Journal of Information Systems Engineering & Management, 1:2 (2016), 111-121

ISSN: 2468-2071

E-banking services: Why fraud is important?

Rute Abreu[1*], Fátima David[1] & Liliane Segura[2]
[1]*Instituto Politécnico da Guarda, UDI-IPG, PORTUGAL*
[2]*Universidade Presbiteriana Mackenzie, BRAZIL*

ABSTRACT

The purpose of this paper is to answer the importance of fraud that arise from the use of e-banking services more ethical behavior applied to everyday moral problems. On the one hand, the theoretical framework of this paper is based on literature about ethics and fraud, in general, and information and communication technology of the e-banking services, in particular. On the other hand, the empirical framework reflects the practices in this field of research used by banks with public data available on the Portuguese Banking Association. The results of the paper mitigate risks, such as show several threats, vulnerabilities, incidents, impacts and responses that face e-banking services.

keywords

ethics,
fraud,
e-banking services,
Portugal

Received: 26 Jan 2016
Revised: 12 Feb 2016
Accepted: 5 Mar 2016

DOI: 10.20897/lectito.201617

INTRODUCTION

The e-banking services have advantages in financial transactions, but security threats and vulnerabilities must be constantly reduced. Indeed, the integration of fraud on all aspects of the e-banking services requires the profound revision of the traditional commercial paradigms that have been prevailed for last years (Abreu et., 2015). In this framework raises the "good citizen" that desires to do well and needs to avoid harmful behavior (OECD, 2014).

While the "bad citizen" promotes the lack of transparency, wrong attitudes and "hidden" awareness of the nature, level and scope of the financial impact which claims to reduce the social responsibility (Holtz, 2011) and produces high level of degree of materialistic values were less likely to acquire moral (Gavish and Tucci, 2006). This paper deals with ethics and fraud that "become a major hindrance to the development and use of commercial activities on the internet" (Turilli and Floridi, 2009).

The perspective of the citizen and bank-client is focuses on the field of research: ethics and fraud applied to e-banking services. Indeed, these services are define as remote services provided by authorized banks through devices that use information and communication technologies (ICT) under the bank's direct control (Hadnagy, 2011). The impact of e-banking on risk management is complex and dynamic. Furthermore, it is possible to identify strategic, operational, technology, business, reputation and legal risk associated with e-banking fraud. But, management constantly reassesses and updates these risks and, effectively, social engineers are experts in human nature and in mitigation of risks taking into account due to several vulnerabilities (Harris and Spense, 2002).

These risks combine science, technology and human nature and management must mitigate them in order to increase ethics (Wiener, 1954). For all these aspects, necessary encourage internal controls and audit procedures from practical concerns arising in connection with the impact on the society. In a society that is increasingly characterized by the rising of fraud, the research published by (Stamtellos, 2007) on the book "The Human Use of Human Beings" explore the importance of the ethical issues that computer and information technology need to face each day.

*Correspondence to: ra@ipg.pt

Thus, the authors agree with Kitano et al. (2011), when he defends that the problem of modern technology is dangerous due to its inherent complexity and possible mismanagement of the saving power. All these questions sudden raise the need of principles that "good citizens" must follow and it has been presented by Stamtellos (2007): 1. Principle of freedom in which "the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him"; 2. Principle of minimum infringement freedom with "any demand must be exercised in such way that it does not produce any unnecessary infringement of freedom"; 3. Principle of equality that is "what is just for A and B remains just when the positions of A and B are interchanged"; 4. Principle of benevolence in which "good will be between Man and Man that knows no limits short of those of humanity itself."

Recent research (Gulenko, 2013; Conheady, 2014; Benkler, 2006) have shown that, from the security professional's perspective, the engagement with these principles depends on voluntary commitment of each professional and it can be difficult to accomplish (OECD, 2002). The fighting against fraud is fundamental to increase trust and to assessment the bank services to provide relevant help to bank clients. In the literature, several authors detail that the average person's instincts and reactions are fairly predictable. Also, it is elementary to adapt to safe and controlled environments.

The evolution in the area of security guidelines has been beneficial for clients of the e-banking services, because it was recognize the profound importance of ethics and, at the same time, in conjoin efforts of informatics. For example, the Spafford et al. (1989) publish the security guidelines that contain nine principles complementary, such as: "1. awareness, 2. responsibility, 3. Response; 4. Ethics; 5. Democracy; 6. Risk assessment; 7. Security design and implementation; 8. Security management; 9. reassessment principle". Indeed, malicious software and other unethical problems develop strategies promoted by "bad citizens" concerning with promotion of evasion on privacy, violate confidentiality, impaired service, controlling access to resources and lack of consistency (Holyoak and Morrison, 2012).

The Council Recommendation on Principles for Internet Policy Making made by Mitnick (2003) aims to: "1. Promote and protect the global free flow of information; 2. Promote the open, distributed and interconnected nature of the Internet; 3. Promote investment and competition in high speed networks and services; 4. Promote and enable the cross-border delivery of services; 5. Encourage multi-stakeholder co-operation in policy development processes; 6. Foster voluntarily developed codes of conduct; 7. Develop capacities to bring publicly available, reliable data into the policy-making process; 8. Ensure transparency, fair process, and accountability; 9. Strengthen consistency and effectiveness in privacy protection at a global level; 10. Maximize individual empowerment; 11. Promote creativity and innovation; 12. Limit Internet intermediary liability; 13. Encourage co-operation to promote Internet security; 14. Give appropriate priority to enforcement efforts."

All these principles allow to identify definitions about social engineering, such as presented by Floridi (2013) e Jensen and Mackling (1976). Thus, on the one hand, the theoretical framework of this paper is based on literature review about ethics and fraud, in general, and their effect in e-banking services, in particular. On the other hand, the empirical framework reflects the practices that several Portuguese banks and their public disclosure in order to increase the transparency and to reduce the risk.

The structure of the paper is organized as follows. Section 2 gives an overview of ethics and fraud, in general, and on bank services, in particular, through the information and communication technology tools and it focuses on the nature of social responsibility and moral action. Section 3 deals with practical development of bank services that use the ICT tools and present several vulnerabilities. Finally, the section 4 presents conclusions and makes some recommendations.

LITERATURE REVIEW

The effectiveness of ethics and fraud depends on different agents of change that allow "good citizens" to be affected by the inappropriate action and deal with the agency theory in which is affect by the moral hazard versus opportunist behavior (Fama, 1980; Crowther, 2004). In this sense, the payoff of moral hazard on the agency theory needs careful analysis and investigation of the level of trust between "good" and "bad" citizen.

The "good citizen" is affected by asymmetric information, in several situations, especially in bank services. In several e-banks, clients are merely a commercial commodity and satisfaction is not the main concern as consumers. Indeed, bank client shows a vulnerable position, because he is affected by actions of "bad citizen" and face several consequences.

The "bad citizens" acts against rules, norms, standards, policies and laws, very far from the moral and social responsibility point of view. They controls, misuse, manage and design ICT with its "self-interest" and

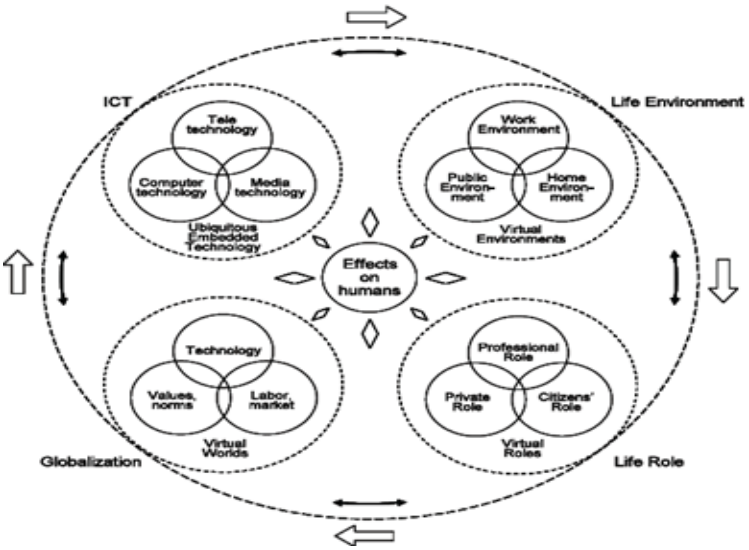

Figure 1. The convergence model on ICT and Psychosocial Life Environment
Source: Bradley (2006); Bradley (2010); APB (2016)

opportunistic behavior (OECD, 2012). These influential ideas put interest of the individual above interest of the collective.

This paper follow the convergence model on ICT and psychosocial life environment presented on Figure 1 that it is centered on the effects on humans. Indeed, Bradley (2006); Bradley (2010); APB (2016) conclude that the use of ICT has changed the human qualities so far: identity, self-perception, social competence, creativity, integrity, trust, dependency and vulnerability. Indeed from this perspective, collective interests are best served through self-interest.

Following this model presented on Figure 1, banks are directly responsible for the safety of their services and ICT systems provide to bank clients. So, the psychosocial life environment allows bank clients to perform transactions electronically without visiting to a branch and act anytime of the day and the night. Indeed, it enables bank clients, firms and society to access accounts, to do business, to obtain information on financial products and services through a public or private network reduce transaction costs and then to provide virtual services with efficiency.

RESEARCH QUESTION

Security of e-banking services is one of the most important are of concerns of regulatory and supervisor agencies, that promote operational transactions in terms of legal and regulatory norms at security and technology issues, for example, the Bank of Portugal is concern with impact of e-banking on its monetary and credit policies (Knack and Keefer, 1997).

As Kitano et al. (2011) defend the ethical actions include three related factors: intentions, action and consequences that affect the nature of moral judgment or professional situation. As OECD (2012) suggests that the pendulum swung too far towards encouraging corporate self-interest at the expense of the public interest. Indeed, the continuing conversion of public service provision to market testing by many governments suggests a strengthening belief that the two interests are not in conflict. Self-interest and altruism (promoting the welfare of others over self) need not be in conflict.

Indeed, the research question is centered on the citizen experiences that are meaningful to the: E-Banking Services: Why Fraud is Important? due to the future decrease of fraud on e-banking services as a key contribution of mitigate the risks to raise ethics and bank interests, needs, strengths, and weaknesses which drive the learning process (Rawls, 1999; OECD, 2011).

RESEARCH METHODOLOGY

Banks need to apply IT strategic and operational plan to mitigate the risks. With regard to the research's theoretical implications, the empirical analysis is supported on the public data available on the Portuguese Banking Association (PBA) and registered on the Bank of Portugal (BP, 2016). So, the sample focuses 33

banks, with information publish between 2004 and 2014. The PBA association is a group of monetary financial institutions that is responsible for 96% of the Portuguese banking system, despite have, at 31 of December of 2014, 33 members that represented 56% of the total number of banks (59) in the Portuguese banking system (Knack and Keefer, 1997).

Also, at international context, Government, payment providers, Platform operators and other stakeholders help to ensure that clients of the e-banking services have adequate access to information and they respect the legitimate interest of each other (Holtz, 211). This report presents the Carbanak malware that started in August, 2013 when the cybercriminals used it in several tests. Thus, the first infections were detected in December, 2013 and then it affects the following Carbanak targets (see Figure 2).

ICT advances offer the potential for increased data security, because as Kaspersky (2015) defend the rise in the level of trust could be related with an increase in economic growth due. The main problem is globalization that transforms a national to international problem. For example, one of the last reports published about fraud in e-banking services has been made by BPI (2016). The explanation of the attack process of the Carbanak Fraud is draw in Figure 3.

Figure 3 uses "spear phishing emails with malicious attachments against employees of the targeted financial institutions, in some cases sending them to their personal email addresses". Also, the attackers used drive by download attacks, but this assumption is not 100% confirmed.

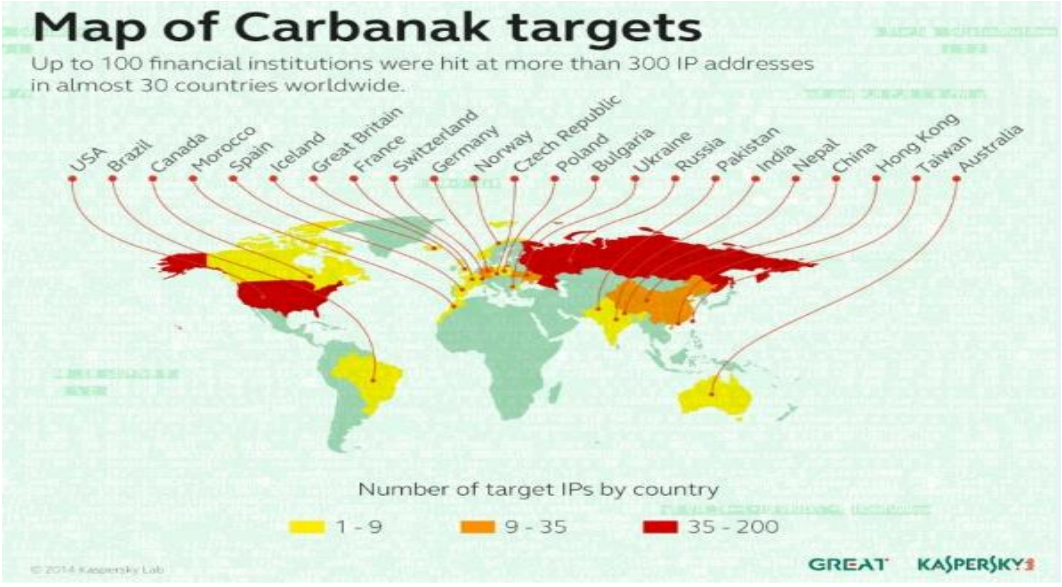

Figure 2. Map of countries target of the Carbanak Fraud
Source: Kaspersky (2015)

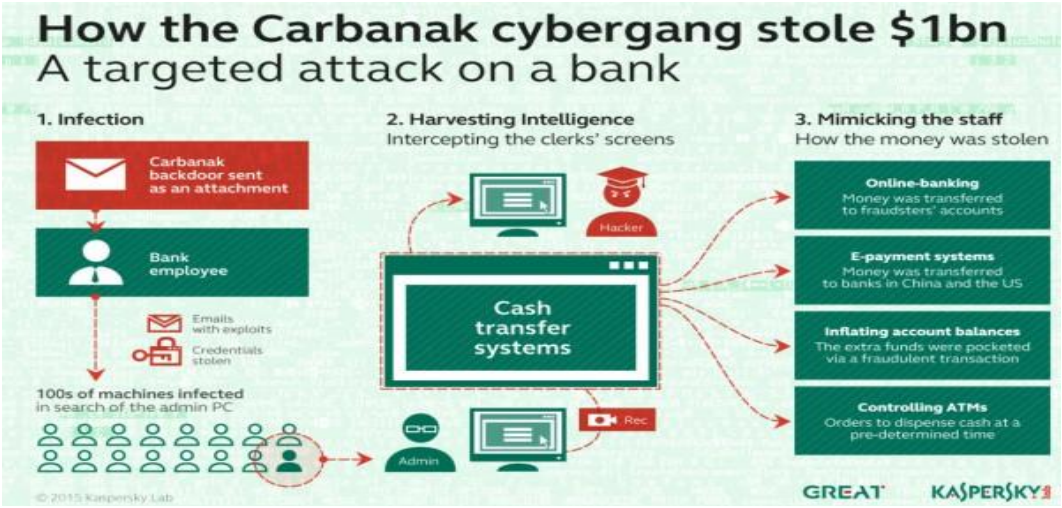

Figure 3. Carbanak Fraud
Source: Kaspersky (2015)

RESULTS AND DISCUSSION

The e-banking service is one of the services available to citizens in general and then the importance of fraud increase with its availability. after the individual registration process, it provides to clients and small businesses several e-banking services, in a simple and secure way, through a computer with internet connection and it is available, normally, 24 hours a day during 365 days a year. In different services on the e-banking, such as: payments of shops and money transfers, it is necessary to end them with codes supported on the individual coordinate card (CGD, 2016). The e-banking code card is a simple, portable and low-cost card with a matrix of character strings, each character string matching a unique coordinate to other units as Figure 4. This card allows to made several services with different codes for each service, but needs to be implement with dynamic two-factor authentication through used password combination and access by token or sms.

The bank clients in order to protect the security of their e-banking account use a dynamic password that needs to be input three straight times to end one service. But, to prevent the thievery of e-banking code card by bad citizens through false websites, Trojan viruses, and hacker attacks, the bank platform show one especially window to remember clients of the dangerous situations as Figure 5.

The citizens must be awareness and avoidance of different techniques of potential online fraud attempts, including the advice of not trusts any online resource simply because it holds the Bank's Identity (see on Figure 6).

Human resources are very important at banks that must promote audits, education, close supervision of staff in sensitive places, segregation of duties and security procedures. As well as ICT maintenance with calibration, measurement procedure, assurance and non-compliance management in order to ensure appropriate measures that faces adherence of the client privacy requirements (see on Figure 7).

Phishing attacks that the use of the Bank's identity on a fake website are another example presented. So, Extended Validation Secure Sockets Layer (EV-SSL) certificates are increasingly being used, but surveillance

Figure 4. CGD e-banking code card
Source: CGD (2016)

Figure 5. Ethics: Information about e-banking card
Source: CGD (2016)

Figure 6. Ethics: Information about entrance
Source: BPI (2016)

Figure 7. Ethics: Information about double safe codes of entrance
Source: Santander Totta (2016)

Figure 8. Fraud 1: false download of application for mobile
Source: CDG (2016)

process needs to trigger and alert transactions with messages which are not normal creating more difficulties to steal. Banks have to use reliable methods with specific requirements for verifying the identity and authorization of new and existing clients which includes a complete fulfills of all constraints and, also, it permits to create and customize all sensible variables (see on Figure 8): logical access, input, processing, output, interface and authorization controls.

In order to ensure compliance with the best international standards, the client of the e-banking services must use a secure messaging system when communicating with the bank (see on Figure 9), but audit trails, violation logging management as networking management audit must be promoted by banks and more important is providing the wellbeing of clients through maintenance robust framework for recovery plans and emergency plans to critical business activities.

IT operations must be supported on service continuity and disaster management with consistency of security of confidential data with proper storage. Also, e-banking services are not allowed to block accounts or services without assigning valid reasons and without prior notice to the client. In this sense, the process of authentication with 3 or 4 successive attempts are made to gain access with an incorrect password then the access is automatically block as shows the Figure 10.

ICT operations must educate clients and help with suspicious emails, like this false email based on evaluation detailed delivery channels (ATM, internet banking, mobile banking). This is a self-assessment rule that it has goal-setting. Another situation happens when banks rely on third party providers for e-banking services, and then management must generally understand the provider's information security program to effectively evaluate the security systems' ability to protect the bank and its client data and as it shows the Figure 11.

Procedures to erase fraud emails are based on security standards. Also, establish a privacy and data protection of the bank client with promotion of controls with erasing and shredding documents. Figure 12 shows an email of the credit card errors that must be faced by the technical non-repudiation problems that it involves creating proof of origin or delivery of electronic information to protect the client against false denial by the recipient that the data has been received as shows the

As other e-banking services, the Figure 13 presents email accounts banks that should raise clients about the awareness of the associated risk that causes fraudulent activities. E-banking services must advise clients to create robust passwords and personal identification numbers that cannot easily be guessed or predicted, also, the password has to be periodically changed.

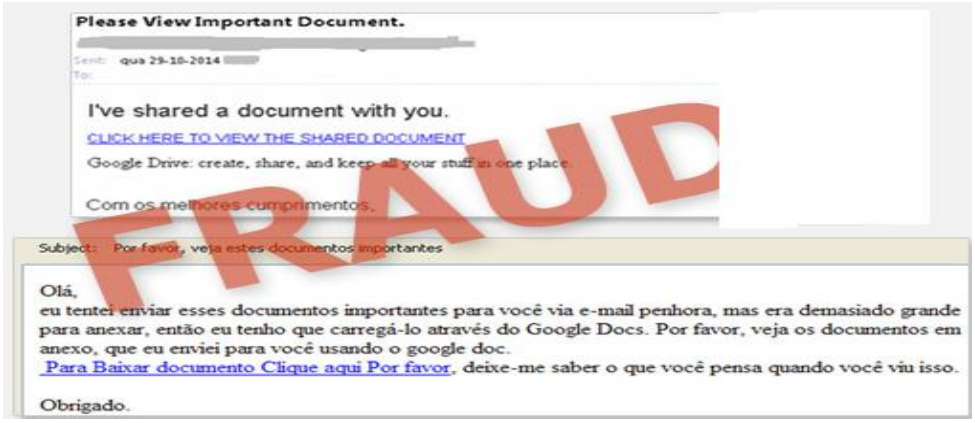

Figure 9. Fraud 2: false email
Source: CDG (2016)

Figure 10. Fraud 3: authentication procedures
Source: CDG (2016)

Figure 11. Fraud 4: Loss, destruction and falsification of control
Source: CDG (2016)

Figure 12. Fraud 5: email of misuse of the credit card
Source: CDG (2016)

Figure 13. Fraud 6: email counterfeit about mobile phone
Source: Santander Totta (2016)

Figure 14. Fraud 7: false annual survey with reward
Source: CDG (2016)

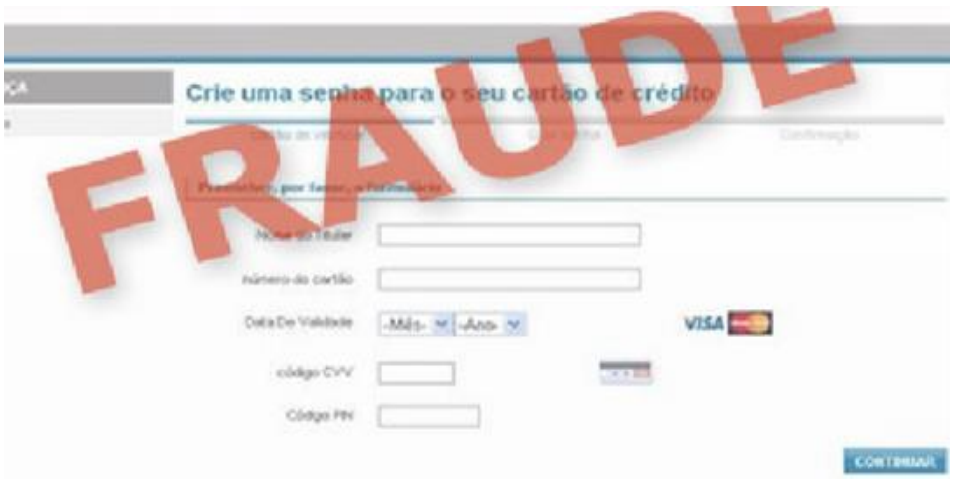

Figure 15. Fraud 8: create password for credit card
Source: CDG (2016)

Understanding the techniques of possible online fraud attempts justifies the alerts to access the bank's online resources from other websites, portals or emails (see on Figure 14).

Another example is the confidentiality of key e-banking information, which is not possible through an instructional tool that allows through computer images to access to false creation of passwords of credit cards as shown on Figure 15.

IMPLICATIONS

Banks should apply methods which involve secure trusted registration and notifications of privileges or offers must be develop with document procedures and specific define duties with segregated functions, for example, price winner should be made by the manager of the client and not by messages that could be false.

The authors aim to synthesize very important tasks to increase security in ICT, diminish fraud on e-banking services and improve the knowledge and skills of bank clients, over the time, such as:

1. Do not download or click software or emails from unknown sources;
2. do not use internet banking in public places, such as: internet cafe, public library, streets and airport corners;
3. install genuine antivirus software and firewall with regular update, so as to prevent the invasion of internet viruses;

4. save important information such as card number, password, and ID number in secret place and without call or save them with this names.

In resume, the e-banking services includes potential benefits to bank client's, such as: availability, because it can be accessed from the internet at anytime and anywhere; initiated feedback and automated feedback; improved communication through several features of the platform that allow communications of clients with banks, for example the announcements, and emails; tracking clients in the course statistics area.

CONCLUSION

The paper focus in advocating the relevance of ethics and fraud on e-banking services, to answer to citizen's, firm's and society needs, according to the real time rapidity characteristics of the process of buying and selling (Huber, 2009; AFME, 2012). The discussion about ethics and fraud at theoretical analysis is complex and dynamic (Hadnagy, 2011; Harris and Spense, 2002; Rawls, 1999; OECD, 2011).

The empirical analysis is based on a sample of 33 banks registered on the Bank of Portugal, between 2004 and 2014 and with public available information with Portuguese Banking Association. The results of the empirical analysis are significantly affected by the strategy of globalization and the increase of the business competitiveness that raise the need for e-banking services to use ICT.

However, these services have been created for the purpose of simplifying the daily life of citizens and firms in order to solve needs and demands of bank clients and based on the recent developments on ICT. The main solutions are authentication, identification, virtual keyboard, matrix, digital certificates, cookies, SMS and hard Token, encryption of communications, traffic control, automatic logout e monitoring and control (Rakesh et al., 2014).

For national and international agencies and regulatory entities that the need to prevent damages to the financial and monetary markets within new financial transactions, because they failed on the security policies to bank clients. This has been seen as necessary and with higher impact on ICT market behavior (IMF, 2012; EC, 2012; Chitrey et al., 2012).

The financial crisis and repeated scandals generated more ICT security and private issues to create a bank sector more safe and with prudential rules (certification authorities, digital signature and certificates, cryptography, inspection firewall, key infrastructure, isolation of mobile services), to be beneficial to the society as whole. For citizens, the extensively use of fraud on e-banking services oblige them to learning more about ethics to stay protected. So, skills and real-life knowledge must develop information sharing between citizens in order to fight fraudulent practices.

For firms, must select qualified technicians with expertise in different but complementary areas in order to reduce their vulnerabilities, like attacks and all the common attack methods adopted by attackers, which conduct to proposals of the research of Chitrey et al. (2012) such as: loss of confidential information to business rivals, physical damage to assets, deprivation of public trust to shareholders and decrease of the public image to markets.

For the society, fraud on e-banking services is constantly embracing day-to-day problems, which increases risks to the complexity of the bank client system. And, it rises due to the lack of understandable information about the scheme used by "bad citizen" and he misuse factually accurate information. Indeed, the society must disclosure, in time and constantly up-to-date, relevant information and decisions to its citizens, which must not be excessive controlled by security departments that reduce transparency.

REFERENCES

Abreu, R., Segura, L., David, F., Formigoni, H., Legčević, J. and Mantovani, F., 2015, June. Ethics and fraud in E-banking services. In *Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on* (pp. 1-6). IEEE.

Association for Financial Markets in Europe (AFME), 2012. *High-level Expert Group on Reforming the Structure of the European Banking Sector*.

Banco de Portugal, 2016. *Sistema de Informação do Banco de Portuga*l. Lisboa: BP.

Benkler, Y., 2006. *The wealth of networks: How Social production transforms markets and freedom*. London: Yale University Press.

BPI, 2016. *Sistema de Informação do BPI*. Lisboa: BPI.

Bradley, G., 2005, July. The Convergence Theory on Information and Communication Technology (ICT) and the Psychosocial Life Environment–The Connected Home. In *Proceedings of the HCI International 2005 conference* (pp. 22-27).

Bradley, G., 2006. *Social and community informatics-humans on the net*. London: Routledge.

Bradley, G., 2010. *The convergence theory on ICT, society and human beings – towards the good ICT society. Triple C, 8*(2), pp. 183-192.

CGD, 2016. *Sistema de Informação da CGD*. Lisboa: CGD.

Chitrey, A., Singh, D., Bag, M. and Singh, V., 2012. *Comprehensive Study of social engineering based attacks in India to develop a conceptual model. International Journal of Information & Network Security, 1*(2), pp. 45-53.

Conheady. S., 2014. *Social engineering in IT security: Tools, tactics, and techniqu*es. New York: McGraw Hill.

Crowther, D., 2004. Corporate social reporting: genuine action or window dressing. In *Perspectives on corporate social responsibility* (pp.140-160).

European Commission (EC), 2012. *Consultation by the high-level expert group on reforming the structure of the eu banking sect*or.

Fama, E.F., 1980. Agency Problems and the Theory of the Firm. *The journal of political economy*, *88*(2), pp.288-307.

Floridi, L., 2013. *The ethics of information*. Oxford: Oxford University Press.

Gavish, B. and Tucci, C., 2006. Fraudulent auctions on the Internet. *Electron Commerce Research, 6*, pp. 127–140

Gulenko, I., 2013. Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Information Management & Computer Security, 21(2), pp. 91-101.

Hadnagy, C., 2011. *Social engineering: The art of human hacki*ng. Chichester: John Wiley.

Harris, L. and Spense, L., 2002. The ethics of ebanking. Journal of Electronic Commerce Research, 3(2), pp. 59-66.

Holtz, P., 2011. Teaching Cyberethics: Value Orientations as predictors of the acquisition of moral competence in a course on the social consequences of information technology. *International Journal of Cyber Ethics in Education, 1*(4), pp. 22-34.

Holyoak, K.J, and Morrison, R.G., 2012. *The Oxford handbook of thinking and reasoning.* Oxford: Oxford University Press.

Huber, M., Kowalski, S., Nohlberg, M. and Tjoa S., 2009. Towards automating social engineering using social networking sites. *Computational Science and Engineering, 3*, pp. 117-124.

International Monetary Fund (IMF), 2012. *Global financial stability report*. New York: IMF

Jensen, M.C. and Meckling, W.H., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), pp. 305-360.

Kaspersky, 2015. Carbank APT. *The Great Bank Robbery*. Moscow: Kaspersky Lab HQ.

Kitano, H., Ghosh, S. and Matsuoka, Y., 2011. Social engineering for virtual 'big science' in systems biology. *Nature Chemical Biology, 7*(6), pp. 323-326.

Knack, S. and Keefer, P., 1997. Does social capital have an economic payoff? A cross-country investigation. *Quarterly Journal of Economics, 112*(4), pp. 1251–1288.

Macer, D., 2007. Computing ethics: Intercultural comparisons. Ethical pluralism and social justice. *In* E. Rooksby & J. Weckert (Eds.), *Information technology and social justice* (pp. 1899–2204). London: Information Science Publishing.

Mitnick, K., 2003. *The art of deception: Controlling the human element of security.* Hoboken: Wiley.

Montepio, 2016. *Sistema de Informação do Mont*epio. Lisboa: Montepio.

OECD, 2002. *OECD guidelines for the security of information systems and networks. Towards a culture of security*. New York: OECD Publishing.

OECD, 2011. *OECD council recommendation on principles for internet policy making.* New York: OECD Publishing.

OECD, 2012. *Improving the evidence base for information security and privacy policies:* Understanding the opportunities and challenges related to measuring information security, Privacy and the Protection of Children Online. OECD Digital Economy Papers, 214, New York: OECD Publishing.

OECD, 2014. *Consumer Policy Guidance on Mobile and Online Paym*ents, OECD. Digital Economy Papers, 236, New York: OECD Publishing.

Rakesh, V., Nabil, H., Rakesh V. and Hossain, N., 2013. *Semantic* Feature Selection for Text with Application to Phishing Email Detection. Information Security and Cryptology, ICISC 2013.

Rawls, J.A., 1999. *Theory of just*ice. London: Belknap.

Santander Totta, 2016. *Sistema de Informação do Santader Totta.* Lisboa: ST.

Spafford, E.H., Heaphy, K.A. and Ferbrache, D.J., 1989. *Computer viruses: dealing with electronic vandalism and programmed threats*. ADAPSO.

Stamatellos, G., 2007. *Computer ethics: A global perspective*. Sudbury: Jones and Bartlett Publishers.

Turilli, M. and Floridi, L., 2009. The ethics of information transparency. *Ethics Information Technology, 11*, pp. 105–112.

Wiener, N., 1954. *The human use of human beings: Cybernetics and society.* New York: Doubleday Anchor.

