Determinants of Cybercrime Victimization: Experiences and Multi-stage Recommendations from a Survey in Cameroon

Jean Emmanuel Ntsama[1,2], Franklin Tchakounte[1,2,6(✉)], Dimitri Tchakounte Tchuimi[3], Ahmadou Faissal[1,2], Franck Arnaud Fotso Kuate[1,2], Joseph Yves Effa[4], Kalum Priyanath Udagepola[5], and Marcellin Atemkeng[6]

[1] Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundéré, Ngaoundéré, Cameroon
{j.ntsama,f.fotso}@cycomai.com
[2] Cybersecurity with Computational and Artificial Intelligence Group (CyComAI), Yaoundé, Cameroon
f.tchakounte@cycomai.com
[3] Department of Human Resource Economics, Faculty of Economics and Management, University of Yaoundé II, SOA, Yaoundé, Cameroon
[4] Department of Physics, Faculty of Science, University of Ngaoundéré, Ngaoundéré, Cameroon
[5] Department of Information and Computing Sciences, Scientific Research Development Institute of Technology, Loganlea, Australia
kalumu@srdita.com.au
[6] Department of Mathematics, Rhodes University, Makhanda, South Africa
m.atemkeng@ru.ca.za

Abstract. Cybercrimes are multiplying and spreading at an elusive speed commensurate with the emerging technologies of the fourth revolution. Their sophistication and user's vulnerability to attacks catalyze their success. Several surveys have been conducted to determine the factors favoring victimization. However, they can only be applied within a contextual framework since each ecosystem has particularities. Attempts in this direction are unavailable in Cameroon where cybercrimes cost 12.2 billion CFA in 2021. This work consists of a semi-direct survey conducted in Cameroon in 2021 to provide the determinants explaining the most frequent cybercriminal techniques, the vulnerabilities left by the users, the most targeted population segments, and the socio-demographic and economic factors justifying this security fragility. The results relate to 370 questionnaires collected throughout the territory. According to descriptive statistics and the chi-square test, the explanatory variables of cybercrime victimization are gender, age, intellectual level, level of digital knowledge, level of Information and Communication Technology (ICT) proficiency, type of equipment used, the mobile and desktop operating system used, the possession of an anti-virus/anti-spam and the marital status. Within this work, we have identified threats and their drivers and a theoretical framework has been provided with several stages that could be followed to contain cybercrime.

R. A. Saeed et al. (Eds.): AFRICOMM 2022, LNICST 499, pp. 317–337, 2023.
https://doi.org/10.1007/978-3-031-34896-9_19

Keywords: Cybercrimes · Victimization · Survey · Cameroon · Attacks · Factors

1 Introduction

The fourth revolution, while beneficial for technological innovations, comes with complexities that leave individuals with technological arrhythmia. Indeed, the rapid evolution and the digital transformation that this carries in all sectors, widen a gap in the appropriation of these technologies during the consumption of services. Catalysts of global economic growth [1], technologies such as the Internet of Things (IoT), and artificial intelligence (AI) to name a few, encourage cybercriminals to take advantage of user vulnerabilities such as lack of awareness or even risks related to their behavior [2]. Cybercrime activities, in this work, include stealing identities, luring users through social engineering techniques, infiltrating malicious applications such as ransomware into systems and networks, stealing confidential codes, and rendering services unavailable [3]. ANTIC recently reported that cybercriminal actions cost the Cameroonian economy approximately 12.2 billion in 2021, representing double the losses in 2019 probably due to the Covid-19 pandemic which promoted contactless activities [4].

These alarming facts make it urgent to revise agile government strategies and policies in the face of cybercrime in order to preserve the integrity of national digital economies. For this, it is important to investigate consumers in various sectors in order to understand and explain the reasons for victimization [5]. Many works have been proposed with a view to determining the factors that may explain cybercrime victimization [6–10]. We note, however, that the results are contextual and specific to the study areas. Obviously, the levels of appropriation, digital governance strategies, infrastructural availability, and socio-cultural and professional habits differ from one country to another.

Consequently, this complementary study, the above-mentioned objective related to victimization, is the first complete one that has been carried out in the Cameroonian context. The study of 370 questionnaires covered the entire national territory in the 10 regions. Its targets were pupils and students, teachers, people from the economic fabric, and public and private administration executives. The research hypothesis is:

H1: Do specific socio-demographic and technical factors capable of reducing victimization to cybercrime? At the end of this study, the objective is to know if it is easier for a user meeting certain conditions in the use of certain digital technologies to be a victim of cyber-crime. In other words, would certain factors more easily determine a cyberspace user to cybercrimes?

An empirical methodological approach was adopted including the following steps: data collection through a semi-directive questionnaire, analysis, descriptive statistical processing, and chi-square tests, and interpretation of the results to better understand this phenomenon. The factors retained are common in the literature. Their choice was also guided by reality and current events on cybercrime in Cameroon and in general. These are determinants related to the socio-demographic, economic, and technical context of the victim. We can cite some such as education, social situation, digital proficiency, level of security, gender, marital status, type of equipment used for access to the target, and the

most targeted types of services, and sectors of activity. This work contributes as follows :

- The collection and processing, despite social instability, of the sample for such a study was carried out for the first time in all regions of Cameroon. It can be arnessed by researchers to advance the field and improve governance strategies.
- The determination through statistical tests of the explanatory variables of the victimization of cybercrimes followed by interpretations and recommendations to guide governance. A multi-stage framework to mitigate cybercrime has been proposed.

The rest of the document is divided into two sections. Section 2 presents the methodology used. Section 3 presents the results, discussions, and recommendations. The document ends with a conclusion and perspectives.

2 Methodology

The survey has been conducted in all the ten regions in Cameroon for sake of representativity. The simple random sampling consisted in taking one sample per region and this in the ten regions by including pupils and students, teachers, people from the economic fabric, public and private administration. The younger people are aware, the more they are prepared to avoid scams. In addition, the long-term goal is to put an indispensable tool to prepare to reduce victimization to cybercrimes in today's and tomorrow's society. Teachers and other parents make it possible to realize the reality of the problem and their awareness as educators give them the tools to better supervise young people. We also considered the gender approach because both women and men are potential victims. Some citizens of neighboring countries have been associated with it because of the geographical situation of Cameroon with other sub-region countries. Thus, out of 430 people questioned, the distribution by region is illustrated in Table 1. The questionnaire was structured in four sections: Identification of the questionnaire (Sect. 0), characteristics of the respondent (Sect. 1), ICT and possession of a digital device (Sect. 2), and victimization to the scam (Sect. 3). The answers to the questions in each of these sections were obtained by direct administration of the questionnaire by the interviewer to the respondent in order to facilitate the latter's understanding and so that the questionnaires obtained at the end of the survey have a low chance of being be rejected.

The profile and location of the targets constituted resistance to the method of online questionnaires. Indeed, the scarce and even unavailable electric power in landlocked areas as well as the lack of aptitude for Web technologies justifies it. The study, therefore, took place face to face during the Covid-19 period and social instabilities linked to the war. There was reluctance on both sides because contact had to be avoided as much as possible. In addition, the survey tailored to the Cameroonian population posed a problem for expatriates on Cameroonian soil, despite being victims of cybercrimes, who could not provide information on the region of origin. These facts, therefore, resulted in an overall 11.63% of invalid questionnaires. We remain with 379 which respects the condition in terms of size and representativity [11]. At the time of the exploitation of the questionnaires and the purification of the database collected, some questionnaires have been rejected for non-compliance due to a high rate of non-responses, inappropriate responses, and empty responses.

Table 1. Repartition of questionnaires

Region	Administered questionnaires	Compliant questionnaires	Invalid questionnaires	Rejection rate	Questionnaire
Adamaoua	30	22	8	26.67%	73.33%
Center	50	46	4	8%	92.00%
East	20	14	6	30%	70.00%
Far North	45	39	6	13.33%	86.67%
Littoral	30	23	7	23.33%	76.67%
North	40	32	8	20.00%	80.00%
North West	60	54	6	10%	90.00%
West	110	108	2	1.82%	98.18%
South	30	30	0	0%	100.00%
South West	15	11	4	26.67%	73.33%
Total	430	379	51	11.86%	88.14%

This study was conducted using research methods, data collection techniques, simple random sampling techniques, and empirical analysis methods used to achieve the expected objectives. The data used in this context are primary data insofar as there is no database available on cybercrime victimization in Cameroon.

Empirically, Descriptive analysis was performed through univariate and bivariate statistics. Univariate statistics, are conducted using graphics and central tendancy indicators (mean, proportion) to explore the distributions of all variables (variables of cybercrime victimization, socio-demographic and economic factors, and technical factors). Bivariate statistics are produced using cross-tables and chi-square statistical tests between the variables of cybercrime victimization and the explanatories factors.

2.1 Approach

The following steps of this study aimed at learning more about victimization in cybercrime attacks.

- Literature review to rely on discoveries of authors;
- Collection of existing attacks technics to get existing experiences;
- Collection of data through a semi-directive survey;
- Use descriptive statistics tools to process data collected;
- Interpretation of results and recommendations.

2.2 Study Variables

2.2.1 Dependent Variable

The dependent variable is the phenomenon studied. This is victimization to cybercrimes, apprehended by question S3Q3 in section 3 of the questionnaire. The S3Q3_1 question makes it possible to identify the forms of scams, as long as the questions ranging from S3Q3_1_1 to S3Q3_3_1 make it possible to capture the mechanisms by which each form of scam occurred. Questions ranging from S2Q3_4_1 to S3Q3_4_3 relate to whistleblowing and preventive measures against cybercrime.

2.2.2 Independent Variables

The independent variables are the potential determinants of cybercrime victimization. It will be a question of identifying among factors that are associated with the studied phenomenon. They are divided into two categories: technical factors (related to ICT) and socio-demographic and economic factors specific to the respondent. The variables belonging to each of these categories are presented in Table 2.

Table 2. Questionnaire skeleton

Variables	N° of question	Codification
I) Variables of cybercrime victimization		
Has ever been a victim of cybercrime	S3Q3	1 = Yes;0 = No
Form of cybercrime	S3Q3_1	1. Financial diversion 2. Ransom 3. Information hacking
	S3Q3_1_1	1. Mobile Money 2. Sending/withdrawing money 3. Internet banking transaction
Financial diversion mechanisms		
Mechanisms of hacking confidential information	S3Q3_2_1	1. Call and SMS 2. Mail 3. Social media 4. Spy website 5. Other
Ransom mechanisms	S3Q3_3_1	1. Via phone 2. Via computer 3. Via smartphone 5. other
II) Independent variables *(i) Socio-demographic and economic factors*		
Sex	S1Q1	1 = Female; 0 = Male
Age	S1Q2	1. [18–26[2. [27–34] 3. [35–42] 4. [43–50] 5. [51–58] 6. 59+
Education level	S1Q4	1. None; 2. Primary; 3. Secondary; 4. Higher
Marital status	S1Q3	1. Married 2. Single 3. Other

(*continued*)

Table 2. (*continued*)

Variables	N° of question	Codification
Carry out an economic activity	S1Q5	1 = Yes; 0 = No
Income level (in CFA)	S1Q6	1. 0–25000 2. 25000–50000 3. 50000–
		100000 4. 100000-200000 5. 200000–
		3000006. 300000+
(ii) Technical factors		
Completed digital training	S2Q2_1	1 = yes; 0 = no
Type of phone	S2Q4_1	1. Cell phone2. Smartphone Android 3. Smartphone iPhone
Tablet operating system	S2Q6_1	1.Windows
Possession of a security software such as anti-virus	S2Q7_2	1 = Yes;0 = no

3 Results

Table 4 in the appendix reveals the results from these methods. It shows the descriptive statistics of the study variables, the crosstab between cybercrime victimization and explanatory/determinant variables as well as p-values of the chi-square tests carried out between the dependent variable, victimization to cybercrime, and the explanatory variables in pairs.

3.1 Distribution of the Studied Population

3.1.1 Questions Validated Per Region

The exploitation of the questionnaires and the purification of the database resulting from the collection, reveal questionnaires rejected for non-compliance. The reason for the rejection of some questionnaires could be the high rate of non-responses or the high rate of inappropriate responses in the places indicated. At the end, the empirical investigations focused on 379 individuals with a rejection rate of 11.63%.

Moreover, the impossibility of balancing the samples by region is justified by:

- the COVID-19 context in which the survey is being conducted;
- the security crisis in which the North-West and South-West regions are plunged;
- the ambient insecurity in the north (Adamaoua, North and Far North) due to BOKO HARAM;
- the existence of areas with difficult access to the East, South and Coastline in the rainy season (Fig. 1).

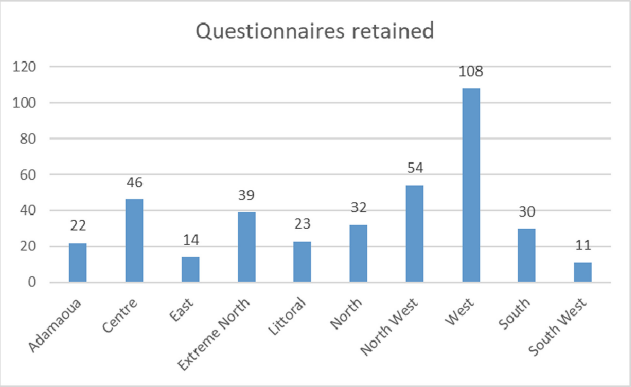

Fig. 1. Distribution of questionnaires in regions

3.1.2 Distribution by Gender and Age

In the sample obtained, 55.15% of individuals questioned are male and 44.85% are female. Men are more willing to respond to questionnaires than women. In addition, the age group under 25 is the most representative within this sample. It is followed by the age groups under 34, then under 42, under 50, under 58 and finally the least represented over 58. This is indicative of a predominantly young population (Fig. 2).

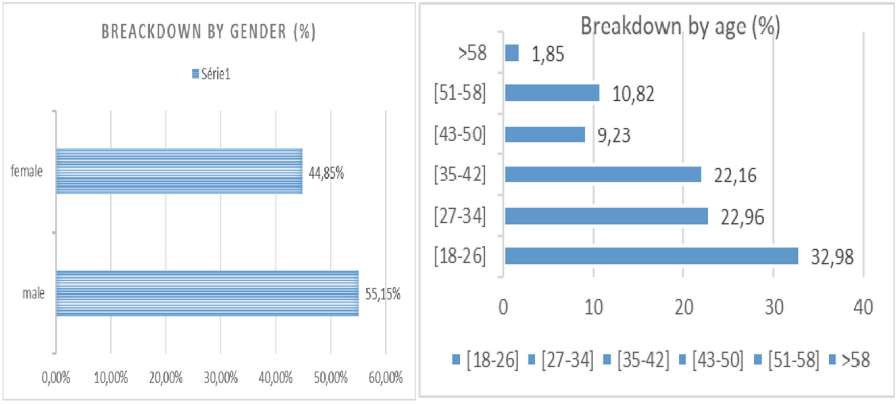

Fig. 2. Distribution of the studied population by gender or age

3.1.3 Distribution by Matrimonial Status or ICT Mastering

The population of single women is the most representative compared to more reserved married women.

It is mainly made up of those who have an average level of mastery of ICT. Cameroon's option was to integrate computer science education at all levels of education (Fig, 3).

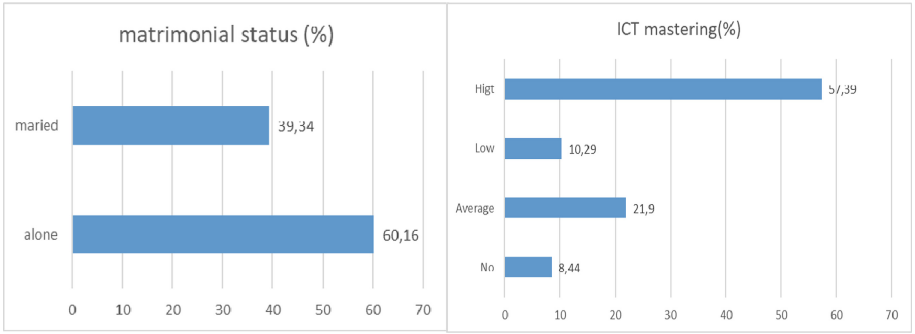

Fig. 3. Distribution of the studied population by matrimonial status or ICT mastring

3.1.4 Distribution According to the Level of Education

The sample contains mostly people with secondary or higher education levels (Fig. 4)

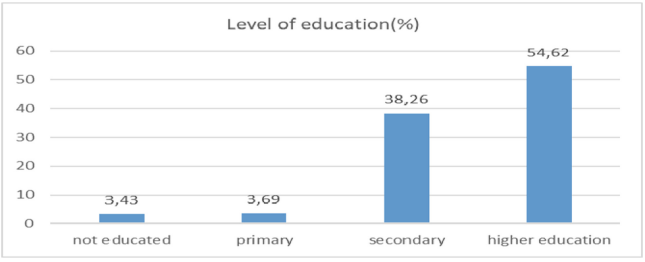

Fig. 4. Distribution of the studied population according to the level of education

3.2 Some Significant Results

3.2.1 Cybercrimes Attacks or Financial Embezzlement Attacks Channels in Cameroon

Most of the cyberattacks are linked to financial embezzlement. Among them, those with mobile money are the most frequent encountered (Fig. 5).

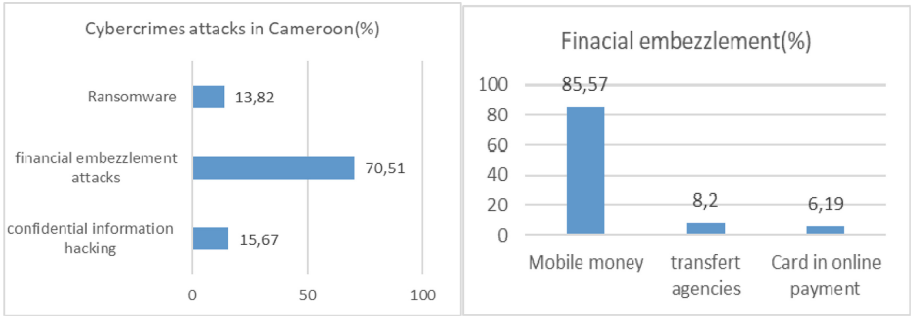

Fig. 5. Frequent types of cybercrimes or financial cybercrime attacks channels in Cameroon

3.2.2 Cybercrimes Attacks Chanel by Ransomware or Information Hacking in Cameroon

The phone is the most used in Cameroon for ransom (98.38%) cases. The cases recorded on a computer or tablet are less.

Of all the channels used for information piracy, 62.2% of cases are by phone call or SMS, then by social networks 25.17%, e-mails 9.45% and finally spy sites 3, 15% (Fig. 6).

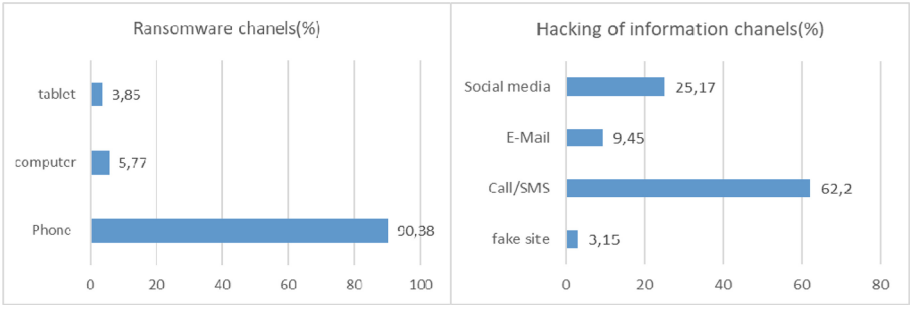

Fig. 6. Ransomware attacks or confidential information hacking attacks channels in Cameroon

3.2.3 Cybercrimes Victimization in Cameroon

Cybercrimes in Cameroon are mostly related to financial embezzlement attacks.

i- *Victims by gender or by age*

Women are more vulnerable to cybercrimes (58.26%) than men (41.74%). Women seem more gullible, more manipulative and more withdrawn than men.

In addition, the elders are exposed due to their low resilience to digital transformation. From 2.61% of young victims under 34 to 25.65% of adult victims over 58 (Fig. 7).

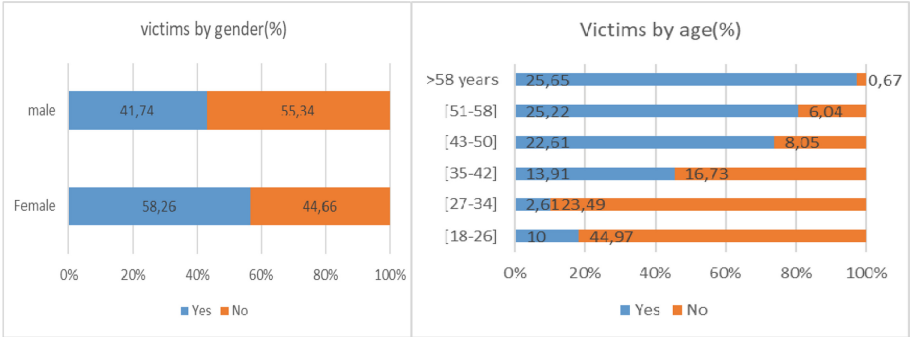

Fig. 7. Cybercrime victimization by gender or age

ii- *Victimization and the level of education*

Victimization and digital knowledge or training to increase awareness Having digital knowledge does not significantly spare cybercriminals. The victimization function is inversely proportional to the level of activity in ICT or awareness (Fig. 9)

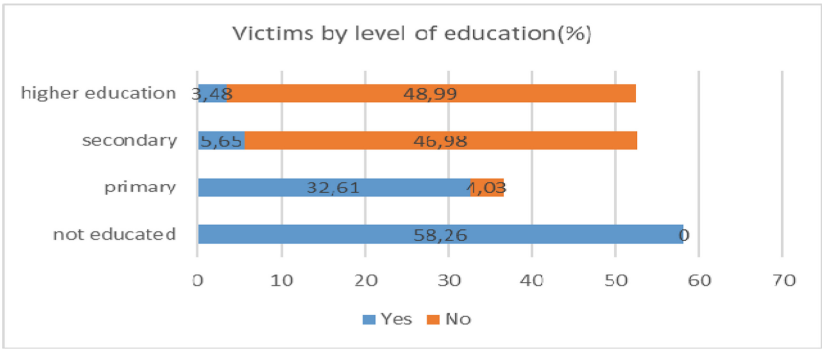

Fig. 8. Cybercrime victimization and level of education

iii- *Victimization and type of phone used or smartphone OS*

Having digital knowledge does not significantly spare cybercriminals. The victimization function is inversely proportional to the level of trainning in ICT or awareness (Fig. 9).

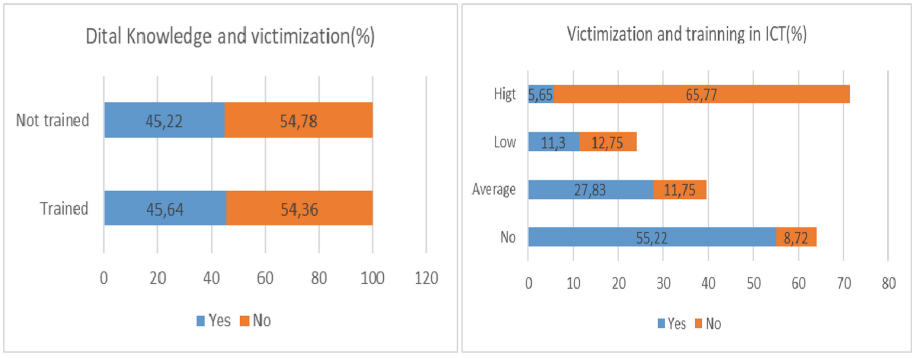

Fig. 9. Victimization and digital knowledge or training in ICT to increase awareness

iv- *Victimization and type of phone used or smartphone OS*

Most victims are killed by Android phones, followed by simple phones and finally by iPhones.. The ease of access to cyberspace by android telephones and their boom in

the landscape of use of digital terminals further exposes the holders of these Terminal Data Processing Equipment (DTE). The Windows Operating System in smartphones is most at risk. We thus have the Windows OS most affected (53.52%) followed by the others (29.58%) and the iPads less affected (16.9%) (Fig. 10).

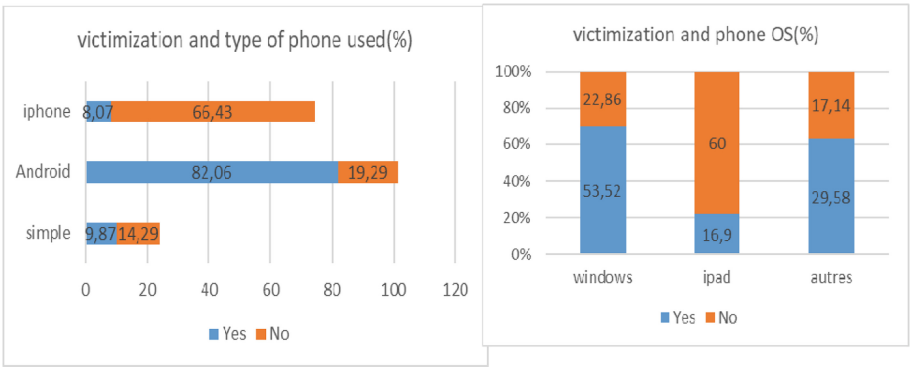

Fig. 10. Victimization and type of phone (OS) used

v- *Victimization and computer OS*

Obviously, the Windows Operating System (OS) is the most exposed. It allows its great use to attack many targets (Fig. 11).

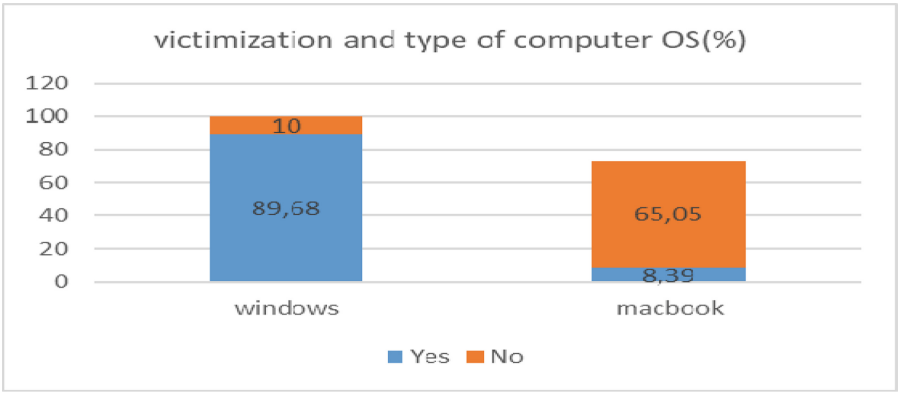

Fig. 11. Victimization and type of computer OS

vi- *Victimization and use of anti-virus/ anti-spam*

The absence of anti-virus exposes systems to spam and other malicious software which opens corridors of vulnerabilities (Fig. 12).

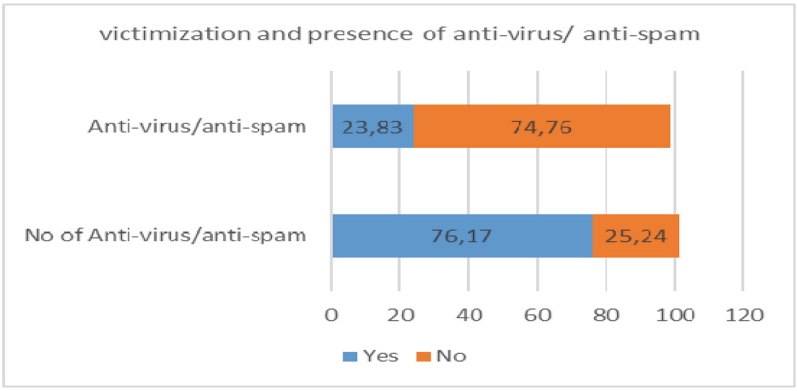

Fig. 12. Victimization and use of anti-virus/anti-spam

vii- *Victimization and economic activity or marital status*

Married women are the segment of the population most affected by cybercrime. i.e., 54.35% of cases compared to single people with 45.65% of cases. The easy gain without the knowledge of the spouse and the repressed fantasies sufficiently explains these figures (Fig. 13).

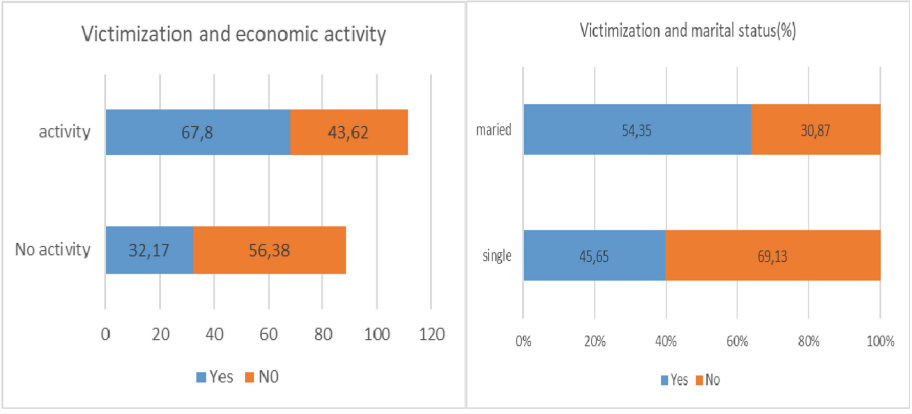

Fig. 13. Victimization and economic activity or marital status

3.2.4 Key Results

Table 3 provides a form of synthesis from all the statistics previously presented. It is a form of map which can be exploited by decision makers to develop policies.

Table 3. Statistics

Statistics	
70.51%	70.51% of cybercrimes are related to financial embezzlement attacks
85.57%	85.57% of cyber-scams target Mobile Money or electronic wallets
98.38%	98.38% of cybercriminal processes exploit social engineering mechanisms
62.2%	62.2% of confidential information hacking activities are done through phone con tact
58.26%	58.26% indicates that the proportion of women is the most vulnerable to cybercrime. 41.74% of men are vulnerable
25.4%	The population segment target by cybercrime is that whose age is above 51 years old (25.4%). This generation of people, which represents 25% of the sample, has great difficulty adapting to digital transformation and is therefore very sensitive to digital deviations
2.48%	Even if the level of victimization is inversely proportional to the level of education, 2.48% of people with a higher level of education are victims of scams. The intellectual level does not automatically reinforce resistance to cybercrime, although it does stir up certain reflexes
54.78%	54.78% of information hacking victims had a very good knowledge of digital technology and its aspects
82.06%	82.06% of attacks occur on Android mobile systems
89.69%	89.69% of users continue to exploit the cracked versions of Microsoft in public and private administrations
76.16%	76.16% of users do not have antivirus or do not care
54,35%	More than half of the population targeted by cyber- scammers has an economic activity
67.83%	67.83% of manipulation cybercrimes are directed towards people carrying out an economic activity

3.3 Observations and Understandings

Some facts are observed. The most vulnerable segment to cybercrime is that one of the women (58.26%) whereas men occupy 41.74% of the vulnerable. Most (70.51%) of the cybercrimes are related to financial embezzlement attacks such as cyber-scams. 85.57% of them essentially target Mobile Money or electronic wallets. Most (98.38%) cybercriminal processes exploit social engineering mechanisms to manipulate and lure users. More than half (62.2%) of confidential information hacking activities is done through telephone contact. The population segment targeted by cybercrime is those whose age is above 51 years old (25.4%). This generation of people, which represents 25% of the sample, has great difficulty adapting to digital transformation and is therefore very sensitive to digital deviations. Even if the level of victimization is inversely proportional to the level of education, 2.48% of people with a higher level of education are victims of scams. The intellectual level does not automatically reinforce resistance to cybercrime, although it does stir up certain reflexes. The proportion (54.78%) of information

hacking victims had a very good knowledge of digital technology and its aspects. The proportion of 82.06% concerns attacks that occur on Android mobile systems within the sample. Most of the victims (89.69%) dispose of Microsoft Windows versions in- stalled in their computers. These victims, in general (76.16%), do not don't have an antivirus or don't care. More than half (67.83%) of the population targeted by cyber- criminals has an economic activity. of manipulation cybercrimes are directed towards people carrying out an economic activity.

Some facts from their oral answers or comments are derived from these observations. Users, tools, and technologies are vulnerable points allowing hackers to express themselves easily. Attackers play with manipulation and weak points to infiltrate (email, social media, SMS, telephone). Since many people are unbanked and attached to Mobile money systems for transactions, cybercriminals learned different flaws from these and leveraged user ignorance and unawareness. Because users continue exploiting Microsoft's cracked versions in public and private organizations, advanced persistent threats (APT) attacks [12] mainly infiltrate ransomware or cyber-espionage exploits. Some testimonies revealed that users have seen their files encrypted and requested to pay a ransom. Answers also show that users are not aware of fake emails and links while using social media, SMS apps, and emails. This study shows that these could be some drivers of cybercrimes.

A respondent told us how she had stolen the mobile money PIN code. She received a call from a very polite someone arguing while nearly crying that there had been a mistake for a deposit in her account. The person kindly asked her to return that money, and 10% is for disturbance. And she innocently checked its account and then saw that it was suddenly empty of a considerable amount. Then tried to call back the caller, but it was too late. This narrative feedback revealed that cybercriminals use social engineering techniques [13] to get users' PIN codes. In this example, for instance, the cybercriminal has initiated a transaction with the victim number as it was herself. But the operation could only continue with the code detained by the legitimate owner.The call was to get the code (before the session timeout) quickly. The cybercriminal tricked the victim into entering this code, and the initial cybercriminal operation was performed until the end. This study shows that the victims are exposed to social engineering attacks.

We have been curious to have some feedback on how the victims are engaged in social media in regards to posts relating to opportunities (job, gains, …). Someone told one of the agents that due to hard daily life, posts of interest are those showing opportunities. He expressed that the only reaction is to look at the name of the concerned institution. In case it is a famous one, he applies. He has already called in the past the number that appeared in the post for further process. And then he sent money in one stage. What is incredible is that he knew that this story was fake many months later when the number of the pretended guy did not ring anymore. Another testimony revealed that the victim has clicked on a link (stipulated to submit files to get entrepreneurial funds) and some days later, access to some confidential accounts was not possible anymore. These situations present clearly how many people behave unknowingly. Based on previous arguments and with regard to cross-table and chi-square tests, the following factors explain the cybercrime victimization: completed digital training (with a p-value of 0.093), level of ICT proficiency (with a p-value of 0.01), type of phone (with a p-value of 0.03), computer operating system (with a p-value of 0.032), posses-

sion of an anti-virus (with a p-value of 0.039), age (with a p-value of 0.01), level of education (with a p-value of 0.02), marital status (0.04) and work status (0.024). Indeed, generations understand and consume technologies differently. It is argued that Youngers are more in contact with these technologies than the older ones. Thus, they are more exposed than older people. However, younger people easily can recognize threat traces since they have faced them a lot. Older people are more vulnerable because they have not known about these issues in their early days. Vulnerable people can be more awareof being assisted with related and adequate digital training. People with prior ICT expertise are less likely to be lured by cybercrimes because of knowledge gained throughout educational processes. The degree of risks is related to the type of mobile smartphone. For instance, Android is most exposed than iOS since it is multi-manufacturers meaning that the manufacturers of devices, operating systems, components, and app stores are different. Everything is centralized by Apple concerning its products. It does not mean that Apple OS is attack-free instead, it means that Android requires vigilance from users to reduce risks [14].

Also, the way users collect and install software determines the degree of exposure to attacks. If people are not aware, they will act with weak behavior letting weaknesses be exploited. For instance, software from unofficial sites, use of unclean USB sticks, unsafe validation of forms, etc. Indeed, the installation of defense utilities constitutes the first line of protection. The status in society may influence behavior when receiving a phishing call or message. For instance, poor people are not likely to be able to look for a huge amount of money required by scammers. In the opposite way, comfortable people in society are likely to take risks in their actions.

3.4 Critical Considerations

This study shows clear interpretations. First, the behavior of people facilitates the activities of cybercriminals. People are unaware of many risks but they are so easily attracted and trapped due to their social precarious situations. In such an ecosystem, ransomware will rapidly be proliferated. People live with scams like flat mates but without minimal awareness requirements or training. Social conditions play a critical role in their victimization since they are looking forward to satisfying basic needs. Unfortunately, there will still be a segment of the population left behind due to the digital transformation advances. Last but not least, mobile money remains to be the target since the population is unbanked. Users, tools and technologies are the points of vulnerability allowing hackers to easily express themselves. Our national systems/platforms are targeted by advanced and persistent threats such as cyber-espionage or e-crime.

3.5 Framework of Recommendations

The framework in Figure 14 depicts the different stages in which governance should be improved to mitigate cybercrime.

3.5.1 Investigation

In this stage, policymakers and company leaders should implement programs to learn from habits and behaviors towards digital transformation and related technologies. This stage should be continuous to observe attitudes and flaws to contain. During this stage's investigations, users should be free to comment and exchange their experiences. The most reliable way should be to put in place a centralized social platform but well oriented to exchange experiences. The architecture can follow the publish/sub- scribe architecture. It does not prohibit surveys like the one in this paper. But the limi- tations will be to merge data with time as well as values or knowledge. Everyone will share experiences concerning cybercrimes and reactions can be provided as well. A background artificial intelligence robot will be exploited to get insights and digest the information presented to people. Decision makers will therefore look at reports anytime to readjust their strategies.

3.5.2 Point of Vulnerabilities (PoV) and Point of Infiltration (PoI) Identification

This stage concerns Chief Information Officers (CIO) and Chief Digital Officers (CDO). In fact, they should perform risk management dedicated to users in their institutions. For that, they should put in place programs to simulate campaigns of cybercrime to the users in order to get their attitudes. Also, they should design filtering rules to track the activities of specific users within a period. The objective will therefore evaluate the likelihood to infiltrate malware such as ransomware or spyware. They will adequately plan for reinforcement sessions.

3.5.3 Distributed Policies Settings

For sake of robustness, agencies in charge of national ICT should collaboratively with related professionals to set policies concerning the exploitation of cracking. This phenomenon is present in many countries in different critical sectors such as administration, private companies, public institutions, etc. They should insist on Iso standards guidelines. More, they should put in place control mechanisms or motivational techniques (awards, etc.) to get people engaged in that. Any legal and declared institution that uses these technologies must agree to these practices. In the case of non-respect, regulated measures will be taken.

3.5.4 Sanitization of Hardware Ecosystem

The manufacturers of devices used to manipulate technology data are possibly unknown and untrusted. If these manufacturers cannot be verified, it poses a problem because the inside can already be infiltrated. Prior quality auditing is required by institutions in charge of that to ensure the protection of consumers. The government should sustain this initiative with infrastructures territorially spread to really guarantee that the minimum is satisfied.

3.5.5 Stimuli Educational Approaches

Cybercrime is ruthless. Educational programs must therefore be adapted to illustrate vivid and touching situations rather than getting learners to recite. This movement implies an inevitable reinforcement of teachers or other training actors. Ongoing programs should be facilitated. For example, we can facilitate registration in open online platforms or national or local sessions bringing together these selected teachers. The program must be gradual and with specific, measurable, achievable, relevant, and time-bound (SMART) objectives. Since the objective is also to reach the general public, it is necessary to target the sectors according to their proximity to the categories of victims and also the most targeted services that have been identified during the studies. Regarding proximity, governmental representations such as district municipalities should be involved as well as parents. Additionally, sensitization programs should be deployed permanently in points of service where people flock such as bill payment places, and financial transactions. The resistance to this is often the language of the targets. For that, information must be provided in several formats (audio, video, text, etc.) well stored in a warehouse. This, therefore, requires people who are well trained in the problems of cybersecurity. The constraint in this stage is to fit learning materials within different ages. For example, a 7-year-old child cannot learn with texts but with interactive materials.

3.5.6 Marketing

This stage is about to disseminate activities of the other stages in media such as TV, Radio, social media, newspaper, and ads.

Fig. 14. Cybercrime mitigation

4 Conclusion and Perspectives

The primary objective of this work was to identify factors that explain victimization in Cameroon. With the help of experiences from respondents and results from the descriptive analysis, cybercriminal techniques, threats as well as behavior weaknesses have been identified. We found technical and socio-demographic ones that are strongly related to victim vulnerabilities. These factors have been justified with proofs and illustrations. Critical considerations have been derived as consequences of understanding.

This study has reflected a critical situation where people of any age suffer from cybercrime and need assistance. In this regard, we have proposed a multi-stage framework with specific activities for policy-makers to sanitize the ecosystem of technologies.

Further research will be concentrated on pushing investigation on attacks such as mobile money and elements to design educational platforms.

Appendix

Table 4. Results

Explanatory variables	Total	Has ever been a victim of cybercrime? No	Yes	chi-square test (p-value)
I- Descriptive statistics of variables related to cybercrime victimization				
Victimisation to cybercrime : Yes	60.69			
No	39.31			
Form of cybercrime: Financial diversion	70.51	-		-
Ransom	13.82	-		-
Information hacking	15.67	-		-
Financial diversion mechanisms : mobile money	85.57	-		-
Sending/withdrawing money	8.25	-		-
Internet banking transaction	6.19	-		-
Ransom mechanisms : Phone	90.38	-		-
Computer	5.77	-		-
Smartphone	3.85	-		-
Other	0			
Mechanisms of hacking confidential information: call/SMS	62.20	-		-
E-mail	9.45	-		-
Social media	25.17	-		-
Spy website	3.15	-		-
II- Descriptive statistics of explicative variables, cross-table and chi-square tests				
Completed digital training : No	54.62	54.36	54.78	0.093
Yes	45.38	45.64	45.22	
Level of ICT proficiency: None	8.44	8.72	55.22	0.01
Weak	21.90	11.75	27.83	
Average	59.37	12.75	11.30	
High	10.29	65.77	5.65	
Type of phone: Cell phone	13.50	14.29	9.87	0.03
Smartphone Android	76.03	19.29	82.06	
Smartphone iPhone	10.47	66.43	8.07	
Desktop operating system: Windows	91.76	10.00	89.68	0.032
MacOS	6.67	65.05	8.39	
Linux	1.57	25.95	1.94	
Tablet operating system: Windows	55.66	22.86	53.52	0.234
iOS	18.87	60.00	16.90	
Other	25.47	17.14	29.58	

(*continued*)

Table 4. (*continued*)

Possession of a security soft-		25.24	76.17	0.039
ware: No	38.23			
Yes	61.77	74.76	23.83	
Sex : Female	44.85	44.66	58.26	0.130
Male	55.15	55.34	41.74	
Age :18-26	32.98	44.97	10.00	0.01
27-34	22.96	23.49	2.61	
35-42	22.16	16.78	13.91	
43-50	9.23	8.05	22.61	
51-58	10.82	6.04	25.22	
>58	1.85	0.67	25.65	
Education level: none	3.43	0.00	58.26	0.002
Primary	3.69	4.03	32.61	
Secondary	38.26	46.98	5.65	
Higher	54.62	48.99	3.48	
Marital status: Single	60.16	69.13	45.65	0.004
Married	39.84	30.87	54.35	
Carry out an economic activity:		56.38	32.17	0.024
No	36.68			
Yes	63.32	43.62	67.83	

References

1. Arakpogun, E.O., Elsahn, Z., Olan, F., Elsahn, F.: Artificial Intelligence in Africa: challengesand opportunities. In: Hamdan, A., Hassanien, A.E., Razzaque, A., Alareeni, B. (eds.) The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success. Studies in Computational Intelligence, vol 935. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-62796-6_22
2. Datta, P.: The promise and challenges of the fourth industrial revolution (4IR). J. Inf. Technol. Teach. Cases **6** (2022). https://doi.org/10.1177/20438869211056938
3. Cascavilla, G., Tamburri, D.A., Van Den Heuvel, W.J.: Cybercrime threat intelligence: a systematic multi-vocal literature review. Comput. Secur. **105**, 102258 (2021)
4. Garg, S., Baliyan, N.: Comparative analysis of Android and iOS from securityviewpoint. Comput. Sci. Rev. **40**, 100372 (2021)
5. Delos Santos, V., et al.: Riskanalysis of home user's vulnerability to illegal video streaming platform. In: 2022 4th International Conference on Management Science and Industrial Engineering (MSIE), pp. 365–372 (2022)
6. Andzongo, S. : Au Cameroun, la cybercriminalité fait perdre 12,2 milliards de FCFA à l'économie en 2021 (Antic). https://www.investiraucameroun.com/gestion-publique/0703-17600-au-cameroun-la-cybercriminalite-fait-perdre-12-2-milliards-de-fcfa-a-l-economie-en-2021-antic. Accessed 19 Aug 2022
7. Ho, H.T.N., Luong, H.T.: Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. SN Soc. Sci. **2**(1), 1–32 (2022). https://doi.org/10.1007/s43545-021-00305-4
8. Borwell, J., Jansen, J., Stol, W.: Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions. J. Digit. Soc. Res. **3**(3), 85–110 (2021)

9. Brands, J., Van Doorn, J.: The measurement, intensity and determinants of fear of cybercrime: a systematic review. Comput. Hum. Behav. **127**, 107082 (2022)
10. Milani, R., Caneppele, S., Burkhardt, C.: Exposure to cyber victimization: Results from a Swiss survey. Deviant Behav. **43**(2), 228–240 (2022)
11. Näsi, M., Danielsson, P., Kaakinen, M.: Cybercrime victimisation and polyvictimisation in Finland—prevalence and risk factors. European J. Criminal Policy Res. **29**, 283–301 (2021)
12. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N.: Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Eur. Soc. **23**(sup1), S47–S59 (2021)
13. Breen, C., Herley, C., Redmiles, E.M.: A large-scale measurement of cybercrime against individuals. In: CHI Conference on Human Factors in Computing Systems, pp. 1–41 (2022). https://wp.stolaf.edu/iea/sample-size/. Accessed 19 Aug 2022
14. Tatam, M., Shanmugam, B., Azam, S., Kannoorpatti, K.: A review of threat modelling approaches for APT-style attacks. Heliyon **7**(1), e05969 (2021)
15. Venkatesha, S., Reddy, K.R., Chandavarkar, B.R.: Social engineering attacks during the COVID-19 pandemic. SN computer science **2**(2), 1–9 (2021)