Le scambaiting sur Youtube

Analyse des buts et procédés décelés dans les vidéos de *scambaiting* et impact de ce type de contenu sur les internautes

CRPC | Chaire de recherche en prévention de la cybercriminalité

Auteure

Jade Philibert, finissante au baccalauréat en criminologie

Pour citer: Philibert, J.(2023). *Le scambaiting sur Youtube. Analyse des buts et des procédés décelés dans les vidéos de scambaiting et impacts de ce type de contenu sur les internautes*. Rapport de stage. Chaire de recherche en prévention de la cybercriminalité.

Ce document est disponible intégralement en format électronique (PDF) sur le site Web de la Chaire de recherche en prévention de la cybercriminalité à : https://www.prevention-cybercrime.ca.

Cette étude a fait l'objet d'une exemption de certificat éthique par le Comité d'éthique de la recherche - Société et culture (CERSC) de l'Université de Montréal.

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Sommaire exécutif

Le Centre antifraude du Canada rapporte qu'il y a eu 91 190 cas de fraudes qui ont été signalés en 2022, ce qui représente une statistique non négligeable. La fraude est définie par le Gouvernement du Canada comme une « tromperie intentionnelle utilisée pour nuire à une autre personne ou pour s'emparer de son argent ou de ses biens de manière illégale ». Avec l'arrivée d'Internet, les différentes méthodes pour commettre des fraudes ont évolué. Étant donné que les individus passent de plus en plus de temps sur Internet, les risques d'en être victime augmentent et s'intensifient.

Le *scambaiting* est un moyen de perturbation de la fraude en ligne qui est une activité relativement récente, il est ainsi important d'en comprendre l'impact. La publication de vidéos de *scambaiting* sur Internet débute au début des années 2000 avec la création de plusieurs plateformes en ligne dont le but est de favoriser le partage de contenu numérique. De plus en plus d'individus pratiquent ce type d'activités contre des fraudeurs étant donné la possibilité de publier rapidement et gratuitement des vidéos.

La présente recherche vise donc, en premier lieu, à mettre de l'avant les buts recherchés des *scambaiters* dans la création de vidéos portant sur le *scambaiting*. En deuxième lieu, l'étude vise à comprendre l'impact de la diffusion des vidéos sur les internautes. Ainsi, l'activité du *scambaiting* est analysée pour en apprendre davantage sur son fonctionnement et ses finalités.

Les résultats démontrent que les buts recherchés par les *scambaiters* le sont à divers degrés, selon les techniques employées par ces derniers. Le divertissement est présent dans l'ensemble des vidéos et plusieurs procédés sont appliqués par les *scambaiters*. Les internautes retiennent davantage les techniques utilisées et les paroles et gestes posés des *scambaiters* qui leur ont procuré du divertissement. De plus, le fait de vouloir ridiculiser par l'emploi d'insultes se voit dans la pratique du *scambaiting* et aussi dans les commentaires publiés par les spectateurs. Certains internautes abordent la prévention et la sensibilisation possible par cette pratique à travers l'explication du modus operandi appliqué par les fraudeurs permet la sensibilisation à la fraude au soutien technique. Il y aurait ainsi un potentiel de sensibilisation à la fraude au soutien technique par la diffusion de vidéos de *scambaiting* sur YouTube.

Table des matières

Introduction

Description du milieu de stage et mandat

La Chaire de recherche en prévention de la cybercriminalité (nommée ci-après « CRPC »), située à l'Université de Montréal, a été créée en septembre 2018 (Chaire de recherche en prévention de la cybercriminalité, 2022a). L'Université de Montréal, Desjardins et la Banque Nationale du Canada sont les partenaires affiliés de la CRPC. Elle est dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée et professeur à l'Université de Montréal. Fyscillia Ream est la coordonnatrice scientifique de la CRPC (Chaire de recherche en prévention de la cybercriminalité, 2022a).

La CRPC a pour mission de « contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention » (Chaire de recherche en prévention de la cybercriminalité, 2022a). La CRPC contribue à cet avancement à l'aide de différents projets de recherche répondant aux divers besoins de leurs partenaires (Chaire de recherche en prévention de la cybercriminalité, 2022a). Plusieurs étudiants de la maîtrise et du doctorat en criminologie sont supervisés par la CRPC pour leur projet de recherche. En plus de la recherche académique, la CRPC vise à constituer et à maintenir un réseau d'individus qui échangent sur la prévention de la cybercriminalité, que ce soit sur le plan local, national et même international. Un autre objectif de ce milieu est de créer et de fournir à ses partenaires et à d'autres organisations des outils pouvant les aider dans leur processus de formation. Étant donné que la prévention et la sensibilisation de la cybercriminalité sont des éléments essentiels à sa mission, une importance est accordée à la vulgarisation des résultats scientifiques trouvés dans les projets de recherche menés par les étudiants et la Chaire. Ces résultats sont diffusés de diverses manières, et ce, pour être accessibles à tous.

Étant donné la mission et les objectifs de la CRPC, la cybercriminalité est le sujet principal du stage. Le mandat de recherche sur le scambaiting, ainsi que la méthode de collecte de donnée à utiliser, a alors été choisi par la CRPC et répond ainsi à un de ses besoins de recherche.

Présentation de la recherche

Le Centre antifraude du Canada (2022) rapporte qu'il y a eu 91 190 cas de fraudes qui ont été signalés en 2022, ce qui représente une statistique non négligeable. La fraude est définie par le Gouvernement du Canada (2022) comme une « tromperie intentionnelle utilisée pour nuire à une autre personne ou pour s'emparer de son argent ou de ses biens de manière illégale ». Avec l'arrivée d'Internet, les différentes méthodes pour commettre des fraudes ont évolué (Koong, Liu et Wei, 2012). Étant donné que les individus passent de plus en plus de temps sur Internet, les risques d'en être victime augmentent et s'intensifient (Wagner, 2009 ; Button et Cross, 2017a).

Le *scambaiting* est un moyen de perturbation de la fraude en ligne qui est une activité relativement récente, il est ainsi important d'en comprendre l'impact. La pratique du *scambaiting* consiste en un individu (nommé ci-après le « scambaiter ») qui entre en communication avec un fraudeur et qui lui fait croire qu'il succombe à ses stratagèmes de fraude dans le but de lui faire perdre du temps (Smallridge, Wagner et Crawl, 2016 ; Sorell, 2019). La publication de vidéos de *scambaiting* sur Internet débute au début des années 2000 avec la création de plusieurs plateformes en ligne dont le but est de favoriser le partage de contenu numérique (Laato et Rauti, 2021). De plus en plus d'individus pratiquent ce type d'activités contre des fraudeurs étant donné la possibilité de publier rapidement et gratuitement des vidéos (Laato et Rauti, 2021). La présente recherche vise donc, en premier lieu, à mettre de l'avant les buts recherchés des *scambaiters* dans la création de vidéos portant sur le *scambaiting*. Plus précisément, des vidéos de *scambaiting* portant uniquement sur la fraude au soutien technique sont retenues comme échantillon de l'étude, étant donné que ce type de contenu est majoritairement présent sur les chaînes YouTube francophones. En deuxième lieu, l'étude vise à comprendre l'impact de la diffusion des vidéos sur les internautes. Ainsi, l'activité du scambaiting est analysée pour en apprendre davantage sur son fonctionnement et ses finalités.

Afin d'approfondir les connaissances sur le *scambaiting*, la revue de la littérature recense les principaux résultats des études antérieures portant sur cette pratique. De brèves explications sur la fraude en ligne, sur le vigilantisme en ligne et sur le digilantisme suivront. Un survol des écrits sur la sensibilisation possible des vidéos YouTube sera ensuite fait. Toutes ces informations sont pertinentes à l'élaboration et à l'explication de la problématique de recherche. La méthodologie qui a été utilisée est ensuite expliquée. Il s'en suit une présentation et une discussion des résultats de l'étude. Pour finir, une conclusion résumant les éléments à retenir est élaborée.

Recension des écrits

La fraude

La définition de la fraude

L'article 380 (1) du Code criminel (2023) est l'article qui élabore la définition globale de la fraude. Cet article mentionne que « Quiconque, par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminé ou non, de quelque bien, service, argent ou valeur » est coupable de commettre une fraude. Plusieurs crimes qui étaient commis dans le monde physique peuvent maintenant, en plus, être commis en ligne (Fitzgerald, 2014). La perpétration des crimes dits « traditionnels » (par exemple le vol d'argent ou d'informations personnelles) peut être facilitée par l'arrivée Internet et ceux-ci feraient davantage de victimes sur un plus vaste territoire (McGuire et Dowling, 2013 ; National Crime Agency, 2016). Donc, bien que la fraude ne soit pas un phénomène nouveau, elle est maintenant plus difficile à détecter, puisqu'elle peut être perpétrée de plusieurs façons (Button et Cross, 2017a).

La fraude en ligne se traduit par la mise en place de plusieurs stratagèmes utilisés par les délinquants et peut se dérouler sur de multiples environnements en ligne, soit sur des forums de discussions, par courrier électronique ou directement sur des sites internet (Younes, 2019 ; Maimon, Howell, Moloney et Park, 2020). La fraude peut être commise par une personne qui se fait passer pour un individu ayant des pouvoirs ou des compétences particulières ou encore par un individu de confiance (Dove, 2020). Lorsqu'une victime communique volontairement des informations personnelles ou de l'argent à un individu, ne sachant pas que ce dernier perpétue des actions criminelles, cela sera considéré également comme un acte frauduleux (Dove, 2020). Cela peut être vu, par exemple, lors d'une fraude amoureuse. Le but des fraudeurs est de berner et de duper des individus avec l'intention de leur soutirer de l'argent ou des informations personnelles (Younes, 2019 ; Poonia, 2014). Ainsi, toute fraude en ligne débute par un contact entre le délinquant (l'individu qui trompe) et la victime (la personne qui est victime de la tromperie) (George, Marett et Tilley, 2004). La communication entre le fraudeur et la victime peut se faire de deux façons, soit de manière synchrone ou asynchrone (Laato et Murtonen, 2020). La première façon se fait le plus souvent par téléphone ou vidéoconférence. Tandis que la seconde se voit généralement lors d'une correspondance qui n'est pas instantanée, par exemple, par l'envoi d'un courriel frauduleux ou encore de messages textes (Laato et Murtonen, 2020).

La fraude au soutien technique

La fraude au soutien technique se déroule lorsque des individus se font passer pour des techniciens d'un centre de soutien technique et tente de soutirer de l'argent à des citoyens en les persuadant que leur appareil informatique est piraté ou qu'il y a des problèmes et virus dans celui-ci (Centre antifraude du Canada, 2023 ; Chaire de recherche en prévention de la cybercriminalité, 2022b). La fraude au soutien technique débute habituellement par l'apparition d'une page web sur le moteur de recherche de la victime qui lui mentionne que son ordinateur est infecté et qu'elle doit appeler le numéro d'assistance inscrit sur cette page web le plus rapidement possible (Miramirkhani, Starov et Nikiforakis, 2016 ; Rauti et Leppänen, 2017). Parfois, la communication peut débuter par un appel de la part du fraudeur. Ces derniers appellent alors aléatoirement des victimes potentielles (Rauti et Leppänen, 2017 ; Centre antifraude du Canada, 2023). Une fois en communication téléphonique avec le fraudeur, ce dernier tente de convaincre la personne que son ordinateur est infecté ou piraté et qu'un support d'urgence est nécessaire pour protéger à nouveau son appareil électronique (Miramirkhani et al., 2016 ; Rauti et Leppänen, 2017). Durant l'appel, le fraudeur demande, la majorité du temps, d'avoir le contrôle à distance de l'ordinateur (Rauti et Leppänen, 2017). Cette demande peut avoir deux buts. Le premier sera de voler des informations personnelles de l'individu une fois connecté à l'appareil électronique et le deuxième, dans la majorité des cas, sera pour avoir un gain financier (Rauti et Leppänen, 2017 ; Centre antifraude du Canada, 2023). En effet, après avoir réussi la connexion à distance, le fraudeur fait un faux diagnostic et mentionne qu'il y a de graves problèmes sur l'ordinateur, par exemple la présence de multiples virus (Miramirkhani et al., 2016). Il tente alors de vendre à la victime un programme de support et de réparation (Miramirkhani et al., 2016 ; Rauti et Leppanen, 2017). L'objectif principal de la fraude au soutien technique est la recherche d'un gain monétaire (Rauti et Leppänen, 2017). En 2021, les pertes occasionnées par ce type de fraude s'élevaient à 347 millions de dollars (Federal Bureau of Investigation, 2022).

Les méthodes de perturbations de la fraude en ligne

Certains citoyens percevaient le contrôle social formel accompli par les autorités comme étant insuffisant pour répondre adéquatement à la fraude en ligne (Durkin et Brinkman, 2009). En effet, les ressources humaines et financières fournies aux autorités policières pour enquêter, détecter et répondre aux différents types de fraudes sont limitées (Button et Cross, 2017b). Plusieurs cas de fraude en ligne ne sont jamais enquêtés par les autorités compétentes étant donné le manque d'effectif et de ressources monétaires. Cela a pour conséquence que celles-ci ne peuvent répondre à tous les cas de fraude (Button et Cross, 2017b). Les différentes méthodes de perturbations de la fraude en ligne ont ainsi été créées pour pallier les lacunes perçues (Durkin et Brinkman, 2009; Loveluck, 2019; Sorell, 2019).

Le vigilantisme et le digilantisme

Pour commencer, il est nécessaire de préciser qu'il est difficile de faire la distinction entre le vigilantisme en ligne et le digilantisme, puisque la majorité de leurs caractéristiques sont communes et que les termes sont parfois interchangés dans la littérature. De même, le vigilantisme en ligne, le digilantisme, ainsi que le scambaiting font partie d'un même continuum de méthodes de perturbation des activités criminelles effectuées en ligne (Smallridge et al., 2016 ; Sorell, 2019). Pour une meilleure compréhension du sujet de recherche, une distinction des concepts sera tentée. D'une part, le vigilantisme est un concept d'abord développé par Johnston en 1996. Ce dernier définit le vigilantisme comme « a social movement giving rise to premeditated acts of force - or threatened force - by autonomous citizens » (Johnston, 1996, p. 232). Le vigilantisme est en fait une action posée par des citoyens pour opérer un contrôle social lorsqu'une norme sociétale est brimée par des individus (Johnston, 1996). Le concept du vigilantisme s'applique également dans l'univers du web. Ainsi, le vigilantisme en ligne est une action posée par des citoyens qui répondent à la commission d'une infraction ou même à la violation de règles ou de normes par certains délinquants (Loveluck, 2019 ; Reichl, 2019). Le vigilantisme en ligne est utilisé par les internautes pour identifier l'auteur de l'infraction, pour l'humilier ou encore pour transmettre aux autorités des preuves de l'activité criminelle (Loveluck, 2019 ; Reichl, 2019 ; Sorell, 2019).

D'autre part, Tom Sorell (2019) définit le digilantisme comme une forme de représailles envers des individus qui posent des actes criminels, et qui, selon les personnes qui font du digilantisme, resteront impunis par la loi. Le digilantisme est particulièrement utilisé dans la « chasse aux pédophiles » (Sorell, 2019, p.154). Dans ce cas bien spécifique, les citoyens pratiquant le digilantisme traqueront sur le web un pédophile pour lui faire part des conséquences qu'ils pourraient lui faire subir. Une des caractéristiques du digilantisme est que la discussion entre le criminel et le citoyen peut se faire devant une audience qui, elle aussi, désapprouve les gestes commis (Sorell, 2019). Cette audience est composée de citoyens qui regardent en direct les individus perpétrant le digilantisme contre certains délinquants (vidéo en live stream).

Une caractéristique commune du digilantisme et du vigilantisme en ligne est qu'il peut y avoir l'utilisation de menaces envers l'auteur du crime (Sorell, 2019 ; Trottier, 2017). Une menace qui peut être utilisée est le dévoilement de son identité. Ceci a pour but de lui faire peur et de l'humilier pour les actes illicites posés (Trottier, 2017). Puisqu'il a caché son identité tout au long des fraudes commises, le délinquant ne veut pas que celle-ci (nom ou visage) soit visible et connue publiquement (Reichl, 2019). Lorsque le citoyen effectuant ces pratiques vient à connaître l'identité du criminel, divers moyens peuvent être utilisés pour dévoiler son identité, soit par des messages sur des forums, des photos ou des vidéos distribués avec l'aide d'une audience, etc. (Sorell, 2019 ; Trottier, 2017).

Le scambaiting

Définition

Les individus procédant au *scambaiting* communiquent avec les fraudeurs, en se faisant passer pour une victime potentielle de la fraude qu'ils perpétuent (Sorell, 2019). Cette pratique peut être vu comme une possibilité de sensibiliser les citoyens à différents types de fraudes, permettant parfois, la prévention de ce crime, mais elle peut aussi être considérée comme du divertissement (Laato et Rauti, 2021). Tel que mentionné ci-haut, le *scambaiting* se retrouve sur le spectre du vigilantisme en ligne et du digilantisme. Toutefois, le *scambaiting* a une composante plus morale que les deux autres moyens de perturbation, puisque des règles publiques entourent la pratique (Sorell, 2019). Toutefois, il n'est pas impossible que le *scambaiting* porte préjudice, lorsque celui-ci ne prend pas seulement la forme d'une communication visant à faire perdre du temps au fraudeur (Sorell, 2019).

Le *scambaiting* peut aussi être perçu comme une forme de lutte contre la fraude (Laato et Rauti, 2021). Les *scambaiters* peuvent, d'une certaine manière, aider les autorités compétentes (Laato et Rauti, 2021). Cette assistance se fait par la diffusion d'informations précises sur les fraudeurs et par la prévention de la fraude en ligne (Laato et Rauti, 2021). Ainsi, le *scambaiting* peut être considéré comme une action ayant pour but de sensibiliser les citoyens aux processus de fraude pour tenter de réduire le nombre de victimes. D'ailleurs, étant donné l'engouement grandissant pour la pratique du *scambaiting* et sa médiatisation sur de multiples plateformes en ligne, de plus en plus d'individus peuvent assister à ce type d'échanges (Laato et Rauti, 2021). Le *scambaiter* use alors de tromperie envers le délinquant puisqu'il le persuade qu'il croit en son identité et en ses mensonges et qu'il succombe à ses différentes techniques de persuasion (Dynel et Ross, 2021 ; Sorell, 2019). Ce qui caractérise l'échange entre le citoyen et le délinquant est la tromperie qui est utilisée par les deux parties (Dynel et Ross, 2021 ; Dynel, 2016).

Buts

Les individus procédant au *scambaiting* ont généralement plusieurs buts ou objectifs (Ross et Logi, 2021 ; Dynel, 2016 ; Laato et Rauti, 2021). Premièrement, ils peuvent vouloir faire perdre du temps aux fraudeurs afin qu'ils aient moins de temps pour trouver d'autres victimes potentielles et communiquer avec ces dernières (Ross et Logi, 2021 ; Sorell, 2019 ; Edwards, Peersman et Rashid, 2017). Laato et Rauti (2021) ont trouvé dans leur recherche que les *scambaiters* utilisent plusieurs techniques pour faire perdre du temps et donc de l'argent aux fraudeurs, en essayant, par tous les moyens possibles, de prolonger les échanges sans raison valable.

Le fait de ridiculiser les délinquants peut aussi être recherché par les *scambaiters* (Laato et Rauti, 2021). Les *scambaiters* peuvent ainsi dénigrer les délinquants en mettant en évidence leurs capacités intellectuelles limitées (Dynel et Ross, 2021). Le fait de vouloir ridiculiser le

fraudeur peut aussi faire partie d'une vengeance (Tuovinen et Röning, 2007). En effet, ce procédé peut parfois être appliqué par une personne qui a elle-même été victime de fraude ou encore par quelqu'un qui connaît personnellement une victime (Zingerle et Kronman, 2011 ; Sorell, 2019 ; Tuovinen et Röning, 2007).

La troisième finalité qui peut être recherchée par la pratique du *scambaiting* est le divertissement. Le divertissement peut être pour le compte des internautes qui écoutent la vidéo en direct (*live stream*), pour les citoyens qui regarderont la vidéo en rediffusion et pour le compte du *scambaiter* lui-même (Laato et Rauti, 2021). Lorsque le *scambaiter* rit ou qu'il y a des insultes, injures et moqueries qui sont dites de la part des deux parties, cela peut être considéré comme une forme de divertissement (Laato et Rauti, 2021). Par ailleurs, l'humour et l'agressivité seraient régulièrement combinés et discernés dans différents médias numériques (Yuan et Lu, 2022). Yuan et Lu (2022) rapportent que l'utilisation d'une communication plus agressive augmenterait la perception de l'humour employé dans les vidéos publiées sur la plateforme YouTube. L'humour agressif est défini comme « any humor that derogates or provides negative information about someone or something » (Janes et Olson, 2000, p.474). Les internautes sur YouTube s'attendent généralement à ce que les vidéos qui y sont publiées soient amusantes et participent à leur divertissement (Yuan et Lu, 2022). L'humour et la moquerie sont régulièrement utilisés par les *scambaiters* dans la pratique du *scambaiting* (Sorell, 2019).

Le quatrième but que les *scambaiters* peuvent rechercher est d'en apprendre plus sur le processus de fraude pour ainsi diffuser les techniques utilisées pour prévenir et sensibiliser les citoyens (Ross et Logi, 2021 ; Laato et Rauti, 2021). Les *scambaiters* vont souvent, dans leurs vidéos, passer des messages de prévention et de sensibilisation sur les pratiques à avoir ou non sur internet (Laato et Rauti, 2021). Toutefois, ce dernier objectif peut aussi avoir une composante égocentrique. Effectivement, pour certains, le but recherché derrière la participation au *scambaiting* est de bien paraître aux yeux de la communauté des *scambaiters* (Tuovinen et Röning, 2007). Ces auteurs vont aussi associer la sensibilisation possible par le *scambaiting* à un « community service » (Tuovinen et Röning, 2007, p.400). En effet, ces chercheurs mentionnent qu'en faisant usage de tromperie et en causant une perte de temps et financière aux fraudeurs, il serait possible pour les *scambaiters* de protéger de futures victimes (Tuovinen et Röning, 2007).

Une source de revenus peut être engendrée par la publication de vidéos sur YouTube (Waseem, 2018). Ainsi, cette part de revenus peut motiver les *scambaiters* à diffuser des vidéos portant sur cette pratique (Laato et Rauti, 2021). Les revenus occasionnés peuvent provenir du nombre de visionnements, des abonnements payants et des publicités dans les vidéos (YouTube, 2022a ; Kim, 2012 ; Laato et Rauti, 2021). Toutefois, cette visibilité peut avoir un aspect négatif. En effet, les fraudeurs sont de plus en plus conscients que plusieurs individus pratiquent cette activité, ils seront ainsi plus méfiants lorsqu'ils recevront des appels (Laato et Rauti, 2021).

Comportements et attitudes

Les *scambaiters* posent divers comportements lors de la perpétration du *scambaiting*. Les *scambaiters* vont souvent utiliser la confrontation à la fin de la pratique du *scambaiting* pour confronter le fraudeur sur ses agissements, tout en dévoilant leur identité (Laato et Rauti, 2021 ; Ross et Logi, 2021). À la suite de cette confrontation, un échange peut survenir entre les deux parties (Laato et Rauti, 2021 ; Ross et Logi, 2021). Certains *scambaiters* vont même jusqu'à s'infiltrer dans l'ordinateur du fraudeur pour récupérer et effacer sur leur ordinateur les informations personnelles sur les victimes ou encore des fichiers et documents que les fraudeurs utilisent pour perpétrer la fraude (Laato et Rauti, 2021). Ces *scambaiters* commettront alors eux-mêmes des comportements illégaux. Avec ce comportement, les *scambaiters* peuvent vouloir transmettre les informations aux autorités compétentes, mais aussi menacer le fraudeur de divulguer l'ensemble de ses informations personnelles, ainsi que son identité sur Internet (Laato et Rauti, 2021 ; Sorell, 2019 ; Trottier, 2017). Également, le *scambaiting* et le vigilantisme en ligne pourraient exacerber des comportements racistes, tel que le rapportent les chercheurs Yékú, (2020) et Nakamura (2014). Un de ceux-ci serait la recherche et la publication de trophées. Ces derniers peuvent être une photo ou vidéo dénigrant et humiliant les fraudeurs (Yékú, 2020 ; Nakamura, 2014 ; Zingerle, A., 2014).

Youtube

La sensibilisation par les vidéos

Avec l'essor des médias numériques, ces derniers ont la capacité d'être utilisés comme moyen de prévention et d'éducation (Latha, Meena, Pravitha, Dasgupta, Chaturvedi, 2020). L'accessibilité à YouTube, ainsi que la possibilité de visionner gratuitement les vidéos pourraient expliquer, en partie, la consommation de ce type de contenu et le nombre d'utilisateurs, qui s'élevait, en 2017, à plus d'un million (Sood, Sarangi, Pandey et Murugiah, 2011 ; International Telecommunications Union-UNESCO, 2017 ; Acuna, Vento, Alzate-Duque, Valera, 2019). Par exemple, pour comprendre des termes et concepts clés et complexes en santé, il faut parfois une capacité élevée en lecture et cela peut être difficile (Berland, Elliot, Morales, Asgazy, Kravitz, Broder, Kanouse, Munoz, Puyol, Watkins, Yang, McGlynn, 2001) et donc, la vulgarisation présente dans les vidéos YouTube pourrait aider les internautes. Les internautes peuvent ainsi s'éduquer, apprendre et être sensibiliser à certains sujets à leur propre rythme (Acuna et al., 2019 ; Gagliano, 1988). En effet, la vidéo peut être regardée à répétition ou encore à différentes vitesses (Acuna et al., 2019 ; Gagliano, 1988). Ceci pourrait expliquer pourquoi les citoyens visionnent des vidéos, plutôt que de prendre un autre moyen pour s'éduquer et se sensibiliser sur un sujet.

En effet, il existe, à ce jour, plusieurs études portant sur l'effet de sensibilisation et d'information des vidéos YouTube pour plusieurs domaines, tels que la médecine, les sciences politiques et la santé publique (Allgaier, 2020). Les vidéos partagées sur YouTube permettent

la consommation passive d'éléments explicatifs sur des sujets, mais aussi stimulent les dialogues entre différentes communautés en ligne suivant le visionnement des celles-ci (Shao, 2009 ; Erviti et Stengler, 2016). Cette consommation et les dialogues qui s'ensuivent pourraient sensibiliser les internautes à divers sujets. Shapiro et Mark (2014) ont analysé, dans leurs études, des commentaires publiés sous des vidéos portant sur les changements climatiques et ont démontré que les internautes commentent souvent des faits ou des informations n'étant pas nécessairement mentionnés dans les vidéos. Ceci suppose que les individus sont non seulement sensibilisés à ce qui est rapporté par la vidéo, mais également à l'enjeu des changements climatiques dans son ensemble (Shapiro et Mark, 2014). Par ailleurs, le type de vidéos, par exemple des vidéos abordant la politique ou des vidéos de divertissement, exercerait une influence sur le nombre de visionnements, ainsi que sur l'information retenue et partagée par les spectateurs dans les sections de commentaires (Möller, Kühne, Baumgartner et Peter, 2019). En effet, les internautes seraient plus engagés à écouter des vidéos de divertissement qui sont drôles et qui ont un visuel attrayant (Khan, 2017 ; Möller et al., 2019 ; Chau, 2010 ; Allgaier, 2020).

Toutefois, lorsque l'humour est utilisé lors de la transmission d'un message sur un enjeu politique, ce propos peut être perçu comme un moyen de divertissement et non d'information, due à l'utilisation de l'humour, nuisant ainsi au développement d'une opinion sur cet enjeu (Nabi, Moyer-Gusé et Byrne, 2007). Cependant, ces chercheurs ont également trouvé que, dans certains cas, les personnes qui trouvent qu'un message est divertissant seront plus disposées à porter une attention particulière aux propos communiqués (Nabi et al., 2007). Ce dernier résultat est conforme avec la littérature portant sur le potentiel de sensibilisation des vidéos de divertissement (Nabi et al., 2007).

Les commentaires

Une étude de Marta Dynel (2014) permet d'avoir plus de détails sur le type de commentaires publiés sous des vidéos mises en ligne sur YouTube. Cette auteure mentionne que les membres de l'audience asynchrone, qui sont des citoyens qui écoutent les vidéos en différé, peuvent laisser un ou plusieurs commentaires sous la vidéo écoutée, peuvent prendre tout leur temps pour le rédiger et même modifier leur publication (Ross et Logi, 2021 ; Dynel, 2014). Ainsi, les commentaires publiés lors de l'écoute de vidéos en direct (par exemple dans un clavardage en direct) et ceux publiés sur YouTube (dans la section commentaire sous la vidéo) ne soulèveront pas nécessairement les mêmes résultats lors de leur analyse.

Le contenu des vidéos, ainsi que le ton employé par les créateurs de contenu auraient un impact sur les commentaires (Edgerly, Vraga, Dalrymple, Macafee et Fung, 2013 ; Porter et Hellsten, 2014). De plus, des études portant sur l'impact du contenu médiatique démontrent que l'élément abordé, ainsi que la manière dont il est exploité, influencent la perception des internautes et donc le ton du commentaire (plus positif ou négatif) (Möller et al., 2019; Ksiazek

2018). Par exemple, l'utilisation d'incivilités par les créateurs de vidéos pourrait occasionner des commentaires avec plus d'incivilités (Edgerly et al., 2013). L'incivilité inclut le « name-calling, contempt, and derision of the opposition » (Brooks et Geer, 2007, p.1). Également, le flaming est défini comme « the hostile expression of strong emotions and feelings » (Lea, O'Shea, Fung et Spears, 1992, p.2). Le flaming serait alors un langage blessant, se manifestant par l'utilisation d'injures et d'insultes et pourrait se retrouver dans la section commentaires des vidéos publiées sur YouTube (Moor, Heuvelman et Verleur, 2010 ; Khan et Jacob, 2013). Khan et Jacob (2013) ont analysés des commentaires retrouvés sous différentes vidéos YouTube provenant de chaînes de divertissement, des chaînes de nouvelles et des chaînes abordant l'environnement. Ces chercheurs ont trouvé que 11% de l'ensemble des commentaires publiés avaient des composantes liées au flaming, ce qui ne constitue pas la majorité (Khan et Jacob, 2013). Donc, la plupart des commentaires laissés par les internautes démontraient une opinion positive envers le contenu des vidéos (Khan et Jacob, 2013). Ainsi, le type de vidéos, son contenu et comment les sujets abordés sont exprimés peuvent influencer la communauté en ligne et sa réaction subséquente au visionnement (Khan et Jacob, 2013 ; Edgerly et al., 2013 ; Möller et al., 2019).

Laato et Rauti (2021) rapportent également que des commentaires portant sur des stéréotypes liés à l'ethnie peuvent être publiés sous les vidéos de *scambaiting*. Toutefois, ce type de commentaires ne serait pas vu sous l'ensemble des vidéos YouTube analysées dans le cadre de leur recherche (Laato et Rauti, 2021). Deux raisons pourraient expliquer le peu de commentaires sur l'ethnie sous les vidéos de *scambaiting*. D'une part, les individus ne publient pas ce type de commentaires ou très peu ou, d'autre part, il y a modération ou contrôle du contenu (YouTube, 2022b). De plus, des commentaires démontrant de la compassion pour certains fraudeurs manifestant des problèmes de santé mentale ont été repérés sous certaines vidéos analysées par Laato et Rauti (2021). Ainsi, à la suite de leurs analyses, les chercheurs tirent la conclusion suivante : les internautes sont divertis par les propos du *scambaiter* lorsque ces derniers (pouvant viser à ridiculiser le fraudeur) sont dits envers les délinquants qui sont effrontés ou encore méchants (Laato et Rauti, 2021).

Problématique

Le *scambaiting* est une méthode de perturbation de la fraude en ligne, tel qu'il est présenté dans la recension des écrits. L'activité du *scambaiting* est de plus en plus populaire et plusieurs chaînes YouTube se dédient à cette pratique depuis quelques années. Par ailleurs, chaque année, plusieurs millions de dollars sont volés par les fraudeurs perpétrant l'arnaque au soutien technique (Federal Bureau of Investigation, 2022). De plus, tel que mentionné ci-haut, les ressources limitées fournies aux autorités compétentes pour combattre la fraude en ligne nous poussent à nous intéresser à d'autres types de méthodes de perturbation envers ce crime (Durkin et Brinkman, 2009 ; Button et Cross, 2017b). Ainsi, en raison de l'impact de cette fraude et dû à la popularité grandissante du *scambaiting*, il est important et primordial de s'intéresser à cette activité pour mieux comprendre son fonctionnement et ses finalités.

La définition du *scambaiting* est bien détaillée dans les différentes études scientifiques (Zingerle, 2014 ; Sorell, 2019 ; Dynel et Ross, 2021 ; Laato et Rauti, 2021). Quelques chercheurs ont examiné, dans leurs études, les procédés et les objectifs derrière le *scambaiting* (Smallridge et al., 2016 ; Sorell, 2019 ; Ross et Logi, 2021 ; Laato et Rauti, 2021 ; Tuovinen et Röning, 2007). Toutefois, il est pertinent de s'intéresser à cette pratique puisque l'engouement pour celle-ci ainsi que sa diffusion sont relativement récents. Ainsi, peu d'études portent sur ce nouveau phénomène. Également, la revue de littérature ne recense aucune étude portant uniquement sur l'étude de chaînes YouTube de *scambaiting* francophones, ce qui est un manque scientifique dans le milieu de la criminologie. Nous supposons que le processus de fraude en ligne peut différer entre les fraudeurs anglophones et ceux francophones. Ainsi, le processus de *scambaiting* pourrait être appliqué différemment.

De surcroît, certaines recherches ont analysé le contenu des commentaires publiés sous des vidéos, mais se sont concentrées majoritairement sur les vidéos en direct (*live stream*). Peu de recherches portent sur l'analyse des commentaires laissés sous des vidéos de *scambaiting* publiées sur YouTube (Dynel et Ross, 2021 ; Ross et Logi, 2021 ; Laato et Rauti, 2021). Tel qu'il a été mentionné ci-haut, dû à la différence qui existe entre les vidéos en direct (live stream) qui sont instantanées et les vidéos sur YouTube, où la publication est permanente, des disparités quant au contenu des commentaires peuvent survenir. Les vidéos en direct peuvent être considérées comme une forme de divertissement plus complète, étant donné l'interaction en continu avec l'audience synchrone (Ross et Logi, 2021 ; Scheibe, Fietkiewicz et Stock, 2016). Au contraire, les vidéos publiées sur YouTube auraient des composantes liées au divertissement, certes, mais auraient également un potentiel de sensibilisation plus grand, par exemple en termes d'information liée à la santé (Khan, 2017 ; Madathil, Rivera-Rodriguez, Greenstein et Gramopadhye, 2015). En effet, les vidéos YouTube peuvent être publiées sur une plus longue période de temps comparativement à des vidéos qui sont uniquement en di-

-rect. Les vidéos YouTube pourraient ainsi avoir un nombre de visionnements plus élevé. Les types de commentaires qu'on retrouve sur YouTube pourraient être influencés par les particularités des vidéos et aussi par la manière dont le créateur de contenu discute et aborde les sujets (Edgerly et al., 2013). L'impact des vidéos sur les internautes, en effectuant l'analyse des commentaires publiés par ces derniers, n'est que peu étudié. Il faut toutefois mentionner que Laato et Rati dans leur étude de 2021, ont analysé les commentaires et en ont tiré des conclusions. Il est alors pertinent de voir si les résultats de ces chercheurs sont distingués dans la présente étude, portant uniquement sur des chaînes YouTube francophones.

L'objectif principal de la recherche est donc de mieux comprendre les procédés mis en place par les *scambaiters* dans leurs vidéos et l'impact de ces dernières sur les internautes. Ainsi, deux questions ont mené à la présente étude :

1. **Quels sont les procédés utilisés par les *scambaiters* et quels sont les buts recherchés par ces derniers à travers la création de vidéos de *scambaiting*?**
2. **Qu'est-ce que les commentaires laissés par les internautes nous apprennent sur l'impact de ce type de contenu sur ces derniers?**

Le premier objectif de recherche est de recenser les procédés mis en place par les *scambaiters* à travers l'analyse de leurs comportements et de leurs attitudes vis-à-vis les fraudeurs. En effet, l'étude de Laato et Rauti (2021) fournit un portrait des comportements posés par les *scambaiters* anglophones lorsqu'ils pratiquent le *scambaiting* (4 types de vidéos). Quelques chercheurs se sont penchés sur les procédés et les buts recherchés dans la pratique du *scambaiting* (Smallridge et al., 2016 ; Sorell, 2019 ; Ross et Logi, 2021 ; Laato et Rauti, 2021 ; Tuovinen et Röning, 2007). Ainsi, l'évaluation du contenu des vidéos pour y recenser les attitudes et les comportements des *scambaiters* en réponse à la tentative de fraude, et ce, pour mieux comprendre les buts des *scambaiters* derrière la création de leurs vidéos est le premier objectif de recherche. Une documentation distincte de la pratique du *scambaiting* est possible étant donné l'analyse de vidéos YouTube de *scambaiters* francophones.

Également, peu de recherches portant sur le phénomène du *scambaiting* abordent les commentaires qui sont publiés sous les vidéos mises en ligne sur YouTube. La deuxième question de recherche permet d'évaluer l'effet de la diffusion des vidéos sur ceux qui les regardent. Ainsi, le contenu des commentaires publiés sous les vidéos analysées dans le cadre de la recherche a été étudié. Avec l'analyse des commentaires, il est possible d'observer si les résultats de l'étude de Laato et Rauti (2021) sont discernables dans les vidéos de *scambaiters* francophones. De plus, une analyse portant sur l'impact de la diffusion des vidéos a été faite. L'étude des commentaires nous a permis d'examiner si les buts recherchés par la pratique du *scambaiting* sont distingués dans les commentaires. La deuxième question de re-

-cherche a donc deux sous-objectifs, soit d'étudier le contenu des commentaires et, par la suite, d'observer l'impact de la diffusion des vidéos sur les internautes.

L'hypothèse de la recherche est que, bien que les vidéos de *scambaiting* présentent un aspect préventif en matière de fraude, le but final recherché par les *scambaiters* serait le divertissement, ce qui serait également illustré par les commentaires publiés par les internautes lors du visionnement des vidéos.

Méthodologie

Provenance de l'échantillon

L'approche méthodologique privilégiée pour cette recherche était une approche qualitative. En effet, les deux méthodes de collecte de données qui ont été appliquées sont l'étude de cas et l'analyse documentaire. La méthode de l'étude de cas est utile et pertinente pour explorer un sujet nouveau et émergeant (Barlatier, 2018). Puisque le *scambaiting* est une pratique récente et qui prend de l'ampleur depuis quelques années, il est possible d'en apprendre davantage sur son fonctionnement grâce à cette méthode de collecte de données. De plus, l'étude de cas permet d'explorer un phénomène en profondeur (Barlatier, 2018). L'analyse documentaire a également été utilisée puisque la collecte de données comportait le visionnement de vidéos YouTube, ainsi que la recension et l'analyse des commentaires sous chacune de celles-ci. La sélection de documents médiatiques publics, soit ici les vidéos de chaînes YouTube, était la première étape de la méthodologie. Ainsi, avec ces deux méthodes de collecte de données, il a été possible de mieux comprendre le phénomène du *scambaiting* et d'ajouter aux connaissances criminologiques actuelles.

Échantillon

Bien que la population cible soit toutes les chaînes YouTube qui font la mise en ligne de vidéos de *scambaiting*, la population accessible était quelque peu limitée. Cette dernière est alors composée de chaînes YouTube uniquement francophones qui sont majoritairement dédiées à la pratique du *scambaiting*. Les vidéos analysées portent sur le *scambaiting* perpétré contre des fraudeurs se faisant passer pour des techniciens Microsoft. Puisque les chaînes francophones qui ont suffisamment de vidéos portant sur la perturbation de ce type de fraude sont tout de même limitées, trois chaînes YouTube ont été étudiées. En effet, ces chaînes ont été choisies puisqu'il y avait plusieurs vidéos portant sur la pratique du *scambaiting*.

Pour chacune de ces chaînes, cinq vidéos ont été écoutées. Étant donné que l'ensemble des vidéos de *scambaiting* analysées portait sur le même type de fraude, la saturation a été atteinte avec le visionnement de ce nombre de vidéos par chaîne. Le modus operandi des fraudeurs étant passablement statique, les *scambaiters* ont peu de flexibilité dans les scénarios d'interactions qu'ils ont avec ces délinquants. Ainsi, consulter davantage de vidéos ou de chaînes n'aurait pas apporté plus de connaissances sur leurs procédés, leurs comportements et leurs buts. Les vidéos choisies ont été publiées entre 2016 et 2022 et sont des rediffusions de vidéos en direct de Twitch ou des vidéos éditées et publiées directement sur YouTube, permettant une analyse complète et versatile de la pratique.

Les vidéos qui ont été choisies pour être analysées sur chacune des chaînes étaient celles ayant le plus de visionnements et qui portaient uniquement sur la pratique du scambaiting. Ainsi, les vidéos de ces chaînes qui ne portent pas sur cette activité n'ont pas été retenues, bien qu'elles aient été plus visionnées que d'autres. De plus, nous avons exclu les vidéos résumant l'échange qu'il y a eu entre le *scambaiter* et le fraudeur lorsque la vidéo diffusant l'entièreté du *scambaiting* était disponible. En effet, bien que les vidéos plus courtes aient plus de visionnements que les vidéos montrant la conversation complète (par exemple, une vidéo de 20 minutes résumant le *scambaiting* effectué est davantage visionnée que la vidéo de *scambaiting* dans son entièreté), les vidéos présentant dans l'entièreté la pratique du *scambaiting* fournissent davantage d'informations pertinentes pour notre étude. Toutefois, si l'appel dans son entièreté n'était pas disponible, l'échange condensé a été utilisé. Également, il est nécessaire de préciser que les vidéos « Best of », malgré un nombre important de visionnements sur les différentes chaînes, n'ont pas été sélectionnées pour la collecte de données. En effet, ces vidéos portent sur plusieurs *scambaiting* condensés en quelques minutes seulement et ne permettent pas d'avoir un aperçu plus détaillé des procédés utilisés par les *scambaiters*.

En plus de l'observation des vidéos, les commentaires laissés par l'audience asynchrone ont également été étudiés. Cette analyse visait à examiner si les vidéos de *scambaiting* ont seulement un intérêt pour le divertissement du public ou s'ils ont aussi un effet de prévention et de sensibilisation à la fraude en ligne (Dynel, 2014 ; Ross et Logi, 2021 ; Laato et Rauti, 2021). En effet, tel que le spécifient Edgerly et ses collègues (2013), les sujets abordés dans les vidéos publiées sur YouTube et la manière dont ils sont exposés par les youtubeurs auraient un impact sur le contenu des commentaires. Donc, lorsqu'ils étaient disponibles, les 30 premiers commentaires de la section commentaires de chacune des vidéos analysées ont été recensés et examinés. Ainsi, le tri « les plus récents d'abord » disponible sur YouTube a été appliqué pour la section commentaires de chacune des vidéos, et ce, dans le but d'avoir un aperçu des commentaires ayant été publiés en premier.

La méthode d'échantillonnage était de type non-probabiliste. Cette méthode consiste à sélectionner des sujets correspondant à la population visée par l'étude, mais de manière non aléatoire (Statistique Canada, 2021). La sorte d'échantillonnage était de type disponible ou de convenance. Cette dernière consiste à prendre ce qui est disponible selon la population accessible. Ainsi, le tri orienté a été appliqué en choisissant des vidéos YouTube qui semblaient appartenir à la population accessible.

Concepts à l'étude

Conceptualisation

Tel qu'il a été mentionné dans la recension des écrits, les *scambaiters* peuvent avoir divers comportements à l'égard des fraudeurs lors de la pratique du *scambaiting*. Le premier concept à l'étude était les buts recherchés par les *scambaiters* par la publication de ce type de contenu. Les différents comportements et attitudes pouvant être considérés comme des manifestations de ces buts ont été examinés. Le deuxième concept à l'étude était les commentaires laissés sous les vidéos analysées. Ce concept s'est divisé en deux dimensions, soit le contenu des commentaires et l'impact des vidéos sur les internautes.

Opérationnalisation

Les buts recherchés par les scambaiters

Les quatre dimensions pour mesurer ce concept étaient la perte de temps, la prévention, le divertissement et le fait de ridiculiser le fraudeur. Ces dimensions sont les thématiques qui ont été repérés dans la littérature (Laato et Rauti, 2021 ; Sorell, 2019 ; Ross et Logi, 2021 ; Dynel et Ross, 2021) et par la suite dans les vidéos. Ce n'est pas l'ensemble des dimensions qui étaient présentes dans chacune des vidéos analysées. Pour savoir si une thématique était présente dans une vidéo, il a fallu évaluer tous les comportements qui confirmaient que la finalité était recherchée par le *scambaiter*. Une liste des comportements posés par chaque youtubeur pour les cinq vidéos écoutées a été construite. Ainsi, une grille de codification avec l'ensemble des procédés (comportements, attitudes, paroles) employés par les *scambaiters* a été créée. Ensuite, il a été possible de diviser tous les procédés posés en sous-thématiques et ainsi voir quels étaient les buts recherchés par les *scambaiters* et comment ceux-ci se manifestent dans les vidéos.

Pour la recherche de perte de temps, en se basant sur notre interprétation, ainsi que sur la littérature, trois grandes sous-thématiques ont été créées. Ces sous-thématiques étaient les actions posées par le *scambaiter*, le fait de feindre des actions (inaction) causant une perte de temps au fraudeur et finalement les propos liés directement à la perte du temps. Pour la thématique de la prévention, les sous-thématiques étaient la mention d'une forme de dénonciation de la fraude, ainsi que la sensibilisation des internautes. Pour la thématique de ridiculiser les fraudeurs, trois sous-thématiques ont été élaborées, soit les insultes dites au fraudeur ou des insultes visant ce dernier, les commentaires liés à l'origine ethnique du fraudeur et la confrontation. Ce dernier comportement a été distingué lorsque le *scambaiter* dévoile son identité ou encore lorsqu'il confronte le délinquant sur ses agissements frauduleux. Pour la thématique du divertissement, l'humour utilisé par le *scambaiter* était la première sous-thématique qui permettait de distinguer la recherche de ce but. La deuxième sous-thématique était la présence d'une forme de fausse panique de la part du *scambaiter*. Des propos directement liés au divertissement vécu par le *scambaiter* ou encore celui souhaité pour les internautes étaient la troisième sous-thématique permettant de cerner la présence de cette finalité dans les vidéos.

Les commentaires publiés par les internautes

La première dimension était le contenu des commentaires. Les commentaires faisant un compliment ou félicitant ou remerciant le *scambaiter* pour son travail ont été ajoutés à la thématique « Discussion générale ». De plus, à partir de la littérature, une thématique « Émotions » a été créée pour y relever le contenu compatissant envers le fraudeur (Laato et Rauti, 2021).

La deuxième dimension était l'impact des vidéos sur les internautes. Pour cette dimension, le contenu des commentaires a également été examiné, mais dans l'optique de distinguer l'impact des vidéos sur les internautes. La première thématique était la perte de temps. Pour évaluer le fait que les internautes perçoivent les procédés qui sont mis en place par les *scambaiters* pour faire perdre du temps, nous devions repérer dans les commentaires du contenu relié textuellement à la perte de temps ou encore une référence à des actions (ou inaction) posées par le *scambaiter* qui font perdre du temps au fraudeur. La deuxième thématique était la prévention de la fraude. Cette thématique a été mesurée par une référence, dans les commentaires, à la prévention possible par les vidéos de *scambaiting*, à la mention d'expériences de fraude ou de tentative de fraude et par le fait que les internautes posent des questions sur la fraude au soutien technique. De plus, le fait de vouloir ridiculiser les fraudeurs pouvait aussi être attribué à certains commentaires ayant été publiés sous les vidéos de *scambaiting*. En effet, lorsque des insultes étaient formulées contre les fraudeurs ou encore lorsqu'il y avait des propos en lien avec l'origine ethnique du fraudeur, la troisième thématique a été attribuée à ce type de contenu. La quatrième thématique était le divertissement procuré par l'écoute des vidéos. Avec la présence de mots, tels que « rire », « MDR », « drôle », « un bon temps », etc., le divertissement a pu être retenu comme étant l'impact qu'a eu la vidéo sur l'internaute.

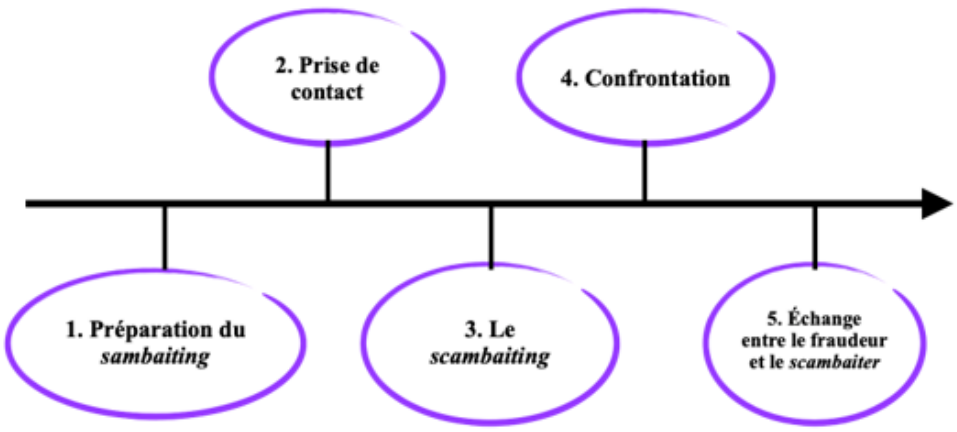
Les revenus qui découlent de la publication des vidéos peuvent aussi être, pour les *scambaiters*, un incitatif au divertissement (Laato et Rauti, 2021 ; Ross et Logi, 2021). Malheureusement, nous n'avons pas été en mesure de quantifier les revenus de chaque *scambaiters*, et ce, dû au manque d'information sur leur chaîne et dans leurs vidéos sur la rémunération reçue. De plus, plusieurs particularités quant à la rémunération sur YouTube font en sorte que la certitude des revenus reçus n'est pas possible (YouTube, 2022a).

Présentation des résultats

Processus du scambaiting

Pour commencer, le processus de *scambaiting* portant sur la fraude au soutien technique sera présenté. Cette explication permettra de mieux comprendre les résultats subséquents expliqués.

Figure 1 – Le processus de *scambaiting*



1) La préparation consiste aux tâches qui doivent être faites avant de pouvoir procéder au *scambaiting*. Les *scambaiters* pourront alors se créer, à l'aide de leurs compétences en informatique, une machine virtuelle ressemblant en tout point à une interface d'ordinateur conforme. Ils devront aussi trouver un ou des numéros de téléphone de faux centres de soutien technique Microsoft pour pouvoir procéder aux appels. Ces numéros de téléphone peuvent être trouvés sur des sites de signalements, tels que Signal-Arnaques, un site européen étant dédié à fournir de l'information sur les fraudes et aux signalements de ces escroqueries (Signal-Arnaques, 2021). De plus, les numéros des faux centres de soutien technique peuvent être fournis directement par le public qui assiste en direct au *scambaiting* (audience synchrone) ou par d'autres *scambaiters*.

2) La prise de contact consiste à appeler un ou plusieurs faux centres de soutien technique et se faire passer pour une victime potentielle. Bien que dans certains cas de fraude au soutien technique, le fraudeur peut aléatoirement communiquer avec les victimes potentielles, dans les vidéos écoutés, les *scambaiters* entrent directement en contact avec les fraudeurs (Centre antifraude du Canada, 2023 ; Rauti et Leppänen, 2017). En début d'appel, les *scambaiters* expliquent au faux technicien qu'il y a une page web qui est apparue sur leur navigateur indiquant qu'il y a un problème avec leur ordinateur et qu'ils doivent appeler immédiatement le numéro qui s'affiche à l'écran.

3) Ensuite, les fraudeurs vont généralement poser des questions au *scambaiter*, par exemple (paraphrases) : « À quel moment avez-vous acheté cet ordinateur ? », « Êtes-vous la seule personne à utiliser l'appareil ? », « Quel est le site ou la plateforme que vous consultiez avant que le message d'erreur apparaisse ? », « Quel est le système d'exploitation de l'ordinateur ? », etc. Les *scambaiters* vont ou non fournir des réponses à ces questions. Nous supposons que les *scambaiters* veulent ainsi ajouter à leur crédibilité de victime potentielle. Par la suite, le *scambaiting* se poursuit et les *scambaiters* mettent en place les différents procédés qui sont expliqués et détaillés ci-après.

4) La confrontation est l'étape où le *scambaiter* dévoile qu'il n'est pas la personne qu'il personnifie, le cas échéant. Si le *scambaiter* avait modifié sa voix durant l'appel, il reprend sa « vraie » voix pour cette étape. Le *scambaiter* dévoile qu'il est au courant de la supercherie en cours et peut confronter le faux technicien sur ses agissements frauduleux.

5) À la suite de la confrontation, un échange entre le fraudeur et le scambaiter, d'une durée variée, peut survenir. Plusieurs sujets peuvent être abordés dans cet échange. Par exemple, le *scambaiter* peut poser des questions au fraudeur sur ses techniques de fraudes et le fraudeur peut aussi poser des questions sur les raisons qui poussent le *scambaiter* à faire cette activité. Le ton de voix des deux parties peut augmenter ou devenir plus agressif.

Les buts et procédés dans les vidéos de scambaiting

Le tableau 1 fait état des buts des *scambaiters*, ainsi que les procédés appliqués pour les atteindre. Les quatre buts recensés sont la perte de temps, la prévention, le fait de ridiculiser, ainsi que le divertissement. Une description de chacun des procédés permet de déterminer de quelle manière ceux-ci ont été repérés dans les vidéos.

Perte de temps

Le but de faire perdre du temps n'est pas nécessairement recherché tout au long du *scambaiting*. Par exemple, la perte de temps est recherchée durant les appels, mais ne l'est pas lors de la confrontation, étant donné que le *scambaiter* cherche à mettre fin à l'appel et donc au *scambaiting* en cours. Les propos liés directement à la perte de temps sont des expressions parfois utilisées par les *scambaiters*. Par exemple (paraphrases) : « je vais prendre mon temps durant la vidéo », « la perte de temps est l'un des objectifs à atteindre », « le but de l'appel est de le faire durer minimalement une heure ». Néanmoins, la recherche de ce but n'est pas souvent textuellement évoquée, ce qui nous pousse à examiner l'impact des deux autres procédés pour mieux comprendre cette finalité.

Le fait de feindre de faire des actions (inaction) a été identifié à quelques reprises dans les vidéos d'un des *scambaiters*. Par exemple, celui-ci va faire semblant d'aller à la salle de bain ou

Tableau 1 – Buts et procédés des *scambaiters*

Buts et procédés	Description
Perte de temps	La recherche de perte de temps peut être présente tout au long du *scambaiting* ou à des moments précis, par la mise en place sporadique de procédés.
Propos liés à la perte de temps	Le *scambaiter* dit textuellement des termes/expressions reliés à la perte de temps souhaitée.
Inaction	Une action est dite être posée, mais ne l'est pas réellement. Le *scambaiter* dit durant l'appel qu'il doit poser un comportement sans le faire réellement, prolongeant la durée de l'appel volontairement.
Actions posées	Une action qui est posée ou une parole qui est dite qui est interprétée comme faisant perdre du temps au fraudeur. La durée de l'appel est prolongée volontairement.
Prévention	La recherche de la prévention peut être présente tout au long du *scambaiting* ou à des moments précis, par la mise en place sporadique de procédés.
Sensibilisation	Comportement/parole/geste lié à la sensibilisation des internautes : passe par l'explication du processus de fraude ou par l'utilisation de message préventif face aux risques liés à la fraude au soutien technique.
Dénonciation	Lorsqu'il y a mention, par le *scambaiter*, que les autorités compétentes seront contactées ou encore lorsque le *scambaiter* fait mention d'une dénonciation sur un site dédié aux signalements de fraudes.
Ridiculiser	Le fait de vouloir ridiculiser peut être présent tout au long du *scambaiting* ou à des moments précis, par la mise en place sporadique de procédés.
Insulte	Insultes ou propos mesquins ou désobligeants envers le fraudeur ou ses compétences en informatique.
Confrontation	Le *scambaiter* révèle la vraie nature de la conversation et confronte le fraudeur sur les comportements illégaux qu'il commet.
Propos liés à l'origine ethnique	Propos gratuits concernant la nationalité, l'ethnie ou l'accent du fraudeur.
Divertissement	La recherche du divertissement peut être présente tout au long du *scambaiting* ou à des moments précis, par la mise en place sporadique de procédés.
Propos liés au divertissement	Le *scambaiter* dit textuellement des termes/expressions reliés au divertissement à son propre divertissement ou à celui souhaité pour les internautes.
Humour	Plusieurs techniques utilisées pour faire rire ou susciter l'amusement du *scambaiter* ou des internautes.
Fausse panique	Mots qui semblent dépeindre chez le *scambaiter* une peur, une crainte et/ou une inquiétude en début de l'appel ou en cours d'appel.

va feindre d'aller chercher son portefeuille. La perte de temps se manifeste aussi par des actions qui sont posées intentionnellement par les *scambaiters*. Ces actions peuvent être de raconter la vie de l'individu qu'ils personnifient ou de dire qu'ils ne comprennent pas les consignes que les fraudeurs donnent et de les faire répéter. Les *scambaiters* peuvent aussi utiliser des interfaces désuètes ou qui ne peuvent être prises en charge par les faux centres de soutien technique rendant ainsi la connexion à l'ordinateur plus longue ou même impossible.

Ces comportements ou cette inaction sont considérés comme faisant perdre du temps au fraudeur, puisque la durée de l'appel est volontairement prolongée.

Tous les *scambaiters* ont au moins un comportement lié à la perte de temps dans minimalement une vidéo. Toutefois, bien que ce but soit recherché par tous les *scambaiters* étudiés, on peut constater une différence en ce qui a trait à la fréquence de l'utilisation des procédés.

Prévention

La prévention s'articule de différentes manières chez les *scambaiters*. En effet, certains profitent de leur plateforme pour communiquer des messages de prévention face aux risques et aux dangers de la fraude en ligne. Parfois, cette prévention se fait à travers l'explication du processus de fraude. La sensibilisation des internautes est alors possible par ces deux mécanismes. L'ensemble des *scambaiters* à l'étude, dans une ou plusieurs vidéos, vont dépeindre en entièreté ou en partie, et ce, de différentes manières, le processus de la fraude au soutien technique. De plus, les *scambaiters* vont mentionner, dans trois vidéos sur quinze, que les actes répréhensibles des fraudeurs et certains éléments les facilitant seront dénoncés aux autorités compétentes ou encore sur des sites de signalement de cas de fraude en ligne.

Ridiculiser

Le but de ridiculiser les fraudeurs est présent dans les vidéos de deux des trois *scambaiters* à l'étude. Étant donné qu'il s'agit d'une fraude au soutien technique, les fraudeurs devraient démontrer un minimum de capacités en informatique, puisqu'ils personnifient des techniciens travaillant pour Microsoft. Les **insultes** portant sur l'insuffisance de connaissances et compétences en informatique des fraudeurs mettent ainsi en évidence le manque d'aptitude de ceux-ci à mener à bien une fraude. Des insultes attaquant personnellement les fraudeurs sont aussi dénotées dans les vidéos visionnées. Les *scambaiters* vont généralement faire usage des insultes à deux moments dans les vidéos, soit en commentant les agissements des fraudeurs avec les internautes qui écoutent l'échange en direct ou encore lors de la confrontation. Ces insultes sont variées (par exemple : « connard », « enfoiré », « bâtard », « incompétent », « sale pute »).

La **confrontation** est relativement semblable pour les deux *scambaiters* qui la réalisent. Celle-ci vise à dévoiler leur identité et/ou à simplement mentionner qu'ils sont au courant de la tentative de fraude en cours. La confrontation peut aussi être un moment où le *scambaiter* pose des questions au faux technicien sur ses agissements frauduleux.

Deux des trois *scambaiters* vont avoir des propos qui ont été interprétés comme étant liés à l'origine ethnique du fraudeur. Plus précisément, ils vont avoir des propos sur l'accent des fraudeurs ou encore vont avoir des paroles dont le but est de se moquer de leur accent. Néanmoins, sur l'ensemble des vidéos analysées seulement deux commentaires liés à l'origine ethnique sont faits.

Divertissement

La présence du divertissement est apparente tant lorsque la vidéo est une rediffusion d'une vidéo en direct (par exemple provenant de la plateforme Twitch) que lorsque la vidéo est publiée directement sur YouTube. Il est possible de voir de quelle manière le divertissement est inclus dans le processus de *scambaiting* par l'observation de multiples comportements et paroles du *scambaiter*, qui peuvent apparaître quelques fois durant le *scambaiting* ou encore être présents tout au long de la vidéo. En effet, les *scambaiters* vont parfois avoir des propos directement liés au divertissement (par exemple (paraphrases) : « Amusez-vous bien », « C'était incroyable »), permettant de percevoir la recherche de cette finalité par les *scambaiters*. Avec l'humour il est possible de déceler si le divertissement est recherché par les *scambaiters*. Au moins un des procédés suivants, mesurant la présence de l'humour, se manifeste dans l'ensemble des vidéos analysées : le rire du *scambaiter*, le montage vidéo avec l'ajout de sons et d'images lors de la diffusion de l'appel de *scambaiting*, l'utilisation d'effets spéciaux et d'effets sonores directement durant l'appel, ainsi que des blagues. Tous ces comportements permettent de voir que le divertissement et l'amusement sont suscités chez les *scambaiters* durant les appels de *scambaiting*, mais aussi que l'emploi de techniques, paroles et gestes a pour objectif d'augmenter le divertissement de la communauté lors du visionnement des vidéos.

Les commentaires

Les commentaires sous les vidéos des *scambaiters* ont été analysés pour y examiner le contenu s'y retrouvant et ainsi observer l'impact des vidéos de *scambaiting* sur les internautes. Les thématiques et sous-thématiques qui ont été repérées sont exposées dans le tableau 2.

Discussion générale

Une grande partie des commentaires analysés (plus de 38% des commentaires) contiennent un terme étant considéré comme faisant partie de la thématique Discussion générale. Cette thématique est mesurée par la présence de compliments et de remerciements. Les compliments visent le *scambaiter* et sa pratique du *scambaiting*. De nombreux internautes félicitent et remercient le *scambaiter* pour ce qu'il accomplit tout en lui démontrant qu'ils apprécient la vidéo.

Tableau 2 – Le contenu des commentaires publiés par les internautes

Thématiques	Sous-thématiques	Description
Discussion générale	Compliment	Propos gentils ou qui félicitent, encouragent le *scambaiter* et/ou sa pratique de *scambaiting*.
	Remerciement	Mention d'un mot pour remercier le *scambaiter* lui-même, pour sa pratique du *scambaiting* ou encore pour remercier de l'impact de la vidéo.
Émotion	Empathie	Mention d'un terme pouvant laisser croire qu'il y a une empathie envers le fraudeur ou des mots compatissants.
Perte de temps		Mention d'un mot relié à la perte de temps ou à une action posée par le *scambaiter* ou son inaction et qui a pour but de faire perdre du temps.
Prévention	Propos liés à la prévention	Mention de mots ou termes liés à la prévention de la fraude en général et/ou par la pratique du *scambaiting*.
	Question éducative	L'internaute pose une question éducative sur le processus de fraude ou sur le *scambating*.
	Expérience	L'internaute décrit ou parle ou aborde une fraude ou une tentative de fraude personnelle ou qu'un de ses proches a vécue.
	Conseil	L'internaute offre un conseil, une idée ou une assistance sollicitée ou non concernant la protection contre la fraude.
Ridiculiser	Insulte	Insultes ou propos mesquins ou désobligeants envers le fraudeur ou ses compétences en informatique.
	Commentaire lié à l'origine ethnique	Propos gratuits concernant la nationalité, l'ethnie ou l'accent du fraudeur.
Divertissement		Mots ou termes reliés à l'action de se divertir, de se distraire, d'occuper son temps de façon agréable ou mots reliés à l'appréciation de la vidéo ou en lien avec le rire/l'amusement procuré.

Les remerciements peuvent être employés seuls, pour remercier le *scambaiter* du divertissement que sa vidéo a procuré et/ou pour la prévention qui découle de cette pratique.

Perte de temps

Quelques internautes vont mentionner, dans leurs commentaires, qu'ils perçoivent la perte de temps qui a été occasionnée par le *scambaiter*. En effet, l'expression « perte de temps » a été remarquée à quelques reprises. De plus, deux commentaires font référence au terme « raconte ta vie » faisant ainsi allusion à une action posée par les *scambaiters* ayant pour but de faire perdre du temps. Par conséquent, certains internautes vont percevoir que les *scambaiters* ont des comportements visant à faire perdre du temps aux fraudeurs. Toutefois, bien que l'objectif de perte de temps soit clairement établi dans la littérature comme étant inhérent au *scambaiting,* la majorité des commentaires ne portent pas sur cette finalité (1,2%) (Smallridge et al., 2016 ; Laato et Rauti, 2021 ; Tuovinen et Röning, 2007).

De plus, le contenu relié à la perte de temps se retrouve majoritairement dans les commentaires sous les vidéos d'un *scambaiter*, pour qui le but de faire perdre du temps est clairement recherché.

Prévention

Des propos directement liés à la prévention, tels que des messages de sensibilisation ou encourageants à la dénonciation et au signalement ont été notés dans les commentaires. Certains commentaires vont mettre en évidence que bien que les vidéos soient amusantes et divertissantes, la prévention et la sensibilisation sont également possibles par leur écoute. De même, certains internautes vont expliquer et détailler des expériences de fraude ou tentative de fraude qu'ils ont vécues. Ce type de commentaires participe à la prévention de ce type de crime de deux manières. D'une part, il est possible de remarquer que les internautes sont sensibilisés à la fraude au soutien technique avec l'écoute des vidéos, puisqu'ils sont capables de reconnaître que c'est cette tentative de fraude ou cette fraude qu'ils ont vécue. D'autre part, la lecture de ces expériences personnelles peut permettre la sensibilisation d'autres internautes aux techniques utilisées par les fraudeurs.

Ridiculiser

Des termes et des mots dénigrants et ridiculisant personnellement les faux techniciens ont été repérés dans les sections commentaires, tels que « vache », « ces saloperies », « vermine », « bande de merde », « ordure », « con ». Bien que des insultes dénigrant les compétences informatiques des fraudeurs ont été repérées dans les commentaires, ceux-ci sont en plus petite quantité que les insultes formulées directement contre le fraudeur. D'ailleurs, peu importe si les *scambaiters* verbalisent ou non des insultes lors des vidéos, celles-ci se retrouveront dans les commentaires publiés. Les commentaires liés à l'origine ethnique du fraudeur tenu par les internautes inclus des propos portant sur l'accent, la nationalité, l'endroit où le faux technicien provient (ou semblait provenir) et l'ethnicité. Il est important de noter que, sur l'ensemble des commentaires étudiés, peu ont du contenu abordant l'origine ethnique du fraudeur (2%).

Divertissement

Les termes ou mots liés à l'humour, soit « rire », « rigoler », « ri », « mdr », « ptdr », « régales », « plaisir », etc. ou encore certaines expressions telles que « XD », « j'aime ou j'adore » ont été catégorisés comme démontrant des signes de divertissement chez les internautes. Plusieurs commentaires ont au moins un mot ou expression relié au divertissement procuré par l'écoute de la vidéo (37%). Ces termes peuvent être employés seuls, en spécifiant un passage de la vidéo qui les a fait rire ou un moment qu'ils ont aimé. Chacune des vidéos analysées ont plusieurs milliers de visionnements ainsi que de nombreux « j'aimes » permettant de supposer

que les internautes ont apprécié les vidéos. Toutefois, le nombre de « j'aime » d'une vidéo ne reflète pas nécessairement le nombre de visionnements.

Discussion

Les objectifs principaux de la recherche étaient de mettre de l'avant les buts et les procédés des *scambaiters* à travers leur pratique du *scambaiting* et de mieux comprendre l'effet de la diffusion de ce type de vidéos sur les internautes. Les buts repérés et expliqués dans les études précédentes sont les mêmes que ceux trouvés dans la présente recherche (Laato et Rauti, 2021 ; Sorell, 2019 ; Ross et Logi, 2021 ; Dynel et Ross, 2021). Le contenu des commentaires a également été examiné pour voir si les finalités recherchées par les *scambaiters* étaient retenues par les citoyens.

Une des hypothèses de la présente recherche était que bien que les vidéos de *scambaiting* présentent un aspect préventif en matière de fraude, le but final recherché par les *scambaiters* serait le divertissement. La même hypothèse a été posée pour les commentaires, c'est-à-dire que l'élément le plus illustré dans les commentaires, de par des termes, des mots et des expressions, serait le divertissement engendré par l'écoute des vidéos. Ces hypothèses sont confirmées par les résultats de l'étude. Effectivement, les *scambaiters* auront une réaction favorable (par exemple, rire) aux nombreux comportements, paroles et techniques utilisées pour augmenter le divertissement dans leurs vidéos. Il est possible de conclure qu'un des buts principaux qui est recherché par *scambaiters* est d'avoir du plaisir sans que les fraudeurs ne le sachent (Dynel et Ross, 2021). Les commentaires publiés par les internautes vont également contenir plus de termes reliés au divertissement, et ce, comparativement aux autres thématiques permettant de déceler l'impact des vidéos (perte de temps, prévention, ridiculiser). Ce résultat est alors similaire à celui de Laato et Rauti (2021, p.741) évoquant que les « *scambaiting* videos are primarily watched for entertainment ». De plus, les commentaires laissés sous l'ensemble des vidéos sont variés. Tel que l'énonce Dynel (2014), les commentaires peuvent porter sur la vidéo en tant que telle (donc des sujets et éléments qui y sont expliqués et abordés), sur des éléments ne faisant pas directement référence au contenu de la vidéo (donc des sujets autres ou des éléments reliés de près ou de loin à ceux abordés) ou encore sur le créateur de contenu ou le youtubeur directement, ce qui est dénoté dans les commentaires analysés dans la présente étude. Par exemple, du contenu remerciant ou offrant des compliments est présent sous l'ensemble des vidéos et en relativement grande quantité (38%). Les quatre buts recherchés par les *scambaiters* sont évoqués de différentes manières par l'audience. Notamment, plusieurs commentaires portent sur la prévention possible découlant de ce type de contenu, ainsi que sur le divertissement occasionné par l'écoute des vidéos. Cette diversité de commentaires permet de conclure que les vidéos ont différents impacts sur l'audience. Tel que mentionné dans la littérature, il y aurait une influence possible entre le contenu des vidéos et celui des commentaires publiés sous celles-ci (Porter et Hellsten, 2014 ; Edgerly et al., 2013).

Les *scambaiters* veulent faire perdre du temps aux fraudeurs par tous les moyens possibles, tel que le constatent Laato et Rauti (2021). Ces techniques se manifestent par des actions ayant pour but de faire perdre du temps et par des comportements considérés comme de l'inaction. Ces stratégies, qui sont aussi abordées par Ross et Logi (2021), Laato et Rauti (2022) et Sorell (2019), confirment que la perte de temps souhaitée est bel et bien illustrée par ces divers procédés. Il est important de noter que la recherche de ce but est davantage illustrée par les actions posées ou l'inaction des *scambaiters* que par des paroles mettant en évidence cet objectif. Les internautes vont aussi à quelques reprises faire référence aux procédés mis en place par les *scambaiters*, permettant de conclure que certains d'entre eux remarquent la perte de temps souhaitée par l'activité du *scambaiting*. Laato et Rauti (2021, p.745) vont aussi mentionner (bien qu'ils trouvent que le divertissement est primordial dans les vidéos de *scambaiting*) que la recherche de perte de temps est « la raison initiale » [traduction] de faire du *scambaiting*. Toutefois, avec l'interprétation que nous faisons des résultats de l'étude, pour ce qui est du *scambaiting* perpétré contre la fraude au soutien technique, nous supposons que le divertissement est très important pour les *scambaiters*. En effet, ceux-ci utilisent plusieurs techniques (blagues, effets vocaux, ajout de sons et d'images durant l'appel ou lors du montage) pour accroître l'amusement lié à la pratique du *scambaiting*. De plus, la finalité de divertissement est davantage prédominante dans les vidéos de deux *scambaiters*, étant donné que le divertissement est combiné, parfois, au fait de ridiculiser les fraudeurs. En effet, la combinaison de communications agressives et humoristiques est observée dans leurs vidéos. Il faut néanmoins préciser que le but de faire perdre du temps est une caractéristique intrinsèque à la pratique de *scambaiting* (Smallridge et al., 2016 ; Sorell, 2019). La perte de temps est donc recherchée de façon inhérente par les *scambaiters*, mais à différents degrés, selon les techniques employées par ces derniers.

Selon certaines études, l'explication du modus operandi et des particularités des arnaques est habituellement présente dans la pratique du *scambaiting* (Dynel et Ross, 2021 ; Ross et Logi, 2021). Effectivement, ce type de sensibilisation est l'un des plus présents dans les vidéos de *scambaiting* analysées et sert à prévenir la fraude en ligne. Laato et Rauti (2021) ont trouvé que les vidéos de *scambaiting* purement à caractère récréatif ont aussi une partie éducationnelle. Effectivement, dans la présente recherche, plusieurs vidéos ayant de multiples manifestations de divertissement ont également un caractère préventif, soit lorsque les *scambaiters* discutent des techniques de fraudes utilisées et des incongruences et erreurs posées par les fraudeurs. Le potentiel de sensibilisation des vidéos a été démontré dans plusieurs études portant sur divers sujets et enjeux scientifiques. Par exemple, les vidéos portant sur les changements climatiques sensibiliseraient les internautes sur cette problématique environnementale (Shapiro et Mark, 2014).

D'ailleurs, pour ce qui est de la prévention, il est pertinent de mentionner que le ton utilisé par les *scambaiters* et la manière dont ils traitent la fraude au soutien technique peut, par moment, avoir un impact sur le contenu des commentaires publiés sous les vidéos (Edgerly et

et al., 2013). Ainsi, plusieurs internautes feront des commentaires à caractère préventif, tel que mentionné ci-haut dans la présentation des résultats. L'utilisation de moyens de sensibilisation par les *scambaiters* se reflète donc dans les commentaires. Contrairement aux résultats de Nabi et ses collègues (2007), qui abordent les sujets d'humour et de politique, l'utilisation de l'humour par les *scambaiters* n'a pas nécessairement nuit au développement d'une opinion face à l'enjeu de la fraude au soutien technique, puisqu'une petite partie des internautes font mention de la prévention possible avec ce type de contenu.

Les internautes vont également faire de la sensibilisation. En effet, les internautes ne vont pas seulement être conscients du caractère préventif de la pratique du *scambaiting*, mais vont aussi faire une forme de prévention en abordant leurs propres expériences. Donc, ce n'est pas seulement les *scambaiters* qui font de la sensibilisation en abordant le processus de fraude (Laato et Rauti, 2021), les internautes y participent également. Ainsi, une forme de prévention est présente dans les deux modes de communication. Par la rédaction de commentaires portant sur leurs expériences personnelles, les internautes publient du contenu varié à caractère préventif. Du fait que les internautes abordent des éléments ne faisant pas directement référence au contenu de la vidéo, nous supposons que ces derniers sont sensibilisés à l'impact de la fraude au soutien technique en général et non uniquement à ce qui est rapporté dans les vidéos. Les résultats de Shapiro et Mark (2014) sur le potentiel de prévention des vidéos YouTube sont en concordance avec les résultats de la présente étude.

L'étude de Yuan et Lu (2022), portant sur le style humoristique, mentionne que des paroles qui sont perçues comme humoristiques pourraient amener des émotions positives à l'audience. Les chercheurs ajoutent que les internautes qui écoutent des vidéos sur YouTube s'attendent habituellement à ce qu'elles soient agréables et amusantes (Yuan et Lu, 2022). Par ailleurs, les individus employant différents types de communication dans leurs publications sur les médias sociaux, dont les styles humoristique et sarcastique, augmenteraient le nombre de visites sur leurs sites (Anderson and Becker, 2018). Un nombre de visionnements plus élevés augmenterait alors la popularité des vidéos (Chau, 2010). Pour augmenter le plaisir de l'audience synchrone, Sorell (2019) rapporte que l'humour peut faire partie intégrante du processus de *scambaiting*. L'ensemble de ces éléments pourraient expliquer pourquoi les *scambaiters* mettent en place des techniques pour accroître le divertissement de l'audience.

De surcroît, Dynel et Ross (2021, p.13) évoquent que l'humour est souvent perpétué « aux dépens » [traduction] des fraudeurs. Ainsi, une partie du divertissement proviendrait du fait que les arnaqueurs ne sont pas informés de l'amusement, des blagues et des commentaires qui sont faits (Dynel et Ross, 2021 ; Sorell, 2019). Dans les vidéos analysées, les *scambaiters* vont souvent utiliser les éléments liés au divertissement (blagues, effets spéciaux, effets vocaux) sans que les fraudeurs ne comprennent ce qui se passe ou en aient conscience. Nous supposons que le divertissement de l'audience est possiblement accru par le fait que les vidéos de *scambaiting* sont publiés sur YouTube sans que les fraudeurs ne le sachent. Ainsi,

les propos de Dynel et Ross (2021) sont en concordance avec les résultats de la présente étude.

Également, l'humour agressif est un type de communication qui est relevé comme étant présent dans certains vidéos de *scambaiting*, ainsi que dans les commentaires. Certains participants de l'étude de Yuan et Lu (2022) mentionnent que l'utilisation d'une communication agressive pourrait parfois augmenter la perception de l'humour dans les vidéos. Le fait de ridiculiser les fraudeurs contribuerait à une forme de divertissement qui est recherché par les *scambaiters* (Laato et Rauti, 2021). En effet, l'humour et l'amusement peuvent être liés à la dévalorisation d'un individu (Ferguson et Ford, 2008).L'humour agressif est également perçu lorsque les *scambaiters* utilisent la moquerie, les insultes et la critique envers les fraudeurs et que cela suscite leur rire (Janes et Olson, 2000 ; Yuan et Lu, 2022 ; Laato et Rauti, 2021). Par exemple, dans les vidéos analysées, des insultes concernant le manque de connaissances informatiques des fraudeurs sont formulées et viendraient soutenir l'idée que ceux-ci n'auraient pas les compétences nécessaires pour être des techniciens en soutien informatique (Dynel et Ross, 2021; Rauti et Leppänen, 2017). Le faire de vouloir ridiculiser le fraudeur est toutefois seulement discerné dans les vidéos de deux *scambaiters* sur trois. De plus, il est possible de distinguer que certains internautes qui formulent une insulte envers un fraudeur vont également ajouter, dans le même commentaire, un mot ou une expression reliée au divertissement procuré par l'écoute de la vidéo. Du contenu insultant le fraudeur est également parfois combiné avec un mot de félicitations envers le travail du *scambaiter*. Ce type de contenu, même s'il n'apparaît pas en grand nombre dans les commentaires, permet de voir le lien qui existe entre l'agressivité et l'amusement. Ainsi, le fait de ridiculiser ou d'insulter les fraudeurs pourrait contribuer au divertissement des *scambaiters*, mais aussi à celui de l'audience synchrone ou asynchrone (Dynel, 2014).

Certains chercheurs mettent en garde que le *scambaiting* et le vigilantisme en ligne peuvent exacerber des comportements racistes, entre autres la recherche et la publication de trophées (Yékú, 2020 ; Nakamura, 2014). Peu de contenu lié à l'origine ethnique du fraudeur a été repéré dans les vidéos de *scambaiting*, ainsi que dans les commentaires. Les résultats de l'étude de Laato et Rauti (2021) sont en concordance avec cette observation. De plus, nous supposons aussi que peut-être que les *scambaiters* évitent d'avoir ce genre de propos, ne voulant pas que leurs vidéos soient retirées de la plateforme due à la monétisation possible de ce contenu (YouTube, 2022a ; YouTube, 2022b). Toutefois, ceci n'est qu'une hypothèse. Peu d'internautes, dans les commentaires, vont tenir des propos liés à l'origine ethnique des fraudeurs, tel que mentionné ci-haut. Pour expliquer ce résultat, nous supposons que soit les internautes ne tiennent pas ce genre de propos ou encore que les commentaires proférant de la haine et donc qui sont à l'encontre des règles de publication sur YouTube sont supprimés par les modérateurs de la plateforme (YouTube, 2022b).

Tel qu'il a été mentionné dans la revue de littérature, les éléments abordés dans différents mé-

dias numériques, ainsi que la manière dont ils sont traités peuvent influencer le ton des commentaires (Edgerly et al., 2013 ; Möller et al., 2019). Dans le cas présent, l'utilisation ou non d'incivilités par les *scambaiters* ou leurs comportements hostiles envers les fraudeurs n'influencent que très peu l'opinion des internautes. En effet, les internautes formulent des commentaires insultant les fraudeurs, et ce, sous l'ensemble des vidéos de *scambaiting* analysées, peu importe si des insultes sont employées par les *scambaiters*. Toutefois, peu de commentaires publiés sous les vidéos peuvent être considérés comme du flaming, puisque, bien que du contenu insultant les fraudeurs soit présent dans les commentaires, ces derniers sont présents en quantité limitée. Également, il y a peu de commentaires négatifs qui visent le contenu des vidéos, le *scambaiter* ou sa pratique de *scambaiting*. Ainsi, tout comme dans l'étude de Khan et Jacob (2013), où 11% des commentaires analysés pouvaient être considérés comme du flaming, peu de commentaires dans la présente étude peuvent être considérés comme hostiles. La majorité des commentaires, tant dans la présente étude que dans celle de ces deux auteurs, exprime de l'appréciation envers le contenu de la vidéo (Khan et Jacob, 2013).

Limites de l'étude

Une limite de l'étude est la taille de l'échantillon. En effet, celui-ci est composé de quinze vidéos provenant de trois chaînes de *scambaiting* et de 413 commentaires, ce qui est assez petit. Puisque nous voulions comparer des individus qui pratiquent le *scambaiting* contre des fraudeurs au soutien technique, ceci a limité le nombre de vidéos disponibles et pertinentes. La saturation a toutefois été atteinte avec cet échantillon. Effectivement, les *scambaiters* utilisent généralement les mêmes étapes pour procéder au *scambaiting* puisque le processus de la fraude au soutien technique est assez statique. Ainsi, le visionnement de ce nombre de vidéos était suffisant pour répondre à la première question de recherche. Une généralisation de l'ensemble des buts et des procédés pour tous les *scambaiters* est néanmoins difficile. Une autre limite de la recherche est qu'il n'y a pas eu d'accord interjuge pour supporter la codification du contenu des vidéos et des commentaires. Ainsi, un biais de codification est présent. Bien que certaines études aient publié sur le sujet et que ceci a permis de définir certaines thématiques et sous-thématiques, il y a eu, pour certains procédés mis en place par les *scambaiters*, une interprétation. La méthode de collecte de données d'étude de cas peut parfois amener une certaine subjectivité à la catégorisation des éléments recherchés dans les études (Barlatier, 2018). Cependant, les *scambaiters* à l'étude utilisent régulièrement les mêmes procédés pour atteindre les buts qui sont recherchés (perte de temps, prévention, ridiculiser et divertissement) ceci à aider à réaliser une catégorisation.

Conclusion

La présente étude a permis de faire un portrait des différents buts et procédés utilisés par les *scambaiters* francophones lors de la publication de vidéos sur le *scambaiting* sur des chaînes YouTube francophones. L'analyse des commentaires sous chacune des vidéos analysées a permis de discerner l'impact de ce type de contenu sur les internautes. La présente étude a démontré que les buts recherchés par les *scambaiters* le sont à divers degrés, selon les techniques employées par ces derniers (tel que le mentionnent Laato et Rauti (2021) dans leur étude). Le divertissement est présent dans l'ensemble des vidéos et plusieurs procédés sont appliqués par les *scambaiters*, participant ainsi à leur propre divertissement et à celui des internautes. Les buts et procédés utilisés par les *scambaiters* auront également un impact sur les commentaires publiés par ceux qui visionnent les vidéos. Les internautes retiennent davantage les techniques utilisées et les paroles et gestes posés des *scambaiters* qui leur ont procuré du divertissement. De plus, le fait de vouloir ridiculiser par l'emploie d'insultes se voit dans la pratique du *scambaiting* (bien qu'il ne soit pas présente dans l'ensemble des vidéos) et aussi dans les commentaires publiés par les spectateurs. Ce but, bien qu'il ne soit pas le premier pour faire ce type d'activité est une composante pouvant se combiner aux techniques de divertissement. Certains internautes abordent la prévention et la sensibilisation possible par cette pratique. De plus, l'explication du modus operandi appliqué par les fraudeurs permet la sensibilisation à la fraude au soutien technique. Ce type de sensibilisation est effectuée d'une part par les créateurs de contenu et d'autre part par ceux qui visionnent les vidéos. En effet, les internautes vont aborder leurs propres expériences de fraude ou de tentative de fraude dans les commentaires, ce qui permet de sensibiliser les autres internautes aux différentes tactiques appliquées par les arnaqueurs. Il y aurait ainsi un potentiel de sensibilisation à la fraude au soutien technique par la diffusion de vidéos de *scambaiting* sur YouTube.

Pour finir, il serait pertinent, pour une prochaine étude, de s'adresser directement à des *scambaiters* pour recueillir davantage d'éléments sur leurs buts et procédés et ainsi avoir un regard impartial sur ce qu'ils veulent accomplir avec la publication de leurs vidéos. Ainsi, il serait possible d'avoir leurs perceptions sur l'utilité des vidéos en termes de prévention et ce que représente réellement cette création de contenu pour eux. Par exemple, est-ce qu'il y a un souhait de faire de la prévention, n'est-ce que pour le divertissement et pour une source de revenus considérable ou encore est-ce qu'il considère cette pratique comme leur métier? Il serait ainsi possible d'avoir leur opinion sur le sujet, tout en ajoutant aux connaissances actuelles sur le *scambaiting*.

Références

Allgaier, J. (2020). Science and medicine on YouTube. *Springer EBooks*, 7–27. https://doi.org/10.1007/978-94-024-1555-1 1

Acuna, N., Vento, I., Alzate-Duque, L. et Valera, P. (2019). Harnessing digital videos to promote cancer prevention and education: a systematic review of the literature from 2013–2018. *Journal of Cancer Education*, *35*(4), 635–642. https://doi.org/10.1007/s13187-019-01624-0

Anderson, A.A. et Becker, A.B. (2018). Not just funny after all: Sarcasm as a catalyst for public engagement with climate change. *Science Communication*, *40*(4), 524-540 https://doi.org/10.1177/1075547018786560

Barlatier, P-J. (2018). Chapitre 7. Les études de cas. Dans F. Chevalier (dir.), *Les méthodes de recherche du DBA* (p.126-139). *Business Science Institute*. DOI: 10.3917/ems.cheva.2018.01.0126.

Berland, G., Elliott, M. N., Morales, L. S., Algazy, J. I., Kravitz, R. L., Broder, M. S., Kanouse, D. E., Muñoz, J., Puyol, J., Lara, M., Watkins, K. E., Yang, H. P. et McGlynn, E. A. (2001). Health information on the Internet. *JAMA*, *285*(20), 2612. https://doi.org/10.1001/jama.285.20.2612

Brooks, D. J. et Geer, J. G. (2007). Beyond negativity: The effects of incivility on the electorate. *American Journal of Political Science*, *51*(1), 1–16. https://doi.org/10.1111/j.1540-5907.2007.00233.x

Button, M., Blackbourn. D. et Tunley, M. (2015). 'The not so thin blue line after all?' Investigative resources dedicated to fighting fraud/economic crime in the United Kingdom. *Policing: A Journal of Policy and Practice*, *9*(2), 129-142. https://doi.org/10.1093/police/pau037

Button, M. et Cross, C. (2017a). 1 - *The dark side of crime. Cyber frauds, scams and their victims* (1re éd.). Routledge.

Button, M. et Cross, C. (2017b). 7 - *Policing and punishment for cyber frauds and scams. Cyber frauds, scams and their victims* (1re éd.). Routledge.

Centre antifraude du Canada. (2022). *Gouvernement du Canada*. https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

Centre antifraude du Canada. (2023, 28 février). *Gouvernement du Canada*. https://antifraudcentre-centreantifraude.ca/scams-fraudes/service-fra.htm#a7

Chaire de recherche en prévention de la cybercriminalité (CRPC). (2022a). *À propos : Mission et objectifs*. https://www.prevention-cybercrime.ca/

Chaire de recherche en prévention de la cybercriminalité. (CRPC). (2022b). *Note de synthèse. La fraude au soutien technique*. https://www.prevention-cybercrime.ca/fraude-soutien-technique

Chau, C. (2010). YouTube as a participatory culture. *New Directions for Youth Development*, 2010(128), 65–74. https://doi.org/10.1002/yd.376

Code criminel (2023). *Code criminel / Codification bilingue 2023*, Carswell, Éditions Yvon Blais.

Dove, M. (2020). *What is fraud and who are the fraudsters?. The psychology of fraud, persuasion and scam techniques* (1re éd., 22-32). Routledge. https://www.taylorfrancis.com/pdfviewer/

Durkin, K. F. et Brinkman, R. (2009). 419 Fraud: A Crime without Borders in a Postmodern World. *International Review of Modern Sociology*, *35*(2), 271–283.

Dynel, M. (2014). Participation framework underlying YouTube interaction. *Journal of pragmatics*, 73, 37-52. DOI: 10.1016/j.pragma.2014.04.001

Dynel, M. (2016). "Trolling is not stupid": Internet trolling as the art of deception serving entertainment. *Intercultural Pragmatics*, *13*(3): 353–381. https://doi.org/10.1515/ip-2016-0015

Dynel, M. et Ross, A. S. (2021). You don't fool me: On scams, scambaiting, deception, and epistemological ambiguity at R/scambait on Reddit. *Social Media + Society*, *7*(3). https://doi.org/10.1177/20563051211035698

Edgerly, S., Vraga, E. K., Dalrymple, K. E., Macafee, T. et Fung, T. K. F. (2013). Directing the dialogue: The relationship between YouTube videos and the comments they spur. *Journal of Information Technology & Politics*, *10*(3), 276–292. https://doi.org/10.1080/19331681.2013.794120

Edwards, M., Peersman, C. et Rashid, A. (2017). Scamming the scammers: Towards automatic detection of persuasion in advance fee frauds. *Proceedings of the 26th International Conference on World Wide Web Companion - WWW '17 Companion*, 1291-1299. https://doi.org/10.1145/3041021.3053889

Erviti, M. C. et Stengler, E. (2016). Online science videos: An exploratory study with major professional content providers in the United Kingdom. *Journal of Science Communication*, *15*(06), A06. https://doi.org/10.22323/2.15060206

Federal Bureau of Investigation. (2022). *Internet crime report 2021. Internet crime complaint center*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ferguson, M. K. et Ford, T.E. (2008). Disparagement humor: A theoretical and empirical review of psychoanalytic, superiority, and social identity theories. *Humor: International Journal of Humor Research*, *21*(3). https://doi.org/10.1515/humor.2008.014

Fitzgerald, M. (2014, Janvier). *Falling Crime or Flawed Statistics*. Dans Presentation at BSC/Mannheim seminar, LSE, 15.

Gagliano, M.E. (1988). A literature review on the efficacy of video in patient education. *J Med Educ*, *63*, 785–792.

George, J., Marett, K. et Tilley, P. (2004). Deception detection under varying electronic media and warning conditions. *37th Annual Hawaii International Conference on System Sciences*, 2004. Proceedings of the. https://doi.org/10.1109/hicss.2004.1265080

Gouvernement du Canada. (2022, 12 mai). *Types de fraudes*. https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/vos-outils-financiers/fraude/fraude-1/3.html

International Telecommunications Union-UNESCO. (2017, septembre). The State of Broadband 2017: Broadband Catalyzing Sustainable Development. *Broadband Commission*. https://www.itu.int/dms pub/itu-s/opb/pol/s-pol-broadband.18-2017-pdf-e.pdf

Janes, L. M. et Olson, J. M. (2000). Jeer pressure: The behavioral effects of observing ridicule of others. *Personality and Social Psychology Bulletin*, *26*(4), 474-485.

Johnston, L. (1996). What is vigilantism?. *British Journal of Criminology*, *36*(2), 220-236.

Khan, M. L. (2017). Social media engagement: What motivates user participation and consumption on YouTube?. *Computers in human behavior*, *66*, 236-247.

Khan, M. L. et Jacob, S. (2013). Advocacy, entertainment and news an analysis of user participation on Youtube. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2579596

Kim, J. (2012). The institutionalization of YouTube: From user-generated content to professionally generated content. *Media, Culture & Society*, *31*(1), 53-67. https://doi.org/10.1177/0163443711427199

Koong, K. S., Liu, L. C. et Wei, J. (2012). An examination of Internet fraud occurrences. Retrieved on 15th July, 441-449.

Ksiazek, T. B. (2018). Commenting on the News. Journalism Studies, 19(5), 650–673. https://doi.org/10.1080/1461670X.2016.1209977

Laato, S. et Murtonen, M. (2020). Improving synchrony in small group asynchronous online discussions. Trends and Innovations in Information Systems and Technologies, 215-224. https://doi.org/10.1007/978-3-030-45697-9 21

Laato, S. et Rauti, S. (2021). scambaiting as a form of online video entertainment: an exploratory study. Advances in Intelligent Systems and Computing, 738748. https://doi.org/10.1007/978-3-030-73689-7 70

Latha, K., Meena, K.S., Pravitha, M.R., Dasgupta, M. et Chaturvedi, S.K. (2020). Effective use of social media platforms for promotion of mental health awareness. Journal of Education and Health Prevention, 9(124), 1-6. DOI: 10.4103/jehp.jehp 90 20

Lea, M., O'Shea, T., Fung, P. et Spears, R. (1992). 'Flaming' in computer-mediated communication: Observations, explanations, implications. Dans M. Lea (dir.), Contexts of computer-mediated communication (pp. 89–112). London: Harvester Wheatsheaf.

Loveluck, B. (2019). The many shades of digital vigilantism. A typology of online self-justice. Global Crime, 21(3-4), 213-241. https://doi.org/10.1080/17440572.2019.1614444

Madathil, K. C., Rivera-Rodriguez, A., Greenstein, J. S. et Gramopadhye, A. K. (2015). Healthcare information on YouTube: A systematic review. Health Informatics Journal, 21(3), 173–194. https://doi.org/10.1177/1460458213512220

Maimon, D., Howell, C. J., Moloney, M. et Park, Y. S. (2020). An examination of email fraudsters' modus operandi. Crime & Delinquency. https://doi.org/10.1177/0011128720968504

McGuire, M. et Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research Report 75. London: Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/file/246749/horr75-summary.pdf

Miramirkhani, N., Starov, O. et Nikiforakis, N. (2016). Dial one for scam: A large-scale analysis of technical support scams. arXiv preprint arXiv:1607.06891.

Möller, A. M., Kühne, R., Baumgartner, S. E. et Peter, J. (2019). Exploring user responses to entertainment and political videos: An automated content analysis of YouTube. Social Science Computer Review, 37(4), 510–528. https://doi.org/10.1177/0894439318779336

Moor, P. J., Heuvelman, A. et Verleur, R. (2010). Flaming on YouTube. Computers in Human Behavior, 26(6), 1536–1546. https://doi.org/10.1016/j.chb.2010.05.023

Nabi, R. L., Moyer-Gusé, E. et Byrne, S. (2007). All joking aside: A serious investigation into the persuasive effect of funny social issue messages. Communication Monographs, 74(1), 29–54. https://doi.org/10.1080/03637750701196896

Nakamura, L. (2014). 'I WILL DO EVERYthing that am asked': scambaiting, digital show-space, and the racial violence of social media. Journal of Visual Culture, 13(3), 257–274. https://doi.org/10.1177/1470412914546845

National Crime Agency. (2016, Juillet). NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016 Need for a stronger law enforcement and business partnership to fight cyber crime. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/357-cyber-crime-assessment-2016/file

Poonia, A. S. (2014). Cyber crime: Challenges and its classification. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(6), 119-121.

Porter, A. J. et Hellsten, I. (2014). Investigating participatory dynamics through social media using a multideterminant "frame" approach: The case of climategate on YouTube*. *Journal of Computer-Mediated Communication*, *19*(4), 1024–1041. https://doi.org/10.1111/jcc4.12065

Rauti, S. et Leppänen, V. (2017). "You have a potential hacker's infection": A study on technical support scams. *Computer and Information Technology*. https://doi.org/10.1109/cit.2017.32

Reichl, F. (2019). From vigilantism to digilantism? *Springer EBooks*, 117–138. https://doi.org/10.1007/978-3-030-22002-0 7

Ross, A. S. et Logi, L. (2021). 'Hello, this is Martha': Interaction dynamics of live scambaiting on Twitch. *Convergence*, *27*(6), 1789-1810. https://doi.org/10.1177/13548565211015453

Scheibe, K., Fietkiewicz, K. J. et Stock, W. G. (2016). Information behavior on social live streaming services. *Journal of Information Science Theory and Practice*, *4*(2), 6–20. https://doi.org/10.1633/jistap.2016.4.2.1

Shao, G. (2009). Understanding the appeal of user-generated Media: A uses and gratification perspective. *Internet Research*, *19*(1), 7-25. https://doi.org/10.1108/10662240910927795

Shapiro, M. A. et Park, H. W. (2014). More than entertainment: YouTube and public responses to the science of global warming and climate change. *Social Science Information*, *54*(1), 115–145. https://doi.org/10.1177/0539018414554730

Signal-Arnaques. (2021, 15 mai). *Guide de Signal-Arnaques. Qu'est-ce que Signal-Arnaques*. https://guide.signal-arnaques.com/fr/signal-arnaques

Smallridge, J., Wagner, P. et Crowl, J.N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology*, *8*(1), 57.

Sood, A., Sarangi S., Pandey, A. et Murugiah, K. (2011). YouTube as a source of information on kidney stone disease. *Urology*, *77*(3), 558–562. https://doi.org/10.1016/j.urology.2010.07.536

Sorell, T. (2019). scambaiting on the spectrum of digilantism. *Criminal Justice Ethics*, *38*(3), 153-175. https://doi.org/10.1080/0731129x.2019.1681132

Statistique Canada. (2021, septembre). Échantillonnage. https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch13/5214895-fra.htm

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, *30*(1), 55-72. https://doi.org/10.1007/s13347-016-0216-4

Tuovinen, L. et Röning, J. (2007). Baits and beatings: vigilante justice in virtual communities. *Proceedings of CEPE*, 397-405

Wagner, C. (2009). Internet fraud on the rise. *The Futurist*, *43*(4), 15.

Waseem, F. M. (2018). Social network YouTube a source of earning. *IEEEP New Horizons Journal*, 46–49.

Yékú, J. (2020). Anti-Afropolitan ethics and the performative politics of online scambaiting. *Social Dynamics-a Journal of the Centre for African Studies University of Cape Town*. https://doi.org/10.1080/02533952.2020.1813943

Younes, M.A.B. (2019). Internet fraud to deceive email by using different technologies. *International Journal of Advanced Research in Computer Science*, *10*(1), 1-4. DOI: http://dx.doi.org/10.26483/ijarcs.v10i1.6349

YouTube. (2022a, janvier). *Monetisation for creators*. https://www.youtube.com/howyoutubeworks/product-features/monetization/#subscriptions

YouTube (2022b, janvier). Que fait YouTube pour protéger la communauté contre la haine et le harcèlement? https://www.youtube.com/intl/fr_lu/howyoutubeworks/our-commitments/standing-up-to-hate/

Yuan, S. et Lu, H. (2022). Examining a conceptual framework of aggressive and humorous styles in science YouTube videos about climate change and vaccination. *Public Understanding of Science*, *31*(7), 921–939. https://doi.org/10.1177/09636625221091490

Zingerle, A. et Kronman, L. (2011). Transmedia storytelling and online representations -- issues of trust on the Internet. *2011 International Conference on Cyberworlds*, 144-151. https://doi.org/10.1109/cw.2011.32

Zingerle, A. (2014). Towards a categorization of scambaiting strategies against online advance fee fraud. *International Journal of Art, Culture, Design, and Technology*, *4*(2), 39-50. https://doi.org/10.4018/ijacdt.2014070104