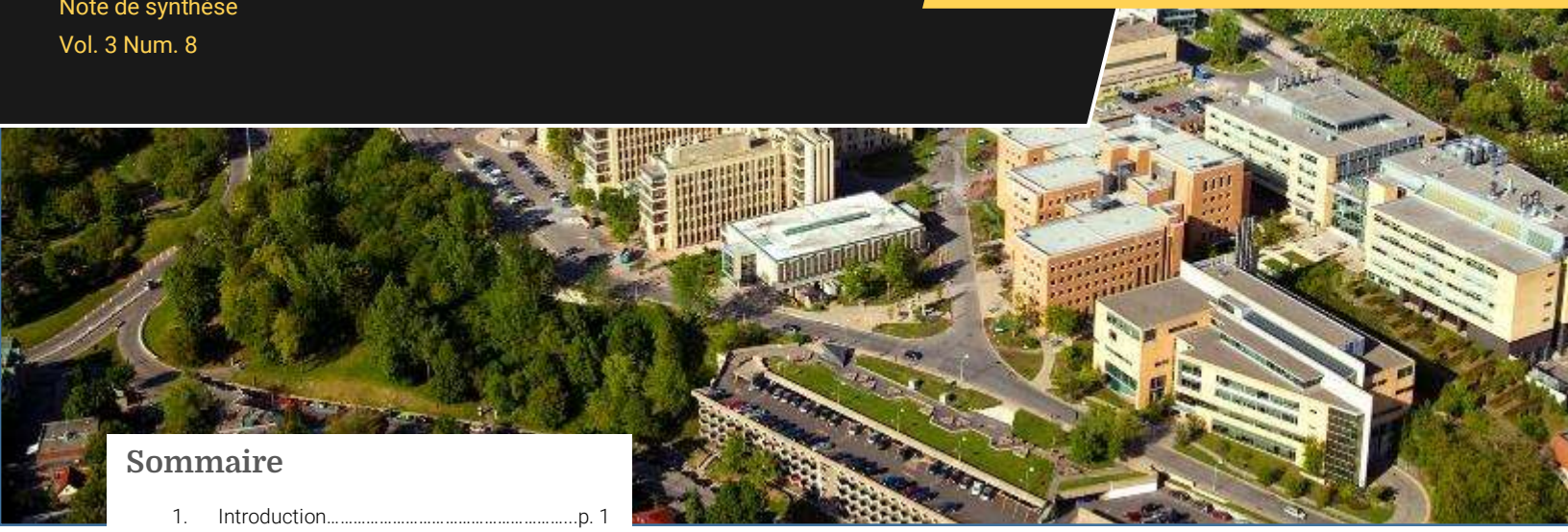
Le scambaiting

Jade Philibert, finissante au baccalauréat en criminologie

Note de synthèse
Vol. 3 Num. 8

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

Philibert, J. (2023). Analyse des buts et des procédés décelés dans les vidéos de scambaiting et l'impact de ce type de contenu sur les internautes. (Rapport de stage, UdeM). Disponible à https://www.prevention-cybercrime.ca/projets-de-recherche

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.

Introduction

Le Centre antifraude du Canada rapporte qu'au 31 décembre 2022, **56 352 personnes ont été victimes de fraudes ce qui représente près de 530 000 000$ de pertes**[1]. Ces statistiques ne sont pas négligeables et démontrent l'importance d'augmenter les efforts en matière de prévention de la cybercriminalité. En effet, les agences d'application de la loi peinent à répondre à la cybercriminalité, et certains citoyens, perçoivent le contrôle social formel comme insuffisant pour répondre adéquatement à la fraude[2,3].

Plusieurs mesures et initiatives, organisationnelles et nationales, s'adressant à un large éventail de la population, ont été mises en œuvre afin de sensibiliser la population aux enjeux des cyberfraudes. Toutefois, des initiatives, issues d'individus agissants seuls ou en groupe de citoyens mobilisés, participent également aux efforts de prévention et de sensibilisation.

Parmi ces dernières, le *scambaiting* sous forme de vidéos en ligne apparaît comme une pratique innovante. **Le *scambaiting* est une activité conduisant un individu (ci-après « *scambaiter* »)[4] à communiquer avec un fraudeur en se faisant passer pour une victime potentielle en se créant une fausse identité**[5,6]. Bien que la majorité des études scientifiques portant sur le *scambaiting* s'attardent davantage sur la fraude par paiement avancé (*advance-fee fraud*), dont la « Fraude 419 »[6,7,8], cette pratique est également utilisée pour contrer

d'autres types de fraudes. Cette note de synthèse dresse un portrait des motivations, des comportements adoptés et des types de *scambaiters* afin de mieux comprendre cette pratique.

Définition

Le *scambaiting* est une pratique par laquelle le *scambaiter* fait croire à un fraudeur qu'il succombe aux stratagèmes de fraude, et ce, principalement dans le but de faire perdre du temps à ce dernier[5]. Prenant place sur des forums de discussions permettant de relater leur interaction avec les fraudeurs, le *scambaiting* s'est peu à peu déplacé vers des plateformes de vidéos en ligne comme YouTube et est considéré comme une forme de divertissement qui permet également la prévention et la sensibilisation de certains types de fraude[9]. En effet, c'est au début des années 2000 que l'on voit apparaître les premières publications de vidéos présentant des échanges entre un fraudeur et le scambaiter[5,9]. **Une des caractéristiques du *scambaiting* filmé est qu'il peut être accompli devant une audience.** Deux formats de diffusion sont possibles, un format asynchrone et un format synchrone[10]. Les internautes peuvent ainsi écouter en direct l'échange entre le *scambaiter* et le fraudeur ou encore le visionner lors d'une rediffusion sur une plateforme en ligne[6,9]. Le public des chaînes de *scambaiting* ne cesse de croître étant donné sa facilité de diffusion et l'engouement grandissant pour la pratique[6,9]. Cette activité peut toutefois se faire sans diffusion ni public[7].

Une autre caractéristique du *scambaiting* est **l'utilisation de la tromperie par les deux parties prenant part à la conversation**[5,11]. En effet, le fraudeur et le *scambaiter* essaient de persuader leur interlocuteur du bienfondé de leur démarche. Cette conversation peut se faire par téléphone, par vidéoconférence, par courriel ou encore par messages textes[12]. Le moyen pour commettre la fraude influencera le choix de méthode de communication pour perpétrer le *scambaiting*. **La majorité du temps, le *scambaiting* est plutôt inoffensif**, puisque le *scambaite*r essaie de duper le fraudeur, tout en suivant des normes relativement éthiques[5,6]. Il s'agit, par exemple, de faire perdre du temps et donc, des opportunités aux fraudeurs[6], bien que les *scambaiters* puissent s'adonner à des pratiques plus ambiguës, à la limite du légal, voire illégal, comme, injecter des logiciels malveillants dans les ordinateurs des fraudeurs pour y effacer les données. Ainsi, le *scambaiting* peut s'inscrire dans le vigilantisme en ligne, car est la motivation générale derrière son application, est de renforcer les capacités de contrôle social de la cybercriminalité, d'augmenter le sentiment de sécurité d'une partie de la population, ou encore de protéger cette dernière contre les actes de fraude et de l'aider à en prévenir l'occurrence[13].

Types de *scambaiters*

Le *scambaiting* est pratiqué par différents types de *scambaiters*, chacun d'eux poursuivant des objectifs distincts[5,15,17]. On retrouve ces différentes pratiques sur des sites tels que, *Scam Alerte*, *Romance scam seekers*, *Website Reporter*, *Bank Guard*, *Safari Agents*, *Inbox drivers* ou bien encore *Trophy Hunter*[17]. ***Scam Alerte* et *Romance scam seekers* ont sensiblement le même objectif, soit de découvrir et de rendre public les différents processus de fraude utilisés par les fraudeurs, pour sensibiliser et prévenir la population**[17]. ***Website Reporter* signale des sites internet frauduleux** afin de contribuer à leur éventuelle fermeture[17]. ***Bank Guard* signale aux autorités compétentes les comptes bancaires utilisés par les délinquants** afin de faire fermer ces comptes et faire perdre de l'argent aux fraudeurs[17]. ***Safari Agents* regroupe des *scambaiters* qui tentent de convaincre les fraudeurs de se déplacer à un endroit, en leur assurant qu'à leur arrivée, l'argent demandé leur sera remis**[17]. Bien évidemment, ces déplacements font perdre du temps et des gains financiers aux délinquants[17]. **Les *scambaiters* agissant au sein d'*Inbox drivers* s'infiltrent quant à eux illégalement dans la boîte courriel du fraudeur** pour envoyer des messages avertissant les victimes potentielles de la fraude qui est perpétrée[17]. Enfin, ***Trophy Hunter* regroupe des *scambaiters* cherchant à acquérir un trophée à la suite de l'échange avec le fraudeur**[15,17]. Ce trophée peut être une photo ou une vidéo drôle ou humiliante du fraudeur[17]. Un document prouvant la perte de temps occasionnée par l'échange peut également constituer un trophée[17]. La publication de ces trophées permet au *scambaiter* de gagner l'admiration des différentes communautés de *scambaiters*[15].

Néanmoins, certains chercheurs mentionnent que les trophées publiés sur des sites comme 419eater.com peuvent viser certaines populations, plus particulièrement africaines, ce qui pourrait être perçu comme du racisme de la part de certaines communautés de scambaiters[7,8,18,19].

Motivations et comportements des *scambaiters* sur les plateformes vidéo

Les motivations

Les *scambaiters* peuvent avoir plusieurs objectifs. **La première motivation recherchée est de faire perdre du temps aux fraudeurs**[6,9]. Les *scambaiters* utilisent habituellement plusieurs techniques pour essayer de prolonger l'échange sans raison valable[9], ne menant à aucun résultat pour le fraudeur[14]. Le but de cet échange est de faire perdre des opportunités de fraudes menant ainsi à une perte de ressources[7], souvent financière. En effet, lorsque les fraudeurs sont en communication avec les *scambaiters*, ils ont moins de temps pour trouver d'autres victimes potentielles et communiquer avec elles[5,7,9]. Le *scambaiter* peut feindre des malentendus durant les conversations ou encore faire semblant de devoir se déplacer de chez soi pour aller chercher ce dont il a besoin, par exemple sa carte de crédit dont il doit communiquer les informations au fraudeur[7].

La deuxième motivation est l'humiliation. L'humiliation a pour but de mettre en évidence la naïveté et la stupidité des fraudeurs[12]. Cette volonté d'humilier est notamment désirée par les victimes de fraude, ou quelqu'un qui en connaît une personnellement[5,7]. En effet, le fait de vouloir ridiculiser le fraudeur qui lui a soutiré de l'argent ou des informations personnelles pourrait être une motivation suffisante pour une victime, de procéder à du *scambaiting* pour se venger[7]. Le *scambaiting* pourrait même avoir un effet thérapeutique pour certaines d'entre elles[5]. Certains actes perpétrés par les *scambaiters* peuvent être considérés comme problématiques et peu éthiques (par exemple, la divulgation d'informations personnelles sur le fraudeur ou bien encore les insultes à caractère raciste), mais qu'ils jugent comme nécessaires pour contrer ceux commis par les fraudeurs, qui sont présentés comme de mauvaises personnes[8].

La troisième motivation des *scambaiters* est de faire la prévention de la fraude en ligne. En effet, le *scambaiting* permet d'en apprendre davantage sur le processus de fraude et les techniques utilisées par les fraudeurs et ainsi sensibiliser les spectateurs, qui sont autant de victimes potentielles[6,7,9]. La diffusion vidéo sur des plateformes en ligne permet ainsi d'ajouter un caractère préventif[7] à cette activité de divertissement[9]. D'ailleurs, les *scambaiters* vont souvent transmettre des messages de prévention dans leurs vidéos, tout en sensibilisant aux différentes pratiques à adopter sur internet[9]. Cependant, **l'objectif de sensibilisation peut aussi avoir une composante égocentrique**. En effet, le *scambaiter* peut avoir la volonté de bien paraître aux yeux de la communauté des scambaiters[7,15]. Ces individus ne désirent pas nécessairement faire de la prévention, mais souhaitent plutôt gagner l'admiration de leurs pairs[7]. De surcroît, le *scambaiter* peut travailler en collaboration avec des entreprises offrant des services d'accès internet et de téléphonie ou des banques, et ce, pour entraver les stratagèmes mis en place par les fraudeurs[6,7]. La prévention peut aussi se faire par l'accumulation d'informations sur le fraudeur, telles que son nom, son prénom et sa photographie[6,7]. Celles-ci peuvent être transmises aux autorités compétentes[7,9]. Ainsi, la pratique du *scambaiting* peut aider à protéger des personnes à risque d'être victime d'une fraude[14].

La quatrième motivation des *scambaiters* est le divertissement. La diffusion sur des plateformes en ligne de vidéos reflète cette finalité de divertissement. De plus, des sites internet, tels que *419 Eater*, *Scam o Rama* et *scambuster419.co.uk* mentionnent que **le *scambaiting* vise habituellement à avoir du plaisir tout en aidant la communauté**[7]. Les individus pratiquant le *scambaiting* sont souvent encouragés par les différentes communautés de *scambaiters* à partager leurs expériences et tactiques de scambaiting[9]. De surcroît, le divertissement peut à la fois concerner les internautes ou encore le *scambaiter*, qui prend plaisir à pratiquer cette activité[5,9]. Dans les vidéos, le *scambaiter* démontre son amusement de la situation dans laquelle il met

le fraudeur, en riant ou, lorsqu'un des deux ou les deux perdent patience et s'insultent ou s'injurient[9]. De plus, le *scambaiter* échange en même temps avec l'audience synchrone (celle qui écoute la vidéo en direct), alimentant le divertissement des deux parties[6]. Ces échanges entre internautes et *scambaiter* peuvent porter sur les actions et les propos du fraudeur ou sur les prochaines étapes du scambaiting[6]. Par conséquent, la sensibilisation et le divertissement sont très importants pour les différentes communautés de *scambaiters*.

Les sources de revenus qui peuvent découler de la diffusion des vidéos de *scambaiting* représentent également une motivation des scambaiters[9]. Ces derniers peuvent obtenir un revenu[9] grâce aux visionnements des vidéos, aux abonnements payants, aux dons de leurs abonnés et aux publicités dans les vidéos[16]. Certains *scambaiters* peuvent même vivre de cette pratique ce qui leur permet d'avoir plus de temps pour la création de contenu, ainsi que sur la recherche de nouvelles stratégies de *scambaiting*, et ce, pour augmenter le divertissement dans les vidéos[9]. Toutefois, cette popularité peut avoir un aspect négatif puisque les fraudeurs, étant de plus en plus conscients de cette pratique, sont plus méfiants et connaissent l'identité et les pratiques de leurs adversaires[9].

Les comportements

L'humour et la moquerie sont régulièrement utilisés par les scambaiters[5,9]. L'humour peut servir de divertissement pour l'audience qui regarde les vidéos ou encore pour ridiculiser le fraudeur. **Les *scambaiters* procèdent également à la confrontation**. Celle-ci est souvent utilisée à la fin des vidéos pour dévoiler leur identité et confronter l'arnaqueur sur ses comportements illégaux[6,9]. Toutefois, ce ne sont pas tous les *scambaiters* qui décident de dévoiler qui ils sont et de confronter le fraudeur sur ses agissements. De plus, la confrontation peut parfois soulever des questionnements éthiques puisque les *scambaiters* peuvent menacer de causer du tort au fraudeur[9]. Certains *scambaiters* vont même jusqu'à avoir des comportements illégaux, tels que de s'infiltrer dans l'ordinateur du fraudeur pour récupérer et effacer ses fichiers[9]. À la suite de cette confrontation, le fraudeur va soit avouer son implication dans des stratagèmes de fraude ou mettre fin à la discussion[6,9]. La confrontation peut également servir à faire prendre conscience au fraudeur de l'impact de ses actions sur les victimes[6].

Conclusion

Étant donné son caractère récent et singulier, **le *scambaiting* est un sujet d'intérêt pour mieux comprendre les moyens de prévention de la cybercriminalité**. Les *scambaiters* peuvent être considérés comme des individus participant aux efforts de prévention de la cyberfraude afin de protéger les victimes potentielles des fraudeurs[14,15], tout en divertissant un public en forte croissance[9]. **Toutefois, certains comportements peuvent soulever des questionnements éthiques**[2,3,9]. Cette note de synthèse met donc en lumière l'importance de s'intéresser scientifiquement à cette activité, puisqu'elle permet, tout comme le vigilantisme en ligne et le digilantisme, de perturber les fraudeurs dans leurs pratiques criminelles et de participer aux efforts de prévention de la cybercriminalité.

Recommandations

Continuer à étudier le *scambaiting* permettrait d'en apprendre plus sur les stratégies de perturbation qui sont appliquées et sur les justifications intrinsèques à cette activité. En effet, **des études qualitatives auprès des *scambaiters* permettraient de mieux comprendre leur point de vue dans la création de ce type de contenu et la manière dont ils retiennent l'attention de leur auditoire et communiquent avec lui**.

La diffusion à plus grande échelle de ce contenu permettrait de sensibiliser les citoyens aux différentes techniques de fraude qui sont expliquées par les *scambaiters*. En effet, peu d'études portent sur le *scambaiting* et son potentiel de prévention et de sensibilisation[7,9]. Les citoyens pourraient bénéficier de ces contenus, plus accessibles et distrayant que les programmes de prévention conventionnels, pour obtenir davantage d'informations sur les différents types de fraudes, ce qui les inciterait à signaler les tentatives ou les fraudes subies plus régulièrement.

Étant donné la popularité grandissante du scambaiting, il serait pertinent d'effectuer des

recherches sur l'impact réel de cette activité sur les opportunités de fraude des délinquants[8], que ce soit sur la fraude en général ou d'un type de fraude en particulier.

Références

[1] Centre antifraude du Canada. (31 décembre, 2022). *Gouvernement du Canada*. https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

[2] Sorell, T. (2019). Scambaiting on the spectrum of digilantism. *Criminal Justice Ethics*, *38*(3), 153-175.

[3] Ross, A. S. et Logi, L. (2021). "Hello, this is Martha": Interaction dynamics of live scambaiting on Twitch. *Convergence*, *27*(6), 1789-1810.

[4] À noter que le terne « croque-escroc » est également utilisé en France.

[5] Yékú, J. (2020). Anti-Afropolitan ethics and the performative politics of online scambaiting. *Social Dynamics*, *46*(2), 240-258.

[6] 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.

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

[8] Cross, C. et Mayers, D. (2020). Scambaiter narratives of victims and offenders and their influence on the policing of fraud. *Policing: A Journal of Policy and Practice*, *15*(4), 2148-2164.

[9] Laato, S. et Rauti, S. (2021). Scambaiting as a form of online video entertainment: an exploratory study. *Advances in Intelligent Systems and Computing*, 738-748.

[10] Dynel, M. (2014). Participation framework underlying YouTube interaction. *Journal of pragmatics*, *73*, 37-52.

[11] 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).

[12] Laato, S. et Murtonen, M. (2020). Improving synchrony in small group asynchronous online discussions. *Trends and Innovations in Information Systems and Technologies,* 215-224.

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

[14] Chen, W., Wang, F. et Edwards, M. (2022). Active countermeasures for email fraud.

[15] Zingerle, A. et Kronman, L. (2011). Transmedia storytelling and online representations - issues of trust on the Internet. *International Conference on Cyberworlds*, 144-151.

[16] YouTube. Monetisation for creators. YouTube. https://www.youtube.com/howyoutubeworks/product-features/monetization/#subscriptions

[17] 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.

[18] 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.

[19] Byrne D. (2013). 419 Digilantes and the frontier of racial justice online. Radical History Review, 117, 70–82.