UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido

http: revistas.udistrital.edu.co/ojs/index.php/visele/index

VISIÓN ELECTRÓNICA

A CURRENT VISION

Technology and bank fraud

La tecnología y el fraude bancario

***José Custodio Najar Pacheco*[1], *Helena Clara Isabel Alemán Novoa.*[2]**

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: 22/07/2017
Recibido: 02/08/2017
Aceptado: 21/09/2017

Keywords:
Cybercriminals
Electronic banking
Fraud On-Line
Hackers
Malicious code
Trojan.

Palabras clave:
Ciberdelincuentes
Banca electrónica
Fraudes On-Line
Hacker
Código malicioso
Troyanos.

ABSTRACT

Technology plays a major role in the development of the economy of a country and in general in organizations. It is known that it is used in the massive media, the Internet, known by society, which favors all, in this case banking, which allows its users facilities as the constant development of technology and easy setup supports, and also neglecting safety. In addition to the vulnerabilities in the configuration, technology, humans, applications, platforms, among others; exploited by Cybercriminals organizations operating at an international level, causing incalculable losses to the banking system, the worrying thing is that is growing. However, some banks are required to meet minimum safety standards, there will always be risks, in this way it won't be possible to achieve information security one hundred percent.

RESUMEN

La tecnología juega un papel trascendental en el desarrollo de la economía de un país y en general de las organizaciones. Para darse a conocer utiliza los medios masivos de comunicación, el Internet, conocido por la sociedad, lo cual favorece a todos, en este caso a la banca, que permite a sus usuarios facilidades, por cuanto la constante aparición de tecnología y fácil configuración así lo admite, descuidando la seguridad. Además de las ulnerabilidades en la configuración, la tecnología, el ser humano, las aplicaciones, las plataformas, entre otras; aprovechadas por organizaciones de Ciberdelincuentes que operan a nivel Internacional, produciendo pérdidas incalculables al sistema bancario, lo preocupante es que va en crecimiento. No obstante, a pesar de que algunas entidades bancarias están obligadas a cumplir la norma de los estándares mínimos de seguridad, siempre habrá riesgos, así nunca se podrá lograr la seguridad de la información en un ciento por ciento.

[1]Systems Engineering- Universidad de Boyacá, Telematics specialist – Universidad de Boyacá, Telecommunications Management Specialist-Universidad Central de Bogotá, Mg(c). Information security– Universidad Internacional de la Rioja, España; Teacher at Fundación Universitaria Juan de Castellanos. Email: jnajar@jdc.edu.co, jnajar_pw@yahoo.com.

[2]Systems Engineering- Universidad de Boyacá, Mg(c). Information security Universidad Internacional de la Rioja, España, Pedagogy for Autonomous Learning Development Specialization, Universidad Nacional Abierta y a Distancia, Teacher at Fundación Universitaria Juan de Castellanos. Email: haleman@jdc.edu.co.

Citar este artículo como: J. C. Najar, H. C. I. Alemán. "Technology and bank fraud". Visión Electrónica, algo más que un estado sólido, Vol. 11, No. 2, 289-298, july-december 2017. https://doi.org/10.14483/22484728.12922

1. Introduction

Nowadays, Organizations, independent of their size, company name, type of service, in health, education, and banking; be these: public, private, mixed. Even regardless of their geographical location, they need to make themselves known and develop their own activities. The easiest and relatively cheapest way is with the use of the Internet, since it is an easily accessible, also relatively accessible service to everyone.

Similarly, society today, to develop their daily activities uses the Internet. On occasions as a means of consultation but also of an obliged form, because at present some Organizations provide their services through this medium, so the user must interact, as part of the culmination of a process.

Technology and its constant evolution has facilitated that society and Organizations make massive use of this service, which has allowed its easy installation, configuration and use.

The information traffic through the network of networks is undoubtedly surprising. So, there will always be curious to know what data flow, which for your knowledge by strangers will depend on how safe it is. Consequently, it will be related to technological, physical, logical, human and configuration factors, among others.

Thus, at present, one of the Organizations most highly exposed to all kinds of crimes is Banking, so there are organizations of cybercriminals dedicated to attack them, they do not waste opportunity, they use any form and medium as in this case malicious software, which is responsible for stealing banking data, by creating malicious codes to steal information from banks in a high percentage, web attacks to them, on-line fraud as a result of misusing of technological facilities, emails asking for important information whose objective is to obtain the bank account numbers from fraudulent banking sites. E-mails from seemingly accounts of the same organization are served by employees. Thus, achieving the theft of approximately 1000 million dollars, and the most worrying thing is that every day the actions of hackers is more sophisticated, which leads to the organizations that they must reinforce their security. Similar to audit the access and use of data as it was expressed by Oracle. (c) [1].

Electronic banking plays a transcendental role in any society, allowing transactions to be carried out online, but in the same way they are exposed, since hackers seek to appropriate information related to banking identity when they are online, as they attack the computer, in order to search for identity theft or use malicious software, which allows hackers to appropriate data such as user names, passwords, among others. It is a worrisome situation since approximately 75 % of users use the internet to carry out this type of activity. Therefore, there is a responsibility of the parties and even the developers of the applications and platforms, the most oppressive one is that crime is organized and it has experts on cybernetics, lawyers, accountants and even financiers.

Thanks to the constant evolution of technology, it becomes increasingly easy to control, carrying out a number of activities from any place and at any time with the use of mobile devices and their ease of handling. However, the security of these is not the most appropriate, it is used by hackers, who can take advantage of economic resources, and even can attack and disable websites and a considerable number of daily attacks. The most surprising thing with the use of mobile technology is that pirates managed to appropriate personal information from 15 million wireless users.

On the one hand, the security of the information of the banks and their users is difficult to achieve, since it will always be exposed, for many and diverse reasons. In this way, there will always be the responsibility of the parties. The reality is that everything that is done to achieve security is important in order to minimize the risks and make it more difficult for criminals to act, because as we can see, in reality, the security of information will never be achieved one hundred percent.

On the other hand, it is intended to make known that effectively the security of information in banking is difficult to achieve, since many factors such as technological, physical, logical, human and configuration intervene, among others. Therefore, the information may be known by unauthorized persons both internal and external to these Organizations, despite better configuration and greater investment made in the interest of information security. This will always be available to cybercriminals

1.1. Technology and banking fraud

Today the reality is that communications have allowed us to see the world with different eyes, because we can observe everything and do it from anywhere in the geography, with a simple click. So, large organizations for its operation depend on communications, without which it would not be allowed or facilitate its operation in an agile and timely manner. Health systems, the stock

exchanges of the world, banking, control systems for public services in large cities, traffic signaling systems, etc. Among many others, they make possible and facilitate the existence of humanity.

While it is true, mass communication systems facilitate and allow organizations at all levels to make themselves known and present their services in a globalized market and this may be what makes them very competitive, since they are already visible anywhere in the world; this is thanks to the existence of technology, which allows easy installation and configuration.

At present, in the network of networks circulates a large amount of important information, less important, encrypted, and not encrypted. According to its importance or value that each of its owners wants to give it. The most ironic thing is that there will always be someone who is monitoring the information that goes through the network, in order to select what information you are interested in and especially to which organization this belongs to.

The most desired information today by cybercriminals and organizations dedicated to committing crimes is related to banking.The organizations of cybercriminals dedicated to commit this type of crime, spare no effort to use any trickery in order to achieve their mission, "Brazil, along with Mexico and Peru, lead the development of this malicious software, which steals bank data of users in Latin America ", due to the attacks of"Trojans ", a malware that provides remote access from an infected computer to an attacker, according to Fabio Assolini, senior security analyst at Kapersky [2].

Likewise, these cyber-pirate organizations appropriate important information related to bank customers, thus seizing several million companies and individuals from around the world, in relation to the United States Department of Justice, announcing the charges against a Russian presumed to be orchestrated the plan [3], likewise, in 80 % criminals create codes with the intention of stealing information from banks, likewise, attacks on the Web are more frequent every day [4].

The constant emergence of technology has also allowed the increase in the use of electronic mail, numerous goods and services, the use of banking, among others, which although it is certainly facilitating the development of a number of activities in all areas, both personal and organizational, with the use of the network of networks. Unfortunately, it has also appeared those who have taken advantage of misusing these facilities, leading to the creation of various forms of crime and fraud that are becoming increasingly frequent, among which we can highlight the so-called On-Line fraud, as exposed by Javier Bicarregui Garay [5], in the ECONOMIC STUDIES BULLETIN.

Nowadays, the use of electronic mail is very personal and important, since it has become a relatively cheap and easy to use as a means of communication. It is used by public and private organizations, educational institutions, research institutions, banks, etc; there are some institutions and people for security using more than one email account, banking for their customers' requests emails, as part of their processes and of course it is important. Taking advantage of this massive use of mails, criminals send information to their accounts, in order to get important data, which aims to obtain bank account numbers, among others [6] or very similar websites [5], but if they are false, since they are sent from fraudulent banking sites in which it is alerted that an alleged fraud has been detected with a credit card associated with the recipient, they have become one of the most recent ways to capture unsuspecting and make them victims of a fraud.

In addition to, if the recipient is a customer of the bank and he has a credit card, he could click on that link, and at that moment a new phase of deception arises [7]. In the same way, the technique used by the delinquents of the mailings from accounts apparently of the same organization, are attended by employees. In this way, they obtain access to the network of the organization, in that opportunity through this modality, the theft of approximately 1,000 million dollars was achieved to banks in Russia, Eastern Europe, China and the United States [8]; or also by users, who can easily fall into the trap of responding to emails, where they are asked to update data from their electronic banking card, using misleading information, which makes the customer respond, this is because users may have never been alerted about the existence of false email addresses [9].

At present, the industry that is most exposed to these type of situations is banking, for which it is obliged to comply with the standard related to minimum security standards, which are required by the Superintendency of Banks; and they are obliged to comply to protect the information of both the bank and its users. However, according to Daniel Atik, an ex-hacker says that while it is true that the national banking system complies with all security standards, vulnerabilities are latent. As a result, no one is safe, even the bank where he has his personal account has twice alerted him that his credit card has

been cloned. There are "more protected sectors than others, such as banking, but that does not mean that the data is 100 % safe,"says Jorge Vidal, Expert Service security expert, especially in the case of Chile that has the lowest penalties for computer crimes, says Francisca Aros, OS-9 Carabineros [10] and most worrying is that the actions of hackers is increasingly sophisticated, which leads to organizations must strengthen their security and audit access and use of data as expressed by Oracle. (c) 2016 [1].

On the one hand, the use of electronic banking plays a very important role in our environment, since it facilitates the advancement of a series of processes among the most important banking transactions. In this case, the user plays a very significant role when staying online, as hackers seek to appropriate information related to online banking identity. They attack the PC, not the electronic banking systems, because hackers use identity theft or malicious financial software applications that they have already installed on a PC to appropriate data such as user names, passwords and even secrets that the user provides to the user. bank and that ratify answers to questions such as What was your first car?, As stated by César Augusto Giraldo Briceño [11], currently about 75 % of users use the Internet to perform usual banking operations, as technology allows , in addition to the ease in the use of mobile devices; However, there is fear in relation to security, as it is not exempt that they may suffer attacks and deceptions, although it is evident that security does not exist 100 %, as stated by Miguel Santos, CEO of Technisys [12], but you can use tools to reduce the risk. However, in some way or another, the user is responsible for the security of his data, as he must have a good discipline in handling of the technology.

But this is not the case, given that despite the growth of threats by those who make use of online services, customers are unaware of a large number of risks to which they are exposed due to the execution of unknown programs, which can cause damage to the equipment and in some cases become spies and even copy the pulsations when the keyboard is used [13], those are captured by the criminals [13], which surely becomes the responsibility of the user; but in one way or another, banks must also collaborate with the measures that are strictly necessary, in relation to authentication, in order to protect their customers. According to the study, Easy Solutions, a company specialized in detecting electronic fraud, showed that 95 % of the clients consulted knew the threat of computer viruses, but only 36 % knew about phishing and only 26 % of pharming, for Latin America [14]. So, from one side or the other, there is really responsibility of the parts.

On the other hand, sometimes criminals exploit vulnerabilities left by application developers, which are exploited by hackers for data theft, [15] and electronic service platforms, which are used by users to make payments and online purchases. In addition, on some occasions users provide personal information in an innocent way, data that is used by hackers, to commit illicit, obtaining, fatal results. On one occasion, he stole 10,000 million pesos, which affected more than 15,000 users of different banks [16]. The way criminals operate has no limits, the attackers managed to steal 40 million debit and credit card numbers and personal information to 70 million customers, from a self-service chain in the US, since they installed malicious software in a point terminal of sale [17]. On the other hand, the criminals managed the theft of data belonging to users of 40 million credit cards [18]. Currently there are applications developed by criminal gangs, which are used to violate the services of the virtual banking of bank employees and the unsuspecting use of computers by the officials of the affected companies [19].

As It can be seen, effectively every day, computer crimes are increasing and are becoming increasingly difficult to detect, and therefore to control. They are presented against public and private organizations, educational institutions, banking, industry and commerce. These crimes are still being investigated. The most disturbing thing is that the organizations dedicated to committing crimes with the use of the Internet are well organized, they include: Cybernetics experts, lawyers, accountants and even financiers. In a sophisticated manner and without "firing a single shot", cyber criminals are already made at about $ 1 billion Colombian pesos a year, according to a study by Fedesarrollo and the Colombian Chamber of Information Technology and Telecommunications (CCIT), which has become a serious law problem and order [20]. Due to the fact that, some officials of organizations lend themselves or are part of criminal gangs, in that case in complicity with a bank official, they were loaned for the theft of at least $ 10 billion of business accounts [21]. There are also officials who have taken advantage of their positions and with the use of the internet to make transfers to their personal accounts [22], as a result, what security can be expected is that nobody can be trusted in. Security only exists in our mind, if we think about it. Those responsible for the security of information and the management of it in organizations, on many occasions have taken ownership of it, without authorization. They access files remotely to extort and steal passwords from bank accounts, and the most worrying thing is that those have been increasing every day [23]. In the same way,

victims have increased every year, as a consequence of the theft information related to bank accounts [24].

Computer crimes are becoming more frequent every day, as they access databases of banks, other institutions, social networks, emails, among others, in an abusive manner, in order to obtain information and even to clone cards. This crime is increasing [25]. Recently, the authorities captured a network made up of 17 people, including a Spanish, who were engaged in making electronic transfers, through illegal bank accounts, obtaining him sent $160,000 million Colombian pesos to 350 accounts of a bank. Some of these were inactive or had little balance [26].

Therefore, computer crimes are "the order of the day" and the most frequent are those related to attacks that seek users of online banking, as they go after the theft of information, which will be used to commit fraud, whitening accounts, make transfers to false accounts that are then unoccupied through ATMs. This is due to the fact that, users may not make good use of the Internet service [27], the most worrying thing is that they are getting bigger every day.

All this is achieved thanks to the constant appearance of new technology and new mobile devices, which of course facilitates the realization of daily activities, where people and organizations do from any place and at any time. However, the security of these is not the most appropriate, which is exploited by hackers, who manage to go after information and economic factor of users, and even attack and disable a website. About 500,000 attacks are known daily [28], but to be alarmed and not go so far and to worry about those who like to constantly update on technology, it is surprising what happened recently with mobile technology, which cyber pirates have appropriated personal information from 15 million T- Mobile wireless customers [29].

This a really worrying situation in view of any reality, since mobile devices are also used to commit bank fraud through the Internet, and the most alarming thing is that they are getting bigger every day. Thus, it is estimated that cyber attacks are around US $ 1500 million per month [30]; in other occasions the delinquents use the modality of "the fraud of the telephone key", with this information of the victim, they can control his mobile, and manage to carry out transactions [31] without any inconvenience, as well as the theft of keys and the cloning of cards [32], in all kinds of businesses. Given this situation, an organization designed an application to be installed on mobile phones, which is safer than current security systems, according to Mauricio Gaueca [33], because this does not mean that the data is 100 % safe [10], for many and diverse reasons whatever they can be such as human, technological, financial, etc.

Similarly, there are geographical places where the demand for technology allows easy penetration of equipment, which facilitates access to the use of banks participation, especially in countries such as Brazil, Chile and Venezuela, with a participation of 43 %, although it is not representative enough, perhaps it is due to the lack of security and infrastructure. In addition, to the fact that in the region where one of these countries is located, there are high rates that have shown attacks on the networks [34].

Likewise, there are frauds with the cards, which has always been a problem, in this situation it is normal that there is concern. Therefore, and for the protection of its users, anything that is done is valid. In this case appeared a card that when it was going to be used to make purchases had an extra layer of security, compared with most buyers in the United States, corresponded to a chip embedded in all credit and debit cards in Europe, which managed to reduce fraud by 65 % in the last decade according to MARCRI [35]. Nowadays, of course, the handling and use of normal cards as we know and use them is easy, so there are criminal gangs, dedicated to the manipulation of cards, for example increasing your withdrawal limit and withdrawing cash from ATMs, as happened recently by a criminal organizations that managed to withdraw money from ATMs in countries such as: Belgium, United Kingdom, Canada, Dominican Republic, Estonia, France, Germany, Italy, Japan, Latvia, Malaysia, Mexico, Romania, Spain , Thailand and the United Arab Emirates, managed to steal $ 45 million [36].

The bands dedicated to commit a crime, use numerous tricks, in order to advance a number of criminal activities. So hackers in this opportunity do not directly offense on customer accounts, if not on financial institutions, posing as employees, with the use of "phishing"techniques, achieving the theft of at least about 1,000 million dollars to a hundreds of banks around the world [37].

Actually the banking sector is still the most affected by the cybercriminals organizations together with the telecommunications and government companies, from which considerable resources and important information are extracted, which will be used to increase their crimes. Recently, the bank was surprised with a theft of 45 million dollars and the form of operation was the cloning of cards and increase the withdrawal limit of ATMs.

On this occasion, thieves withdrew in 27 countries and from different continents, including Colombia. Their sagacity and their mode of operation of these organizations have no limit. In 10 hours, they managed to get $40 million Colombian pesos, making 36,000 transactions [38]. Crime has no limits, they have bands dedicated exclusively to cloning of both debit and credit cards, which are used to withdraw money from ATMs until they are completely vacated, thus they have appropriated the money from 40 accounts [39]. Likewise, once the criminals manage to have access to data bases of prepaid debit cards, they are organized in global networks, achieving in a short time from different countries, empty ATMs, in this case, up to the theft $45 million US dollars [40].

As it can be seen, bank fraud is a scourge that affects everyone, and the most difficult thing is that every day are more difficult to detect, because the way of operating of criminals is increasingly sophisticated. The important thing is to be aware that this situation affects the parties, thus the important part and essential thing is monitoring and in this way it will be possible to be much more efficient in the efforts in order to prevent and at the same time to detect situations that can affect entities and users [41].

Currently, the frauds presented with cards, as a result of cloning, online fraud, identity theft, fraud for online purchases, among others, are some of the cybercrimes that occur daily, as a result of the use of the service of the Internet, which can cause disastrous results. However, some countries do not have laws to be punished [42], thus "leaving the door open" to criminals.

The cybercriminal organizations are well organized, their form of operation is part of this, which leads them to operate at any time and from anywhere in the world, they also know that they are the target of the authorities, since it is a global scourge , to which a battle must be fought, for which it is necessary to create a common front in which most countries of the world participate, in order to be able to carry out investigations and advance captures [43], but the reality is that it is not possible since there are countries in which they do not even have internal regulations, which makes it difficult to control these kinds of organizations [42].

Currently, the constant emergence of technology as a fundamental factor of Innovation is very important and effectively evidenced, which must play a fundamental role in society, as in the case of IT, which must meet with a minimum in terms of protection of the information of those who use them, for the development of diverse daily activities. Thus, these systems must be protected, in order to minimize .ªttacks targeting Internet providers, casinos and betting companies, financial institutions and banks" [44], among others, which are minimized if they are maintained the protection systems updated constantly, but this does not mean that the data is 100 % Safe [10].

In general, any organization today to be competitive and make itself known, has a communication system, which well organized is represented by a CPD, of any size, which will have at least servers, routers, switch, telephones, video cameras, where important information will flow from and to the organization and if some of these devices are affected by Heartbleed, which affects not only websites, but also gadgets to connect to the Internet [45], in which security you can at least think. Thus, the situation continues to be increasingly chaotic, according to research the actions of the new computer viruses is surprising, they are capable of infecting equipment as if it were a human flu, they are able to do it through the air with the use of wireless connections WiFi [46], or as if it were a biological pathogen such as the cold, since they do it by jumping autonomously from one WiFi network to another one [47], although they are tests performed by some researchers, others with worse intentions. It can cause unexpected situations, especially to organizations that turn out to be very selective and attractive on the part of the Cybercriminals in this case a bank, with which every day is more surprising to act, to become a real "nightmare" for professionals computer security, since the Troidean Dridex can spy on the bank transactions of its victims, the theft of personal data and the installation of malware [48].

Cybercriminals do not have a presentation to carry out their way of committing crimes. They use different means and forms, in order to obtain information about the users of the banks, they access databases from other organizations, where users have made payments for services or products with the objective of appropriating credit card numbers, validity dates and security codes, and then making fraudulent purchases using these data [49], and the most surprising and ironic thing is that they are increasing bank fraud, despite all the efforts that have been made, for the first quarter of 2017, 1.5 million claims were reported for fraud in the banking sector, which represents 18,000 of them per day, corresponding to an increase of 10 % with respect to 2016, according to Condusef [50], so that security can be at least thought.

2. Conclusions

The information, whatever it may be, as the most important asset of a given organization and depending on the type, requires special attention in its protection; so the configuration and initial installation of "Systems" of any company is essential for its proper functioning, since it is the starting point to avoid being highly exposed, because if they leave vulnerabilities, they will surely be exploited by criminals IT workers, who are well organized and on the lookout for opportunities.

The constant emergence of technology and communications, make the world every day is closer, so you can see events almost instantaneously, the movements of the stock market, global conflicts, and the economy of countries, among others. At the same time, it makes it possible to carry out a number of important, less important daily activities that are of vital importance in the development and proper functioning of any country.

Today, the economy of a country is not conceived, nor the functionality of banking without having Internet service. Their organizations sell and provide their services through this medium in which intervene: technology, institutions, users, applications, platforms, all together constitute the functionality of banking, which allows to establish an important service, but at the same time it is attractive because of its "raison d'être", a number of services easily, quickly, from anywhere and with different technology, since it allows easy access and use, which from any point of view it is highly important. In the same way, appear those who want to take advantage of this amount of benefits that technology allows without a doubt and it is when those who are interested in acting in an inappropriate way to want to know what specific information through the network of networks, in order to appropriate the resources of banking organizations and users.

Because of the daily appearance of technology that is easy to install, configuration and use, which is ultimately what interests users, security is been left out. Similarly, the irresponsibility of the users by not managing technology responsibly, the implementation of applications and platforms not designed with minimum security, the use of wireless technology with the non-application of some security standards, the lack of responsibility of some institutions and users who are not aware of the importance of handling some important information, are situations that have taken advantage of the Cybercriminal Organizations in order to achieve their goals, appropriate the resources of some of these, finding results not flattering: Theft of more than $ 100 million to companies and individuals around the world, theft of approximately $ 1000 million to banks in Russia, Eastern Europe, China and the United States, theft of $10,000 million pesos affecting more than 15,000 users of different banks, with complicity of bank official theft of at least $ 10 billion c business accounts, by electronic transfers, through bank accounts in an illegal manner, obtaining him remittance of 160,000 million pesos, towards 350 accounts of a banking entity, appropriation of personal information of 15 million customers of the T-Mobile wireless service, posing as employees, with the use of phishing techniques, achieving the theft of at least 1,000 million dollars to a hundred banks around the world, theft of 45 million dollars and the way of operation, cloning cards and increasing the withdrawal limit of ATMs, in this opportunity, they withdrew in 27 countries and from different continents, including Colombia.

As it can be seen, the insecurity in the banks is worrying because even though these institutions are obliged to comply with the norms related to minimum security standards, in favor of their users and clients. However, it is said that while it is true that the banking system complies with all security standards, vulnerabilities are latent, therefore, no one is safe, because as you can see it will always be exposed, for many and various reasons. What prevents that one hundred percent of information security can be achieved.

References

[1] K. Chacón, "¿Qué traerá el Big Data para el 2016?", 2016, [Online] available at: https://www.elfinancierocr.com/tecnologia/que-traera-el-big-data-para-el-2016/NOGIWPHMGNCLZPVCI7A5PZVP5I/story/

[2] La Estrella de Panamá, Çada segundo se crean tres virus informáticos en el mundo", 2014, [Online] available at: http://laestrella.com.pa/vida-de-hoy/tecnologia/cada-segundo-crean-3-virus-informaticos-mundo/23797216

[3] El Financiero, "Más $100 millones fueron robados por hackers a clientes bancarios en todo el mundo", 2014, [Online] available at: https://www.elfinancierocr.com/tecnologia/\mas-100-millones-fueron-robados-por-hackers\-a-clientes-bancarios-en-todo-el-mundo/EIJQ2Z3QDNFX3JVDV7TQGKKPP4/story/

[4] Portafolio, "Perdidas por delitos informáticos suman US$93.000 millones", 2012, [Online] available at: https://www.

portafolio.co/economia/finanzas/perdidas-delitos-informaticos-suman-\us-93-000-millones-91548

[5] J. Bicarregui, "El fraude on-line: Nuevo escenario, vieja picaresca". Boletín de estudios económicos, vol. 63, no. 194, 2008, pp. 311-332.

[6] J. Girón, "Tarjetas bancarias. Consumo y Fraude", 2012, [Online] available at: https://delitosinformaticos.com/10/2012/fraudes/tarjetas-bancarias-consumo-y-fraude

[7] "ProQuest" june 17 th 2012. [Online]. Available: http://search.proquest.com/docview/916320389/6B698638C0DB4AD2PQ/3?accountid=38880

[8] La República, "Hackers robaron US$ 1.000 millones a cien bancos desde el 2013", 2015, [Online] available at: https://larepublica.pe/tecnologia/857573-hackers-robaron-us-1000-millones-a\-cien-bancos-desde-el-2013

[9] "ProQuest" august 28 th 2010. [Online]. Available: http://search.proquest.com/docview/747887409/EA3E95248B77417CPQ/12?accountid=38880

[10] M. Riveros, "ProQuest" february 13 th 2016. [Online]. Available: http://search.proquest.com/docview/872468892/D44D1BFD35914EC4PQ/7?accountid=38880

[11] C. A. G. Briceño, "ProQuest" october 24 th 2011. [Online]. Available: http://search.proquest.com/docview/900175823/4A82F030AA74424FPQ/1?accountid=38880

[12] "ProQuest" march 08 th 2015. [Online]. Available: http://search.proquest.com/docview/1661232740/B470E9AB3BBD45F5PQ/4?accountid=38880

[13] "ProQuest" september 19 th 2011. [Online]. Available: http://search.proquest.com/docview/890773510/506FB36C89094925PQ/2?accountid=38880

[14] "ProQuest" october 14 th 2010. [Online]. Available: http://search.proquest.com/docview/757839777/442AE3024CD41BFPQ/10?accountid=38880

[15] "Efe, el comercio mundo" may 27 th 2015. [Online]. Available: http://elcomercio.pe/mundo/actualidad/hackers-roban-datos-100000-contribuyentes-\eeuu-noticia-1814165?ref=flujo_tags_52201&ft=nota_2&e=titulo

[16] "EL TIEMPO" june 17 th 2014. [Online]. Available: http://www.eltiempo.com/politica/justicia/cae-red-que-robo-mas-de-10-mil-millones-de\-pesos-de-pagos-en-internet-/14131823

[17] "ProQuest" march 06 th 2014. [Online]. Available: http://search.proquest.com/docview/1504411439/E860F132E7D4420EPQ/4?accountid=38880

[18] "El Comercio Tecnologia" december 19 th 2013. [Online]. Available: http://elcomercio.pe/economia/mundo/datos-40-millones-usuarios-tarjetas-credito\-habrian-sido-robados-noticia-1675475

[19] "COLPRENSA" november 12 th 2013. [Online]. Available: http://www.eluniversal.com.co/colombia/capturadas-10-personas-por-delitos-informat\icos-141499

[20] "DINERO" november 27 th 2014. [Online]. Available: http://www.dinero.com/edicion-impresa/pais/articulo/crecimiento-delitos-ciberneticos-colombia/203563

[21] "el pais.com" may 22 th 2015. [Online]. Available: http://www.elpais.com.co/elpais/judicial/noticias/cayo-red-robo-10-mil-millones-bancos

[22] "El Comercio LIMA" august 18 th 2009. [Online]. Available: http://elcomercio.pe/lima/ciudad/contador-robo-mas-500-mil-soles-internet-em\presa-donde-trabajaba-noticia-329587?ref=flujo_tags_517598&ft=nota_39&e=titulo

[23] "SEMANA" november 08 th 2012. [Online]. Available: http://www.semana.com/nacion/articulo/delitos-informaticos-han-aumentado-colombia-\advierten-especialistas/267571-3

[24] "El Comercio Tecnologia" april 14 th 2014. [Online]. Available: http://elcomercio.pe/tecnologia/actualidad/eeuu-18-usuarios-internet-sufrio-robo-datos-\noticia-1722729?ref=flujo_tags_517598&ft=nota_4&e=titulo

[25] "El país" december 31 th 2012. [Online]. Available: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento

[26] "El tiempo" december 16 th 2014. [Online]. Available: http://www.eltiempo.com/politica/justicia/caen-17-miembros-de-delincuencia-informatica/14983836

[27] E. S. Botero, "Delitos informáticos", september 03 th 2012. [Online]. Available: https://seguridadinformatica5.files.wordpress.com/2012/06/delitos_informaticos.pdf

[28] "ProQuest" november 09 th 2015. [Online]. Available: http://search.proquest.com/docview/1731752413/E981122312D94ECCPQ/1?accountid=38880

[29] "ProQuest" october 01 th 2015. [Online]. Available: http://search.proquest.com/docview/1718227312/7C5A9C55BC1A4A1DPQ/1?accountid=38880

[30] "Portafolio" july 21 th 2013 . [Online]. Available: http://www.portafolio.co/economia/cifras-fraudes-bancarios-colombia

[31] M. A. González, "El Comercio MUNDO" november 21 th 2013. [Online]. Available: http://elcomercio.pe/mundo/actualidad/toma-nota-como-evitar-robo-dinero-tus-cuentas-bancarias-noticia-1662309?ref=flujo_tags_517598&ft=nota_7&e=

[32] M. Avila, "Panamá América" october 18 th 2015. [Online]. Available: http://www.panamaamerica.com.pa/economia/985-de-robos-los-clientes-bancarios-son-cibernéticos-996819

[33] "ProQuest" april 14 th 2013 . [Online]. Available: http://search.proquest.com/docview/1326594536/9525AB6711CB4907PQ/5?accountid=38880

[34] "ProQuest" november 10 th 2015. [Online]. Available: http://search.proquest.com/docview/1732086655/3AE55873BEC141E7PQ/3?accountid=38880

[35] MARCRI, "Proquest", december 18 th 2014. [Online]. Available: http://search.proquest.com/docview/1638488868/74A36B28079A4DC4PQ/5?accountid=38880

[36] "ProQuest" may 10 th 2016 [Online]. Available: http://search.proquest.com/docview/1349812891/EF8A2385D5BC4FEBPQ/9?accountid=38880

[37] "ProQuest" february 16 th Febrero 2015. [Online]. Available: http://search.proquest.com/docview/1655242898/D9C8EAFF7DF74896PQ/4?accountid=38880

[38] M. O. Guerrero., "ProQuest", may 20 th 2013. [Online]. Available: http://search.proquest.com/docview/1353058744/681F7D888725476DPQ/5?accountid=38880

[39] "El tiempo.com" march 3 th 2015 . [Online]. Available: http://www.eltiempo.com/colombia/otras-ciudades/cae-banda-que-cometia-delitos-informaticos-en-ibague/15331777

[40] "ProQuest" may 10 th 2013 . [Online]. Available: http://search.proquest.com/docview/1349812155/D39D05FBDF8849FCPQ/3?accountid=38880

[41] Soyentrepreneur, "Entrepreneur" june 15 th 2012. [Online]. Available: http://www.soyentrepreneur.com/los-principales-crimenes-bancarios.html

[42] "ProQuest", june 19 th 2013. [Online]. Available: http://search.proquest.com/docview/1369253907/662B7C45C8C6477DPQ/4?accountid=38880

[43] "Redaccion tecnosfera, el tiempo" october 14 th 2014. [Online]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/solo-hay-cien-capos-del-cibercrimen-en-el-mundo-director-de-europol/14685479

[44] "ProQuest" april 23 th 2015 . [Online]. Available: http://search.proquest.com/docview/1674960283/B852AF5085904980PQ/1?accountid=38880

[45] "ProQuest" april 15 th 2014 . [Online]. Available: http://search.proquest.com/docview/1516015993/F3037EAA6BB4462DPQ/35?accountid=38880

[46] "BBC MUNDO" february 27 th 2014. [Online]. Available: http://www.bbc.com/mundo/noticias/2014/02/140227_tecnologia_virus_informatico_gripe_aa

[47] C. Zahumenszky, february 26 th 2014. [Online]. Available: https://es.gizmodo.com/crean-un-virus-informatico-que-puede-propagarse-de-una-1531668282

[48] G. Duran, november 28 th 2015. [Online]. Available: http://jarabacoadigital.com/v2/

asi-es-dridex-el-troyano-bancario-que-roba-\
tus-datos-personales/

[49] "Conexión security" april 18 th 2017. [Online]. Available: http://www.conexionsecurity.com/index.php/novedades/item/566-cibercriminales-roban-datos-bancarios\-de-los-clientes-del-portal-gamestop

[50] R. A. Rebolledo, august 15 th 2017. [Online]. Available: https://www.eleconomista.com.mx/finanzaspersonales/Phishing-y-otros-5-casos-de-fraudes-bancario\s-en-el-2017-20170815-0130.html