FISHING AS A CYBERCRIME IN THE INTERNET BANKING SYSTEM: ECONOMIC AND LEGAL ASPECTS

Oleksandr Ilchenko, Sumy State University
Volodymyr Chumak, Kharkiv National University of Internal Affairs
Serhii Kuzmenko, Mariupol State University
Oleksandr Shelukhin, Azov Maritime Institute of the National University Odessa Maritime Academy
Artem Dobrovinskyi, Kharkiv National University of Internal Affairs

ABSTRACT

The paper describes the concept of phishing as one of the types of cybercrime in the field of Internet fraud. The author identifies the features of phishing and its main purpose. When investigating the essence of phishing as a cybercrime, attention was paid to the main methods of its implementation. The legal and regulatory framework was determined, in relation ot which international regulation and counteraction to negative phenomena of cybercrime, including phishing, is carried out. Particular attention is paid to the issue of determination of responsibility for commitment of cybercrimes, among which phishing is not an exception, at the legislation level in different countries of world. Significant obstacles in the field of full implementation of Internet banking were characterized. The importance of counteracting fraud in the system of economic safety of the bank, including phishing, was established.

Keywords: Phishing, Cybercrime, Cyberspace, Internet Banking.

INTRODUCTION

In the conditions of the rapid development of the society in the field of technology of the XXI century, the Internet has taken an important place in the life of almost every person in the world, since it provides access to information, a fast data transfer process, and most importantly- the opportunity to carry out banking, trading, exchange operations, funds remittance, etc.

As a global trend, the transition to non-cash payments is no longer a novelty. However, not all countries of the world have such a rapid process, because it depends on many factors that can slow it down, in particular from the lack of awareness about the benefits and convenience of cashless settlements, the level of distrust in the safety of the use of such types of payments, etc.

As a result of the steady increase in the number of different banking services, it becomes clear that the determination of the quality of the bank operations is not only the criterion of the existing set of services, but also depends on the level of implementation of computer technology, which simplifies interaction between the bank and the client. The use of Internet technologies by banks is due to the presence of many factors, including the need for customer service with minimal costs on large territorial scales, ensuring the maximum degree of universality of banking

services and their convenience, existence of a high level of competition in banking services, etc. Expansion of the market for banking services has led to the emergence of remote service, which includes Internet banking.

Given the fact that the Internet-based operations has become a mass phenomenon around the world, crimes committed through the use of computer technologies and using various means of access to the virtual world have become widespread. Such crimes are called "*cybercrime*" (or "*cyberfraud*"). A vivid example of cybercrime is phishing, which today has become the most popular and most dangerous kind of crime of this kind.

LITERATURE REVIEW

Phishing is a kind of internet fraud aimed at gaining access to confidential user data - their logins and passwords. This is accomplished through the mass mailing of emails on behalf of popular brands, as well as personal messages within various services, for example, on behalf of banks, or within social networks. Kazykhanov & Bayrushin (2016) define the main purpose of today's phishers as receiving information from users about their credit cards, as well as their accounts. The phishing is aimed at search for client's credentials as one of the most common ways of fraudulent behaviour with payment cards on the Internet, due to the increasing number of electronic banking operations and shopping on websites. Rajab (2019) states that such data is necessary for the perpetrator to access financial information and conduct banking operations as the card owner. A web-site that is visually similar to the original design of the website is even created with the aim to deceive users.

When investigating the issue of the nature of phishing, Kazykhanov & Bayrushin (2016) note that there are very frequent cases when the letter contains a direct link to a web-site that is externally difficult to distinguish from the real one or web-site with a redirection. After a user goes to a fake page, fraudsters try to use various psychological techniques to force a user to enter their login and password on the fake page, which he/she uses to access the cabinet on the web-site, which allows fraudsters to access their accounts and bank accounts.

One of the phishing methods is also the direct search for a victim to further reception of confidential information about her/his bank card details and personal data. The feature of the investigated type of fraud lies in the fact that the victim itself participates in a crime committed by the perpetrator. The said above speaks of the presence of victim's "*mediation*" activities. In this regard, Pivovarov & Tereschenko (2015) conclude that a significant reduction in potential risks for the general population is possible by studying typical varieties of victim's behaviour, personal characteristics, etc. When predicting victims, their psychological and socio-demographic characteristics and online routine measures should be taken into account. According to Whitty (2017), victims of cyber-crime more often meet the following criteria: they are older, have increased victimization due to lack of intellectual development, inexperience in using the Internet, credulity, absent-mindedness and inattention, in the presence of which the fraudster can influence them.

METHODOLOGY

The methodological basis for the study of phishing as a cybercrime in the field of Internet fraud was dialectic, comparative-law and system-structural methods. So, the dialectical method

was used to determine the essence of the concept of phishing and to establish its features. Using the comparative-legal method, the regulatory and legal framework, as well as the features of the regulation of this issue at the level of legislation in Ukraine, was determined, with regard of which the international regulation and counteraction to the negative phenomena of cybercrime, including phishing, is carried out. The system-structural method has allowed to make generalization and presentation of the results on the basis of the totality of the latest scientific publications devoted to the study of the problem of cybercrime.

FINDINGS AND DISCUSSIONS

The study of phishing as a cybercrime in the field of Internet fraud involves the determination of the regulatory framework that regulates this issue. So, at the international level, the United Nations solve the issue of counteraction to cybercrime through the introduction of the Global Cybersecurity Program (GCA), which includes the following areas: (1) legal measures; (2) technical and procedural measures; (3) organizational structures; (4) program of raising competence; (5) international cooperation (Global Cybersecurity Agenda, 2019).

The issue of counteraction to the negative phenomena of cybercrime, including phishing, is also important in the European Union. Fundamental principles of combating cybercrime are contained in the following international legal instruments: (1) United Nations Convention against Transnational Organized Crime, (United Nations Convention, 2000) Palermo, December 12; (2) European Convention on Mutual Assistance in Criminal Matters, 5 195 signed in Strasbourg, April 20 (European Convention, 1959); (3) The Convention on Cybercrime, 2001, signed on November 23, 2001 in the city of Budapest. In particular, the provisions of the Council of Europe Convention on Crime in cyberspace include the criminalization of offenses committed using computer devices in order to interfere with the work of communication networks and data theft; improvement of national legislation in the fight against cybercrime; development of international cooperation (Convention on Cybercrime, 2001).

A comprehensive EU document in this area was the EU Cybersecurity Strategy adopted in 2013. The document covers all aspects of cyberspace, including the internal market, justice, internal and external policies. According to the EU Cybersecurity Strategy, among the priorities of the EU's international policy in the cyberspace, the following are defined: (1) freedom and openness: In order to use the fundamental rights of a person and a citizen in cyberspace, appropriate principles are defined; (2) the application of EU law in cyberspace to the same extent as in the physical world; (3) development of the potential of cyber security through cooperation with international partners and organizations, private sector and civil society (European Union Global Strategy, 2013).

Particular attention is paid to the issue of determination of responsibility for commitment of cybercrimes, among which phishing is not an exception, at the legislation level in different countries of world. So, Art. 263a of the German Criminal Code provides for liability for computer fraud, which means the intention of obtaining for him-/herself or a third person an unlawful property benefit by damaging the property of another person by affecting the result of processing the computer data, developing incorrect programs, using incorrect or incomplete data, unlawfully using data or influencing such a process by some other unlawful influence (German Criminal Code, 1871).

The Austrian Criminal Code contains a rule that establishes liability for fraudulent access to data that is recognized as property damage caused to obtain an unlawful benefit to a perpetrator or a third person by influencing the processes of automated data processing through special programs, input, modification or destruction of data or in any other way that affects the processing of data (Austrian Criminal Code, 1974).

The French experience in regulation of cyberspace, an important place in the regulatory framework of which is the Law on compulsory registration of web-site owners and the criminal liability of providers for the provision of hosting to unidentified users, is also worthy of note. This law establishes the criminal liability of providers for provision of information about the authors of the web-sites to any third parties; provision of a place on the server to unidentified users by providers; provision of incomplete or inaccurate information by the authors of French web-sites. The responsibility for web-sites, which authors are not identified, shall be borne by the provider, and possible penalties include imprisonment for a six months (Buiadzha, 2017).

As for the current Ukrainian legislation, the responsibility for cybercrime is provided in section VI of the Criminal Code "*Crimes against property*", part. 3 of Art. 190 and is called fraud committed by illegal operations using computers. The definition of fraud is given in part 1 of Art. 190 of the Criminal Code of Ukraine as a gaining possession of someone else's property or the acquisition of the right to property by deceit or abuse of trust (Criminal Code of Ukraine, 2001).

Ukraine also has a specialized Law "*On the basic principles of ensuring of cybersecurity of Ukraine"* dd October 5, 2017, which determines the legal and organizational principles for protection of the vital interests of man and citizen, society and state, national interests of Ukraine in cyberspace, the main goals, areas and the principles of state policy in the area of cyber security, powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, and basic principles of coordination of their activities for ensuring cybersecurity. It is important to note that the said Law defines a cybercrime (computer crime) as a socially dangerous guilty act in and/or using cyberspace, the liability for which is provided for by the law of Ukraine on criminal liability and/or which is recognized as a crime by international treaties of Ukraine (Law of Ukraine, 2017).

Malik & Islam (2019) point out that cybercrime incidents have a negative impact on the efficiency of banking system organization, but information security weakens the negative impact of cybercrime on it. The understanding of information security weakens the negative impact of cybercrime on organizational activities, therefore, it is advisable to create security training courses for HR managers to raise awareness of employees about cybercrime.

According to lkhatib & Alaiad (2016), the problem of ensuring the safety of online banking services, confidentiality of transactions or services provided by the bank, as well as the lack of legal regulation of e-banking, remains a significant obstacle to the full implementation of Internet banking. Taking into account the above, according to Klochko et al. (2016), there is a need to increase the level of banking safety and ensure public confidence in the banking system by ensuring its stability.

Countering the fraud in the system of economic safety of the bank, including phishing, in addition to the financial goal of reduction of operating costs, is a significant way to improve the quality of the bank's relationship with customers and ultimately promotes customer loyalty (Hoffmann & Birnbrich, 2012).

RECOMMENDATIONS

The problem of counteracting cybercrime requires compliance of current legislation with the current level of development in the field of information technology that can be achieved through purposeful work on harmonization, improvement and adaptation of national legislation to international requirements and standards. In this context, it is expedient to work on the interaction and coordination of activities of law enforcement and judicial authorities, and special services in the area of counteraction to negative phenomena of cybercrime. At the same time, the need to intensify cooperation on counteraction cybercrime at the international level deserves an important attention.

CONCLUSION

Every year, the volume of global economic losses from cybercrime is growing steadily, indicating the real threats and challenges of cybercrime in the virtual space. Phishing is not an exception and involves illegal activity in cyberspace, including in the system of Internet banking.

Despite the fact that phishing is very common today in the area of online fraud as a cybercrime in the Internet banking system, the level of awareness of the population about such a phenomenon is not high. The search for a victim of phishing is facilitated by inadequate intellectual development, inexperience in using the Internet, victim's credulity, absent-mindness, inattention, psychological negative qualities, in the presence of which the fraudster can influence them.

Today, there is an increase in the number of phishing frauds, especially those related to the Internet banking system, and more and more people around the world become their victims. The solving of the issue of counteracting cybercrime, including phishing, is possible through a comprehensive approach to this issue, which should include legal measures, technical and procedural measures, international cooperation, etc.

REFERENCES

Austrian Criminal Code. (1974). As amended up to Act of October 25. Retrieved from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296

Buiadzha, S. (2017). Positive experience of legal regulation of the fight against cybercrime in EU countries. *European political and law discourse, 4*(4), 41–46.

Convention on Cybercrime. (2001). Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true

Criminal code of Ukraine. (2001). As amended up to act of November 23. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14

European Convention. (1959). *On mutual assistance in criminal matters*. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030

European Union Global Strategy. (2013). Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/area/foreign-affairs_en

German Criminal Code. (1871). As amended up to act of December 18. Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.pdf

Global Cybersecurity Agenda. (2019). Retrieved from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Hoffmann, A.O.I., & Birnbrich, C. (2012). The impact of fraud prevention on bank customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing, 30*(5), 390-407.

Kazykhanov, A.A., & Bayrushin F.T. (2016). Phishing, as a problem for specialists of the department of information security. *International scientific journal Symbol of Science, 10*(2), 53–54.

Klochko, A.N., Kulish, A.N., & Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. *Russian Journal of criminology*, *10*(3), 618–620.

Law of Ukraine. (2017). On the basic principles of cybersecurity protection of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

lkhatib, K., & Alaiad, A. (2016). The influences of privacy, security, and legal concerns on online banking adoption: A conceptual framework. *Online Banking Security Measures and Data Protection, 9*(1), 1-14.

Malik, M.S., & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26*(1), 1-11.

Pivovarov, V.V., & Tereschenko, K.V. (2015). Fraud with bank cards: separate issues of victimological prevention. *Carpathian legal magazine. Series: Law Sciences, 10*(1), 132–137.

Rajab, M. (2019). Visualisation model based on phishing features. *Journal of Information and Knowledge Management*, *20*(1), 1-11.

United Nations Convention. (2000). *Against transnational organized crime.* Retrieved from https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-12&chapter=18&clang=_en

Whitty, M.T. (2017). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292.