Zdzisław Półkowski
Jacek Gruber
Ionut Cosmin Deaconescu

E-Fraud

1. Introduction

Most business transactions are concerned with three types of security. First, they wish to ensure the positive identity of the customer, and that all transactions are sent to the right customer. Secondly, they want to protect sensitive customer information, such as credit card numbers, bank account numbers, or other personal and financial data. Thirdly, they want to make sure that the data is not altered or changed as it is transmitted across the Internet [1].

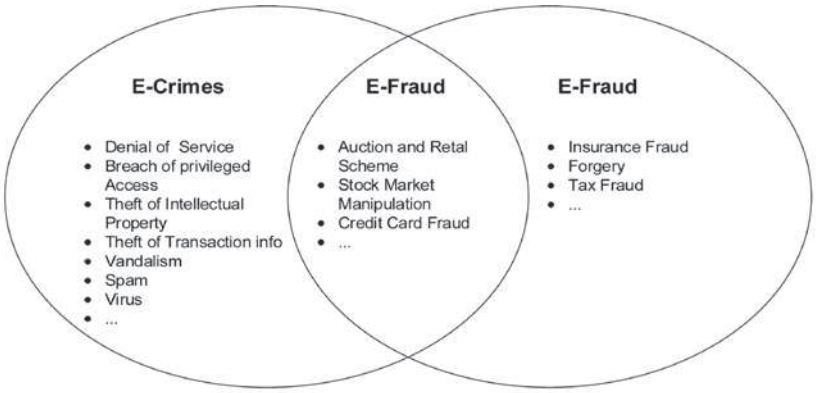

Fig. 1. Examples of e-crime, fraud, and e-fraud [2]

2. Definitions of e-fraud

E-fraud (Electronic-**FRAUD**) refers to any and all types of deception perpetrated online. Numerous definitions of e-fraud have been advanced in the e-crimes literature. Graham (2001) defines e-fraud as:

"a fraudulent behavior connected with computerization by which someone intends to gain dishonest advantage".

In this definition e-fraud equates to, and supersedes, the term *computer fraud*. Some definitions specify e-fraud in relation to electronic commerce or the Internet such as Smith (2001) in which e-fraud is seen as "any dishonest activity that involves the Internet as the target or means of obtaining some financial reward". The USA Department of Justice also defines e-fraud in relation to the Internet.

> *"a fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme*".

Alternatively, some studies define such crimes as 'Internet fraud' [2].

According to other sources:

> *"E-fraud in defined as a deception deliberately practiced to secure or unlawful gain where part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on a computer network"* [3].

3. Classification of e-fraud

You can distinguish the following types of e-frauds:

- Phishing is a type of e-fraud where someone is cheated to give away personal financial data (credit card numbers, account numbers, pin codes, passwords etc.) to the fraudster. The victim is convinced to give away the data through spoofed e-mails and fraudulent spoofed websites where trusted brands are used,
- Online extortion is an e-fraud based on a threat which is presented to a company. The company is asked to pay a sum of money to the fraudster, otherwise the fraudster will expose the company's website to a denial of service attack.
- A fraudster can collect credit card numbers by using false merchant sites. On these websites the victims are offered free or very cheap services, and the victims are asked to provide their credit card details in order to pay for services or to verify their age or similar personal details in exchange for free services. Later, the credit card details are used by the fraudster.
- A sophisticated type of e-fraud is triangulation. In this type of fraud the fraudster operates from a website which offers goods at heavily discounted rates and the goods are also shipped before payment. The site appears to be legal. The customers must provide the name, the credit card number etc. when buying. When the customer makes an order, the fraudster orders the same product (in the name of the customer) from another, legal, website with the stolen credit card details. After a while the credit card details from the customer are used to buy goods, both to the

fraudster and to other customers of the fraudster's website (that is, buying goods from another website which the customer has ordered from the fraudster's website). The purpose of this fraud is to cause a lot of confusion in order to buy some time for the fraudster's website to operate on and collect credit card numbers.

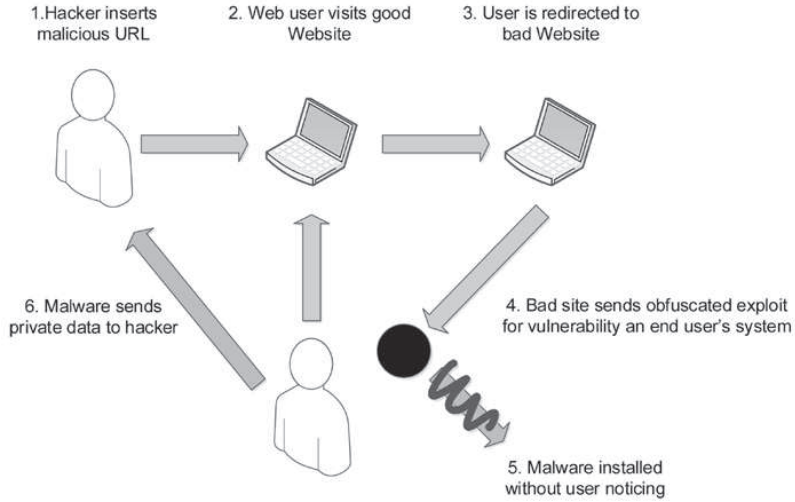

Fig. 2. How Phishing is Accomplished [11]

- Business-to-business fraud is an e-fraud scheme where a company or an organization uses the Internet to commit fraud against other companies or organizations. This is possible due to the systems used in e-commerce. A company (the fraudster) can for example neglect to update price reductions on their products in automatic systems which companies (the victims) use to buy goods from the fraudster's company using the Internet. The victims will not notice that they are being overcharged unless they manually compare the prices to the market prices.
- Internal fraud is another type of e-fraud. An employee can, for example, steal information from a workplace by e-mailing the information to a personal e-mail account. Plagiarism and academic misconduct can also be carried out using the Internet. In these cases the fraudster uses information found on the Internet and either claims that the information is from a fraudster or uses the information in a different context and thereby alters its meaning.
- It is also possible to do money laundering using the Internet. Gambling websites provide a big opportunity for a money launderer. Money can be laundered by, for example, opening an account on a gambling website, putting in some dirty money, gambling for a small amount of it and then withdrawing the remaining amount.

Thereby a legitimate source (a gambling website) is provided for the dirty money. If an owner of the gambling website is in cooperation with money launderer, the person may as well lose the whole amount on the gambling website, providing a legitimate income for the owner of the gambling website [3].

4. Methods to fraud electronic payment systems

In the existing financial market the are many products and useful payments systems for traders and clients, but on the other hand, causes that some types of electronic payment instrument offences are committed by computer professionals. For this reason it is vital to focus on fraud electronic payments. Fraud electronic payment instruments started by manually changing cards, a method called „delete and copy" mode consisting of grating the surface of lost or stolen cards, then sticking to it [4] the numbers from other cards.

Fig. 3. Revised e-fraud model

Developing the IT field causes the emergence of ATMs[1] and electronic payment instruments on the electronic market, but even if the producers and their issuers have taken security measures by introducing authentication codes, criminals, often operating in organized groups, have identified many different methods to fraudulently obtain confidential data of these modern means of conducting transactions and electronic transactions, to withdraw money from bank accounts.

The major methods of electronic payment fraud are skimming, phishing, forking and the latest methods discovered and applied in committing such crimes: the ATM blast method, as well as the so called "electronic pick-pocketing".

4.1. Fraud by the Skimming method

Skimming is an illegal action, which involves stealing confidential data and information of a bank account from the magnetic strip of a card after they are transferred to a fake card or unlawfully detained and then used fraudulently [5]. This action raises major investigative bodies in identifying and proving criminal activity of those involved in such cases and injury recovery [6]. By the skimming method both CVC[2] or CVV[3] codes are copied, also other information is recorded, so that institutions issuers are not able to distinguish between genuine and counterfeit cards [7].

1 Automated Teller Machine.

2 Card Verification Code.

3 Card Verification Value.

4.2. Fraud by the Phishing method

Expansion of the Internet and the rise of web pages, social networks portals lead offenders to turn to those areas, which contain a huge database of personal information such as birth dates, family relations, residence details, places frequented, etc., which can be obtained by them effortlessly, and subsequently used fraudulently [8].

Phishing is a form of criminal activity in the area of cybercrime, which involves creating web pages and sending false messages to customers performing electronic transactions, as, for instance, offering the cheapest on the Internet, in order to obtain confidential data and information, required for a card or a bank account authentication, using manipulating techniques on the identity of a person, an institution or a company [9].

The phishing method involves, in most cases, the offender sending an email, or instant messaging programs or mobile services, in which the user is required to submit his or her confidential data to gain some awards, or is informed that the data is necessary to remedy technical errors that led to deleting the original database. The email is usually indicated in a web address that contains a copy of the actual website of the card issuing institution or company.

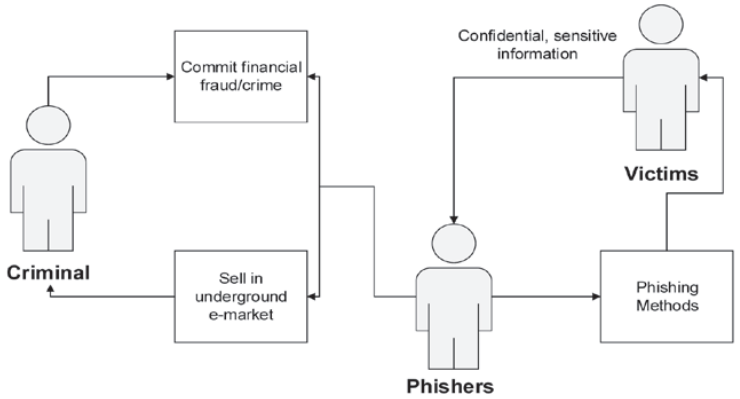

Fig. 4. From Phishing to Financial Fraud and Crime [11]

In most cases, the phishing messages include links to a web page apparently true in other situations, require the recipient to send, accept and download a particular file. By clicking the link in the e-mail received, the user will be redirected to a fake site, a clone of the entire website or only the pages from which the customer is required to transmit the card number, the account PIN[4] and other data required for authentication.

4 Personal Identification Number.

The fictional website will receive confidential data sent by the client and will send the transaction receipt by e-mail, as an institution or official company would do so that the customer does not suspect anything, while the perpetrators have all the details they need to commit fraud on bank accounts.

Fraudsters who have ordered goods or services are relatively easy to detect, but research bodies take a long time to identify and track the sites administrators because they can work almost anywhere in the world [10].

Phishers (or other criminals) obtain confidential information by methods ranging from social engineering to a physical theft. The stolen information (e.g., credit card numbers, social security numbers) is used by the thieves to commit financial fraud or is sold in the underground Internet marketplace to other criminals, who then use the information to conduct financial crime [11]. The graph above describes how such systems work.

4.3. Fraud by the Forking method

The unique method invented and used by members of organized criminal groups specializing in fraud of electronic payment instruments, especially the cards was called the Forking method and was first implemented in March 2012.

Criminals can apply this method by introducing the card slot of a real cash dispenser for a bank account from which to withdraw a small amount of money. After they receive the money from the first ejection, fraudsters perform identically, another ejection, this time requesting a substantially higher amount accepted by the bank. When preparing the ATM dispensing money, the offender shall cling a specific tool and extract it, canceling the transaction before debiting takes place so that the card holder keeps the money fraudulently withdrawn [12].

Investigators consider this method as one rudimentary, lacking complexity and ingenuity, but easy to apply, given its simplicity and the tools of the offense.

4.4. Fraud by the „ATM explosion" method

A newly discovered ATM explosion method, also called the Dutch method, has been used by criminals since 2012. With this method, the criminals use a mixture of oxygen and acetylene inside an ATM and produce a spark with an electric ignition device.

The mode of operation involves placing the gas – a mixture of acetylene and oxygen- with an electric cable for a remote use through a tube with a cylinder in the ATM slot, Then, the explosion is triggered. Immediately after the detonation and destroying the ATM, criminals extract the money from the box, that is supposed to protect the money against fire and other factors [13].

4.5. Fraud by the „Electronic Pickpocketing" method

A new type of crime in the electronic payment instruments, is based on producing a growing number of cards that work according to the principle of the RFID[5] technology, widely used in security badges and electronic toll systems. Criminals, acting usually in large crowded, shopping centers, through a close reading device the size of an iPad, steal data [14] from cards hidden in bags, purses, wallets or pocket.

Withdrawing RFID cards and chip cards from the market is the easiest and the fastest way to fight against this crime. On the other hand, if customers accept this type of card, they can keep the cards in metal covers, aluminum foil, cans for business cards or covers made of special materials.

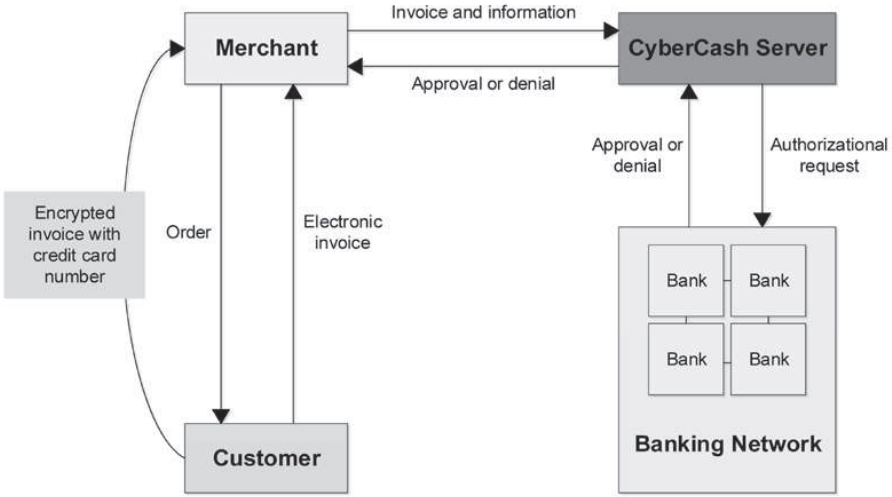

Fig. 5. An Online Payment Using Cybercash Software [15]

4.6. Other ways to fraud electronic payment systems

In addition to the methods presented above, members of organized criminal groups have adopted other ways to fraud electronic payment instruments, especially those used in a less extensive way as compared to those we frequently use, respectively the Lebanese loop method using sensors, sending cards, opening an account in the halls of institutions, and many others [16].

5 Radio-Frequency Identification, is an automatic identification method that relies on storing and retrieving data by touch or within a few meters, using radio waves. Currently globally in circulation about 200 million cards that work on this principle.

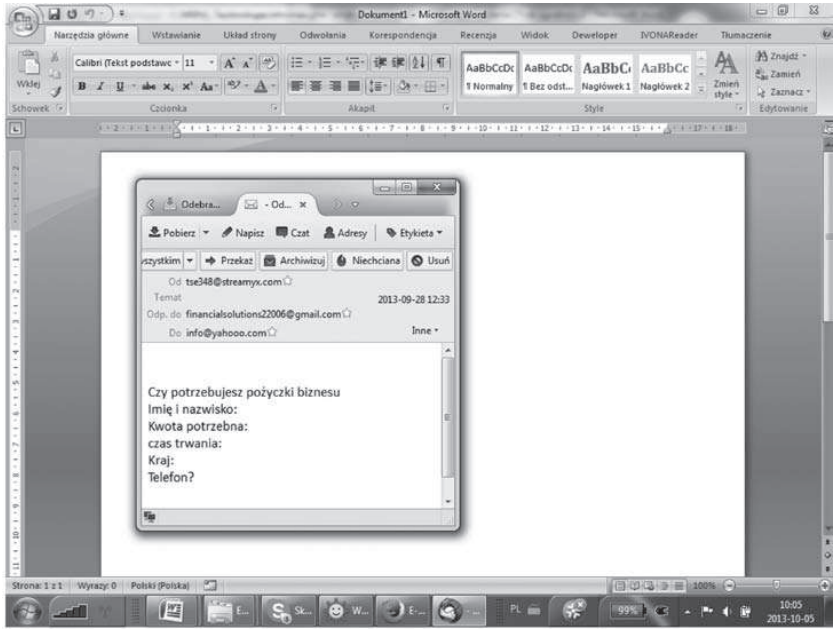

Fig. 6. Screenshot of a fraud mail

5. Case studies

The following cases are examples of performed and discovered fraud activities concerning the USA, followed by cases from Poland and Romania, given to illustrate the character and the scale of the phenomenon.

Case 1 – Money Laundering

Ross William Ulbricht denied charges that he ran a billion-dollar online drug "bazaar" and plotted a murder-for-hire, his lawyer said after persuading a judge to postpone a bail hearing until Oct. 9.

Ulbricht, curly-haired, clean-shaven and wearing a red jail jumpsuit with his hands and legs shackled, made his second appearance in federal court in San Francisco the same week after being arrested by the FBI on October 1, at a city public library.

"We deny all charges and that's the end of the discussion," defense attorney Brandon LeBlanc told reporters outside the courtroom today after U.S. Magistrate Judge Joseph Spero agreed to give him time until next week to compile more financial information for a bail proposal.

Prosecutors say Ulbricht ran the "Silk Road Hidden Website" and was known as "Dread Pirate Roberts" or "DPR," after a character in the 1987 film "The Princess Bride." Federal agents seized Silk Road, along with digital currency Bitcoins worth $3.6 million, and shut down the site on October 2. Prosecutors said, in court filings in Manhattan, that the site generated more than a billion dollars in illicit sales and took in $80 million in commissions in less than three years.

The prosecutors called the site "the most sophisticated and extensive criminal marketplace on the Internet," and charged Ulbricht with narcotics-trafficking conspiracy, computer-hacking conspiracy and money-laundering conspiracy. Ulbricht was also indicted in federal court in Maryland for allegedly trying to arrange the murder of an employee he feared would become a witness against him [17].

Case 2 – Anonymous attack on FBI

Minutes after the U.S. Department of Justice shut down notorious file-sharing site Megaupload.com, the department's own website was brought down in a cyber attack orchestrated by the hacker group called Anonymous (...).

The group also disabled the sites of Universal Music, the RIAA, the U.S. Copyright Office, Broadcast Music Inc., the FBI and the Motion Picture Association of America in what it called its "largest attack ever." By late evening, however, most sites were back online.(...)

Megaupload.com, dubbed by prosecutors as "Mega Conspiracy," was accused of engaging in a scheme that took more than $500-million away from copyright holders and generated more than $175-million in proceeds from subscriptions and advertising, according to the indictment unsealed on Thursday.

At one point, Megaupload was estimated to be the 13th most frequently visited website on the Internet. Users could upload material to the company's sites, which then would create a link that could be distributed. The sites included video, music and pornography, as well as child pornography and terrorism propaganda videos, according to the indictment [18].

Case 3 – Hackers hit FBI and NATO 'for fun'

A gang of hackers who attacked computers at the Pentagon and NATO for 'laughs' were jailed yesterday for their campaign of havoc. The four British hackers acted as 'latter-day pirates', crashing computer systems and stealing confidential data including passwords and credit card details (...).

Three of the hackers were teenagers, the youngest only 16, yet they attained celebrity status on the internet, where one bragged: 'We are gods now.' They boasted about their ability to attack high-profile targets, including Sony, the FBI and the UK's Serious Organized Crime Agency (...).

Working from their bedrooms, often in their parents' homes, they accessed the confidential details of 26.4 million Sony customers and 74,000 would-be X Factor contestants in the US. They released police officers' personal details onto the internet after an attack on Arizona State Police and another raid left the website of Britain's Serious Organized Crime Agency disabled for 12 hours.

Prosecutor Sandip Patel said the gang had displayed extraordinary computer skills but added: 'These defendants acquired destructive tools to use on the Internet. They are at the cutting edge of a contemporary and emerging species of international offending known as cyber crime [19].

The conspirators never met but were members of the online group LulzSec, which used the motto 'Laughing at your security since 2011'. Some attacks involved stealing users' data but others simply hijacked sites. (...)

All four defendants admitted a single charge of conspiring to target computers at Sony, 20th Century Fox, US broadcaster PBS, Nintendo, the NHS, Arizona State Police and News International [43].

Case 4 – Hackers attack FBI partner website

A group of hackers responsible for a string of high-profile cyber attacks claimed to have stolen email addresses and passwords from associates of an FBI-affiliated security program.

The hackers, who called themselves „Lulz Security," or LulzSec, said they had attacked the website of the Atlanta chapter of InfraGard in retaliation for US efforts to classify hacking as an act of war (...).

„We also took complete control over the site and defaced it," Lulz Security" said in a statement at their website, Lulzsecurity.com.

"Lulz Security" later claimed to have compromised more than one million passwords, email addresses and other data from SonyPictures.com, a site which features movie trailers and email updates on upcoming releases [44].

The group posted thousands of stolen Gmail, Hotmail, AOL, Yahoo and other email addresses and passwords on Pastebin where they were publicly accessible (...) [45].

The hackers marred PBS Web pages with graffiti, exposed account information of member stations, and posted a fake story about the late rap musician Tupac Shakur being alive in New Zealand [20].

6. Examples of case studies in Poland

Case 1 – Skimming Gang

In this case, a gang specializing in skimming, forgery or fraudulent cards and using the money was smashed by police officers and prosecutors from several European countries.. Officers from Lublin were those who found out about the group.

The Romanian police arrested a total of five people. It was possible through the cooperation of prosecutors and police investigators from the department for combating economic crime in Lublin, the Police Headquarters, Europol and law enforcement forces in Romania and Sweden, - said Krzysztof Hajdas the press department of the National Police Headquarters. He added that the Polish aspect of this case began at the turn of 2009/2010, in Lublin with a number of thefts from ATMs. The police detained three people. They were driving a car that a few days earlier was observed near one of the mugged ATMs - said Hajdas.

When the car was stopped, it turned out that the citizens of Romania were in possession of counterfeit ATM cards. They were sent to prison, and the prosecutor's office sent the court indictment to them [21].

Case 2 – Skimming in Poland

In Szklarska Poręba three Romanians were arrested for trying to skim copy data from ATM cards . Foreigners were arrested shortly after they installed the device to copy data.

The police learned that one of the ATMs in Szklarska Poręba might have a device mounted onto in order to download the data, and organized an ambush. It turned out that the scammers actually had prepared to copy the security code from the client cards.

The police detained a 29-year-old citizen of Romania, who hovered near the ATM. His partners also appeared. In the hotel room nearby, the officers found a skimming device, a laptop and various types of magnetic cards.

Criminals may be sentenced to 25 years imprisonment [22].

Case 3 – Poland Busts Online Fraud Group with Russian Links

On February 27, in Warsaw, - Poland's Internal Security Agency informed that it had completed an investigation against a group suspected of luring money from Internet users and transferring a part of its profit to accounts in Russia.

The agency said a group of 12 people, based in the city of Radom in central Poland, used the phishing technique to lure money from unaware users.

"The money they received during such activities has been transferred to recipients, including in Russia, via a chain of bank accounts," the Internal Security Agency said in a statement.

The group performed about 800 transfers, totaling at least $230,000.

The suspects, whose names were not disclosed, admitted their guilt in full [23].

7. Examples of case studies in Romania

Case 1 – Romanian Cybercrime

Following a four-day trial, a federal jury in Brooklyn returned a verdict convicting David Ojo of conspiracy to commit wire fraud and identification document fraud. The defendant was a member of an international organized crime conspiracy, operating in Romania, Bulgaria, and the United States, that defrauded victims of tens of thousands of dollars through an Internet scam.

Trial testimony showed that the defendant and his co-conspirators advertised used cars for sale on websites like Craigslist and eBay. Some buyers who responded to the advertisements were told variations of a story that the seller of the car had been called to active duty in Afghanistan and needed to sell his car quickly. The victims were promised that their purchases would be handled by an eBay or Google Checkout agent, who would hold their payments in escrow until they had received the car. Once the victims agreed to buy the cars and wired payments through Western Union, they never received any cars or heard from the purported sellers again [24].

The defendant worked with individuals in Romania and the United States to make and use false Pennsylvania and Delaware driver's licenses, which they used to claim the money that the victims had wired through Western Union. The defendant was personally responsible for making or directing more than 30 separate money pick-ups in which victims were defrauded out of more than $80,000. (...)

When sentenced by the Honorable Allyne R. Ross, the defendant faced a maximum penalty of 20 years' imprisonment [46].

8. Application of data mining for fraud detection in IT systems

It follows from the above- made stage, that despite the many undeniable advantages of the Internet as a medium of communication and the environment, business and banking operations, the Internet also poses a range of threats.

The means of protection against these threats, among other intrusion detection systems, are very significant. The purpose of these systems is to detect attacks on the environment servers, business services and the networking environment. There are various methods of data mining, which can be used to detect attacks on the network infrastructure systems. Detecting an attack is the problem of classification of network traffic for traffic safety or traffic accompanying attacks on infrastructure and related abuses in business IT systems.

The effectiveness of data mining methods for detecting e-Fraud has been analyzed in numerous articles describing the models and methods implemented in statistical packages, for example in STATISTICA. Many of these items can be found in the reading room on the StatSoft portal [25]. Article [26] describes how to use the STATISTICA program and data mining methods to detect fraud on the example of transactions completed in an online store - in this case the detection of customers who do not pay for the purchased goods in the online shop. Paper [27] deals with the methods that are used in data mining. However, article [28] describes the problems the effectiveness of predictive data mining in a variety of dedicated systems to detect and prevent fraud incidents and e-Fraud. In [28] there are examples of the creation of appropriate data mining projects in STATISTICA, which have the ability to run and evaluate the effectiveness of different methods of data mining to prevent abuse of e-Fraud.

The process of data mining project in STATISTICA was presented in article [29]. Paper [30] describes how to detect fraud on the example of detecting money laundering. For the detection of many types of attacks e-Fraud is made possible by data mining of network traffic in the network and Internet infrastructure, business systems, as well as other important network infrastructure, IT systems, such as military systems - both defensive and offensive. Such applications of data mining methods are discussed in article [31]. This article examines the effectiveness of classification and the efficiency of detecting attacks by means of specific methods, namely: k Nearest Neighbours - KNN, Classification and Regression Trees - C & RT, Chi-squared Automatic Interaction Detection (CHAID), and network neural. It has been shown that the most efficient for the task of classifying traffic on anomalies and irregularities - the KNN method - achieved the average results of the rankings in over 70% of cases and showed a low standard deviation. Other methods have not proven to be very effective. For the type of attack traffic, such as, for example, for a Denial of Service – DoS, Classification and Regression Trees was the most effective method with the result of the attack detection of more than 80%. The Neural Network and k Nearest Neighbours method achieved the result of over 70%. However, Neural Networks obtained a standard deviation of 8%, a relatively large one.

9. Conclusions

Since no it has not been required so far to classify all kinds of fraud in a non ambiguous way, it is not possible to use any of them to predict frauds in new environments, such as the Internet. Combining the existing classification systems or taxonomies is not considered as an option, due to the diversity of the goals pursued by each methodology.

Instead, there are telecom case studies compared to e-fraud case studies showing that the concepts from the telecom cases are already existing in the e-fraud cases. This conclusion, however, cannot be made for all real world frauds, which would represent a majority of the concepts, since frauds have a long history in the telecom environment [3].

Out of a comparison between e-fraud and telecom fraud cases studies the following challenges with e-fraud prevention and detection may be found:

- Anonymity
- Automation
- Available victims
- Fraud cost
- Speed
- Ambiguity
- Lack of interconnection
- Novel users

But the following possibilities with e-fraud prevention and detection have also been found:

- Interpretation
- Available data

These differences are extracted from a comparison between e-frauds and telecom frauds, but are they considered as representing the differences between e-frauds and real-world frauds. The major consequence of the challenges is that e-fraud cases are more scalable in both finding and dealing with victims [3]. The results discussed in [25] show that it is worthwhile to use data mining to detect fraud.

This paper examines the use of IT systems in the e-fraud context. Although IT systems can give users a lot of benefits, their use is still a complicated issue, in particular in the security aspect. Using the Internet seems to be the most commonly preferred method to perform payments and use banking systems. Many people use this sort of solutions without even being aware of it. The analyzed cases show that there are many problems with e-fraud. It should be noted that analyzed cases in Poland, Russia and Romania have shown that e-fraud problems are very common and many people lose a lot of money. For this reason, users may feel discomfort due to the work on the Internet.

In Poland and in Romania there are a lot security solutions to reduce the number of the problems in payment and banking systems. On the other hand, Internet users, do not have enough information on this topic.

Apart from the e-fraud, the security of data issues must be considered. The trends observed currently in this area include new regulations in the EU, Poland and Romania which are related to improving the security of banking and payment systems.

Streszczenie

Oszustwa internetowe

Elektroniczne oszustwa i matactwa stanowią największą część wszystkich przestępstw komputerowych. Nadużycie jest rodzajem oszustwa, na którego wystąpienie nie ma bezpośrednich dowodów.

Celem niniejszego artykułu jest analiza obecnego stanu przestępstw komputerowych w wybranych krajach w kontekście aktualnego wykorzystania systemów internetowych. W pierwszej części artykułu autorzy przedstawiają różne definicje i klasyfikacje e-oszustw. Kolejna część poświęcona jest prezentacji wybranych metod oszustw systemów płatności elektronicznych. Jej ostatnia część skupia się na prezentacji *case studies* dotyczących e-oszustw w Polsce i Rumunii. Przeprowadzone badania stanowią wkład w zrozumienie metod oszustw elektronicznych.

Summary

E-Fraud

On-line fraud and cheating constitute the biggest part of all computer crime. Cheating is a kind of fraud that does not have direct evidence of its appearance. The purpose of this article is to analyze the current state of e-fraud in selected countries in the context of contemporary Internet system. In the first part of the paper, the authors present various definitions and classification of e-fraud. The next part of the paper is devoted to presenting methods to fraud electronic payment systems. The last part of the work will be focused on case studies concerning e-fraud in Poland and Romania. This study brings its contribution to the understanding of the methods of e-fraud. To prepare this article, information available from the Internet, as well as the official websites of government institutions, banks, portals, European Union, national and international media was used.

Bibliography

1. Akintoye K. A., Araoye O. I., *Combating E-Fraud on Electronic Payment System,* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.259.3383 [Accessed 25 November, 2013].
2. Malakedsuwan P., Stevens K., *A Model of E-fraud,* http://www.pacis-net.org/file/2003/papers/e-business/233.pdf, University of NSW, Sydney 2003, p. 4 [Accessed 15 November, 2013].
3. Bergman B., *E-fraud: State of the art and countermeasures,* Linkoping University, Sweden 2005.
4. Turban E., Lee J., *Electronic Commerce 2010,* Pearson, 2010, p. 484.
5. Card Skimming, http://www.scamwatch.gov.au/content/index.phtml/tag/CardSkimming [Accessed 21 November, 2013].

6. *How ATM card skimming and PIN capturing scams work,* http://www.slideshare.net/worldstuff/how-to-detect-atm-card-skimming-and-pin-capturing-scams [Accessed 23 November, 2013].
7. Olteanu G. I., *Methodology Criminology – Structures criminal and illegal activities carried out by them*, Editura AIT Laboratories s.r.l, Bucharest 2008, p. 65.
8. *E-mails Phishing and Scams,* http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201112_en.pdf, p. 2 [Accessed 23 November, 2013].
9. *How Phishing Works,* http://computer.howstuffworks.com/phishing.htm [Accessed 22 November, 2013].
10. Milletary J., *Technical Trends in Phishing Attacks,* www.cert.org/archive/pdf/Phishing_trends.pdf, p. 4 [Accessed 14 November, 2013].
11. King D., Lee J., *Electronica Commerce 2010A Managerial Perspective,* Pearson 2010, p. 486.
12. *Beware the cash trap! Claw-like devices inserted into ATM slots can steal notes in latest hole-in-the-wall scam,* http://www.dailymail.co.uk/news/article-2236213/Claw-like-devices-inserted-ATM-slots-steal-notes-latest-hole-wall-scam.html [Accessed 17 November, 2013].
13. *Best Practice for ATM Security, Overview of ATM security situation, forecast, and best practices,* GRGBanking Equipment (HK) Co. Ltd, 27.05.2011, http://www.grgbanking.com/en/exh/images/Best%20Practice%20for%20ATM%20Security%20-GRGBanking.pdf, p. 11 [Accessed 4 November, 2013].
14. *Identity Theft – Electronic Pickpocketing,* http://pueblo.org/sites/default/files/documents/scam-alerts/January%202011%20-%20Identity%20Theft-Electronic%20Pickpocketing.pdf, p. 1 [Accessed 3 November, 2013].
15. Da Costa E., *GlobalE-Commerce strategies for small businesses*, MIT 2001, p. 69.
16. Benoni B. B., *Electronic Payment Systems Fraud*, Bucharest 2013.
17. *Accused Cyber-Bazaar "Pirate" Has Bail Hearing Delayed,* http://www.bloomberg.com/news/2013-10-04/alleged-cyber-bazaar-pirate-ulbricht-bail-hearing-delayed.html [Accessed 15 November, 2013].
18. *Hackers Attack FBI Justice Department Websites After Megaupload Shutdown,* http://news.nationalpost.com/2012/01/19/hackers-attack-fbi-justice-department-websitesafter-megaupload-shutdown/ [Accessed 28 November, 2013].
19. *Hackers Who Thought They Were Gods,* http://www.dailymail.co.uk/news/article-2325624/Hackers-believed-gods-cyberspace-jailed-attacks-CIA-FBI-NHS-computers.html[Accessed 25 November, 2013].
20. *Hackers Attack FBI Partner Website,* http://www.alternet.org/rss/breaking_news/607507/hackers_attack_fbi_partner_website[Accessed 14 November, 2013].
21. *Policjanci i prokuratorzy rozbili gang zajmujący się skimmingiem,* http://www.polskieradio.pl/5/3/Artykul/314723,Policjanci-i-prokuratorzy-rozbili-gang-zajmujacy-sie skimmingiem [Accessed 13 November, 2013].

22. *Trzech Rumunów aresztowanych za próbę skimming,* http://www.dziennikbalty cki.pl/artykul/161915,szklarska-poreba-trzech-rumunow-zatrzymanych-za-probe skimmingu,id,t.html [Accessed 8 November, 2013].
23. *Poland Busts Online Fraud Group with Russian Links,* http://en.ria.ru/crime/20130227/179717075/Poland-Busts-Online-Fraud-Group-with-Russian-Links. Html [Accessed 9 November, 2013].
24. *Defendant In Romanian Cybercrime Ring Convicted Of Wire Fraud And Identification Document Fraud Conspiracies,* http://www.justice.gov/usao/nye/pr/2013/2013aug09.html [Accessed 7 November, 2013].
24. Gruber J., Jozwiak I., Mosio Ł., *Freud detection business systems using data mining method*, Sil. University of Techn. Publishing House, Gliwice 2013, pp. 61–71.
26. http://www.statsoft.pl/czytelnia/czytelnia.html [Accessed 7 November, 2013].
27. Demski T., *Creating and using data mining model using STATISTICA Data Miner provisions on fraud detection example,* StatSoft Polska, http://www.statsoft.pl/czytelnia/czytelnia.htmll, 20/05/2012 [Accessed 16 November, 2013].
28. Sokołowski A., *The methods used in data mining,* StatSoft Polska, 2002.
29. Wątroba J., *Examples of predictive problem solving using data mining techniques,* StatSoft Polska, 2002.
30. Wątroba J., Kowalski T., Demski T., Data mining and its implementation in STATISTICA DataMiner, StatSoft Polska, 2002.
31. Kuijlen T., Migut G., *Detection of fraud and money laundering,* StatSoft Polska, 2004.
32. de Lange J., Longoni A., Screpnic A., *Online payments 2012, Moving beyond the web, May 2012, E*COMMERCE Europe, p. 57, www.innopay.com [Accessed 25 November, 2013].
33. Polasik M., Maciejewski K., *Innovative payment services in Poland and abroad,* Warsaw, 2009, http://www.nbp.pl/publikacje/materialy_i_studia/ms241.pdf, p. 12 [Accessed 25 November, 2013].
34. *Proposal for a Regulation establishing technical requirements for credit transfers and direct debits in euros and amending Regulation (EC) no. 924/2009, COM (2010) 775,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010PC0775:EN:NOT. [Accessed 24 November, 2013].
35. The Paypers, *Romania: e-commerce market to surpass EUR 160 million,* 2011.
36. http://www.aerotranslate.com/webmoney/other-online-payment-systems-in-russia. Html [Accessed 18 November, 2013].
37. http://www.freewebs.com/mkurnia/chap6.doc, p. 2 [Accessed 13 November, 2013].
38. *Electronic Payment Systems,* http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf, p. 15 [Accessed 19 November, 2013].
39. *Online Payment Systems for E-Commerce,* http://www.oecd.org/internet/ieconomy/36736056.pdf, p. 4 [Accessed 20 November, 2013].

40. Oshkalo A., *What is the Most Popular E-Currency in Russia,* http://www.russian search-tips.com/2012/04/what-is-the-most-popular-e-currency-in-russia/ [Accessed 9 November, 2013].
41. *Payments in Russia,* http://www.payboutique.com/payments-russia[Accessed 8 November, 2013].
42. *Identity Theft – Electronic Pickpocketing,* http://pueblo.org/sites/default/files/documents/scam-alerts/January%202011%20-%20Identity%20Theft-Electronic%20Pick pocketing.pdf, p. 13 [Accessed 4 November, 2013].
43. *Hackers Who Thought They Were Gods,* http://www.kanyiokeke.com/2013/05/hack ers-who-thought-they-were-gods.html [Accessed 2 December, 2013].
44. *Hackers claim another Sony attack,* http://phys.org/news/2011-06-hackers-sony.html [Accessed 26 November, 2013].
45. *Hackers claim new Sony cyberattack,* http://phys.org/news/2011-06-hackers-sony cyberattack.html [Accessed 26 November, 2013].
46. *Defendant in Romanian Cyber Crimes Ring Convicted of wire Fraud and Identification Document Fraud Conspiracies,* http://www.fbi.gov/newyork/press-releases/2013/ defendant-in-romanian-cyber-crime-ring-convicted-of-wire-fraud-and-identification document-fraud-conspiracies [Accessed 29 November, 2013].