ЕКОНОМИКА
ISSN 0350-137X, EISSN 2334-9190, UDK 338 (497,1)
Vol. 63, october-december 2017, № 4
P. 97-104

**Živanka Miladinović Bogavac**[1]
University Union „Nikola Tesla“, Belgrade
Business and Law Faculty, Belgrade

SCIENTIFIC REVIEW ARTICLE
DOI:10.5937/ekonomika1704097M
Received November, 03, 2017
Accepted: November, 30, 2017

# BUSINESS SCAM IN SABER SPACE

**Abstract**

*Security can very easily be compromised by human factors. Human fantasy, stupidity, and ignorance of security rules are often key factors that contribute to security breaches. As more advanced security technologies are developed that make it difficult to find technical failures, attackers are increasingly turning to the human factor as a central element in the information and communication infrastructure, without which computers or networks cannot function without which. The use of human weaknesses often does not require any investment and implies a minimal risk. It is precisely these circumstances that led to the emergence of Nigerian fraud and its existence in cyber space for two decades.*

***Key words:*** *security, technologies, human factor, fraud.*

**JEL Classification:**K10, K20, F39

# ПОСЛОВНЕ ПРЕВАРЕ У САЈБЕР ПРОСТОРУ

**Апстракт**

*Безбедност може врло лако бити угрожена људским фактором. Људска лаковерност, глупост али и непознавање безбедносних правила су често кључни фактори који доприносе нарушавању безбедности. Како се развијају савршеније безбедносне технологије, које отежавају проналажење техничких пропуста, нападачи се све више окрећу људском фактору као централном елементу у информационо-комуникационој инфраструктури, а без ког рачунари или мреже не би могли да функционишу. Коришћење људских слабости често не изискује никаква улагања и подразумева минималан ризик. Управо су ове околности довеле до појаве нигеријске преваре и њеног егзистирања у сајбер простору већ 2 деценије.*

***Кључне речи:****безбедност, технологија, људски фактор, превара.*

## Introduction

„Nigerian scam“is a specific way of committing the crime of fraud as a form of cybercrime. This scam arose due to the development and the global role of the Internet, which offered its users easier communication. The emerging forms of this scam involve

[1] zivankamiladinovic@gmail.com.

©Друштво економиста “Економика” Ниш
http://www.ekonomika.org.rs

false business proposals, while the amount of money that the victim owes to pay, and who, when communicating with the fraudster, appears to be necessary, is incomparably less than the amount that should be gained after the successful completion of the work. This scam was made according to the model of the Spanish prisoner to the popular type of scam in the 18th century, on the principle of Pigeon Drop which implies the investment of a smaller amount of money to ensure the gain of a larger sum or some other higher material gain. These models fall into the abuse of trust abuse, emphasizing the secrecy, the confidentiality of „work" and the need for the victim to be a person of extraordinary trust. The Nigerian scam existed even before the expansion of the Internet, when it was sent by post (from the mid-80s of the 20th century), but the appearance of the Internet is experiencing its boom.

Victims (mugus - the Nigerian name), after receiving such a message, get the impression that happiness has smiled and that they have been entrusted with trust and honor, and that they will get millions upon completion of their work. They are solely required to pay the sum of money, for humanitarian purposes, as aid, and for which they will be rewarded in a number of ways. Therefore, „fraud 419" or „Nigerian scam" is called „advance fraud", and the names „scheme 419", „Nigerian scheme" are also known. The name 419 refers to a member of the law of fraud in the Nigerian law. A safe way of making wages to victims, which from the perspective of the victim can act both legally and illegally, in any case, it is sufficiently appealing that the victim can often refuse to deny him. The embezzlement of the money invested, for which it will be multiplied, is followed by mostly fairy-tale and heartbreaking stories. Cyber criminals in the execution of the Nigerian fraud were persistent and spent months actively communicating with the victim, in order to „soften"her and to gain her trust. In addition, victims are often uncomfortable to refuse the person who has invested so much time and effort in gaining their trust.

When the victim agrees to pay the money, she is subsequently required to pay new payments due to new costs and expenses, and with the constant indication that millions only have not arrived at her account. For this scam, the addiction is identical to that of a gambler, or games of chance. Naive users risk a small amount of money in order to earn millions. There is always the chance that everything will be lost. Even when a certain amount of money is paid, and when fraudsters in the capacity of business partners seek new payments for newly born job costs, the victim is preoccupied with the belief that the gain will eventually come.

## Phases of executing Nigerian fraud

Some authors describe the Nigerian fraud as part of the following stages:

1. The allegedly official office of a foreign government or agency sends a letter, email or fax;
2. the letter presents a business proposal for transferring millions of dollars to the victim's personal bank account, and offers a certain percentage as „first aid";
3. The letter encourages the victim to travel overseas to learn details;
4. The letter also requires the victim to provide a blank company memorandum, bank account information and telephone numbers;

5. The victim receives various documents with official stamps, stamps, logos, etc., which prove the authenticity of the offer and leave the impression of the authorities.

Finally, the victim is required to pay in advance the money for various taxes, for registration, permits, etc. (Петровић, 2004, p. 148-150).

The first steps in executing this scam are related to creating accounts on free Gmail, Hotmail or Yahoo platforms by contacting targets. The email address is conceived to be associated with an authoritative person or institution, to which the victims will be settled and will not check in the commercial registry agency whether there is such a company in their country or whether there is any prior user experience on the Internet with them. E.g:

vangtc.state.gov@usa.com,
info@willyjacklawfirm.gov-tg.com,
fbi.gov@zing.vnus,
military.gov@gmail.com,
western_union_money_transfer@hotmail.fr,
westernunionpaydepartment@videobank.it,
kingsjack222222@sify.com,
info@alegrete.rs.gov.br,

The next step is to search for the victim. Names and email addresses are taken when you sign up for free portals. In this way, fraudsters can collect several thousand addresses in a few days.

As a sender, there may be persons who actually exist, but their identities are stolen without their knowledge, and the perpetrators use them to hide their true identity or that the trust of the victims of fraud and confidence will be gained by the strength of the authority of certain individuals. Electronic messages are addressed to any recipient of the message and from them cannot be seen to who the sender addresses, and their context is such that the recipient of the message can easily think that the message relates to him right away.

The text of the messages is mostly written in English to be understood by people all over the world to whom the message arrives. However, criminals sometimes speak in the victim's language, for example, in Russia; Nigerian letters are translated into Russian via electronic translators, which are easily noticed due to inconsistent language constructions with a large number of errors. The content of the message is always such that it aims to combine the emotional and greedy side of man's nature. Often, in the background, there is a heartbreaking, romantic, fairy-tale story, which suggests a place for a supporting role that will fall victim to. The victim is shown here as a hero, as a courageous accomplice in great things, which targets the ego of the victim. This type of fraud has exploited the primary instinct of human greed, because the expression of humanity is richly rewarded, but also the need to affirm its own value. Basically, this scam is an imaginary solution to the problem; recipients see these suggestions as a light in a tunnel, a type of salvation, or a call to humanity.

In the first message, the fraudsters do not mention that the recipient should pay some money, but mostly their applications refer to help with transferring money to the account in their country, and for what will be rewarded. However, already in the following message, the executor of the scam „unexpectedly"encounters various small

costs, which the only recipient of the message can reconcile either due to a blocked account, or because of the inability to pay in another country. Basically, the use of bribe costs, bank fees, lawyers' fees, inability to make payment in the country from where the letter is sent, etc. are used as an excuse.

The profit that the addressee can generate includes millions of dollars that will be shared by alleged investors at the end of the deal with the victim of fraud, and the promised percentage of earnings goes up to 40% of the amount of money that is the subject of „work". There are also cases in which value goes up to 50%.

If the victim of a scam accepts the offered „job", perpetrators of this scam can deal with the different circumstances that communication with the victim imposes. In a short period of time, they can create a false order, photos and provide other evidence to support their story, such as forged seals, signatures, false content, and so on. In order to convince the victim of the truthfulness of the work, perpetrators communicate via mobile phones using prepaid SIM cards, which they can easily cast and then buy new ones for further communication. Fraud cheaters hire lawyers, bank employees, and other professionals, sometimes involved in communication, bringing the victim even deeper into the misconception and keeping it in a false belief that it really is a real, not a fictitious business.

Nigerian deception tools are: forged documents, wireless transfers of money for the transfer of unlawfully acquired funds, technical means that allow them anonymous communication, web-based e-mail, electronic orders pre-downloaded from the right users, fax machines for sending faxes when exchanging documentation with victims of fraud, the services of telecommunication services for direct communication with the victim of fraud, as well as fake websites on the Internet damaged the victim is misled to communicate and cooperates with representatives of the legal and legitimate institution (Dyrud, 2005, p. 11).

Naive citizens, wanting to earn a large sum of money in a very short time, agree to send their personal information and the bank card number. Of the victims, most often they are asked to pay money through Western Union and Money Gram due to the speed of transfer of funds and anonymity of the payee, which reduces the possibility of discovery of perpetrators. As the injured party pays a certain amount of money according to the instructions of the perpetrators of criminal offenses, the postponement of cash transactions related to the payment of the promised sum of money is followed. There are constantly emerging new costs for the injured party in the name of job realization and new delays, the „express" payment of money is constantly promised, and the victim of fraud persuade that the investment in the agreed job will be paid off in many cases.

Psychological pressure on the victims of fraud is additionally done by stating that the secrecy of „work" is necessary, since corrupt officials of some state would have appropriated money for themselves if they found out that it exists (Buchanan and Grant, 2001, p. 39-47). Sometimes the victim of fraud also exerts himself above himself (for example, when, after they find out that they are deceived, the victims of fraud continue to communicate in order to recover money, find the perpetrators, etc.). Criminal offenders rely on the fact that, during the time she passes until the victim finds that she is deceived (i.e., while she realizes that the promised money does not exist), the money transfer she made to their accounts will be paid, and the injured party will not arrive blocking transfer in time.

When the victim pays the required amount, the cheat never arises again, and the chance to get tracked is minimal. The fact is that perpetrators of these crimes use information technology to hide their identity and physical location in order to hinder the efforts of police services to detect them. Messages are sent mainly from the Internet cafes, whereby every trace of the true identity of the scams is lost. In Nigeria, in areas such as, for example, Lagos or Festak, there are many Internet cafes that are open for this purpose, and their working hours are from 22.30 hours to 07.00 hours to avoid the control carried out by the state officials (Chawki, 2006, p. 39-64).

Unlike the victim, the perpetrator of fraud is only on gain. At the time it was discovered, 15 years ago, a journalist from the West asked one of the fraudulent schemes 419, „How much does this fraud cost?". When asked by a journalist, the fraudster replied: „Two dollars. The dollar is to pay the Internet clock in the cafe and another dollar to drink coffee".

The most risky countries from which this type of fraud is committed are the countries of West Africa: Nigeria, Ghana, Benin, Ivory Coast, Togo and Burkina Faso. Out of the territory of West Africa, the most risky countries whose territories are involved in these types of fraud are South Africa, Spain and the Netherlands. Here is a Nigerian diaspora. Interestingly, in Russia, a variant of Nigerian fraud has emerged in which a wealthy businessman offers large sums of money to help transfer money to another country.

Because of such scams, citizens who are, guided by human, emotional or business reasons, and sometimes by greed, have greatly begun to communicate with a wealthy stranger, and have agreed to send money without prior verification, believing to senders using „methods social engineering" to convince them of the truth of their story.

It is considered that there is a big „dark figure" when „Nigerian scams" are concerned because of the damaged faces or are not aware that they are deceived, or they are embarrassed by the environment to report that they have been damaged. The victims are often afraid to report such cases as perpetrators of the criminal acts convince them that they themselves are guilty of the fact that the job could not be realized, threatened to sue them...

Although the Nigerian scam exists for a long time and at first glance does not act seriously, the data suggests that fraudsters make good money. Despite the growing awareness of this phenomenon, they find new victims. According to research by the Dutch organization UAGI (Ultrascan Advanced Global Investigations), the loss caused by the Nigerian scams has so far amounted to more than 82 billion dollars, and only in 2013 it is 12.7 billion dollars. In Serbia, according to the High-Technology Crime Prosecution, the first case of Nigerian fraud was reported in 2009, and the damage was $ 2,500 (Telegraph).

In addition to these material losses, there are cases where the victims were physically endangered and even the case of death. This is the case of wealthy Greek George Macronali, who arrived in Nigeria in 2004 and was arrested on arriving after illegally staying, after which he was asked for a large sum for his redemption.

In the process of processing this type of fraud, it appears to be a problem initially initiated from the regions of Nigeria, Senegal and Benin, and international police cooperation with these countries has not led to significant results to date. Because of this, and the fact that sums of up to 1000 euros are rarely investigated in the context of

international crime and the voluntary participation of the victim in the scam, fraudsters sometimes use Skype, where they even use the camera, They do not hide their identity. Unfortunately, due to the poor economic situation in Nigeria, participants in this criminal offense are young highly educated people who cannot find a job.

In 2008 and 2009, in the territory of the Republic of Serbia, injured persons reported nine criminal acts of fraud with elements of „Nigerian fraud", but the perpetrators are unknown. These crimes were damaged by the citizens of the Republic of Serbia and companies from our territory, and the total property damage amounted to more than 60,000 euros. The injured persons sent money to perpetrators of crimes through Western Union and Money Gram.

## Examples of Nigerian letters

We will list some typical examples of Nigerian letters.

1. My dear friend,

Please apologize for sending this letter without your consent. I think that you are a respected, appropriate person, taking into account the fact that I was looking for a database on the Internet during my discreet search for an international partner who could help me in realizing my business. My name is Mr. Daniel A. Anaorh. It necessitated me to contact you about this offer, looking for an overseas partner for this offer. I am a banker and am now in the position of the general auditor in this bank. I have the ability to finance the US with $ 10,500,000 (ten million and five hundred thousand dollars) belonging to one of my clients, Mr. Client died of a heart attack in 2011. If his money is not transferred, he will belong to the state. So, please, make a contract whereby we can jointly help transfer this money and I promise you 40% of the sum. If you agree with my business proposal, further details of transferring money will be sent to you as soon as I receive your mail. Please send me your personal email address:

In anticipation of your recent response:

With respect,

Daniel A.Anaorh.

Perhaps one of the most eminent Nigerian letters is:

2. My name is Bakare Tunde; I am the brother of Nigeria's first Nigerian cosmonaut, Nigeria BBC Nigeria Abaka Tunda. My brother became the first African cosmonaut, who went to a secret mission to the Soviet station „Salut 8 T"far away in 1979. Later he took part in the Soviet „Soyuz T-16" flight to the secret space station „Saljut-8 T". When, in 1990, the Soviet Union broke up, he was stationed at the station. All the Russian crew members managed to return to the ground, only for the brother there was no place in the cosmic plane. From then till now he is in orbit and only rare cargo „Progress"supplies it necessary. Regardless, my brother did not breathe spirits, but he longs to go home to his native Nigeria. During these long years spent in the cosmos, his salary has reached a sum of 15,000,000 US dollars. Now this sum is kept at a bank in Lagos. If we manage to access the money, we will be able to pay Roskosmos the necessary sum and organize for my brother a return to Earth. The requested Roskosmos sum is 3,000,000 US Dollars. However, in order to obtain the sum, we need your help, given that all Nigerian foreigners are banned from us.

Your everlasting,

Doctor of astronaut Bakare Tunde.

## Conclusion

Based on the examples of Nigerian letters we can learn about their common lines:

- As a sender of letters, a wealthy and prominent person from a distant state appears, mostly a king, president, etc. or a high-ranking official of a bank who finds out about the death of a lonely rich man and asks for help in transferring the assets of a wealthy deceased;
- the subject of the e-mail mainly attracts attention, whether it is an „ambulance" or „partnership";
- at the beginning of the story, the sender presents in detail his tragic fate and details related to age, information about his family, family tragedies, which seeks to get close to the recipient of the message, and the story of this unexpected interlocutor is in any case very fairy;
- from the recipient of the e-mail, assistance is requested in transferring money to his country of residence, in his or her newly opened account, whereby he insists on the speed of reaction and transfer of money;
- the sender of the message wishes to leave the impression that no business endangers or damages anyone, but that their cooperation will avoid the loss of money;
- also, the sender wants to make sure it's safe and easy business;
- fraudsters are used by humanity, the desire to help and the companion of the recipient of the message;
- the subject of the offer is a large salary, even up to 50% of the total amount, which usually amounts to several million dollars;
- in each Nigerian letter, discretion and secrecy are required.

It is also interesting that the creators of the Nigerian letters received the 2005 Antinobello Prize for „literature"for the entire gallery of colorful characters, who need a small sum to become rich. As their inspiration does not disappear, we witness the daily occurrence of new content of Nigerian letters and attempts to deceive naive victims. And if it seems overwhelmed, this type of scam has its own victims whose number is constantly increasing.

## References

*419 UNIT AFF STATISTICS & ESTIMATES*,http://www.ultrascan-agi.com/public_html/html/419_statistics.html,accessed 12.04.2016.

Buchanan, J. and Grant, A. (2001). *Investigating and Prosecuting Nigerian Fraud*, „U.S. Attorneys" Bulletin, vol. 49, no. 06, USA.

Chawki, M. (2006). *Anonymity in Cyberspace: Finding the Balance between Privacy and Security*, Revista da Faculdade de Direito Milton Campos, Nova Lima, vol. 11, Brasil.

Dyrud, M. (2005). *I brought You a good news An analysis of Nigerian 419 Letters*, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA.

*Internet prevare decenije*,http://www.informacija.rs/Clanci/Internet-prevare-decenije.html, accessed 12.04.2016.

N*igerianCyberScammers – LATimes*,http://www.latimes.com/la-fg-scammers20oct20-story.html, accessed 12.04.2016.

*Nigerianspam*,http://www.nigerianspam.com/people-affected-419-scam.htm, accessed 12.04.2016.

*Telegraf, OBEĆAVAJU VAM MILIONE EVRA, A VI SE LOŽITE? Evo kako pljačkaju Srbe!*, http://www.telegraf.rs/vesti/1286463-obecavaju-vam-milione-evra-a-vi-se-lozite-evo-kako-pljackaju-srbe-foto, accessed 12.04.2016.

Бојовић, В. (2005). *Сајбер криминал – изазов компјутерске ере*, Билтен Окружног суда у Београду, no. 68, Београд.

Вићентијевић, М. (2008).*Кривична дела против безбедности рачунарских података*, Избор судске праксе: стручно-информативни часопис, age 16, no. 7/8, Београд.

Закон о кривичном поступку, („Сл. гласник РС", no. 46/2006 and 49/2007).

*Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, („Сл. гласник РС", no. 61/2005).

Петровић, С. (2004).*Компјутерски криминал*, Војноиздавачки завод, Београд.

Шешић, З. (2006). *Кривичноправна заштита безбедности рачунарских података*, Нова решења у кривичном заонодавству и досадашња искуства у њиховој примени, Саветовање, Златибор, Београд.