Scambaiting as a Preventive Tool in the Fight against Cyberfrauds: the Case of Romance Scams

Renaud Zbinden[1], Olivier Beaudet-Labrecque[1], Flore Grandjean[1], Cloé Gobeil[2], Luca Brunoni[1], David Décary-Hétu[2], Cristina Cretu-Adatte[1]

[1]Insitut de lutte contre la criminalité économique, HEG Arc // HES-SO, [2]Université de Montréal

This paper follows a presentation made during the "Conférence sur la réponse aux incidents et l'investigation numérique" on June 7th 2022 in Lille, France (https://conf.cecyf.fr/event/1/).
This paper is published in the Journal on Cybercrime & Digital Investigations by CECyF, https://journal.cecyf.fr

Abstract

The following paper discusses the potential of using scambaiting techniques to mitigate online fraud. It draws from the experience and the results of a recent project led by the authors, in which researchers posed as targets on dating platforms and interacted with criminals engaging in romance scams – a prominent type of fraud that generates massive economic and emotional damages. The aim of the project was to model their modus operandi, use the gathered data to explore possible ways to disrupt and frustrate further criminal conduct, and evaluate the potential of such techniques. After providing the scientific context of the project, this paper will detail the methodology and the strategies used by the research team for their scambaiting experiment. A brief survey of the most interesting results will then be presented. The last part of this paper will focus on the challenges and opportunities of using scambaiting as a law enforcement tool to fight online fraud.

Keywords: Covid-19, cybercrime, romance scams.

1 Introduction

For several years, cyber scams have been gaining in importance all over the world. The Covid-19 pandemic and its constraints have only amplified this evolution, attracting even more victims and criminals to the cyberspace. The repression of these phenomena is sometimes limited by barriers that are beyond the control of the prosecuting authorities, such as the complicated mechanisms of international cooperation, and the difficulties related to the identification of authors. At the same time, in the majority of cyber scams, the modus operandi used by criminals is not innovative. They are well known to the authorities, who are multiplying their prevention efforts among the population. However, it is evident that such measures – which mainly and traditionally consist in information and awareness campaigns – are not sufficient, and cannot be the only preventive tool used by authorities. Innovative and proactive measures must be explored to improve the effectiveness of the fight against cyber scams.

Among the avenues that have been little explored to date, there is scambaiting. The term "scambaiting" generally refers to the practice of assuming the role of a potential victim of online fraud and interact with one of its perpetrators. In the last years, it has emerged as a social phenomenon, thanks to the rise of youtubers and other streamers, who film and diffuse such interactions. They tend to waste perpetrators' time, expose them and humiliate them, which creates a form of entertainment that captures their audience. In the eyes of the general public, scambaiting has thus become associated with a form of internet vigilantism.

One type of fraud that lends itself to scambaiting is romance scams. In it, fraudsters usually use a fake profile to contact victims and offer the pretense of a romantic relationship. Once the victims develop feelings, fraudsters trick them or manipulate them into transferring money – often by putting forward urgent medical expenses or business needs and opportunities. Besides creating important economic damages, romance scams also impact the personal and emotional sphere of victims, usually by creating feelings of insecurity and uneasiness that in turn lower their quality of life.

The research team has been monitoring romance scams for years. During the Covid pandemic [1], it led an exploratory study on the inner working of romance scams, conducted through the observations and analysis of scammer-victim interactions. Researchers used modified profiles based on their own pictures to open accounts on dating platforms and hold conversations with scammers. This was done for research purposes only: no data was transmitted to law enforcement authorities, and no information about the fraudsters was divulged to the general public.

The exploratory study led to a better understanding of the phenomenon in Switzerland, and allowed the team to update and perfect its message to the media and the public with regard to prevention. It was also evident, however, that the collected information could, potentially, be employed in a more active way in the fight against romance scams – namely by disrupting and frustrating further criminal actions. For this to be possible, however, the scambaiting activities and the subsequent data collection would need to be carried out by law enforcement authorities.

In order to test these hypotheses and evaluate the potential of using scambating techniques in the fight against cyber scams, the research team decided to launch a new project, which would also expand the study field to three French-speaking countries: Switzerland, France and Canada. The project, which was founded by the Interpol Foundation for a Safer World, took place in 2021 and 2022.

2 State of the Art

Scambaiting first emerged during the nineties as a reaction to the proliferation of email scams such as advanced fees scams (also known as 419 scams) [2] [3]. Due to the ineffectiveness of the authorities' counteractions, internet users took matters into their own hands and started engaging with scammers in order to thwart their criminal activities. Since then, scambaiting has developed and has become a global social phenomenon.

As cyber scams evolved beyond basic email scams, the response of scambaiters also took new forms [4]: simple email exchanges have given way to more complex scambaiting strategies, which are often filmed and broadcasted to an audience on media platforms [5].

While most scambaiters justify their actions by claiming they are protecting society and victims, their underlying motivations may be varied [6]. Researchers who have studied scambaiters forums have remarked that several of them pursued less honorable goals, such as humiliating scammers, ridiculing them, and/or gaining a personal following by publicly displaying their scambaiting successes [5] [7].

Most of the work on scambaiting has focused on its social perspective and very few researchers have effectively explored its potential as a tool to fight cyber fraud. Many of them were rather critical in this regard; Byrne [2], for example, stated that while the scammer community often claims their work has an impact on real crime and even results in arrests, she has found no concrete and verifiable cases thereof. Cross and Mayers [8] emphasized the possibility for scambaiters to pass on information to the authorities, but they were not able to find any evidence of such processes, nor of their effectiveness.

Zingerle [9] [10] [11] is probably one of the only researchers to have taken an interest in the potential of scambaiting. Among other things, he analyzed the different strategies used by scambaiters and their possible impacts on the fight against cybercrime. Sorell [12] also looked at the forensic function of scambaiting in different types of scams and stated that it may produce positive effects on the criminal phenomenon.

Despite these efforts, the potential of using scambaiting in the fight against cybercrime is an area of research that has been left vastly unexplored. The project presented in this paper aims at beginning to fill this gap, especially with regard to the role scambaiting can play if adopted as a law enforcement technique.

3 Methodology

3.1 Preliminary Phase

The positive outcome of the project relied on conducting a large quantity of direct interactions with romance scammers who were convinced of targeting a potential victim. It was paramount, however, that this was achieved while respecting a series of non-negotiable ethical and legal considerations. The researchers faced the challenge of developing a methodology that maximized the possibility of pertinent interaction, but also created a controlled environment in which scambaiters acted according to a strict code of conduct, which eliminated the risk of interacting with regular users.

Such methodology was developed through a preliminary phase. The team drafted a first protocol based on a literature review [13] [14] [15] [16] and used it to observe the phenomenon on several dating platforms, identify fraudulent accounts, and hold basic interaction to gather data about their methods.

This phase allowed the team to select two platforms on which to conduct the study – both of which are available in all three countries. First of all, it was observed that platforms that required the disclosure of banking information and required a paying subscription were less attractive to scammers and would make their presence less prominent. Platforms that executed strict controls allowing them to strongly limit the quantity of fake accounts were also excluded. Finally, the team privileged platforms that didn't limit the daily number of interactions, messages, and contacts at the disposal of each user.

Researchers created several different profiles and posed as potential victims of different ages. The observed activity indicated that middle-aged women were the most attracting targets for romance scammers. It was thus determined that the main phase of the research should be conducted using feminine profiles within this age bracket.

Throughout the preliminary phase, the team used the return of experience to build a scambaiting guide to carefully direct the activities researchers would engage in while using such profiles. The guide has been drafted with the help of legal professionals and ethicists to ensure that the highest standards were respected.

3.2 Main Phase

Two researchers were selected to conduct the scambaiting experience in the three countries: one was responsible for Switzerland and France, and the other for Canada. This choice was made because of the linguistic differences between European and Canadian French, as well as due to the necessity to work in different time zones. The experience was divided into three periods of one month each, to be carried out subsequently in each of the countries. The scambaiters were provided with the scambaiting guide and were personally coached by the research team to make sure they integrated its teachings. The coaching sessions also served to familiarize the scambaiters with typical situations, and to provide them with further advice and good practices.

Three different profiles of middle-aged women were created – one to be used in each country, and on both platforms. Each was carefully constructed and included a fictional backstory that the scambaiters could rely on during their interactions. Common characteristics included a secure/affluent financial situation, a good education, and a sentimental life marked by deception or grief. All profiles were linked to an e-mail address and a phone number which would be used for all interactions with scammers outside of the platforms. The scambaiters participated actively in the creation of the profiles, contributing details and backstories that they would be comfortable using during their interactions with the scammers.

Once the scambaiters assumed control of the profile, they begun a first selection process aimed at identifying potential fraudulent accounts with which to interact. The main priority was to effectively distinguish between fraudulent accounts and regular users, and contact only the former. The scambaiting guide listed several criteria and red flags that helped with this task. Scambaiters could easily check, for example, if a profile was linked with a real social network account, and could resort to image search platforms to verify that a profile picture had not been stolen from another person or a database.

The scambaiters then proceeded to express interest for said profiles following the method put in place by the platforms (for example by "liking" the profile). If interest was reciprocated, scambaiters then applied a second test, which included small exchanges with the target account, to once again verify that they were not interacting with a regular user. Besides double-checking that the images used by the fraudster were not authentic, the scambaiters would pay close attention to the exchanged messages: the research team's experience indicates, for example, that scammers tend to introduce themselves in a direct, matter of fact fashion ("Hello, my name is Mark, I am 46, I am a widow and have no children") and often state, early in the exchange, that they are looking for a long term love relationship.

At this point, scambaiters could begin the core phase of the experience, which consisted in a simulated romantic interaction with the fraudster. This process was also detailed and regulated by the guide, which instructed scambaiters about what they could expect and how they should react. For example, fraudsters almost systematically demand to move the conversation from the dating platform to an instant messaging service. This ensures that they can continue the fraud attempt even if their fake account on the dating platforms is banned. From this point on, fraudsters tend to be very active and demanding in their interactions: to maximize the effectiveness of the process, the guide recommended that scambaiters did not hold conversations with more than 4-5 fraudsters simultaneously.

During this crucial phase, scammers begin to lay the groundwork for the money demand. The latter however is usually not immediate and can intervene weeks after the initial contact – sometimes even months. A very high importance was therefore placed on the scambaiters' conduct during this period. On one hand, they should be careful to maintain the illusion that they were under the fraudster's spell, even if the latter made mistakes, such as including incoherences in their messages. They were allowed to develop a complicity with the fraudsters and act as if they were experiencing romantic feelings. On the other hand, researchers were instructed to never, in any circumstances, encourage fraudsters to accelerate the money demand or otherwise push them to engage in criminal behavior.

The scambaiters were instructed to collect all interactions with the fraudsters, as well as to catalogue specific data such as telephone numbers, e-mail addresses, and the banking information used for the money requests. In order to obtain data related to the hardware and software employed by fraudsters, as well as to help determine their location, a website that advertised the rental of a mountain chalet was created. The scambaiters could easily direct fraudsters toward the website by integrating the chalet in their backstory (e.g. by claiming they owned it or planned to rent it).

4 Results

The results obtained during the scambaiting experiment surpassed the research team's expectations. Out of 15,424 profiles encountered on the selected platforms, 1,534 profiles were suspicious according to the guide's criteria. Given the limited time and resources, it was not possible to interact with every single profile and confirm their fraudulent nature. In total, exchanges were conducted with 188 scammers. Of these, 51 made requests for money within the time frame of the experiment. Such requests were usually made after two to three weeks, but sometimes after only a few days or hours. The requested amounts generally ranged from 100 to 5,000 euros. The payment methods proposed by the scammers were mainly bank transfers, but also included cryptocurrency payments, gift cards and payments via international money transfer agencies.

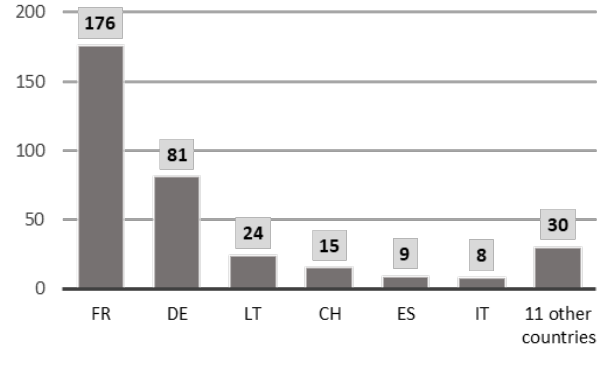

Fig. 1. Bank Accounts per Country (n=348).

During the entire project, the research team collected 348 bank account numbers. These accounts were mostly from European countries (Figure 1), notably France, probably for linguistic reasons, and Germany and Lithuania, which are home to many digital banks. Moreover, out of the 69 banking institutions identified, four European banks alone – despite being minor players in the European market – made up half (50.7%) of the collected accounts (Figure 2). It is important to note that the five banking institutions preferred by scammers were all digital banks.

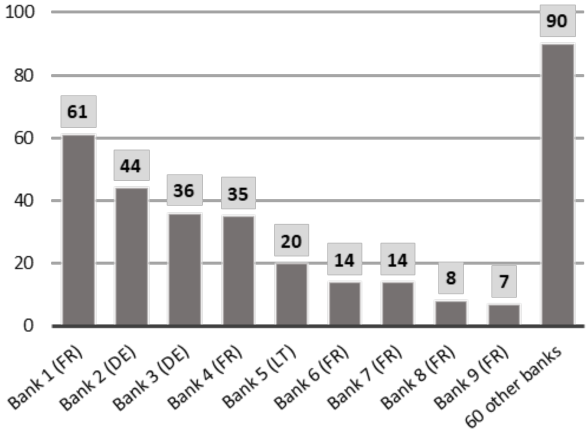

Fig. 2. Bank Accounts per Institutions (n=348).

In addition to bank account numbers, the team was able to collect 140 telephone numbers. As mentioned above, after a few interactions on dating platforms, scammers quickly try to switch to another discussion channel, to avoid having their account blocked and losing contact with their victim. Instant messaging applications working with real phone numbers were the most used second channels. The phone numbers collected were mainly from France (53.6%), Ivory Coast (17.9%) and the United States (13.6%) (Figure 3). Of the 75 French telephone numbers, 59 were from a single telephone operator (78.7%) (Figure 4). Again, it should be noted that this telephone operator represents only a tiny part of the French telephone market and is very largely over-represented in the collected sample.

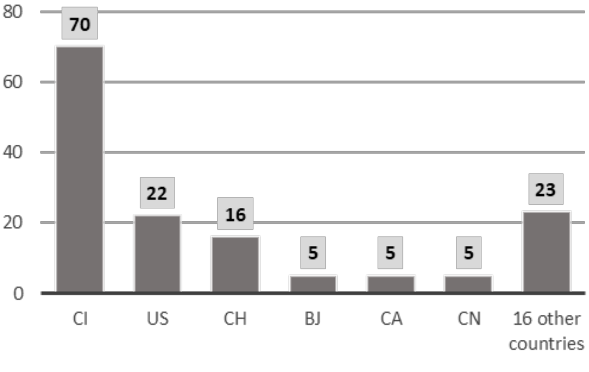

Fig. 3. Phone Numbers by Countries (n=140).

As mentioned above, scambaiters also sent scammers a link to a website advertising the rental of a mountain chalet. During the whole experiment, 146 different IP addresses connected to the website. About half of them (47.9%) were from Côte d'Ivoire (Figure 5). The other visitors of the website were from the United States (15.1%), Switzerland (11.0%), Benin (3.4%), China (3.4%), and Canada (3.4%). The remaining connections were from 16 other countries. Some scammers may have used VPN connections, thus masking their true location and using one that matched their story. The data collected through the website also allowed the research team to determine that most of the scammers use a mobile device (65.1%), and only a minority employ a desktop computer (34.9%).

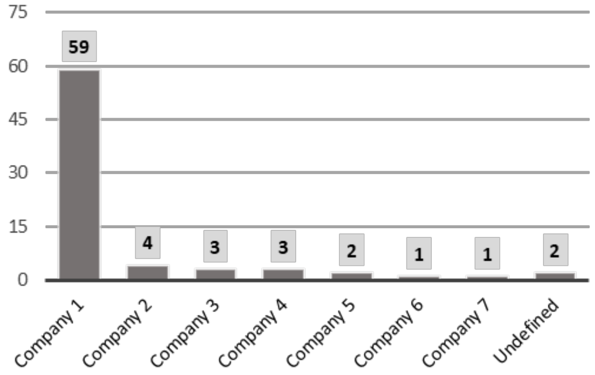

Fig. 4. French Phone Numbers by Telecommunication Company (n=75).

Finally, during the interactions, the research team noticed an important difference between the expertise levels of the scammers. The most experienced scammers, for example, made the effort to avoid mistakes in their writing and were consistent in the stories they told. Those who were identified as the most competent were also good listeners, attentive to details, and able to maintain a good level of conversation. They built the relationship with their victims patiently, and carefully planned every step following an established modus operandi.

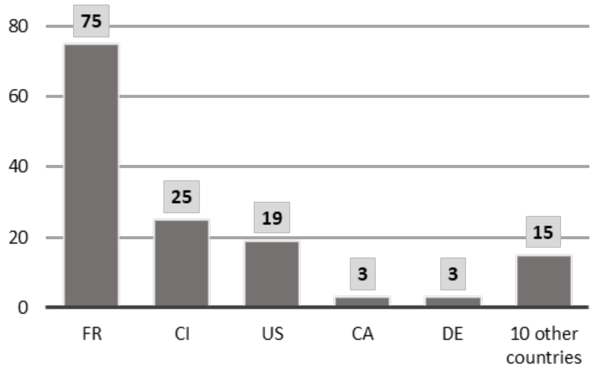

Fig. 5. Website Visitors per Country (n=146).

5 Findings and Discussion

The first findings of the project suggest that scambaiting can indeed play a role in the improvement of the fight against cyber scams. The nature of the information collected could allow for targeted disruption actions by law enforcement authorities, and thus complicate the work of scammers. It also makes it possible to gather intelligence, to identify economic actors who are frequently involved in the scammers' operating methods, and to obtain a representative image of the latter's criminal behavior at a given time.

On the other hand, scambaiting has limits from a legal, ethical and financial point of view. While law enforcement agencies engaging in scambaiting activities will operate in a less ethically complicated territory than researchers, as they pursue their natural objective of disrupting and limiting criminal activity, they must also evaluate the ethical and legal implications of their actions.

5.1 Perturbation Potential

In the case of romance scams, scambaiting has produced valuable data that could be employed by law enforcement authorities to disrupt and frustrate further criminal action. Data such as bank account numbers and telephone numbers could be communicated to the relevant service providers, which could proceed to interrupt the service, blacklist accounts, and block transactions. Information about cryptocurrency wallets and accounts could be used to trace the movements of the proceeds of the scam, thus identifying other linked addresses.

Sometimes, fraudsters utilize money mules as intermediaries before directing the proceeds of their crime to the ultimate beneficiary. If a financial institution is made aware that one of its accounts is being used for this purpose, it could inform the account holder, and the latter will not risk being deemed complicit in money laundering. Such interventions would create a series of new obstacles, and thus make the criminal activity more complicated and less attractive.

In the same vein, accounts identified as fraudulent on dating platforms could be reported and deleted. From a scambaiting perspective, this should be done after changing the channel of discussion, so as not to lose contact with the offender. Also, the photos and descriptions used by the fraudsters could be made available for public prevention purposes.

5.2 Gathering Intelligence

If it is used methodologically and follows a strict protocol, scambaiting can provide an accurate picture of a criminal phenomenon at a given time. In the case of this study, the team was able to establish the proportions of suspicious and fraudulent profiles on two dating platforms. The results suggest that there is considerable room for improvement in detecting and eliminating fake profiles, as those are often easily identifiable to the trained eye.

The results also show that some economic actors are frequently involved in the criminal processes used by fraudsters. A very small number of banks were housing the majority of accounts used to recover illicit funds. This leads the project team to believe that fraudsters open accounts in banking institutions where opening processes are quick, simple, and probably cheap. This also raises the question of due diligence within these banks. On the other hand, most of the other banks involved were linked to only one or two accounts. It is difficult to determine if these accounts were opened by cybercriminals or if they are held by money mules. Some mobile phone operators were also over-represented in the sample, especially the French one. The reasons for this are probably the same as for bank accounts: quick, simple and cheap processes with a low level of control.

The computer data collected through the fake rental website indicates that fraudsters seldom take precautions while carrying out their modus operandi. Very few of them tried to hide their IP address and most of them have clicked on the transmitted link without hesitation. It is interesting to note that the majority (65.1%) of fraudsters were using mobile devices, while the literature often considers that these activities are carried out in Internet cafés and with the use of desktop computers or laptops [17] [18].

Through cross-analysis, the team was also able to determine that different fraudsters sometimes used the same bank accounts. This suggests that they might operate as a criminal network, at least for operational details. The research database was also compared to the French-speaking Swiss police database, revealing that some names and bank accounts were not only related to other romance scam cases, but also to other types of scams such as sextorsion, fake ad fraud, and inheritance scam, highlighting the versatility of the criminal networks. Less than 5% of the data collected matched the contents of the police database; this shows that scambating could be an effective information-gathering tool for law enforcement authorities.

5.3 Precautions

One of the main prerogatives of any scambaiting activity should be to effectively identify fraudulent profiles and avoid false positives. In the case of romance scams, the guide put in place by the research team proved to be highly effective: if used correctly, the listed criteria and red flags reduce the risk of interacting with regular users to virtually zero.

Thus, the scambaiting activities had little to no impact with the normal operation of the platforms. From an ethical point of view, the mere presence of the scambaiters' profiles within the pool of potential contacts on platforms in which fake profiles and dormant profiles abound represents an acceptable trade off.

Before deploying scambaiting as a law enforcement tool for other types of online frauds, agencies should therefore implement and test a protocol that successfully allows agents to target criminals, and criminals only. As the present study shows, this can be achieved through a preliminary phase that generates knowledge and training material susceptible to ensure that scambaiters are fully prepared for their task.

The identification criteria generated by such processes can also be employed for more general sensibilization and prevention purposes. In the case of romance scams, private citizens can easily apply them by themselves, thus reducing the risk of being victimized.

5.4 Legal Challenges

Scambaiting and perturbation activities also raise legal considerations of a procedural, criminal and civil nature. Depending on the State in which it is carried out, the characteristics of the perpetrator and the use made of the data collected, it may be considered a special measure in the same sense as police infiltration, and require judicial authorization. From an ethical point of view, scambaiting is less problematic when carried out by police authorities than by private citizens such as researchers, as long as it is conducted within the legal framework that limits police activities.

Scambaiting, by its nature, involves agents hiding their police identity – a strategy that is usually highly regulated within law enforcement. In Switzerland, for example, agents who do not disclose their identity need to conform either to the rules of "undercover investigations" (Section 5 of the Criminal Procedure Code (CrimPC)) or of "undercover enquiries". The first pursue the objective of "infiltrating a criminal environment in order to investigate particularly serious offences" (art. 285a CrimPC), while the second aim at investigating crimes by "entering into or pretending to wish to enter into fictitious transactions" (art. 298a CrimPC).

The scambaiting activity described in this paper, if conducted by Swiss police officers, would seem to fall in the latter category, and therefore be subject to less strict requirements – it would not necessarily require, for example, the authorization of a public prosecutor if conducted for less than one month (art. 298b.2 CrimPC). However, it is up to authorities wishing to engage in scambaiting to determine exactly the nature and the extent of their agents' operations, to ensure that those are compatible with the applicable legislation, and to seek the appropriate authorizations. They would also need to continuously monitor such operations, to make sure that they do not cross the line between enquiries and investigations or exceed the one-month time frame.

In Switzerland, in both undercover investigation and enquiries, the agents "may not generally encourage others to commit offences" and "must limit their activities to substantiating an existing decision to commit an offence" (art. 293 and art. 298c.2 CrimPC). The research team took inspiration from this rule to create the code of conduct included in the scambaiting guide. Scambaiting activities conducted by law enforcement will also benefit from guidelines and coaching that frame the conduct of the agents, as each type of scam will present different characteristics and pitfalls. Thus, the risk of inciting a criminal act can be mitigated by creating a guide establishing clear rules that direct the scambaiters' activity and behavior.

Perturbation activities such as backlisting telephone numbers and bank accounts have of course the potential of causing monetary damage. Such damage can also be created outside of the context of an individual's criminal activity – for example, through the inability of using a bank account for legitimate purposes. Potentially, victims could attempt recovery through civil law, and challenge the opportunity and necessity of the backlist. The risk of false positives – qualifying a real person as a scammer – also exists, especially if scambaiters are not disciplined in their activity. Therefore, a high level of scrutiny should be applied by law enforcement authorities before taking such measures.

5.5 Financial Considerations

Scambaiting is a technique that requires the use of important human resources, and therefore has a heavy financial impact. The work of a full-time scambaiter during three months was necessary to collect the data mentioned above. Of course, this is also because scambaiting is particularly energy consuming in the case of romance scams, mainly because prolonged interactions are often needed before valuable information can be collected.

Recent research has shown that it could be possible to automate some steps of the scambaiting process, such as the identification of the fraudsters' profiles. Suarez-Tangil et al. (2019) [19], for example, created an automatic detection system capable of identifying fake profiles on dating platforms with a success rate of 97%. As artificial intelligence technology evolves, so will the automation processes that will help scambaiting become more efficient.

6 Conclusion

Scambaiting allows to generate a large amount of information on a criminal phenomenon. When collected in a structured manner, this information can be valuable and precise in quantifying the extent of a phenomenon. Such information can also be used to conduct disruptive actions against the criminal activities of scammers. It can also highlight the involvement of some economic actors in the processes used by scammers and draw attention to possible security gaps and breaches of their obligations. As such, it has the potential of reinforcing the action of law enforcement against cyber scams. In order to be effective and act within the legal and ethical boundaries that apply to their public mission, however, law enforcement authorities should establish a protocol that is functional to both the data collection and the relative planned disruption activities.

In view of the constant increase in the number of cases of cyber frauds around the world, the difficulty of prosecuting the perpetrators and the limits of the strategies currently in place, the potential of scambaiting cannot be overlooked. Further work needs to be done, by both researchers and public authorities, in order to better integrate scambaiting activities in law enforcement actions, as well as to develop techniques that are at the same time more efficient and less costly.

This paper has been made possible thanks to the contribution of the RCSO Economie & Management program and the Interpol Foundation for a Safer World.

Author details

Renaud Zbinden

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
renaud.zbinden@he-arc.ch

Olivier Beaudet-Labrecque

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
olivier.beaudet-labrecque@he-arc.ch

Flore Grandjean

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
flore.grandjean@he-arc.ch

Cloé Gobeil

Université de Montréal
3150 Jean-Brillant, Montréal, Canada, H3T1N8
cloe.gobeil@umontreal.ca

Luca Brunoni

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
luca.brunoni@he-arc.ch

David Décary-Hétu

Université de Montréal
3150 Jean-Brillant, Montréal, Canada, H3T1N8
david.decary-hetu@umontreal.ca

Cristina Cretu-Adatte

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
cristina.cretu-adatte@he-arc.ch

References

[1] O. Beaudet-Labrecque, R. Zbinden and S. Langel, “Romance Scam: Ergebnisse einer experimentellen Studie in der Schweiz”, *Kriminalistik*, 6/2021, pp. 369-372.

[2] D. N. Byrne, “419 Digilantes and the Frontier of Radical Justice Online”, *Radical History Review*, Issue 117, pp. 70-82, 2013.

[3] J. Smallridge, P. Wagner and J. N. Crowl, “Understanding Cyber-Vigilantism: A Conceptual Framework”, *Journal of Theoretical & Philosophical Criminology*, 8, pp. 57-70, 2016.

[4] A. S. Ross and L. Logi, ““Hello this is Martha”: Interaction dynamics of live scambaiting on Twitch”, *Convergence: The International Journal of Research into New Media Technologies*, Vol. 27, Issue 6, pp. 1789-1810, 2021.

[5] M. Dynel and A. S. Ross, "You Don’t Fool Me: On Scams, Scambaiting, Deception, and Epistemological Ambiguity at R/scambait on Reddit", *Social Media + Society*, Vol. 7, No. 3, pp. 1-14, 2021.

[6] L. Tuovinen and J. Röning, “Baits and Beatings: Vigilante Justice in Virtual Communities”, Proceedings of CEPE 2007, *The 7th International Conference of Computer Ethics: Philosophical Enquiry*, pp. 397-405, 2007.

[7] L. Nakamura, "’I WILL DO EVERYthing that am asked’: Scambaiting, Digital Show-Space, and the Racial Violence of Social Media", *Journal of Visual Culture*, Vol. 13, No. 3, pp. 257-274, 2014.

[8] C. Cross and D. Mayers, "Scambaiter Narratives of Victims and Offenders and Their Influence on the Policing of Fraud", *Policing: A journal of Policy and Practice*, Vol. 15, Issue 4, pp. 2148-2164, 2020.

[9] A. Zingerle and L. Kronman, “Humilitating Entertainment Or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud”, in *Proceedings of the 2013 International Conference on Cyberworlds,* pp. 352-355, 2013.

]10] A. Zingerle, “Towards a Categorization of Scambaiting Strategies against Online Advance Fee Fraud”, *International Journal of Art Culture and Design Technologies*, Vol. 4, No. 2, pp. 39-50, 2014.

[11] A. Zingerle, “Scambaiters, Human Flesh Search Engine, Perverted justice, and Internet Haganah: Villains, Avengers, or Saviors on the Internet?”, in *Proceedings of ISEA2015, 21st International Symposium on Electronic Art*, pp. 261-268, 2015.

[12] T. Sorell, “Scambaiting on the Spectrum of Digilantism”, *Criminal Justice Ethics*, Vol. 38, No. 3, pp. 153-175, 2019.

[13] M. Whitty, “Anatomy of the Online Dating Romance Scam”, *Secrutiy Journal*, Vol. 28, No. 4, pp. 443-445, 2015.

[14] M. T. Whitty and T. Buchanan, “The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial”, *Criminology & Criminal Justice*, Vol. 16, No. 2, pp. 176-194, 2016.

[15] M. T. Whitty, “Do You Love Me? Psychological Characteristics of Romance Scam Victims”, *Cyberpsychology, Behavior, and Social Networking*, Vol. 21, No. 2, pp. 105-109, 2018.

[16] P. Anesa, “Lovextortion: Persuasion Strategies in Romance Cybercrime”, *Discourse, Context & Media*, Vol. 35, 100398, 2020.

[17] M. Offei, F. K. Andoh-Baidoo, E. W. Ayaburi and D. Asamoah, “How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance Fraud?”, *Information Systems Frontiers*, Vol. 24, pp. 475-491, 2022.

[18] J. Beek, “How Not to Fall in Love: Mistrust in Online Romance Scams”, in F. Mühlfried (ed.), *Mistrust*, pp. 49-70, 2018.

[19] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stinghini, A. Rashid, M. Whitty, “Automatically Dismantling Online Dating Fraud”, *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 1128-1137, 2019.

PAGE LEFT BLANK