Current and Ongoing Internet Crime Tendencies and Techniques. Preventive Legislation Measures in Romania

Florin Postolache[1], Mihaela Postolache[2]

[1]*Danubius University of Galati, Faculty of Law, florinpostolache@univ-danubius.ro*

[2]*Danubius University of Galati, mihaelapostolache@univ-danubius.ro*

Abstract: Internet crime techniques that pilfer from victims millions each year continue to plague the Internet through a range of methods. Trends and techniques identified by many organizations along with its description are followed by preventative measures that will support you in being informed prior to entering into dealings and transactions over the Internet. Techniques as Auction Fraud, Counterfeit Cashier's Check, Credit Card Fraud, Debt Elimination, Parcel Courier Email Scheme, Employment/Business Opportunities, Escrow Services Fraud, Identity Theft, Internet Extortion, Investment Fraud, Lotteries, Nigerian Letter or "419", Phishing/Spoofing, Ponzi/Pyramid, Reshipping, Spam, Third Party Receiver of Funds are clarified in this paper and, also the internet crime prevention and legislative measures are treated, too.

Keywords: internet crime; e-fraud techniques.

1. Introduction

The Internet is so good, but in some situations so blamed! The various criminal means keeps affecting the internet, making huge loses around millions of euro annually. The current and future trends in stopping the scourge of crime on internet have materialized and in Romania there have been attempting to adapt the legislation and cooperation with other countries. Thus, lately our country has known an increase of the informatics criminality, which brought us a global well-known “brand”, by incorporating the country’s name in labelling the method. In this paper we analyze the most common methods and criminal schemes but also ways to prevent them.

Methods and Means of Preventing Computing Criminality

The auction fraud: involves deceiving one of the parties after a bid made on a specialized site in selling or buying products through auction. In general, there are posted ads of selling products, at very attractive prices. After the auction is made and the product is acquired virtually, the product is paid and often enough the transaction stops here and the buyer does not receive anything. This method is associated to our country and is called the “Romanian auction fraud”. Sometimes the seller directs the victim towards an escrow service that is compromised and/or fake, and that, in the most cases, belongs to the seller. Once the money is electronically transferred, the connection is interrupted and the seller is unreachable.

Therefore the consumers are warned about the risk of such transactions, if they recognize one of the following behaviours:

- The sellers post ads of sale and purchase like it would be in the country, and after closing the transaction, the winner of the auction receives a congratulatory message in which is announced the winner of the auction. But of course, there's a gift, the winner is announced that for the moment the bidder it isn't in the country for various reasons, the most common being the business, career, family. Also we should stay away and from the people that post the auction under a name and the funds to be transferred to another person.
- The person requires that the money transfer to be made digitally, using bank money transfer, such as MoneyGram, Western Union or electronically bank transfer. Using these services, practically the money is lost and can't be recovered in any way.
- The sellers that act as dealers or authorized representatives of the companies in countries where there aren't representatives of those companies. These should be avoided.
- The buyers, that from different reasons require that the transport of the products to the destination should be made through methods that avoid the custom duties, must be avoided also.
- There are doubts in buying the product by paying with credit card, and the name or the destination address of the product doesn't correspond with the one from the card. It is advisable to receive the card holder's authorization before sending the product.

To prevent this type of fraud we must take into account the following aspects:

- Before the offer, contact the seller and ask him any questions you have about the product;
- Make sure of the seller's feedback;
- Treat with caution the people outside your country;
- Make sure you fully understand the terms of restitution and the security policies;
- Calculate the shipping charges before buying;
- Be wary if the seller accepts only bank transfers or cash;
- Ensure the legality of a escrow service if it's used;
- It must be taken into account the product assurance;
- Be wary if you receive unsolicited offers.

Usually the specialized sites in online transactions such as eBay or PayPal are making known the methods of additional security and offer tips to prevent fraud.

The credit card fraud: is an unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or goods. The identification data submitted on the credit/debit cards can be stolen after there are made transactions on unsecured websites, or there can be obtained after an identity or acts theft. Since these data are getting in the hand of the criminals, they usually make transactions on your money. This type of fraud can be avoided if we take into account the following considerations:

- Ensure that the site where you make the transaction is safe and it has a reputation before providing online your credit card number and the identification data.
- We mustn't always give credibility to the sites just because they pretend to be safe.
- The reputation of the sources from where we acquire the goods must be grate.
- The situation of the count must often be consulted to avoid unauthorized payments.
- Previously it is indicated a small study on the person or company from where we buy the product.

- Under no circumstances you should provide the information submitted on the credit cards or the PIN, to request, via e-mail or at unsolicited phone calls.

The identity theft: appears when someone appropriates another person's personal information without their knowledge with the purpose to commit theft or fraud. The identity theft is forerunner of committing other types of frauds. Usually the victim is convinced to reveal personal sensible information in order to participate in a legitimated business, or sometimes as response to a request by email to update the identification or affiliation information, or renewal of the data of the bank account or as a result of applying some requests concerning a job. In preventing this type of crime we must take into account of the following aspects:

- The accessed web sites are secure before submitting the number of the credit card;
- The preliminary information concerning the business or the fact that the site is legitimate;
- In the identification data is preferably a physical address then just a mailbox;
- Under no circumstances the cards are not thrower neither the statements;
- Make sure that you don't have missing bills from which to show the identification data of the account;
- Do not provide to anyone your identification data of the card or the PIN;
- The credit card number or identification data aren't provided by telephone unless if you make the call.
- Consult monthly the made transaction to prevent or to discover the frauds.
- Report unauthorized transactions to the bank or towards the card company as soon as possible.

Blackmail and wringing information from the internet: implies breaking and taking the control over the data base, with the promise of giving the control back in exchange of the required or received funds, or are conditioned by filling a job as web administrator. Similarly, it may be put in jeopardy or compromise the information concerning the data based of the consumers excepting the case in which the funds are received. The preventive measures consist of increasing the network security and identifying the weaknesses from it but updating the existent software.

The investment fraud: is an offer for investments or loans requests, using and trading some value titles using false or fraudulent claims. In this case, we must take into account the following aspects:

- The offer seems too good to be true and the profit is coming immediately;
- It is indicated no to invest until you understand the business;
- Not always the company reputation is ensured by what is written on the website.
- Be circumspect at the bids received by unwanted emails where the profit is immediately and without risks;
- Preliminary research of the parts involved in the business and of the investment's nature;
- Treat with caution the business which involves partners from other countries and also the tax authority's data about the company you want to close the transaction with.

The lotteries: in which you are announced that you won an important sum after a random selection from a database of emails, names, etc. Initially there are required the contact data, then a fee ranging between 1000 and 5000 euro to be required for starting the proceedings. These are the first signs which we must keep in mind if we are scamed:

- Sounds too good to be true;
- You have not participated in a lottery or you treat with persons outside your country;

- Beware of the lottery which charges a tax before delivering the prize;
- Do not answer to the requests through which you must send money to be eligible for future earnings.
- In some countries it is an offense to play in a foreign lottery through email or telephone.

Also the Nigerian lottery or "419", through which a high official Nigerian offers to share a percent from a sum of millions of dollars requesting help in placing the money in foreign banks. At the beginning it requires personal information and then under the pretext of increasing the wining you must pay a certain amount of money.

Phishing and spoofing: are somewhat synonymous, and reefer to electronic documents falsified or fake. Spoofing refers at sending a fake email, which appears as is it was send by someone officially.

Phishing is often combined with a spoofing and is the act of sending an email claiming to have a legitimate business, in the attempt of tricking the receiver in order to disclose personal information such as passwords, card credit numbers and information about bank account. It is interesting that it directs the users to visit a specified website. The site is mostly similar to the original one but of course it is not real and it was created only as an attempt to steal the information about the user. Most of the times these methods make us think that they are coming from a bank; it is advisable to keep in mind the following:

- Any unsolicited email which requests personal information should be treated with suspicion and it must be reported;
- Avoid filling out forms from your email messages that ask the personal information;
- If the email is sent from the bank, it is always advisable to compare the link from the email with the link we are directed to.
- It is advisable to connect to the official site, then accessing the "link" from that unsolicited email.

The Ponzi pyramid: there are pyramidal schemes and they are investment scams in which the investors are promising abnormally high profits at their investments. Actually there is no investment. The scheme is simple, the first investors are paid with the invested money, but by the next investors the system usually collapses. The last investor does not receive dividends and their investment is lost.

According to the above presented schemes, if the "opportunity" seems to be beautiful and true, and the promise of making quick profits is present, it is better to avoid the opportunity.

Also try to fully understand the mechanism before investing and be cautious when you are asked to bring new investors later.

If you think you are a possible victim of this type of scam, it is appropriate to complain to the competent authorities.

2. Internal Legal Regulations Concerning Computing Crime

The cyber crime is a phenomenon in our days, frequently reflected in the mass media. A study indicates that the fear of informatics attacks exceeds in intensity the ordinary one, thefts or frauds. The criminological research on the crimes carried out through the informatics systems is still in the

exploration stage. Even those made so far tend to change in the classic way in which there are watched the infractions in the current justice systems. (Cârjan, 2005, p. 720)

The rise of information technology, of the computer systems started especially in the last century and it has left its mark on all social, economic, civil or military area. As a result of this ascension in the recent years in our country there were initiated legislative penal measures in order to sanction the facts that are offenses specific to the domain which should be the object for penal investigations. Nowadays in Romania there are currently several provisions in the special laws, which regulate different facts about computer systems or information society as a whole. (Dobrinoiu, 2006, p. 140)

The cyber crime includes in addition to the conventional crime acts (fraud, counterfeiting, prostitution, fraud) the offenses in the cybernetic domain (software piracy, the cad theft or falsification of the instruments of electronic payment, malicious networks, electronic terrorism, harassment via email, etc.) (Stancu, 2007, pg. 4-5)

The evolution of the informational technology offers both advantages and disadvantages and the latter refers primarily to the multitude of possibilities for breaching in any domain that appeals to the cybernetic systems (financial-banking, aviation, national security, military, medical, educational, social, etc.).

In the last years the Romanian legislature was concerned with developing a framework that regulates the access and development of activity through the computer systems in different sectors. Currently, there are in effect more legal provisions integrated in special laws which regulate different facts about the computer systems or the information society as a whole. Thus, there are considered relevant the following legal provisions: Law no. 365/2002 on the regulation of electronic commerce, G. D., No. 1308/2002 concerning the appearance of the methodological norms for applying the Law nr 365/2002; G. O. nr 130/2002 on the legal regime of distance contracts, amended through the Law 51/2003; Law 81/1996 on the Copyrights and related rights, together with the Law nr. 285/2004; Law nr 506/2004 on the processing the data with personal character and protection of the private life in the sector of electronic communications; Law no. 64/2004 on the ratification of the Convention of Europe Council on cyber crime; Law nr. 196/2003 concerning the preventing and combating the pornography, as amended by Law no 496/2004.

In our country, the legal regulation applicable in this moment, and the most important, in the matter of informatics crime is the Law 161/2003 concerning some measures for ensuring the transparency and exercise of the public dignities, of the public functions and the business environment, preventing and sanctioning the corruption. This introduces a number of 7 infractions, which corresponds to the presented classifications with the analysis of the Convention provisions on the cyber crime, grouped in the group Title III of the law. The text was a rapid adaptation to the Romanian environmental of the Convention provisions and is an effective tool in combating this scourge.

The goal of this normative act is the preventing and combating the cyber crime, through specific measures of prevention, discovering and sanctioning of the committed infractions through the computer systems, ensuring the respect of the human rights and protection of the personal data (art. 34).

The normative act does not provide a definition of the “computer crime” (as also it can’t do even the Convention of the Europe Council). Such a definition is in fact very difficult to be stated, considering the wide variety of the criminal matters that have been discovered so far, but and the daily avalanche of the new criminal acts in this area.

For preventing and discovering computer offenses, the law requires the involvement of authorities and public institutions with competences in the field, service providers, NGOs, civil society representatives that promote policies, practices, measures, procedures and minimum standards of security information systems, such as the Ministry of Justice, Ministry of Administration and Interns, Ministry of Communication and Information Technology, the Romanian Intelligence Service and Foreign Intelligence Service (which must continuously update the database of cyber crime) and the National Institute of Criminology.

3. International Legal Regulations Concerning Computer Criminality

Having roots almost in the entire world's countries and without any central authority, the internet is considered by the civil liberalists and online activists as a true free market of all kinds ideas. We cannot take into consideration their Sisyphean struggle to keep the Internet off the legal constrains by imposing some civil or penal sanctions for the negligent or illegal activities; it would threaten the expansion and the spirit of this network (Vasiu, 1998, pg. 125-126)**.**

The necessity of juridical regulation of the Internet results from some committed facts in this network already fall under the existing laws. The fact that such behaviours have moved their development location does not alter their criminal nature. In many countries there are a series of normative acts which, although they didn't aim at the dissemination of the obscene materials in the Internet network, for example, there are applicable and there are applied in the case of committing these acts through the reminded network.

Thus, in Great Britain there are several laws that incriminate various aspects of the obscenity: Obscene Publications Act of 1959, Protection of children Act from 1978, Indecent Displays Act from 1984, Criminal Justice Act from 1988 or the Criminal Justice and Public Order Act from 1994 (Vasiu, 1998, pg. 131-133)

Supporting the fight against the cross border crime, the EU authorities have adopted several measures designed firstly to strengthen the cooperation in the judicial – penal domain with other non member states of the Union and with international organizations. Thus, we consider the following steps:

3.1. Organization of United Nations

The resolutions 55/63 from January 2001 and 56/121 from January 2002 on combating the use of information technology for criminal purposes invite the member states:

- To make joint efforts to combat cyber crime;
- To adapt the legislations in this context;
- To cooperate and to exchange information in this domain at international level;
- The qualified institutions train personnel to meet the demands of these activities;
- To protect according the law the confidentiality and integrity of the informatics systems;
- To preserve the electronic data and to allow the quick access in case of investigations;
- To ensure in due time the investigation of the computer infractions, gathering the evidences and the exchange of information.

- To educate the population about the methods for preventing and protecting from computer infractions.
- According to the possibilities to adapt at the computer systems for helping detecting criminal actions and to gather evidences and track down the perpetrators.
- To find solutions for combating the computer criminality this does not affect the individual liberties and the right to citizens' private life.

3.2. The Economic Organization for Cooperation and Development

OECD had an important contribution in the development of the international cooperation against the computer crime recommending the states to adapt their national legislations so that the illegal acts and crimes related to the computer environment have a similar juridical feature at international level. These recommendations were designed to create a uniform juridical framework at international level in order to fight against the cyber crime.

3.3. The Group of the 8 (G8) – which has between 1998 and 2000 the basis of the effective cooperation, creating an international network of contacts that include experts and institutions able to intervene and facilitate the immediate investigation of the penal act related to the computer crime. We remember that in June 2001 the Council of Europe recommends to all the European states to join the network of contacts created by G8.

3.4. European Union and Council of Europe

2005/222/JHA – In 2005 a Framework Decision of the European Council on the attacks against the information systems it is recommended that the member states consider as infractions the illegal access at the computer systems, illegal interception and alteration of the computer data and it imposes some rules concerning the international cooperation.

This is the first document designed to standardise at European level the efforts of combating the computer crime.

The Directive 2006/24/EC of European Council and of the European Parliament on the storage of generated data or processed by the providers of networks and services of electronic communications designed for the public is established in the first document at international level desigmated to ease the gathering of electronic evidences concerning the computer infractions.

3.5. OSCE – Organization for Security and Cooperation in Europe

According to the decision 7/06, it recommends the member states to become party to the Convention to Fight against cyber crime, of the European Council, and encourages states to join the network G8 concerning the cyber crime.

This decision is important because it grants an equal importance to the computer infractions and to the electronic device gathering.

3.6. Interpol – the first institution that has organized international meetings of experts in the computer crime. Having 184 members from all the continents and its role being the one to facilitate the international cooperation of the police agencies, Interpol has made continuous efforts in the fight against the computer crime.

In this way it has been created an international network of contact points aiming the identification of experts in all the countries able to provide assistance in investigating the computer crime.

However the role of Interpol in investigating and combating illicit material information is limited because of the way this organism is built. The reaction time is quick enough to gather evidences in computer matter due to the volatility of the communicated data in the computer networks; this volatility imposes a time to react in only few seconds or minutes in order to collect evidence.

3.7. The Convention Concerning the Computer Crime of the European Council

The ETS 185 – from 23 November 2001 in Budapest is the first effort towards a treaty on cyber crime. The Convention was signed by 46 countries of which 4 are not members of the Council. Out of these 24 countries (including Romania) they have ratified the Convention, the United States being the only non member country that has ratified it. Subsequently, on 28 January, 2003, it was submitted for signature towards the member states "The Additional Protocol for the Convention on the cyber crime, concerning the criminalization of the acts of racist and xenophobic nature committed through the computer systems". Romania has also signed this Additional Protocol on October 9th, in 2003.

The Convention and the Additional Protocol established the basic framework for investigating and punishing the criminal offenses committed through a computer, as well as for interstate cooperation, which also required stopping this scourge.

The Convention brings firstly the necessity for penal criminalization of some acts such as: the illegal access at a computer system, illegal interception of the information transmission, information fraud, infant pornography on the Internet, violation of the property rights and other related rights, etc. Also it introduces new channels of communication in fighting against this type of infraction and it defines a common set of standards for the criminalization of the illicit facts related to the information technology.

4. Conclusions

The problem of information security is placed with priority on the work agenda of those responsible, in the attempt to unite their efforts to harmonize the legislations. The Governments have acknowledged the need for a common criminal penal policy to stop it, through efficient strategies and norms, the information warfare and cyber attacks among the most technical and tactical.

In the fight with the cyber crime it is necessary a good framework well established in terms of prevention, detection and punishment. Through that international act to which it is party, Romania is obliged to develop a legislative system specific to this type of infractions. Moreover, the "old" infractions are done today through modern means (computer theft), at distances of thousands of kilometres, the international cooperation being vital to combat this scourge. Recently, the media announced the creation of a new generation of viruses that attack GSM terminals and unfortunately it

is not just a new direction of these attacks. The law 161/2003 represents a beginning, but for keeping up the huge infraction diversity which takes place with a simple keyboard and a simple mouse click, therefore the legislative activity must not stop here.

An example concerning the necessity to incriminate the most serious of these crimes is the following: presenting a real case, namely, the president of the Cinenet Company from California, Jim Jarrad – has decided to let the computer to work overnight to finish a large download. In its absence, a hacker has accessed he's PC through DSL connection and he has installed a program that had allowed him to control the computer, to steal important files and to delete information from the hard drives. Jarrad escaped of the disaster due to a lock system, and the error message that has found the second day indicated that something it was not right. He lost two weeks of investigations on the issue, during which he learned more then he wanted about hackers eventually being obligated to format the hard disk to get rid of the auto multiplication program of the hacker. This case is far from being unique. Everyday we are informed through the media of cases of some banks or important institutions, either to interrupt the activity, or with the purpose of committing another crime as the one of theft through information means.

5. References

Cârjan, L. (2005). *Criminalistică. Tratat./ Criminalistics. Treaty*. Bucharest: Editura Pinguin.

Dobrinoiu, M. (2006). *Infracţiuni în domeniul informatic/Offences in informatics*. Bucharest: C.H. Beck.

Stancu, E. (2007). *Tratat de criminalistică/Treaty of criminalistics.* 4th revised edition. Bucharest: Universul Juridic.

Vasiu, I. (1998). *Criminalitatea informatică./ Cybercrime.* Bucharest: Nemira.

http://www.riti-internews.ro/ro/cybercrime.htm.

http://www.legi-internet.ro/conventie_crim_info.htm.

http://www.criminalitate.info/

http://en.wikipedia.org/wiki/Computer_crime.

http://www.rbs2.com/ccrime.htm.

http://www.justice.gov/criminal/cybercrime/