exemple, on pourrait proposer un contenu interactif pour stimuler la curiosité et l'intérêt des individus sur une plus longue période. Il semble que les jeux et les formations interactifs en ligne soient efficaces pour augmenter l'intérêt (Chung & Zhao, 2004; Song & Zinkhan, 2008) et développer les habiletés des utilisateurs leur permettant d'éviter d'être victimes d'hameçonnage (Sheng et al., 2010). Par exemple, en 2003 le Home Office a développé un site « *good2besecure* » qui visait à sensibiliser les étudiants à la sécurité. Le site comprenait des jeux interactifs (e.g., fermer les fenêtres afin d'empêcher un cambrioleur de venir dérober ses biens). Le but de marketing derrière cette initiative était de rejoindre le plus d'individus possibles en comptant sur le bouche-à-oreille (McCreith et Parkinson, 2004).

Cinquièmement, puisque les campagnes de prévention interactives sont peu courantes, cela pourrait faire en sorte de susciter la curiosité des individus et amener ceux-ci à en parler avec leur entourage. L'aspect « ludique » de ce type de campagne de prévention pourrait inciter les plus jeunes à regarder le contenu et à s'informer davantage sur la cybersécurité. Une autre stratégie prometteuse à intégrer à la campagne serait d'employer des « quiz interactifs » pour tester leurs connaissances. Cela pourrait motiver les participants à s'informer davantage des sujets qui les intéressent, après avoir constaté leurs lacunes en lien avec des sujets précis.

Sixièmement, en plus des moyens utilisés pour transmettre l'information, il pourrait s'avérer utile de revoir la diversité des sujets abordés dans la campagne. Dans le cas de la présente campagne, plusieurs thèmes étaient abordés. Sur la base de la documentation consultée, il apparait plus utile et possiblement plus efficace de miser sur un thème unique (par exemple, le vol d'identité) ou sur un nombre limité de sujets pour simplifier le message préventif. Il est possible que les moyens à déployer pour sensibiliser les clients sur un thème donné ne conviennent pas à tous les thèmes. Cela permettrait donc d'adapter la campagne en fonction du sujet ciblé. Même si cela a le désavantage d'avoir à concevoir des stratégies différentes en fonction du type de cybercrime, cela pourrait s'avérer plus efficace de procéder ainsi.

Septièmement, les campagnes de préventions actuelles visent essentiellement à informer les clients et le public sur les moyens de protection à leur disposition et à les sensibiliser à l'importance de les utiliser. Cette approche ne semble pas suffisante si l'objectif est que les clients mettent en pratique les moyens enseignés. En effet, les recherches consultées indiquent que le fait d'être bien informé ne garantit pas toujours une meilleure protection (voir Bada et al., 2015). De plus, plusieurs études ont démontré que les utilisateurs ignorent souvent les recommandations de sécurité et que les sessions d'information en « cyberhygiène » ne semblent pas avoir les impacts voulus (Cain et al., 2018). Il apparait donc important de revoir les façons de sensibiliser la population. Il a été démontré que les utilisateurs ne vont pas adhérer à de nouvelles mesures de sécurité s'ils estiment que les coûts (efforts) seront plus élevés que les bénéfices (sécurité) (Bada et al., 2015; Herley, 2009). Par exemple, les campagnes insistent beaucoup sur la sélection de mots de passe forts afin de bien se protéger contre les fraudes. On recommande également aux usagers de ne pas écrire leur mot de passe sur un morceau de papier ET d'avoir un mot de passe différent qui n'est pas un mot commun pour chacun de leurs comptes (Stajano, 2011). Pour un nombre important d'individus, cela représente en moyenne plus de 25 différents mots de passe à se rappeler (Florêncio & Herley, 2007), le nombre de comptes ne cessant d'augmenter (Adams & Sasse, 1999; Stajano, 2011). Ainsi, plusieurs utilisateurs seront peu enclins à appliquer ce conseil et à ne pas en tenir compte car l'effort nécessaire pour se rappeler de tous ces mots de passe pourra les décourager. Il serait préférable de revoir la manière de sécuriser les appareils et comptes à partir de moyens exigeants peu d'effort. En effet, l'effort demandé aux utilisateurs de nos jours est difficile à gérer.

Pour illustrer, une stratégie (en lien avec les mots de passe) pouvant améliorer la sécurité de l'individu tout en lui demandant peu d'effort serait d'employer un facteur d'authentification double (qui utilise un code d'identification valable une seule fois sur son téléphone en plus d'un mot de passe usuel). Cette procédure n'exige pas de changer ses habitudes ou encore d'avoir à définir et à mémoriser à répétition de nouveaux mots de passe. Cela pourrait rassurer les utilisateurs qui ne se sentent pas en mesure de bien se protéger en ligne ou, encore, ceux qui craignent d'oublier leurs mots de passe. De plus, ajouter un facteur d'authentification double n'est pas une mesure de sécurité qui nécessite des connaissances particulières de la part de l'individu. Une autre possibilité serait d'avoir ses mots de passe en ligne encryptés et mémorisés par l'intermédiaire de iCloud ou Google (par exemple). Cela permet aux utilisateurs d'avoir des

mots de passe compliqués et différents pour chaque site, tel que suggéré par les experts. Or, pour ce qui est des mots de passe, PIN, etc., qui ne sont pas sur Internet, l'utilisateur a quand même le problème d'avoir à les mémoriser. C'est pourquoi Stajano (2011) a suggéré l'utilisation d'un système de remplacement aux mots de passe intitulé Pico. Initialement basée sur un système avec un jeton physique, Pico est maintenant une application pour les téléphones intelligents. Les utilisateurs ont deux options pour l'utiliser : scanner un code QR ou utiliser Bluetooth. L'option Bluetooth pourrait être la plus intéressante pour les utilisateurs puisque la connexion peut se faire de manière automatique. Par exemple, lorsqu'un individu utilise son ordinateur, il suffirait que son téléphone intelligent soit dans le champ capté par le signal Bluetooth afin de se connecter (Krol et al., 2017). L'application Pico est présentement étudiée et en cours de révision par une équipe du Laboratoire d'informatique de l'Université de Cambridge en Angleterre. Bref, les concepteurs des campagnes de prévention doivent prendre en compte les efforts perçus associés à l'application des conseils proposés car cette variable est déterminante pour la mise en pratique de ceux-ci (Bada et al., 2015).

Huitièmement, il pourrait aussi s'avérer utile de mieux tirer profit des postulats du modèle HBM dans la conception des campagnes. Ce modèle suggère que les croyances des personnes (à propos de la menace perçue et de leur sentiment d'auto-efficacité) sont des facteurs importants dans l'adoption des comportements de prévention. Il serait sans doute bénéfique que les campagnes de prévention et de sensibilisation revoient leur stratégie et ne se limitent pas à offrir de l'information. Il semble en effet nécessaire d'utiliser des méthodes de persuasion misant sur la connaissance des facteurs psychologiques de motivation et sur les façons de modifier (ou d'influencer) les croyances et les comportements des personnes. S'appuyant sur leur recension des écrits, Bada et se collaborateurs (2015) sont d'accord avec cette nouvelle approche et pensent que celle-ci pourrait augmenter considérablement l'efficacité des mesures préventives en cybercriminalité. Selon ces auteurs, trois conditions sont requises pour que les mesures de sensibilisation à la protection des cybercrimes fonctionnent : 1) reconnaitre et accepter que les conseils fournis sont pertinents ; 2) comprendre les mesures qu'ils doivent appliquer pour se protéger ; et 3) avoir la volonté (ou une réelle motivation) à mettre en pratique les mesures.

Neuvièmement, une piste prometteuse serait de rendre plus explicites ou visibles les risques réels auxquels s'expose la population (en évitant de créer des peurs ou de l'anxiété) pour

susciter une réelle prise de conscience. Cela pourrait prendre la forme de présentation de témoignages, de cas vécus qui mettent bien en évidence les conséquences des cyberfraudes et en insistant sur les moyens disponibles qui auraient permis d'éviter la victimisation (cela semble préférable aux « discours d'experts »). Il serait aussi important de tenir compte des différences culturelles dans la préparation des stratégies de prévention (certaines communautés sont plus sensibles que d'autres à certains types de messages et il serait sans aucun doute important de considérer cette variable). Bref, un message clair, démontrant la pertinence et la simplicité du moyen de protection, qui met en valeur l'importance du sentiment de sécurité et d'auto-efficacité et qui est arrimé aux valeurs culturelles de la population ciblée aura plus de chance d'avoir l'effet voulu (sensibiliser et influencer l'adoption des comportements sécuritaires).

Enfin, dixièmement, il serait pertinent d'effectuer plus d'études utilisant un protocole expérimental. En effet, la recension des écrits semble indiquer qu'il y a relativement peu d'études expérimentales dans le domaine de la prévention des cybercrimes. Par conséquent, on connait peu les effets réels des campagnes ou programmes de prévention. Dans une autre étude, il serait intéressant d'utiliser un protocole expérimental (et réaliser un pré et un post-test chez différents groupes de participants distribués aléatoirement - groupe exposé à la campagne et groupe contrôle non exposé) afin de déterminer si la campagne produit les effets escomptés. Des expérimentations utilisant des mises en situations pourraient aussi renseigner les chercheurs sur l'efficacité de leurs mesures (par exemple, en envoyant un faux courriel d'hameçonnage aux clients qui avaient répondu au sondage afin de déterminer quel pourcentage de participants ont tout même accédé au lien après avoir été sensibilisé à ne pas le faire dans la campagne de prévention). Ce type d'approche s'est avéré efficace pour comprendre les effets des interventions préventives (Kumaraguru et al., 2007). Sinon, il pourrait être intéressant d'inciter les clients à répondre à nouveau à un sondage plus exhaustif après quelques semaines et leur demander si leurs habitudes en matière de sécurité informatique ont changées. Par exemple, quelles précautions ont-ils pris en recevant des courriels avec des liens URL ? L'ajout d'une question par rapport à leur perception d'auto-efficacité pourrait être une bonne idée puisque cela permettrait d'évaluer si celui-ci est en hausse après la campagne de prévention.

5.4. Points forts et limites de l'étude

La présente étude comporte plusieurs points forts. Premièrement, la consultation a été menée auprès d'un échantillon assez représentatif de la population générale. Le nombre de

participants est élevé (plus de 1400), ce qui ajoute à la fiabilité des résultats. Le sondage a été conçu par une équipe d'experts en marketing et a été réalisé par une firme ayant l'expertise et le savoir-faire en matière de consultation publique. Les clients ont été sondés peu de temps après la fin de la campagne. Les données ont été vérifiées et analysées avec rigueur.

Par contre, on retrouve aussi certaines limites. La première étant le petit nombre de questions rendu disponible pour réaliser ce mémoire. Le nombre de questions en lien avec le sentiment de sécurité était assez limité (les questions se rapportaient seulement sur le sentiment envers l'IF). Il aurait été intéressant d'avoir des questions sur le sentiment de sécurité personnelle, le sentiment d'auto-efficacité, les menaces perçues et sur l'évaluation plus précise de la pertinence des messages préventifs. La collecte de données était davantage arrimée aux besoins de l'institution financière que sur les facteurs jugés déterminants provenant du modèle théorique. Enfin, comme dans tout sondage, il y a un risque d'erreur provenant de différents biais possibles : désirabilité sociale, indifférence, réponses aléatoires, etc. Pour toutes ces raisons, il est important de considérer les résultats obtenus avec prudence.

Conclusion

La cybercriminalité est un phénomène en pleine croissance. Avec le développement rapide des nouvelles technologies informatiques et numériques, avec l'utilisation accrue de l'Internet dans toutes les sphères d'activités et avec l'expansion de tous les services en ligne, il y a de nouvelles opportunités pour les fraudeurs et les arnaqueurs de commettre des cybercrimes en s'en prenant à tous les types d'utilisateurs. Qu'il s'agisse d'individus, de groupes de travailleurs dans les différents milieux de travail ou d'institutions de toutes sortes (financières, scolaires, gouvernementales, etc.), personne n'est à l'abri d'être une victime des cybercriminels. Les conséquences et les coûts de la cybercriminalité (tant pour la population générale que pour l'économie, les organisations du monde du travail et de la finance et les gouvernements) sont considérables et justifient que tous les moyens soient mis en œuvre pour les prévenir. La recension des travaux effectuée dans la présente étude a démontré que la prévention de la cybercriminalité est un défi de taille, tant par sa complexité que par la difficulté à proposer des moyens efficaces, adaptés aux besoins de tous pouvant réduire l'incidence de ces crimes. Les campagnes de prévention (gouvernementales ou provenant d'organisations privées) sont des stratégies de plus en plus répandues mais dont l'efficacité demeure encore aujourd'hui

relativement limitée. Cette étude a d'ailleurs démontré que bien que la campagne de prévention a été perçue de façon positive par la majorité des répondants sondés, la portée de son impact n'a pas été aussi grande que l'on aurait pu espérer. En effet, moins d'un quart des répondants avaient vu l'affiche et/ou la campagne de prévention et de ce nombre très peu se rappelaient le message véhiculé. La campagne semble avoir porté fruit principalement auprès d'un seul groupe de clients : les personnes plus âgées et mieux nanties. Ainsi, il est encore nécessaire d'améliorer les campagnes de prévention afin de les rendre plus efficaces auprès de toute la population à laquelle elle s'adresse. Une des pistes prometteuses dans ce domaine consiste à ne pas viser uniquement sur l'éducation et la sensibilisation des personnes en matière de protection informatique mais plutôt d'adopter une conceptualisation de la prévention en utilisant une perspective multidisciplinaire qui intègre les connaissances issues de la criminologie, de l'informatique, de la psychologie et de la santé publique. Tel mentionné précédemment, les futures campagnes de prévention devraient avoir des messages moins généraux et viser davantage des problèmes spécifiques. En ayant pour cible un message général, il y a de fortes chances que l'impact de la mesure soit plus faible et qu'un plus petit nombre d'individus se sentent interpelés. En combinant les stratégies préventives issues de diverses disciplines, le résultat pourrait s'en trouver améliorer car cela permettrait de rejoindre et de mieux cibler les populations vulnérables que l'on cherche à sensibiliser. Il est à souhaiter qu'un plus grand nombre d'études scientifiques regroupant des équipes multidisciplinaires soient réalisées afin d'arriver à concevoir et évaluer les effets de nouvelles stratégies de prévention de la cybercriminalité.

Références

Accenture (2017). Canada Cybercrime Survey 2017. Retrieved from https://www.accenture.com/ca-en/company-news-release-canada-cybercrime-survey-2017

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40‑46.

Agence du revenu du Canada. (2019). À bas l'arnaque – Protégez-vous contre la fraude. Retrieved from https://www.canada.ca/fr/agence-revenu/organisation/securite/protegez-vous-contre-fraude.html

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*, 47-87.

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.

Al-Ali, A. A., Nimrat, A., & Benzaid, C. (2018). Combating cyber victimisation: Cybercrime prevention. In H. Jahankhani (Ed.), *Cybercriminology* (pp. 324-340). Switzerland: Springer Nature Switzerland AG.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*, 276-289.

Andrews, D., Nonnecke, B., & Preece, J. (2003). Electronic survey methodology: A case study in reaching hard-to-involve Internet users. *International Journal of Human-Computer Interaction, 16*(2), 185-210.

AOL & NCSA (2005). AOL/NCSA Online Safety Study. Retrieved from https://docplayer.net/957058-Aol-ncsa-online-safety-study-conducted-by-america-online-and-the-national-cyber-security-alliance-december-2005.html

Armitage, R. (2013). *Crime prevention through housing design: Policy and practice*. London, UK: Palgrave MacMillan Ltd.

Bachmann, M. (2007). Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA. *International Journal of Cyber Criminology, 2*, 213-227.

Bada, M., Sasse, A., & Nurse, J. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118-131.

Baer, V. E. H. (1988). Computers as composition tools: A case study of student attitudes. *Journal of Computer-Based Instructions, 15*, 144-148.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal of a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 244-254.

Bauman, A. E., Bellew, B., Owen, N., & Vita, P. (2001). Impact of an Australian mass media campaign targeting physical activity in 1998. *American Journal of Preventive Medicine, 21*(1), 41-47.

Belanger, F., Negangard, E., Enget, K., & Collignon, S. (2011). When users resist: How to change management and user resistance to password security. *Pamplin College of Business Magazine.*

Benenson, Z. (2016). Exploiting Curiosity and Context: How to Make People Click on a Dangerous Link Despite Their Security Awareness, presented at Black Hat Conference, Las Vegas, 2016. New York: Black Hat Publishing.

Bertrand, J. T. (2005). Systematic review of the effectiveness of mass communication programs to change HIV/AIDS-related behaviors in developing countries. *Health Education Research*, *21*(4), 567–597.

Bertrand, J. T., O'Reilly, K., Denison, J., Anhang, R., & Sweat, M. (2006). Systematic review of the effectiveness of mass communication programs to change HIV/AIDS-related behaviors in developing countries. *Health Education Research, 21*(4), 567-597.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*, 253-264.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*, 400-420.

Bowers, K., & Johnson, S. (2003). *Reducing burglary initiative: The role of publicity in crime prevention* (Home Office Research Study 272). London, UK: Home Office.

Bowers, K., & Johnson, S. (2005). Using publicity for preventive purposes. In N. Tilley (Ed.), *Handbook of crime prevention and community safety* (pp. 329-354). Devon, UK: Willan Publishing.

Brantingham, P. J., & Faust, F. (1976). A conceptual model of crime prevention. *Crime & Delinquency, 22*, 284-296.

Brantingham, P. L., & Brantingham, P. J. (1993). Environment, routine, and situation: Toward a pattern theory of crime. In R. V. Clarke & M. Felson (Eds.), *Routine activities and rational choice*. New Brunswick, NJ: Transaction Pub.

Brennan, S. (2011). Les perceptions des Canadiens à l'égard de la sécurité personnelle et de la criminalité, 2009. Retrieved from https://www150.statcan.gc.ca/n1/pub/85-002-x/2011001/article/11577-fra.htm

Brennan, S., & Dauvergne, M. (2010). *Statistiques sur les crimes déclarés au Canada*. Ottawa, Statistique Canada.

Bright, J. (1992). *Crime prevention in America: A British perspective*. Chicago, IL: Office of International Crime Justice, The University of Illinois at Chicago

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology, 10*(2), 223-244.

Brunton-Smith, I. (2017). Fear 2.0 Worry about cybercrime in England and Wales. In Lee, M., & Mythen, G. (Eds.), *The Routledge International Handbook on Fear of Crime* (pp. 93-105). London, UK: Routledge.

Bureau de la concurrence Canada (2018). Mois de la prévention de la fraude. Retrieved from https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03662.html

Button, M., Lewis, C., & Tapley, J. (2009). A better deal for fraud victims: Research into victims' needs and experiences. *National Fraud Authority*. Retrieved from https://researchportal.port.ac.uk/portal/files/1924328/NFA_Report_1_15.12.09.pdf

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

Button, M., Tapley, J., & Lewis, C. (2013). The "fraud justice network" and the infra-structure of support for individual fraud victims in England and Wales. *Criminology and Criminal Justice, 13*(1), 37-61.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior, 23*(3), 1273-1284.

Casswell, S., & Duignan, P. (1989). Evaluating Health Promotion: A Guide for Health Promoters and Health Managers. 28pp, November. Auckland: Department of Community Health.

Cellar, D. F., Nelson, Z. C., Yorke, C. M., & Bauer, C. (2009). The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement. *Journal of Prevention & Intervention in the Community, 22*(1), 43-52.

Centre for Internet Security (CIS). (2019). October: National Cybersecurity Awareness Month. Retrieved from https://www.cisecurity.org/blog/october-national-cybersecurity-awareness-month/

Challinger, D. (2003). *Crime Stoppers: Evaluating Victoria's program.* Canberra, AUS: Australian Institute of Criminology.

Chavez, N. M. (2018). *Can we learn from hackers to protect victims?* Retrieved from Electronic Theses, Projects, and Dissertations. (690)

Cheung, C., & Lee, M. K. O. (2000). Trust in Internet Shopping: A Proposed Model and Measurement Instrument, *AMCIS 2000 Proceedings,* 681-689.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Chung, H., & Zhao, X. (2004). Effects of perceived interactivity on web site preference and memory: Role of personal motivation. *Journal of Computer-Mediated Communication, 10*(1).

Claar, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model* (Doctoral dissertation) Retrieved from Utah State University.

Claar, C. L., & Johnson, J. (2010). Analyzing the adoption of computer security utilizing the health belief model. *Issues in Information Systems, 11*(1), 286-291.

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Albany, NY: Harrow and Heston.

Clarke, R. V. (2005). Seven misconceptions of situational crime prevention. In N. Tilley (Ed.), *Handbook of crime prevention and community safety*. Portland, OR: Willan Publishing.

Clarke, R. V. (2010). *Situational crime prevention: Successful case studies* (2nd ed.). Boulder: Lynne Rienner.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry & N. Morris (Eds.), *Crime and justice* (Vol. 6, pp. 147-185). Chicago: University of Chicago Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 44, 588-605.

Conklin, W. A. (2006). *Computer security behaviors of home PC users: A diffusion of innovation approach* (doctoral thesis). Retrieved from Dissertations & Thesis: Full Text (Publication No. AAT 3227760)

Crime Survey of England and Wales (CSEW). (2019). Crime in England and Wales: year ending March 2019. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019

Crime Stoppers International (2018). About Crime Stoppers International. Retrieved from https://csiworld.org/about-us

Cross, C. (2013). "Nobody's holding a gun to your head. . . " examining current discourses surrounding victims of online fraud. In K. Richards, & J. Tauri (Eds.), *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference* (pp. 25-32). Brisbane: Queensland University of Technology.

Cross, C., Richards, K., & Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support. *Final Report, Criminology Research Council, Australian Institute of Criminology*. Retrieved from http://www.crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends & Issues in Crime and Criminal Justice*, 474, 1-6.

Curtin, R., Presser, S., & Singer, E. (2000). The effects of response rate changes on the index of consumer sentiment. *Public Opinion Quarterly, 64*, 413-428.

Davidson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), 154–168.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Day, D.M., & Wanklyn, S.G. (2012). *Identification and Operationalization of the Major Risk Factors for Antisocial and Delinquent Behaviour among Children and Youth.* NCPC Research Report. Ottawa, ON: Public Safety Canada.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7.

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, schemes and swindles: A review of consumer financial fraud research. *Financial Fraud Research Centre.* Retrieved from: http://longevity.stanford.edu/wp-content/uploads/2017/01/Scams-Schemes-Swindles-FINAL-On-Website.pdf

Delbosc, A., & Currie, G. (2012). Modelling the causes and impacts of personal safety perceptions on public transport ridership. *Transport Policy*, *24*, 302–309.

Dhiri, S., Goldblatt, P., Brand, S., & Price, R. (2001). Evaluation of the United Kingdom's "Crime reduction programme". In B. C. Welsh, D. P. Farrington & L. W. Sherman (Eds.), *Costs and benefits of preventing crime* (pp. 179-201). Bouler, CO: Westview Press.

Dictionnaire Larousse (2019). Prévention. Retrieved from https://www.larousse.fr/dictionnaires/francais/pr%c3%a9vention/63869?q=pr%c3%a9vention#63152

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior, 60*, 508-513.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367.

Downing, S. (2013). Technology and crime prevention. In D. A. Mackey, & K. Levan (Eds.), *Crime prevention* (pp. 163-192). Burlington, MA: Jones & Bartlett Learning.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Symposium On Usable Privacy and Security (SOUPS)*

Fafinski, S. and Minassian, N. (2009) *UK Cybercrime Report.* Retrieved from http://www.garlik.com/file/cybercrime_report_attachement

Farrell, G., & Pease, K. (2006). Preventing repeat residential burglary victimization. In B. C. Welsh, & D. P. Farrington (Eds.), *Preventing crime: What works for children, offenders, victims and places* (pp. 161-176). New York, NY: Springer.

Farrell, G., Phillips, C., & Pease, K. (1995). Like taking candy: Why does repeat victimization occur? *British Journal of Criminology, 35*(3), 384-399.

Felson, M. (2002). *Crime and everyday life* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Ferreira, A., & Lenzini, G. (2015). An analysis of social engineering principles in effective phishing (pp. 9–16). IEEE.

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web - WWW '07*, 657.

Financial Fraud Action UK. (2019). Publications. Retrieved from https://www.financialfraudaction.org.uk/publications/

Finckenauer, J. O., Gavin, P. W., Hovland, A., & Storvoll, E. (1999). *Scared Straight: The panacea phenomenon revisited*. Prospect Heights, IL: Waveland Press.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417.

Ganzini, L., McFarland, B., & Bloom, J. (1990). Victims of fraud: Comparing victims of white collar and violent crime. *Bull Am Acad Psychiatry Law, 18*(1), 55-63.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, *57*(7), 768–775.

Garland, D. (1996). The limits of the sovereign state: Strategies of crime control in contemporary society. *British Journal of Criminology, 36*, 445-471.

Get Cyber Safe. (2017). Campaigns. Retrieved from https://www.getcybersafe.gc.ca/cnt/rsrcs/cmpgns/index-en.aspx

Gill, M., & Pease, K. (1998). Repeat robbers: Are they different? In M. Gill (ed.), *Crime at work: Increasing the risk for offenders* (pp. 143-153). London, UK: Palgrave Macmillan.

Gilling, D. (1997). *Crime prevention: Theory, policy, and politics*. London, UK: Routledge.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *J Comput Virol, 2*(1), 13-20.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Gourbesville, O. (2007). Faut-il avoir peur d'Internet ? *Pour, 3*(195), 21-26.

Goyder, J., Warriner, K., & Miller, S. (2002). Evaluating socio-economic status (SES) bias in survey nonresponse. *Journal of Official Statistics, 18*(1), 1-11.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358.

Grigg, D. W. (2010). Cyber-agression: Definition and concept of cyberbullying. *Australian Journal of Guidance and Counselling, 20*(2), 143-156.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology, 36*(3), 173-192.

Grohe, B. (2011). Measuring residents' perceptions of defensible space compared to incidence of crime. *Risk Management, 13*(1/2), 43-61.

Heath, L., & Gilbert, K. (1996). Mass media and fear of crime. *Amer. Behav. Sci., 39*(4), 379–386.

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime victimization. In C. A. Cuevas & C. M. Rennison (Eds.), *The Wiley handbook on the psychology of violence* (pp. 555-570). Chichester, UK: Wiley Blackwell.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *NSPW '09 Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, 133-144.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Hipp, J. R. (2010). Resident perceptions of crime: How much is "bias" and how much is micro-neighborhood effect? *Criminology, 48*(2), 475-508.

Hirschi, T. (1986). On the compatibility of rational choice and social control theories of crime. In D. B. Cornish & R. V. Clarke (Eds.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 105-118). New York, NY: Springer-Verlag.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. New York, NY: Routledge.

Holt, T. J., & Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics*. New York, NY: Routledge.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45.

Ifinedo, P. (2012). Understand information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Jackson, J. (2011). Revisiting risk sensitivity in the fear of crime. *J. Res. Crime Delinquency, 48*(4), 513-537.

Jacobs, J. (1961). *The death and life of great American cities*. New York, NY: Random House.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2005). Social phishing. *Communications of the ACM*, 94-100.

Jahankhani, H. (2013). Developing a model to reduce and/or prevent cybercrime victimization among the user individuals. In B. Akhgar & S. Yates (Eds.), *Strategic intelligence management: National security imperatives and information and communications technologies* (pp. 258-268). Oxford, UK: Butterworth-Heinemann.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jeffery, C. R. (1971). *Crime prevention through environmental design*. Beverly Hills, CA: Sage Publications.

Kennedy, D. M., Braga, A., & Piehl, A. M. (2001). *Reducing gun violence: The Boston gun project's operation Ceasefire* (National Institute of Justice Research Report). Washington, DC: US Department of Justice.

Keown, L-A. (2010). Les precautions prises pour éviter la victimisation : Une perspective selon le sexe. *Tendances Sociales Canadiennes*, *89*.

Kiesler, S., & Sproull, L. S. (1986). Response effects in the electronic survey. *Public Opinion Quarterly, 50*, 402-413.

Kim, M.-J., Chung, N., & Lee, C.-K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism Management*, *32*(2), 256–265.

Kirwan, G. (2011). Presence and the Victims of Crime in Online Virtual Worlds, 8.

Kitchen, T., & Schneider, R. H. (2002). *Planning for crime prevention: A transatlantic perspective*. London, UK: Routledge.

Klenowski, P. M., Bell, K. J., & Dodson, K. D. (2010). An empirical examination of juvenile awareness programs in the United States: Can juveniles be "Scared Straight"? *Journal of Offender Rehabilitation, 49*, 254-272.

Kowalski, R. M., & Giumetti, G. W. (2017). Bullying in the digital age. In E. Martellozzo & E. A. Jane (Eds.), *Cybercrime and its victims* (pp. 167-186). London, UK: Routledge.

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems, 2019*, 1-11.

Krol, K., Aebischer, S., Llewellyn-Jones, D., Dettoni, C., & Stajano, F. (2017). Seamless authentication with Pico. *2nd IEEE European Symposium on Security and Privacy.*

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong., J., & Nunge E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *CHI 2007: reach beyond: conference proceedings: Conference on Human Factors in Computing Systems, San Jose, California, USA, April 28-May 3, 2007*. New York, N.Y: Association for Computing Machinery.

Lab, S. P. (2010). *Crime prevention: Approaches, practices, and evaluations* (7th ed). New Providence, NJ: LexisNexis.

LaRose, R. (2010). The problem of media habits. *Communication Theory, 20*, 194-222.

Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of personality and persuasion tactics in email phishing attacks. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting*. 1331-1333.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445-454.

Li, Q. (2007). New bottle but old wine: A research of cyberbulling in schools. *Computers in Human Behavior, 23*(4), 1777-1791.

Mackey, D. A. (2013). Introduction to crime prevention. In D. A. Mackey, & K. Levan (Eds.), *Crime prevention* (pp. 1-29). Burlington, MA: Jones & Bartlett Learning.

Maras, M.-H. (2017). *Cybercriminology*. New York, NY: Oxford University Press.

Mayhew, P. (1979). Defensible space: The current status of a crime prevention theory. *The Howard Journal of Penology and Crime Prevention, 18*, 150-159.

Mayhew, P., Clarke, R. V. G., Sturman, A., & Hough, J. M. (1976). *Crime as opportunity* (Home Office Research Study, 34). London, UK: H.M.S.O.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *Institute for Homeland Security Solutions*

McCreith, S., & Parkinson, S. (2004). *Crimes against students: Emerging lessons for reducing student victimisation* (Home Office Development and Practice Report, 21). London, UK: Home Office.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. Retrieved from https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn36762-eng.pdf

McPeake, J., Bateson, M., & O'Neill, A. (2014). Eletronic surveys: How to maximise success. *Nurse Researcher, 21*(3), 24-26.

Mendelsohn, H. (1973). Some reasons why information campaigns can succeed. *Public Opinion Quarterly, 37*(1), 50-61.

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, *54*(1), 198–205.

Mitchell, E. A., Aley, P., & Eastwood. J. (1992). The national cot death prevention program in New Zealand. *Australian Journal of Public Health, 16*(2), 158-161.

Moore, D. L., & Tarnai, J. (2002). Evaluating nonresponse in mail surveys. In R. M., Groves, D. A., Dillman, J. L., Eltinge, & R. J. A., Little (Eds.), *Survey nonresponse* (pp. 197-211). New York, NY: John Wiley & Sons.

Morgan, M. G., Fischhoff, B., Bostrom, A., & Atman, C. J. (2002). *Risk communication: A mental models approach*. Cambridge: Cambridge University Press.

Morse, J. M., & Richards, L. (2013). *Read me first for a user's guide to qualitative methods*. Thousand Oak, CA: Sage.

Newman, O. (1972). *Defensible space*. New York, NY: Macmillan.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Ngo, T. F., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational-level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Norton (2019). Good cyber hygiene habits to stay safe online. Retrieved from https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

O'Donnell, A. (2019). Create an effective security awareness training program. Retrieved from https://www.lifewire.com/create-an-effective-security-awareness-training-program-2487717

Öğütçü, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.

O'Keefe, G. D., & Mendelsohn, H. (1984). *Taking A Bite Out of Crime: The impact of a mass media crime prevention campaign*. Washington, DC: National Institute of Justice.

O'Keefe, G. D., Rosenbaum, D. P., Lavrakas, P. J., Reid, K., & Botta, R. A. (1996). *Taking A Bite Out of Crime: The impact of the National Citizens' Crime Prevention media campaign*. Thousand Oaks, CA: Sage.

Olds, D. L., Eckenrode, J., Henderson, C. R., Kitzman, H., Powers, J., Cole, R., Sidora, K., Morris, P., Pettitt, L. M., & Luckey, D. (1997). Long-term effects of home visitation on maternal life course and child abuse and neglect: Fifteen-year follow-up of a randomized trial. *Journal of the American Medical Association, 278*, 637-643.

Organ, D. W., & Paine, J. B. (1999). A new kind of performance for industrial and organizational psychology: Recent contributions to the study of organizational citizenship behavior. In C. L. Cooper & I. T. Robertson (Eds.), *International review of industrial and organizational psychology 1999*, Vol. 14, pp. 337-368). New York, NY: John Wiley & Sons Ltd.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 148-169.

Pease, K., Ignatans, D., & Batty, L. (2018). Whatever happened to repeat victimisation? *Crime Prev Community Saf, 20*, 256-267.

Petrosino, A., Turpin-Petrosino, C., & Buehler, J. (2003). Scared Straight and other juvenile awareness programs for preventing juvenile delinquency: A systematic review of the randomized experimental evidence. *The Annals of the American Academy of Political and Social Science, 589*, 41-62.

Petty, R. and Cacioppo, J. (1986). *Communication & Persuasion: Central & Peripheral Routes to Attitude Change*. New York, NY: Springer-Verlag.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Homeland Security & Emergency Management, 11*(4), 489-510.

Ponemon. (2017). Cost of Data Breach Study. Retrieved from https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 367-395). New Brunswick, NJ: Transaction Publishers.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Public Safety Canada. (2015). Canada's Cyber Security Awareness Initiative, "Get Cyber Safe". Retrieved from https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2011/20111003-1-en.aspx

Quine, S., & Morrell, S. (2008). Research: Perceptions of personal safety among older Australians: Perceptions of personal safety. *Australasian Journal on Ageing*, *27*(2), 72–77.

Redmiles, E. M., Acar, Y., Fahl, S., & Mazurek, M. L. (2017). *A summary of survey methodology best practices for security and privacy researchers*. Technical report.

Redmill, F. (2002). Some dimensions of risk not often considered by engineers. *Computing and Control Engineering Journal, 13*(6), 268-272.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(5), 1-15.

Regoli, R. M., Hewitt, J. D., & DeLisi, M. (2010). *Delinquency in society* (8th ed). Sudbury, MA: Jones and Bartlett Publishing.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139.

Reyns, B. W., Henson, B., & Fisher, B. S. (2014). Cybercrime. In J. M. Miller (Ed.), *The encyclopedia of theoretical criminology* (pp. 215-222). New York: Wiley-Blackwell

Rhee, H-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Rhee, H-S., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*(2), 221-232.

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273.

Riley, D., & Mayhew, P. (1980). *Crime prevention publicity: An assessment* (Home Office Research Study, 63). London, UK: Home Office.

Robinson, M. B. (1996). The theoretical development of "CPTED": 25 years of responses to C. Ray Jeffery. In W. Laufer, & F. Adler (Eds.), *The Criminology of Criminal Law: Advances in Criminological Theory Volume 8* (pp. 427-462). New Brunswick, NJ: Transaction Publishers.

Rosenbaum, D. P., Lurigio, A. J., & Lavrakas, P. J. (1989). Enhancing citizen participation and solving serious crime: A national evaluation of Crime Stoppers program. *Crime and Delinquency, 35*, 401-420.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*(4), 328-335.

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1994). *The health belief model and HIV risk behavior change.* Preventing AIDS. Springer.

Sacco, V. F., & Trotman, M. (1990). Public Information Programming and Family Violence: Lessons from the Mass Media Crime Prevention Experience. *Canadian J. Criminology, 32*(1), 91-105.

Sacco, V. F., & Silverman, R. A. (1981). Selling crime prevention: The evaluation of a media campaign. *Canadian Journal of Criminology, 23*, 191-202.

Sansfaçon, D., & Waller, I. (2001). Recent evolution of governmental crime prevention strategies and implications for evaluation and economic analysis. In B. C. Welsh, D. P. Farrington, & L. W. Sherman (Eds.), *Costs and benefits of preventing crime* (pp. 225-247). Bouler, CO: Westview Press.

Scam Alert Singapore (2018). Resources. Retrieved from https://www.scamalert.sg/resources/posters

Scamwatch. (2019). Scam statistics. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics

Schaefer, D. R., & Dillman, D. A. (1998). Development of a standard e-mail methodology: Results from an experiment. *Public Opinion Quarterly, 62*, 378-397.

Schmid, K. L., Rivers, S. E., Latimer, A. E., & Salovey, P. (2008). Targeting or tailoring? Maximizing resources to create effective health communications. *Mark Health Serv, 28*(1), 32-37.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* New York: John Wiley.

Self-Brown, S., Rheingold, A. A., Campbell, C., & de Arellano, M. A. (2008). A Media Campaign Prevention Program for Child Sexual Abuse: Community Members' Perspectives. *Journal of Interpersonal Violence*, *23*(6), 728–743.

Shader, M. (2003). Risk factors for delinquency: An overview (NCJ 207540). Washington, DC: Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Retrieved from http://ncjrs.gov/pdffiles1/ojjdp/frd030127.pdf

Sheeran, P., & Orbell, S. (2000). Self-schemas and the theory of planned behaviour. *European Journal of Social Psychology, 30*(4), 533–550.

Sheeran, P., & Webb, T. L. (2016). The intention-behavior gap. *Social and Personality Psychology Compass, 10*(9), 503-518.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191.

Simon, H. (1957). *Models of man, social and rational: Mathematical essays on rational human behavior in a social setting*. New York, NY: Wiley.

Skogan, W. G. (1990). *Disorder and decline: Crime and the spiral of decay in American neighborhoods*. Berkeley, CA: University of California Press.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385.

Song, J. H., & Zinkhan, G. M. (2008). Determinants of perceived web site interactivity. *Journal of Marketing, 72*, 99-113.

Stajano, F. (2011). Pico: No more passwords! In B. Christianson, B. Crispo, J. Malcolm, & F. Stajano (Eds.), *Security protocols XIX* (LNCS 7114, pp. 49-81). Berlin, Germany: Springer-Verlag Berlin Heidelberg.

Star, S. A., & Hughes, H. M. (1950). Report on an educational campaign: The Cincinnati plan for the United Nations. *American Journal of Sociology, 55*(4), 389-400.

Statistics Canada. (2011). Self-reported Internet victimization in Canada, 2009. Retrieved from http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-eng.htm

Statistics Canada. (2014). Police-reported cybercrime in Canada, 2012. Retrieved from https://www150.statcan.gc.ca/n1/pub/85-002-x/2014001/article/14093-eng.htm

Statistique Canada. (2018a). L'incidence du cybercrime sur les entreprises canadiennes, 2017. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm

Statistique Canada. (2018b). Statistiques sur les crimes déclarés par la police au Canada, 2017. Retrieved from https://www150.statcan.gc.ca/n1/fr/pub/85-002-x/2018001/article/54974-fra.pdf?st=o7SoMie8

Steenkamp, J.-B. E. M., De Jong, M. G., & Baumgartner, H. (2010). Socially desirable response tendencies in survey research. *Journal of Marketing Research, 47*(2), 199-214.

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security, 20*(1), 29-38.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Symantec. (2017). Internet Security Threat Report, 2017. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Tavakoli, M., & Yaacob, S. (2018). URL cues on phishing detection. *Open International Journal of Informatics, 6*(4), 80-91.

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation, 27*(2), 237-246.

Thrasher, F. M. (1936). The Boys' Club and juvenile delinquency. *American Journal of Sociology, 41*, 66-80.

Tremblay, R. E., Vitaro, F., Bertrand, L., Leblanc, M., Beauchesne, H., Boileau, H., & David, L. (1992). Parent and child training to prevent early onset of delinquency: The Montreal Longitudinal-Experiment Study. In J. McCord & R. E. Tremblay (Eds.), *Preventing antisocial behavior: Interventions from birth through adolescence* (pp. 117-138). New York, NY: Guilford Press.

Tversky, A., & Kahneman, D. (1989). Rational choice and the framing of decisions. In B. Karpak & S. Zionts (Eds.), *Multiple criteria decision making and risk analysis using microcomputers* (pp. 81-126). Berlin, Germany: Springer-Verlag Berlin Heidelberg.

U.S. Bank. (2019). Fraud prevention: Helping you to stay safe. Retrieved from https://www.usbank.com/about-us-bank/online-security/fraud-prevention.html

United States Department of Homeland Security. (2017). About Stop. Think. Connect. Retrieved from https://www.dhs.gov/about-stopthinkconnect

van Dijk, J. J. M., Mayhew, P., & Killias, M. (1990). *Experiences of crime across the world: Key findings of the 1989 from the International Crime Survey*. Deventer, The Netherlands: Kluwer Law and Taxation Publishers.

van Dijk, J. J. M., & Steinmetz, C. H. D. (1981). *Crime prevention: An evaluation of the national publicity campaign*. The Hague, The Netherlands: Ministry of Justice, Research and Documentation Centre.

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *Cyber Psychology & Behaviour, 11*, 499–503.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146-1166.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.

Wahlberg, A. A. F., & Sjoberg, L. (2000). Risk perception and the media, *J. Risk Res., 3*(1), 31–50.

Walklate, S. (2007). *Imagining the victim of crime.* Berkshire, UK: Open University Press.

Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research*, *8*(2), 183–205.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63.

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10), USA, 11*, 1-16.

Wash, R., & Rader, E. (2015). Too much knowledge? Security beliefs and protective behaviors among US internet users. *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15), Canada, 309-325.*

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7.

Williams, F. P., McShane, M. D., & Akers, R. L. (2000). Worry About Victimization: An Alternative and Reliable Measure for Fear of Crime. *Western Criminology Review 2*(2). Retrieved from http://www.westerncriminology.org/documents/WCR/v02n2/williams/williams.html

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows: The police and neighborhood safety. Retrieved from http://www.lakeclaire.org/docs/BrokenWindows-AtlantaicMonthly-March82.pdf

Wood, E. (1961). *Housing Design: A Social Theory.* New York: Citizens' Housing and Planning Counsel of New York.

Wright, J. P. (2009). Rational choice theories. Retrieved from https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0007.xml#obo-9780195396607-0007-div1-0008

Wu, M. (2006). *Fighting phishing at the user interface* (Doctoral thesis). Retrieved from Massachusetts Institute of Technology

Annexe - Questionnaire

Q_1 Vous souvenez-vous d'avoir vu un affichage (soit physique ou en ligne) de l'IF sur le thème de la sécurité informatique dans le dernier mois ?

1=Oui
2=Non

Q_2a Où avez-vous vu un affichage de l'IF sur le thème de la sécurité informatique ? *Cochez tous les réponses qui s'appliquent à votre situation.*

1=Dans une caisse
2=Sur un panneau d'affichage
3=Dans le transport en commun (autobus, métro)
4=Sur un site web
5=Sur les réseaux sociaux
90=À un autre endroit <précisez> (précisez)
99=*Je préfère ne pas répondre

Q_TXT1 Voici une affiche que vous avez pu voir au cours du dernier mois. Prenez le temps de l'observer et de lire le message.

(affiche cyberhygiene)

Q_3 Aviez-vous vu cette affiche auparavant ?
1=Oui
2=Non

Q_4 Globalement, que retenez-vous du message que veut transmettre l'IF ?

<<_____>>

Q_5a Après avoir regardé cet affichage de l'IF qui vise à promouvoir des comportements sécuritaires à adopter au quotidien, quel est votre niveau d'accord avec ces énoncés suivants ?

Cet affichage améliore l'opinion que j'ai de l'IF
1=Totalement en désaccord
2=Plutôt en désaccord
3=Plutôt en accord
4=Totalement en accord
9=*Je ne sais pas/je préfère ne pas répondre

Q_5b Cet affichage a un impact sur votre sentiment de sécurité envers l'IF

Q_5c Il est crédible que l'IF fasse ce genre d'affichage
Q_5d J'apprécie que l'IF informe ses clients sur ce sujet

Q_TXT2 Voici la section du site de l'IF qui propose des articles sur la cyberhygiène.

(capture d'écran du site)

Prenez quelques minutes pour regarder le contenu et lire les titres des articles.

Q_6 Aviez-vous déjà accédé à cette section du site soit en cliquant sur la publicité ou encore en naviguant sur internet ?

1=Oui
2=Non

Q_7 Quels sont les éléments qui vous plaisent de la campagne de sensibilisation (affichage et site web) ?

<<_____>>

Q_8 Quels sont les éléments que vous n'appréciez pas ?
<<_____>>

Q_9 Dans cette section du site de l'IF sont regroupés des conseils pour protéger vos appareils, vos comptes et votre identité.

Pour vous, ces conseils sont-ils…?

4=Très utiles
3=Assez utiles
2=Peu utiles
1=Pas du tout utiles
9=*Je ne sais pas/je préfère ne pas répondre

Q_10a Quel est votre niveau d'intérêt à recevoir des conseils sur les sujets suivants ?

La protection de vos appareils (ordinateurs, téléphones mobiles et tablettes)

1=Pas d'intérêt
2=Un peu d'intérêt
3=Beaucoup d'intérêt
9=*Je ne sais pas/je préfère ne pas répondre

Q_10b La protection de vos comptes bancaires

Q_10c La protection de votre identité

Q_11 Y a-t-il des sujets en lien avec les comportements sécuritaires à adopter pour lesquels vous apprécieriez recevoir de l'information ?

<<_____>>

Q_12 Après avoir vu cette campagne, votre sentiment de sécurité envers l'IF a-t-il…?

5=Augmenté beaucoup
4=Augmenté un peu
3=Ni augmenté ni diminué
2=Diminué un peu
1=Diminué beaucoup
9=*Je ne sais pas/je préfère ne pas répondre