International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A PRACTICAL APPROACH TO FIGHT AGAINST SCAMMING AT THE NATIONAL LEVEL IN SUBSAHARAN AFRICA: CASE OF CAMEROON

Ebot Ebot Enaw
University of Yaounde I, Cameroon
National Advanced School of Engineering
Department of Computer Sciences

Abstract

With the ever growing adoption of Internet and ICT in our daily life especially in Africa, the continent has experienced a surge in cybercrimes in the past decade. New cyber-threats taking advantage of the insecure and unstable nature of the cyberspaces of African countries have emerged including scamming. Thanks to the key role ICT/Internet plays in the social and economic development of a country, mitigating these threats is therefore a top priority for governments. For this to happen, governments need to have a good understanding of these threats as well as the environmental issues that foster the spread of the threats.

This paper first of all presents an analysis of the scamming phenomenon in a typical developing country based on several social and environmental criteria including the profile of the perpetrator and their victims, their modus-operandi and secondly presents the measures that governments need to take to mitigate the threat. Our article is structured as follows: section 1 introduces the topic, section 2 presents some research papers related to the topic, section 3 delimits the problems, section 4 presents the methodology used, section 5 presents the main categories of scamming, section 6 proposes our solutions to mitigate scamming, section 7 analyzes the scamming phenomenon in Cameroon, and section 8 presents a conclusion.

Keywords: *scamming, social engineering, cybercriminality.*

1 Introduction

Our society is increasingly dependent on ICT and Internet to assist us in almost every aspect of daily life including communication. Although ICT/Internet are very useful, some individuals use them to commit illegal activities usually called cybercrimes. Several types of cybercrimes exist each with its own specificity and environment. With the development of Internet across sub-saharan Africa, other forms of cybercrimes taking advantage of the socio-economic environment of sub-saharan countries marked by abject poverty have emerged namely scamming. The aim of this paper is to provide a social and environmental analysis of the phenomenon so as to better apprehend it and then propose pragmatic measures to tackle this phenomenon. Our analysis is based on the Cameroon context and will first of all present the different types of scamming along with their inherent characteristics, the profile of the victims and scammers and secondly lay out some measures that can be taken to mitigate this threat.

2 Related work

Some research papers related to this topic have been published namely [1] which presents a detailed analysis of the methods employed by scammers to influence the judgment and the psychology of victims as well as the psychological mechanisms that drive the reaction of a person to a scam. Their analysis was based on interviews, scamming material text mining and behavioral experiment. [2] explores attacks as binary decision problems as the attacker has to decide whether to attack someone or not without knowing at first glance if it will be profitable for him. It ends up showing that as victim density decreases, the fraction of users that can be profitably attacked decreases drastically. [3] presents the major aspects and underlying constructs of social engineering and the relations between them. Through literature review and interview they came up with an improved model of social engineering attacks.

3 Problem statement

According to MacAfee report on the economic impact of cybercriminality published in july 2013, cybercriminality cost 500 billions of dollars to the global economy. With the ever growing adoption of ICT/Internet in subsahara African countries, its contribution to the GDP of these countries is increasing year by year. However, new forms of cybercrimes emerged including scamming: that consists of deceiving or abusing the confidence of somebody through Internet (mail, web, ToIP) in an effort to obtain money or something else of value. Scamming takes advantage of the socio-economic environment of sub-saharan countries marked by abject poverty and the desire to get out of poverty by all means. It destroys the credibility of the cyberspaces of these countries and as such reduces the potential contribution of ICT/Internet to their GDP. Given the level of poverty of these countries and the opportunity that ICT/Internet represents for the development of their economies as well as the well-being of their population through projects like Ecommere, E-learning, E-health and E-government, it is therefore mandatory for them to take appropriate measures to mitigate this threat in order to reinforce the credibility of their cyberspace and in turn leverage the benefits of ICT/Internet to develop their economy and improve on the well-being of their citizens.

4 Methodology

In an effort to lay out measures that sub-Saharan African countries should take to mitigate the scamming phenomenon, we adopt the following approach. We first conduct an assessment of the phenomenon and the environment in which it operates in order to identify the inherent characteristics of scamming and the environmental factors that influence it. Then, based on the results of the assessment phase, we developed a platform that is meant to provide all stakeholders(Telco, CIRT, Law enforcement) with a way of putting their skills and know-how together in order to mitigate scamming. Some measures that need to be implemented at the national level, are finally proposed.

5 Manifestations of scamming

Internet scamming consists of cheating or abusing the confidence of somebody through the Internet (mail, web, ToIP) in an effort to obtain money or something else of value. Internet scamming can be classified into four main categories:

- Art: In this type of scamming, the scammer deceives his victim that he owns a valuable and renowned art object that he wants to sell. The scammer usually presents some photography and videos of the object to the victim and requests for a certain sum as advance payment, before the said object can be delivered
- Animal: In this type of scamming, the scammer deceives his victim that he owns an animal that he wants to sell to the victim. The scammer usually presents some photography and videos to the victim and requests for a certain sum as advance payment, before the said object can be delivered
- Lottery: In this type of scamming, the scammer deceives his victim that the victim has won a lottery and for him to receive his price, he should send a processing fee
- Inheritance: In this type of scamming, the scammer deceives his victim that he is the heir of an important wealth but he needs a certain amount of money for administrative procedures charges.

In order to communicate with their victims through the Internet, scammers use various channels namely websites, emails, chat services like skype. However, the first contact is usually made through Internet forums and spams whereby they post their messages.

6 Our Solution

After analyzing the scamming phenomenon as well as the environmental factors that influence it, we came up with the conclusion that at the national level, two types of measures need to be taken: technical and non-technical. For the technical part, we developed a platform through which all stakeholders (victims, law enforcement, Telco) will interact and put their skills and know-how together to help investigate and take appropriate measures aimed at mitigating scamming. However for the platform to be really effective other non-technical measures need to be taken also. The technical and non-technical solutions will be developed in subsequent sections.

6.1Technical solution

Given the specificities of the scamming landscape, mitigating the threat requires adopting a participative approach. In this regard, we developed a system enabling all stakeholders to collaborate in order to mitigate scamming. The system is made up of five modules as depicted in the figure below. These modules are described in the sections below.

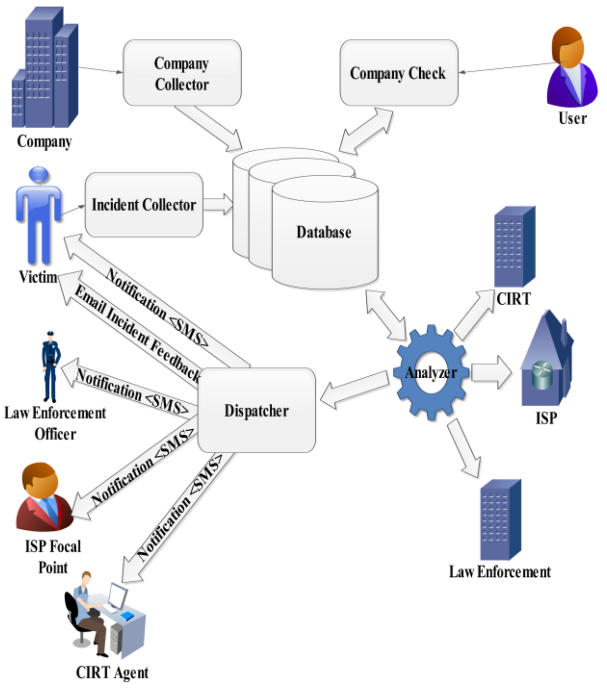

Figure 1: Architecture of the technical platform

6.1.1 Company collector

This module allows businesses that are installed in Cameroon, to register their details in the system. When a business submits its details, the information is verified by ANTIC in collaboration with the Ministry of Finance and Ministry of Small and Medium size enterprises in order to ascertain correctness of data provided. Once the information provided is authenticated, the business is inserted in the database as a regular company installed in Cameroon.

Each year, the Ministry of Finance and the Ministry of Small and Medium size enterprises verify the authenticity of company data and if the data are no longer authentic, or the company no longer exists, its status is changed on the system accordingly. Information provided by companies is described in the following table.

Table 1: Data provided by companies

Information	Description
Name	Name of the company
location	Address of the company's main and branch offices and GPS coordinates if available
Social network	A link to the business profile on social network like facebook and twitter
website	URL of the website of the company
Email	List of Emails through which the company can be reached
Phone numbers	Phone numbers through which the company can be reached
Business	Description of the companies activities
Tax slip	A scan copy of the tax slip of the current

6.1.2 Company check

This module is aimed at providing a way for a user or a business to verify the authenticity of information of a business claiming to be established in Cameroon. The verification can be made through several criteria namely: email, phone number, company name, website. When a user chooses the criteria on which he wants to make the verification and enters its corresponding value, the module checks the database to see if there is a company that matches the specified value and displays the result. To anticipate on the fact that a user can misspell the data to be verified, the system also displays the results that are close to the words that the client entered in his query.

The Cameroon government will subsequently advice partner countries, to sensitize their citizens on the usage of this module, accessible to all individuals and businesses around the world so that when someone receives an email, an SMS or a phone call from a person/business claiming to be in Cameroon, he could verify the authenticity of the information through the module.

6.1.3 Incident collector

This module collects incidents from individuals or companies which are victims of scamming. In order to submit an incident, the victim has to provide some information that will be stored in the database. The information required in the form is provided in the following table:

Table 2: Incident data

Information	Description
Name	Name of the person that filled the form
Date of birth	The birth date of the individual reporting the incident
Gender	Gender of the individual reporting the incident
company	The name of the individual/company that was targeted by the scammer
Address	Address of the victim
website	URL of the website of the victim
Email	Email of the person that fill the form
Phone numbers	Phone number of the victim and that of the person that fill the form
Description	Description of the incident
Evidences	It can be the copy of the email along with its full header, a document sent by the scammer or a copy of the SMS, etc.

This module also acts as a ticketing system since when a victim submits an incident, a copy of the information he provides along with the incident identifier generated by the system is sent to him through email. This identifier will permit the victim to follow the handling process of his incident.

6.1.4 Analyzer

This module interacts with three stakeholders: CIRT (Computer Incident Response Team), Telecom operator and Law Enforcement as follows:

When a victim submits an incident to the platform through the "Incident collector" module, a CIRT analyst will first analyze the incident in order to develop a procedure to eradicate or contain the incident, identify and localize the scammer, assign a priority to the incident, determine whether the incident is related to other reported incidents. To get the geolocation and the identity of the scammer, a request might be sent to Telecom operator.

When Telco receives the request, an attempt to obtain the geolocation and the identity of the scammer, will be made based on the evidences sent by the CIRT agent namely the IP address and the phone number. The result is sent to the CIRT analyst and law enforcement officers through the Analyzer module.

When the incident is reported to law enforcement officers, it gets investigated and the finding are posted on the platform.

It is worth mentioning that during the process described above, the victim is informed regularly on the evolution of the process through messages provided by the "Dispatcher" module.

All the email addresses as well as phone numbers involved in scamming activities are stored in the database so that when someone queries the platform with these information, the system immediately alerts the user.

6.1.5 Dispatcher

This module is aimed at sending alert and information by email and SMS.

Normally, information (acknowledgment of receipt of the incident, acknowledgment of receipt of the subscription of a business, notification of an update on a case) are sent by email but for high priority cases, notifications are sent by SMS.

This module is also in charge of sending the final report of the incident to the victim once the CIRT analyst closes the incident.

6.2 Non-technical measures

In order to mitigate scamming in developing countries, and given the specificities of this threat and the African environment which were presented in previous sections. Some measures that Governments, especially those of sub-Saharan Africa countries should take at the national level were identified, in addition to the technical platform described above. Most of these measures have already been experimented in Cameroon, they include:

- Developing a legal framework related to cybersecurity ;
- Developing a National cybersecurity strategy ;
- Organizing a national sensitization campaign across the country. This campaign is aimed at sensitizing people on key issues related to cybersecurity including: the legal framework related to cybersecurity, cybersecurity threats, cybersecurity best practices. The sensitization campaign targets mainly young people (universities and secondary school students) between the ages of 18 and 30 years and employees of governments and private companies that represent the strata of society that is more prone to scamming. In Cameroon, since the beginning of the sensitization campaign in 2013 a decrease of 20% of complaints related to cybercrimes has been observed ;
- Requiring Internet Service People to store the log of all internet transaction for 10 years as stated in the Cameroon law on cybersecurity and cybercriminality
- Requiring Internet Service Providers to provide their clients with a cybersecurity best practices guide
- Requiring Cybercafe to check and log the identity of clients before granting them access to Internet

7 Some results

Based on data gathered through the Incident Collector module and law enforcement, we conduct an analysis of the scamming phenomenon in Cameroon.

7.1 Scamming originating from Cameroon

According to data gathered from the platform and law enforcement, there were 519 scamming cases between 2006 and 2013 involving scammers located in Cameroon. The distribution of these scamming among the categories that were previously identified is depicted in the following table.

Table 3: distribution of scamming originating from cameroon with respect to categories

Categories	Numbers	Percentage
Animal	327	63%
Art	125	24.08%
Lottery	21	4.05%
Heritage	46	8.87%
TOTAL	519	100%

Based on the results of law enforcement investigations, we analyzed the social profile of the scammer on several aspects (age, gender, profession) and we came up with the following results:

Regarding the gender, 94.3% of scammer were male and only 5.7% were female as depicted in the following table.

Table 4: distribution of scamming originating from cameroon with respect to gender

Categories	Number of Male involved	Number of female involved	TOTAL
Animal	589	2	591
Art	137	46	183
Lottery	21	0	21
Heritage	46	0	46
TOTAL	793	48	841

By analyzing the age of scammers we came out with the following table:

Table 5: distribution of scamming originating from cameroon with respect to age

Categories	14-18	18-25	25-30	30-40	40+	TOTAL
Animal	17	366	130	41	37	591
Art	3	24	86	53	17	183
Lottery	1	11	8	1	0	21
Heritage	3	22	11	7	3	46
TOTAL	24	423	235	102	57	841

By analyzing the profession of scammers, we came out with the following table:

Table 6: distribution of scamming originating from cameroon with respect to profession

Categories	Animal	Art	Lottery	Heritage
Universities student	389	96	15	19
Secondary school students	54	5	0	2
Unemployed	129	80	6	25
Employed	9	2	0	0
TOTAL	591	183	21	46

Given that Cameroon is bilingual with two official languages English and French. A quick analysis of the first language of scammers revealed that most are English speaking as revealed in the table below.

Table 7: distribution of scamming originating from cameroon with respect to first language

Scamming Categories	French	English	TOTAL
Animal	181	410	591
Art	80	103	183
Lottery	10	11	21
Heritage	20	26	46
TOTAL	291	550	841

From the tables presented above, we can deduce the following assertions:

- More than 92% of scamming pertain to the Art and Animal categories ;
- More than 78% of scammers are between the ages of 18 and 30 years ;
- More than 65% of scammers have English as their first language ;
- More than 90% of scammers are university students or unemployed youths.

7.3 Scamming targeting Cameroon citizens

Using data collected from the platform, an analysis of the profile of the victims based on some aspects including: gender, age, profession and origin, was conducted.

This analysis revealed that between 2006 and 2013, 117 cameroonians were registered as victims of scamming. The distribution of this scamming among the categories enumerated previously is provided in the following table.

Table 8: distribution of scamming targeting cameroon citizens with respect to categories

Categories	Numbers	Percentage
Animal	0	0%
Art	0	0%
Lottery	76	64.9%
Heritage	41	35.1%
TOTAL	117	100%

Regarding the gender of victims, more than 88% were women and 12% were men.

Table 9: distribution of scamming targeting cameroon citizens with respect to gender

Categories	Number of Male	Number of female	TOTAL
Animal	0	0	0
Art	0	0	0
Lottery	8	68	76
Heritage	6	35	41
TOTAL	14	103	117

By analyzing the age of victims we came up with the following table:

Table 10: distribution of scamming targeting cameroon citizens with respect to age

Categories	14-18	18-25	25-30	30-40	40+	TOTAL
Animal	0	0	0	0	0	0
Art	0	0	0	0	0	0
Lottery	0	0	10	55	11	76
Heritage	0	0	8	28	5	41
TOTAL	0	0	18	83	16	117

We also analyzed the profession of victims and we obtained the following results:

Table 11: distribution of scamming targeting cameroon citizens with respect to age

Categories	Animal	Art	Lottery	Heritage
Universities student	0	0	25	14
Secondary school students	0	0	0	0
Unemployed	0	0	5	1
Employed	0	0	46	26
TOTAL	0	0	76	41

As previously stated, Cameroon is bilingual with English and French as official languages. After analyzing the first language of the victims, the following result was obtained:

Table 12: distribution of scamming targeting cameroon citizens with respect to first language

Scamming Categories	French	English	TOTAL
Animal	0	0	0
Art	0	0	0
Lottery	20	56	76
Heritage	14	27	41
TOTAL	34	83	117

From the tables depicted below, we can deduce the following assertions:

- cameroonian have been victims of two types of scamming lottery (65%) and heritage (35%)
- More than 88% of victims were women
- More than 70% of victims are between 30 and 40 years old
- More than 70% of victims have English as their first language
- About 60% of victims are employed and 33% are universities students
- Internet penetration is around 7% but around 50% of young people between 16-30 years living in cities have access to Internet

7.3 Environmental factors

From the analysis of the environment, we identified some factors that influence the surge of scamming in Cameroon. These include:

- The low rate of cybercriminality awareness: Most Cameroonian including scammers are not aware of the cybercriminality law that was enacted in 2010 and in which scamming and other forms of attacks are punishable. This makes scammers believe that scamming is just a joke that is not subject to prosecution;
- Lawyers and law enforcement are not trained enough on cybersecurity as well as digital evidence collection and analysis ;
- Internet Service Providers have not deployed Internet metadata storage and monitoring facilities ;
- Cybercafes where most cameroonian access Internet from, do not require their customers to identify themselves with their national identity card before granting them access to the Internet ;
- The standard of living is high with a high rate of unemployment among youths and more than half of the population earns less than 2$ a day ;
- There is a proliferation of cybercafes around universities, which offer low cost access to the Internet.

8 Conclusion and future work

We live in a world where Internet/ICT is playing an important role in almost every aspect of our daily life and that valuable role is still growing day by day. Due to its tragic history, Africa was left out of the Internet/ICT development that spread across Europe and USA for many years since it had to address some basic and urgent issues like famine, social conflicts, etc. Nonetheless, in the last ten years, Africa has embraced ICT/Internet which is playing an important role now in the modernization of the continent in key areas including governance (Egovernance), health (E-health), and education (Elearning) and actively participate in the development of the economy. However, with the development of ICT/Internet in Africa, new threats adapted to the context of the continent have emerged namely scamming. In this paper we conducted a social and environmental analysis of the scamming phenomenon in Cameroon, which is high in the ranking of countries affected by scamming. We identified environmental factors that influence the spread of scamming as well as the profile of scammers and victims. We then proposed firstly a technical platform aimed at providing a way for all the stakeholders to put their skills together in order to investigate on scamming cases as well as providing assistance to victims and secondly some non-technical measures that countries need to take at the national level to mitigate this threat.

Future work can include leveraging the artificial intelligence theories and knowledge available on scamming to build a system that can automatically detect and prevent scamming to a certain extent.

References

[1] "The psychology of scams: Provoking and committing errors of judgement, University of Exeter School of Psychology" University of Exeter School of Psychology, May 2009.

[2] Cormac Herley, "Why do Nigerian Scammers Say They are from Nigeria?" *Microsoft Research*, 2012.

[3] Lech J. Janczewski, Lingyan Fu," Social Engineering based attacks: Model and New Zealand perspective"*whitepaper*, International Multiconference on Computer Science and Information Technology, 2010.

Biography

Dr. EBOT EBOT ENAW obtained his B.Eng hons degree from Liverpool University in Electronic Engineering in 1989. He later obtained an M.Eng degree in Telecommunication Engineering from The University of Manchester England in 1991. He returned home where he was recruited in the University of Yaounde I, as an assistant lecturer. He pursued his university studies and obtained a PhD in Computer Sciences from the National Advanced School of Engineering of the University of Yaounde I, where he is currently a senior lecturer. His area of specialization include: computer network security, cryptography and formal specification and verification; theorem proving and model checking. He has published some research articles in international journals including *A system for collecting security alert and diffusing customized security bulletin, International Journal of Advanced Computing, Volume 3 Number 2, page 27-34.* In 2006 he was appointed Director General of the National Agency for Information and Communication Technologies Cameroon, a position he occupies till date. Major activities of the agency include amongst others: securing the Cameroon cyberspace through three key services: Computer Incident Response Team (CIRT), Public Key Infrastructure (PKI) and Computer Security Audits.

Dr. EBOT EBOT ENAW may be reached at ebotenaw@yahoo.com