Email fraud: question of motive

JANKO ŽUFIĆ
Faculty of Educational Sciences
Juraj Dobrila University of Pula
Ronjgova 1, 52 100 Pula
CROATIA
jzufic@unipu.hr

MARKO POGARČIĆ
Municipality of Rijeka
Ul. Žrtava fašizma 7, 51000, Rijeka
CROATIA
marko.pogarcic@gmail.com

IVAN POGARČIĆ
Polytechnic of Rijeka
vukovarska 58, 51000, Rijeka
CROATIA
ipogarcic@veleri.hr

Abstract: Mail, regardless of the form or manner of implementation, is the way of communication. Traditional forms or modern use of ICT are standardized forms of human communication. This does not mean, of course, the exclusion of (non)human communication e.g. machine - machine. The assumption of standards as an accepted form of communication realization often becomes necessary due to all aspects of this communication. Communication takes place in a communication channel, which implies a sender-receiver relationship. The channel and the primary sender-receiver axis may be, and most often are, of an altering character, which means that the roles change during the realization of the communication. In doing so, the form of realization is not so important. Since e-mail is a form of communication, predominantly human, it also implies certain forms of human behavior. However, it does seem that these features are not standardized, and even less implied in some cases. All deviations from the established moral and ethical norms can be seen as deformations in behavior during email communication. These norms should be a reflection of the cultural, ethical and moral framework of a certain, specific community, and respect for them should be understood and guaranteed. Accordingly, participants of such communication can find themselves in different situations, so they behave differently. The paper presents a summary review of various fraud attempts via email, which is owned by one of the authors. The data were collected in a database for a period of seven years. This paper is a continuation of two previous investigations that treated the time of email fraud (day of the week and hour of the day). This paper is a continuation of analysis on a broader database with the subject of analysis being a motive of fraud. Motive articulation can serve for further action that can eliminate negative aspects of email.

Key-Words: - eMail, fraud, attempt, communication, ACTE, GDPR

1 Introduction

Communication as a process is not exclusive to people. Both plants and animals communicate in their own way. What is inherent in all forms of communication is the shape/form that is used for operative communication. Such a form is commonly called a message. Finally, it is necessary to define communication from pragmatic and technical aspects for the needs of a clear and unequivocal relationship sender - recipient. Although the technical aspect of this overview is not so important, the advantages and disadvantages of such a relationship, which may be both causative and consequential, will be now and then taken into account. It is important

to keep in mind that the altering character of communication binds the cause and effect in such a way that after one stage of communication the consequences can be the cause so on until the end of communication. The technical aspect of communication is not necessarily strictly related to ICT and/or computer environments, unless email is viewed strictly as a form of communication. In this case, it is necessary to assume certain technical capabilities and equipment as necessary aids for communication as well as for the analysis and calculations required for this paper.

From a pragmatic point of view, way of managing communication and the purpose of the message that is the subject of communication is important. As the information is regularly based on decision-making, the message must be transmitted effectively and efficiently. Even more because in message management there is the possibility of misuse and/or the possibility of intentional or unintentional destruction of information or message in its entirety. This usually results in inappropriate risk in making decisions.

The subject of this paper is primarily the research of motives or drivers for possible attempts of email fraud. In addition to this analysis, the authors will give their view of the recent circumstances, decisions and efforts that are brought about and are happening in the global context in order to prevent possible negativity. In earlier papers [1], [2] the authors tried to identify areas where damage could be caused by the abuse of email as a form of communication. This paper attempts to identify the generic frameworks of such intentions and attempts. Giving the generic framework provides the opportunity to consider all the necessary elements of such communication. Another aim of this research is to consider the legal framework in which email communication is conducted and the possibility of sanctioning inappropriate attempts and behavior in communication.

In this way email appears as a subject involved in the area that is now recognized as a special kind of forensics - computer forensics.The need to define the legal framework derives from the premise of a possible judicial dispute and the determination of the disputed elements of email communication. Such circumstances, due to the specificity of electronic communications, require additional specific elements of legal regulation of email. Research covered by the paper is conservative. It starts with the assumption that there are real possibilities and ways of inappropriate, punitive and criminal behavior, i.e. that they can happen realistically.

As in the previous two papers, the location and time of the research is limited to email on the computer of one of the authors of the paper and research. With this paper, the authors check the validity of the hypothesis that the problems and consequences of possible email frauds can be legaly articulated. However, unlike previous research in this paper the authors concentrate on the articulation of motives that trigger potential "offenders". For this purpose, the research was aimed at: to determine the material and factual circumstances in which a specific type of offense – eCrime - may occur. This term required a suitable definition given in the paper [2]. The definition has a working character, which does not exclude its scientific value. According to the authors, eCrime is any offense that can be legally defined, regulated, resolved and sanctioned by appropriate legal acts adopted at the community level within which eCrime has been committed.

The previous works included the author's classification of the severity of the possible eCrime, hypotheses about the scope of its perpetration and suggestions for protecting the participants in accordance with legal norms and legal remedies. Just like then, it again wants to emphasize the shortcomings and/or the lack of educational content in the field of communication, both formal or informal. [3]

The research is based on data collection and analysis in the period from January 2011 to March 2018. This period of seven years is considered by authors as appropriate for the quality of the research carried out.

2 eCrime - motives and consequences

As the main object of this research is the motive or motivation for (non)appropriate

behavior in email communication, it is necessary to determine the motives and accept the working definition.

According to [4] the motive is any excitement that drives an individual's behavior toward a particular goal. In practice, the term motive is often replaced by expressions such as: need, desire, will, reason, urge, aspiration, purpose, etc.

For each criminal attempt or case it is necessary to have a "trigger" - a motive explaining the specific action. What is the real motive for email fraud can not exactly be determined for several reasons. Communicating with email is specific because the sender's identity in one hand is questionable or, at least, concealed if the sender is not appropriately detected.

The second reason is the fact that concealment can be performed in several different ways in the technical domain of email. As soon as the mail is placed in the * .com, * .yahoo, * .gmail domain, due to the size of these domains, more effort is needed to make valid conclusions in specific cases.

The third reason lies in the consumer characteristics of the technical aids by which email is realized. Consumerism is usually accompanied by insufficient training of users of technical aids, especially ICT equipment, and relative shallowness in establishing bonding relationships in using them. This very often leads to controversial situations that easily end in court disputes.

Of course, there are other, more delicate reasons as each concrete realization of email is specific to itself. Determining the motive for attempt of fraud is obviously not easy, but at least it can define a generic framework and make a raster/categorization of the motives of fraud and offense attempts. Analysis of the collected data can point to some motive categories and their intensity. It should be noted that the authors attempt to define intensity in this paper according to their own discretion based on the analysis of the data collected.

Perhaps not the last reason, but certainly important, that can help determine the motives lies in the legal framework governing e-mail communication. The legal frameworks, consciously or unconsciously, determine the concrete actions of the participants in email communication, that is, the indirect severity of the possible offense, and consequently the consequences.

Below is a description of regulating relations in electronic communications, the legal aspect of the motive as a crime, setting up a hypothesis before analyzing data, and analyzing data and making conclusions.

2.1 Regulating relations in electronic communication

Communication is basically the interaction of two or more elements aligned mutually to one another. In system theory communication is usually represented as a bipolar relation between the emitter/sender and receiver of the material that is being exchanged during communication. Fig. 1 is a generic overview of communication at the definition level at a given moment [5].

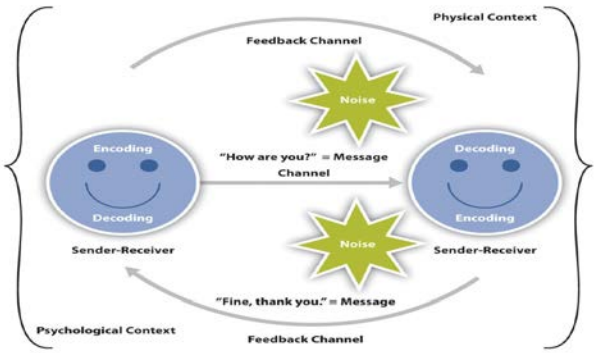


Fig 1. Communication Source: http://www.managementguru.net/wp-content/uploads/2014/03/communication.jpg , Downloaded 9/4/2017)

i.e. it can be observed from a pure mechanical /mechanistic point of view. In the specific case, the environment in which the service is realized is usually more sophisticated and goes beyond the presented generic form. When communication is put into the ICT environment, much is changed. Of course, it is necessary to assume that there are infrastructure options for such a realization of email communication. Such possibilities are a prerequisite for setting a general hypothesis and making conclusions. In such circumstances, eCitizens, eGovernment, eAdministration, eLearning are more and more frequently used, so we can also talk about eCrime. Some countries / states implement their plans and activities on the realization of eState

status When such circumstances are reached, the prefix may be omitted.

The way an e-mail is transmitted is dependent on the communication infrastructure. Therefore, electronic mail regulation is generally regulated at the state level and/or is most often under the influence of state agencies such as telecommunications and electronic media agencies. Of course unless telecommunications are in private hands. And even when legal regulation goes beyond the right of ownership. Within the framework of these laws, the concept of electronic mail is also defined. Posebno je potrebno naglasiti da se u ePošti pojavljuje i stalni učesnik eOperater kao posrednik u komunikaciji kojeg također treba pravno tretirati.It is especially important to point out that in email there is a permanent participant eOperator as a mediator in communication that should also be legally treated.

In the specific case of the Republic of Croatia, the Post Office Act would be lex generalis, or general law. The term electronic mail is regulated in Article 2, subparagraph 11 of the Electronic Communications Act [6]. In the quoted provision electronic mail is any text, voice, sound or image message transmitted over a public communications network that can be stored in the network or in the terminal equipment of the recipient until the recipient accepts it. Subparagraph 20 of the cited Article defines public communications service as an electronic communications service that is publicly available on a market basis.

The Electronic Communications Act in Article 107 foresees the unwanted electronic communications, as well as the negative and positive manner and the use of electronic communications. Positive standardization foresees that the use of electronic mail and other forms of electronic communications for the purpose of direct promotion and sales is permitted only with the prior consent of subscribers or service users. Negative standardization is characteristic because it defines that it is forbidden for the purpose of direct advertising and sales, to send e-mails, including SMS and MMS, that are misrepresenting or concealing the identity of the sender by whom the email or message is sent and which is contrary to special regulations on electronic commerce, as well as sending an e-mail or message without the correct e-mail address or number at which the recipient may, without charge, submit a request to prevent further communication, or electronic mail or message that encourages recipients to visit web sites that are contrary to special regulations on electronic commerce.

In particular, the Council of the Croatian Postal and Electronic Communications Agency has adopted the Ordinance on the manner and conditions for the prevention and suppression of abuse and fraud in the provision of electronic mail services. [7]

The Ordinance prescribes the manner and the conditions for the prevention and suppression of abuse and fraud in the provision of electronic mail services, the protection of subscribers from unwanted electronic mail, and the fulfillment of obligations of operators and subscribers in the protection of electronic communications networks and services. The Quoted Rule defines unwanted e-mail as "...every message for which there is no reason to appear in the mailbox of the subscriber". The Ordinance provides for the prevention and suppression of abuse by prescribing the obligations of an electronic mail service provider. Specifically defined are measures for the protection of subscribers, technical measures, organizational measures and protection measures against spam (anti-spam measures). The legal acts of the Republic of Croatia are aligned with the acts adopted at the level of the legislative bodies of the European Union.

2.2 Cause-and-effect connection of sending and receiving fraudulent e-mail

Most ICT users are everyday witnesses, and also "victims", of receiving emails where they are informed that they can win or have won several hundred thousand or millions of euros, dollars etc., or they can get a work visa for certain countries of the world, or that they are able to inherit a cousin from e.g. Sierra Leone for which they did not know existed until then. All these are tempting deals, especially for naïve users. The most common condition for realizing the content of a fraudulent email message is to send the sender personal information (name, surname, residence address and country name, current or giro account number, email). The basic question is actually the reason-motive for sending the email and even more why we should send feedback to the sender. Today's ICT provides sophisticated solutions that make each person accessible. Though it is a good and altruistic intention, it can not often prevent anyone from abusing it.

What causes abuses?

Since 2008, when the economic crisis began officially around the world, the crisis of morale

and the spiritual crisis also began. Surviving in such a world causes an individual to try to find any way to acquire the means to improve his own existence.

Authors are of the opinion that this is a fundamental motive-cause for fraudulent behavior of users via email in which a fraudulent sender represents what does not need to be his true identity; second, regardless of the domain of the mail, it does not have to be sent from a country whose domain it contains but can be sent from any server in the world. Anonymously and without much trace. The reason is the fact that the development of ICT is not adequately followed by adaptation of the legal system and many regulations that are trying to regulate its application in everyday life.

At EU level, texts are being considered on a daily basis and attempts to bring about legally relevant regulations that cover the above mentioned issues.

One of the essential regulations is the General Data Protection Regulation to be applied from 25 May 2018, also known as the GDPR Regulation. It should be noted that the Directives issued by the competent authorities of the European Union are compulsory in all EU Member States and at the same time in the countries that are candidates for entry into the European Union and which are bound by the Stabilization and Association Agreement. GDPR as a basic objective prescribes the protection of personal data that must be provided by all organizations regardless of whether they are personal data of users, clients or employees. Organizations must at all times know where and for what purpose they can be used. Likewise, in the event that someone decides to withdraw the privilege of using their personal data, the organizations must be able to do so within the set deadline.

At the same time, the said Regulation prescribes and defines what makes personal data all the more. Thus, it is cited that the personal data is: name, address, e-mail address, IP and MAC address, GPS location, RFID tags and cookies on websites, phone number, photos, video footage of individuals, personal identification number, biometric data (fingerprint, eye iris), education and professional information, payroll data, credit information, bank account information, health data, sexual orientation, voice, and many other data pertaining to an individual whose identity has been identified or can be identified.

The effect of the said Regulation is that all foreign companies handling EU citizen data are also subject to this Regulation. So 92% of companies in the United States now say that adjustment to GDPR is one of their highest priorities, or 54% consider them the highest priority. Although it is a European regulation, GDPR affects the redesign of data protection of many foreign companies, including Facebook, Google, Microsoft and many others. The same regulation should, in the opinion of the author, apply analogously to the natural persons who collect the personal information provided by the recipients of fraudulent emails.

In addition to the Regulation, within the EU legal system, the Directives are adopted, which by their nature are not binding as regulations to apply immediately, but EU Member States are obliged to implement them as soon as possible in their legal system (only the name of the Directive or the guideline actually defines nature of these legal regulations, which is to instruct the legislator of each Member State to apply the rules of the Directive to its legal system, by allowing them to adopt rules that provide greater legal protection than the Directive). Currently in consideration is the proposal for a Directive of the European Parliament and of the Council on the fight against fraud and counterfeiting of non-cash means of payment and the replacement of Council Framework Decision 2001/413/PUP. The reasons and the aims of the proposal state that the European Security Program recognizes that the Framework Decision no longer reflects today's reality and that it does not offer enough solutions to new challenges and technological developments, such as virtual currency and mobile payment.

Although the Directive does not refer to fraudulent conduct through email, it is an example that illustrates the fact that the legal system and regulations are often obsolete in relation to ever faster progress in ICT. At the

level of the Republic of Croatia, the National Security Office has adopted the National Cyber Security Strategy. Its introduction stresses the disparity in the development of these two areas. The focus is on the rapid development and introduction of new services and products while security aspects have had very little impact on broad acceptance. The problem is that users often have very minimal knowledge of the technology they use and are therefore everything is based on blind trust, which often endangers personal data security.

The text of the aforementioned Decision, i.e. the National Strategy, also mentions general objectives, of which it is important to mention the systematic approach to the implementation and development of the national legislative framework, implementation of activities and measures to increase the safety, durability and reliability of cyberspace, establishing a more efficient mechanism for the exchange, reliance on and access to information, strengthening of security awareness, encouragement of development of harmonized educational programs, promotion of e-business development, promotion of research and development, systematic approach to international cooperation, which is described in more detail in the text of the Strategy itself.

Finally, in order to ensure adequate and quality protection of cybernetic security, the legislator included in Chapter Twenty-fifth of the Criminal Code a number of criminal offenses against computer systems, programs and data (Articles 266-273). Thus, unauthorized access, obstruction of a computer system, damage to computer data, unauthorized interception of computer data, computer forgery, computer fraud, abuse of devices and grave offences against computer systems, programs and data are defined as criminal offenses. For these criminal offenses prison sentences from two years to eight years are prescribed, but the legislature remains implausible when it states that the perpetrator will be punished for attempted perpetration of the criminal offense. The legislator therefore stipulated that the perpetrator would certainly be punished but did not specify which criminal sanction would be imposed on him (Criminal Code of the Republic of Croatia as sanctions prescribes fines, imprisonment and long-term imprisonment).

3 Preliminary research

In all three researches that the authors conducted from the beginning of 2011 to 2018, the subject of the study was email. On all three occasions, the authors attempted to set certain hypotheses starting from their own standpoints. In this paper, the authors are focused on the motive that triggers the sender to improper behavior.

The database is made out of a total of 2540 inappropriate attempts to communicate via email with an unknown sender. Data collected, which are of research interest, have shown that:

1. Sender's information is usually incorrect or falsified. Such legitimating is likely to result from the fact that the sender is aware that the recipient is either incapable or has no will nor time to investigate the reliability and security of the data. Most senders sought feedback and tried to make contact with the recipient. According to data on the motive and intention of the sender, the sender could try to recover the message to see if the sender was malicious or not. Out of 2540 attempts to establish a contact, 51.27% of them have directed the mail to another email address so their intent can be taken as suspicious.
2. Domain and subdomain of the sender's account were of the most commonly known character as .com or .org. Only a smaller number of senders were from a localized .com domain so at least this could locate the area from where e-mail came.
3. Mostly the location could not be determined without deeper research of the data. Closer determination was possible only in the case of partial self-detection but then the data could only be taken with conditional correction.
4. Since the sender and recipient do not know each other the motive can only be assumed. From the data collected and

classified it is evident that the final motive has always been an attempt to realize the economic benefit of the sender because they are the initiators of the process. Although economic benefits are most commonly offered to the email recipient.

5. The assessment of the motive is in the domain of personal perception of the author who appears here in the role of the recipient of the service or the person who may be potentially deceived.
6. The author, owner of the eAccount i.e. email, is a person with years of experience in the field of information sciences and communication.

In this regard, the following hypotheses have bee formed:

1. eMail is the form of communication in which senders are not always known or can represent themselves falsely, which an act of legal offense
2. The sender may not have legally correct motives for sending the mail, which may harm the recipient intentionally or unintentionally
3. Sanctioning offenses or improper behavior within the framework of email is usually more difficult than in the case of classical mail or similar forms of communication
4. Motives for inappropriate activities within the electronic mail can be classified but there is no established practice
5. The chosen classification criterion was subordinated to the research goal and at the same time it was the aim of the research.

Theft and fraud over the internet and email are today part of everyday life. Fortunately, only for that part of the population that has the ability to use the Internet and email. Participants of this type of communication: sender, transmitter/transporter and receiver must necessarily be properly profiled. All irregularities are not necessarily intended and may result from ignorance and lack of information. When they are intentional then it is certain that the one who does them possesses the knowledge of how to do it. When the ultimate result is fraud or theft then the initiator is the offender to be sanctioned. If such actions occur at the workplace and within the working hours that has additional legal weight and requires strict treatment and sanction. If the recipient does not know all the technique and methods that the fraudster uses and agrees to the whole process, they are also bear a part of the responsibility. The third participant - operator, is equally important, but its profiling is more concretely resolved. Finer profiling of the sender and recipient requires an attitude of a psychologist that goes beyond the scope of this work and the framework is given according to the own perception of the authors. Authors' views on the profiles of senders and recipients are based on the following terms and conditions [1]:

1. Sender and recipient are participants in the communication of the common type, but in a specific environment
2. Environment is a combination of real and virtual where the real environment is partially represented in the process
3. Participants are in communication without consent and can interrupt communication whenever they wish
4. Participants do not need to know each other at the beginning of the communication
5. Reason for communication at the very beginning is not known to both parties in communication
6. Communication is time-discontinuous, but as a process it has its duration, which is not known at the beginning of communication
7. Possible adverse consequences for sender and recipient may be foreseeable but not known.

3.1. Research data

The subject of the research is e-mail, ie e-mail as a means and possible fraud. Electronic mail is also a form of communication. In this communication, two sides are necessarily involved. For this reason, any fraud will be reversed by both participants. That means no

one frees any responsibility. Not a fool or a cheat. For these reasons, the authors set certain hypotheses exclusively from their own perspectives, pointing to the problems of organizational nature

The biggest problem is the wrong or partial misjudgment of authentication. This violates the law. The second problem is the motive and its correctness. This includes the possibility of damage and the need for sanctions. This work continues with previous research [1],[2] where the classification of inappropriate activities is offered. And now the same, but supplemented database is used, with the instantiation in the previous classification. The authors are now concentrating on the motive. Classification is determined by the research goal and at the same time the aim of the research.

From 2011 until the processing of data, 2527 fraud attempts were eavesdropped on one of the authors' electronic mail. As in the previous two papers and then the data are now repeating the same circumstances. Nevertheless, there is an awareness of the higher level of informatics of the sender and the recipient. That is the chances of fraud being significantly less.

The percentage of senders who return messages directed to other electronic addresses is slightly higher than 55.13%. Such intent can be treated as suspicious. The domain and subdomain in which the sender's account is still of a general character, such as .com. or .org.

It has already been mentioned that subject of this research is misuse of electronic mail, with goal to define treatment of such possibilities from the concept of post traffic in virtual frames, treatment from standing points of information sciences and legal terms – especially of violation legislation. Inappropriate electronic mail is, in this research, considered as possible felony, or, violation, to be more precise. Therefore, this form of post can be called a deception. From that aspect it is necessary to determine factual and material circumstances that enable the process of communication. Hypothetically it is possible to assume partial consequences of such activity, but under condition that, at least to some extension, a motive of initiating communication – sending mail – is clear both to sender and receiver. Precisely the clarity and familiarity of motive will define severity of violation and its possible consequences.

In circumstances when sender and receiver do not know each other, motive can only be assumed. Data collected and classified in the research imply that final motive is always economic benefit of sender, since he is the initiator of the process. In most cases motive is concealed by mutual benefits, but the final intention is to deceive the receiver. Smaller portion of cases belongs to the area of marital and sexual offers, though cases which can be treated as business criminal, have also been registered.

3.2. View data by type of classification

The diagrams in Figures 1,2 and 3 show summary data for the entire collection period.

Diagram in Figure 2 shows the total number of fraud attempts per year between 2011 and 2015. The top of the chart is 2015 years. 2015 is a year of recession, and in some ways, the motive for financial fraud is obvious.

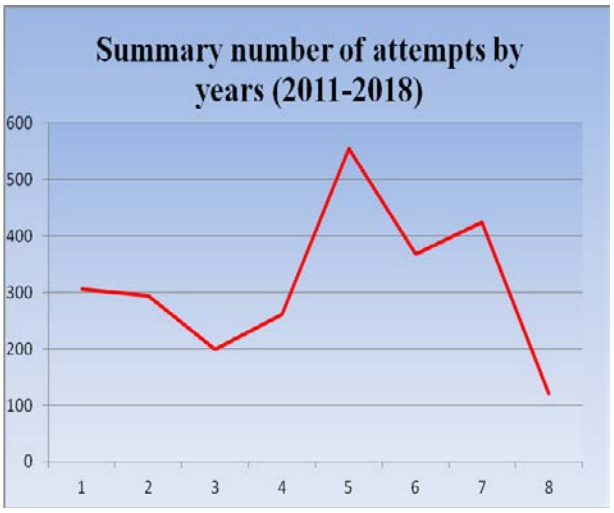


Fig 2: Summary number of attempts by years (2011-2018)

Diagram in Figure 3 shows the total number of fraud attempts per month in a year between 2011 and 2015. The top of the diagram is the month of March. The beginning of spring is the time of general wake-up and increased activity. This is a logical thing in a certain way.

The diagram in Figure 4 shows the number of fraud attempts per month in a year from 2011 to 2015. The top of the chart is the month of

June. An additional motive may be the fact that June is the beginning of annual vacations in the year of the biggest recession.

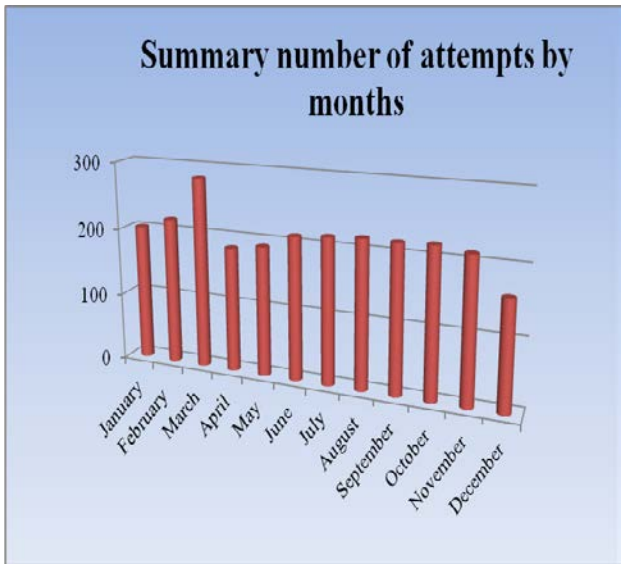


Fig 3: Summary number of attempts by months (2011-2018)

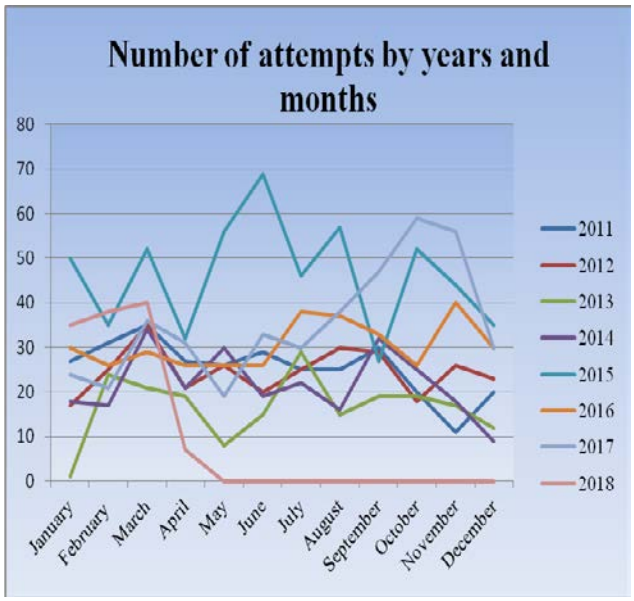
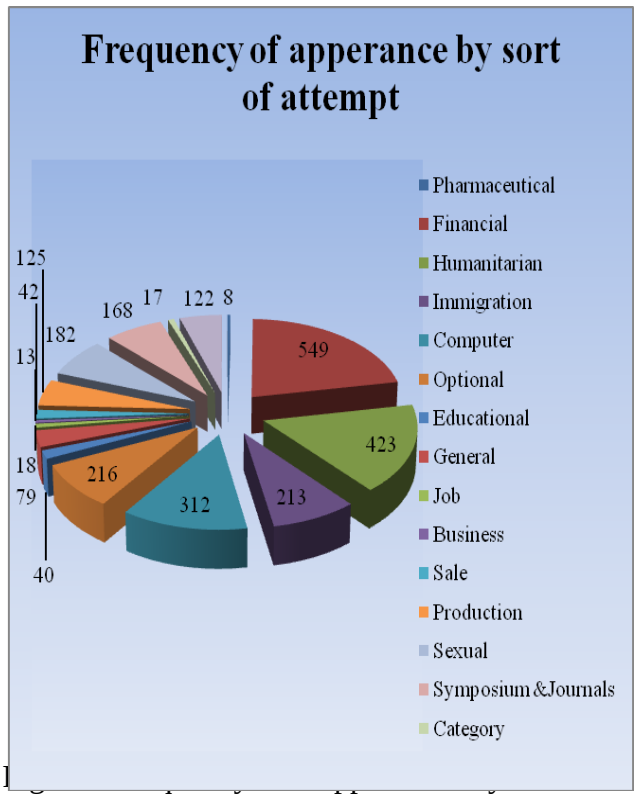


Fig 4: Number of attempts by years and months

Classification of collected data is made in a way that explains the assumed motive of fraud and hypothetical circumstances. Trying to find the sender and gather information about it. The statistics of the above assumptions can be seen in Charts at the Fig 5.

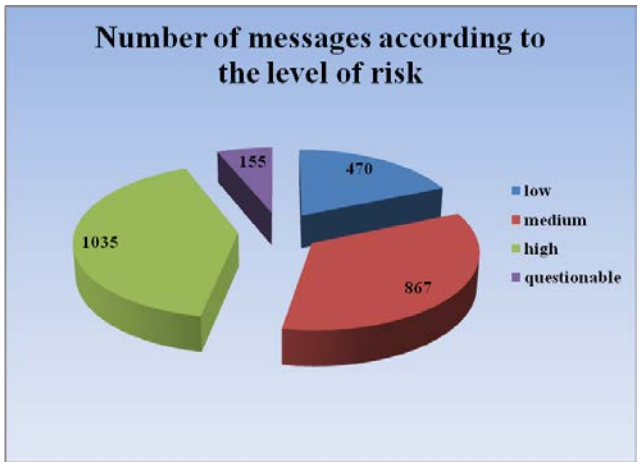
In accumulated data subject to this research, basis has been an attempt to recognize pragmatic approach of sender, from the aspect of receiver and his pragmatic point of views.



attempt

That would be the following criterion for classification and categorisation of selected data. Criterion was made by author, expressed by attempt to recognize sender's primal goal. Analysis has been given in diagram at Picture 4.

The majority of messages were of financial character, where sender offers intermediation in transference of great sum of money or notions of sudden prizes in a variety of games and lotteries. Second in the hierarchy is type of optional messages with the attempts of asking the humanitarian consents to different actions. The third type of messages was connected to receiver's computer and it tried to persuade receiver to send his own authentication data. The other messages are of irrelevant character and they usually can be defined as previous three when certain details are being absorbed. Graph also demonstrate the final motive of deception. The raster clearly alludes of money as the final goal. In diagram at Picture 2 the risk evaluation captured in possible answer of a receiver is displayed.



Picture 5: Number of messages according to the level of risk

In this paper the motive is considered with two aspects. The first aspect is purpose and purpose. The second aspect is the ability to design motifs for the purpose of providing forensic data in the case of a legal dispute.

Attempting to steal identity is an indisputable basic or primary motive. A pragmatic motif is almost always an attempt to secure financial means but at the expense of the recipient. Such circumstances attempt to fraud are defined as criminal proceedings.

4 Conclusion

Determining the motive for an activity is not a simple thing. When we find ourselves in a virtual environment, the motivation is more difficult. However, certain values for motif profiling can be determined. The paper approaches the motif conservatively. The assumption is that e-mail is a fraud attempt or punitive act. From the aspect of computer forensics it is irrelevant, that is, it is important to bring the data into causal connection with the sequences.The data also reads a lot of hacking activities that may be bad for bad intent but may have bad consequences. It also gives some activities that have good intent and purpose, but possible consequences are questionable. For example, e-mail comes from a .edu domain.The motive can be, for example, a student / university research with inappropriate announcements of purpose and goal.

The issue of motivation also requires a psychological approach. Although they possess sufficient knowledge in this area, the authors did not go into more detailed analysis. however, such research can be carried out over the data collected. As much as the data collection continues.

Regulations such as ACTE have offered ultra-liberal possibilities but have led to undeniably bad behavior on the web. Therefore, it was necessary to define the rules of conduct. How much will this make with GDPR will still be seen. Although it is not appropriate, the reader suggests attempting to compare these two legal acts and perhaps carefully analyze the work of the author [8]

References:

[1] Braut, Marino; Pogarčić, Marko; Pogarčić, Ivan. Electronic mail as possibility of inapt communication // *35th Internetional convention on information and communication tehnology, electronics and microelectronics (Mipro 2012), Computers in education (CE) : proceedings* / Čičin-Šain, Marina ; Uroda, Ivan ; Turčić Prstačić, Ivana ; Sluganović, Ivanka (ur.). Zagreb : MIPRO, 2012. 1444-1449

[2] Pogarčić, Ivan; Panev, Ida; Pogarčić, Marko; Cultural Inheritance as Prerequisite to eLearning // *Zbornik 14. mednarodne multikonference Informacijska družba (IS 2011). Zvezek A = Proceedings of the 14th International Multiconference Information Society (IS 2011). Vol. A* Ljubljana : Institut Jožef Stefan, 2011. 411-415

[3] Ainsworth, Heather L.; Eaton, Sarah Elaine; Formal, Non-Formal and Informal Learning in the Science, Onate Press and *Eaton International Consulting (EIC) Inc*, Editor: Jacquelyn Clydesdale, ISBN: 978-0-9733594-5-9

[4] Hrvatska enciklopedija: *Leksikografski zavod Miroslav Krleža*, Zagreb, ISBN 9536036290

[5] Shannon Claude E., Weaver Warren (*The Mathematical Theory of Communication*. University of Illinois Press, ISBN 0-252-72548-41963).

[6] Republika Hrvatska,Official *Gazette 73/08, 90/11, 133/12, 80/13, 71/14, hereinafter ECA*

[7] Electronic Communications Act, *Official Gazette, No. 73/2008* Ministry Of The Sea,

Transport And Infrastructure, Republic Of Croatia

[8] Vitor R. Carvalho : Modeling Intention in Email: Speech Acts, Information Leaks and Recommendation Models *(Studies in Computational Intelligence)*, Springer, 2011, ISBN-13: 978-3642199554