SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2810-4188, ISSN-L 2810-4188
Nº. 1 (2021), pp. 661-666

PHISHING ATTACKS, AS A FAVOURABLE CONDITION FOR TERRORIST ACTIVITIES

I.R. RUSU

Ioana-Raluca RUSU
European Agency for Border Police and Coast Guard, FRONTEX
E-mail:rusu.ioanaraluca@yahoo.co.uk
ORCID: 0000-0003-3393-2069

Abstract

Since attacks of a phishing type can be included in the category of cybercrime, this paper is aimed at presenting some theoretical aspects specific to this type of criminal offence, the goal being to create logical arguments that would result in conclusions liable to be put to use, but also some methods for counteracting this offence in an incipient stage. These cyber attacks are usually based on a user's ignorance about the ease with which he is making available, in a virtual environment, his bank account details, credit card details, other personal data, including access passwords. Thus, the money present in the bank accounts, which constitutes the material object of the offence, will be used, without the knowledge of the legal holders, by hackers for banking transactions, which are difficult to follow, in order to finance terrorist activities.

Keywords: *cyberspace, computer virus, phishing, cybercrime, terrorism*

INTRODUCTION

We consider phishing to be different from the classic computer virus in that the classic computer virus can affect both the hardware and the software, and the hacker mainly aims to destroy or delete files, delete information, block the operating system, etc., whereas the hacker who uses a phishing action is interested, in the initial phase, only in copying some information.

Therefore, when talking about a classic virus we do not refer to the background of the computer system, focusing instead on the form of corruption of the computer system, and "*phishing describes how the problem occurred, rather than how it behaves*" [Anderson, 2021].

According to other specialists, *"phishing is a form of fraud in the online environment which consists in using certain techniques to manipulate the identity of individuals/organizations in order to obtain material benefits or confidential information"* [Neagoe, Borşa, 2016, p. 90].

From our point of view, the most common phishing attacks can be considered as fraud committed by e-mail or by mobile phone and they represent a method by which the hacker, using an electronic message, tries to attract the attention of the customers of an institution, usually a bank, in order to take possession of personal data that will be used for financial transactions in favour of terrorist structures.

Usually, messages such as "*Important message – update of personal data, the failure to confirm the details of the online account will lead to its permanent suspension, or a request to enter a new password or the PIN code on the grounds that it is necessary to confirm or change such data*" [https://www.bancatransilvania.ro/securitatea-informatiilor/despre-phishing], can be found on links that imitate the official page of the banking institution.

I. BRIEF CONSIDERATIONS REGARDING THE PHISING ACTIVITY PROVIDED FOR AT THE LEVEL OF THE EUROPEAN UNION AND IN THE ROMANIAN LEGISLATION

At the level of the European Union, provisions on the prevention, combating and criminalization of terrorism are to be found in EU Directive [DIRECTIVE (EU) 2017/541], and those specific to criminal acts of the phishing type are included in the provisions of Art. 3 par. (1) letter (i) of the same regulatory act issued at European Union level.

Romania pays special attention to preventing, combating and criminalizing acts of terrorism, transposing into national legislation the regulations of criminal rules adopted at European level, this field being regulated mainly by a special law [Law no. 535 of 2004].

Given that the phishing act is a crime that occurs in a space without borders and at the same time follows a strong dynamic, being also characterized by anonymity, it is easy for a terrorist entity [see the definition according to Art. 4 par. 1 of Law 535 of 2004], or sympathizer of this structure, to initiate and perform terrorist acts via computer data systems.

If we refer to phishing attacks from the perspective of terrorism, we will define this type of criminal offence as an illegal interference in cyberspace whose action targets the computer systems of banking structures, or assimilated to such banking structures, in order to control bank accounts belonging to natural persons (individuals) or legal entities for the benefit of and in order to facilitate terrorist capabilities.

Taking into account the characteristics of crimes circumscribed to acts of terrorism and the manner in which terrorist entities initiate, support, carry out or facilitate attacks by using computer or telecommunications networks, in our opinion, terrorist acts of the phishing type form the object of the criminal offence provided for and sanctioned by the provisions of the Romanian special law [article 32 par. 1 letter q of Law no. 535 of 2004], in the case of unauthorized access to computer systems or data or unauthorized transfer of computer data, and those that have as a starting point the terrorist acts of the phishing type are regulated by the provisions contained in Art. 36 of the special law adopted in Romania, in the case of the crime of financing terrorism.

The substance of this paper deals with an analysis of the crime of phishing that is circumscribed to terrorism, from the perspective of Romanian legislation.

II. THE CYBER TERRORISM CRIME OF A PHISHING TYPE

Although the scope of the Romanian legal rule is much more comprehensive in the case of cyber terrorism, we will analyze only the manner in which the crime of cyber terrorism by phishing is provided for and criminalized in the Romanian legislation.

II.1 Legal object

The general legal object consists in the social relations that arise and develop in the human community, at local, national or international level, between individuals, authorities and other institutions, and which are based on mutually beneficial relations, aiming to protect the social value represented, which is, in this case, national security.

The complex legal object is composed of the main specific legal object represented by the social relations affecting the administration of justice through the delay in determining the manner in which the illegal act was committed and through preventing the restoration of legality as soon as possible, while the secondary specific legal object is represented by the social relations regarding the legal circulation of money and the negative impact on the estate of the natural person or legal entity through the diminishment of monetary funds.

II.2 The material object

Given that the specific legal operations concretely refer to tangible assets, in this particular case "*the value being transferred (monetary funds)*" [Lascu, 2001, p. 20], the crime of cyber terrorism of the phishing type has a material object.

II.3 Subjects of the crime

The active subject

It is represented by any natural person or legal person who commits the deed as perpetrator, co-perpetrator, instigator or accomplice. The instigator finds himself in the situation of being the object of a formal concurrence of crimes (multiple offences) [article 38 par. (2) of Law no. 286 of 17 july 2009], because he is also the perpetrator of the crime of instigation, a deed that is provided for and sanctioned, in Romania, by the law on the prevention and combating of terrorism [article 33^2 of Law no. 535 of 2004].

In the case of this crime, taking into account the definition of phishing attacks from the perspective of terrorism, we consider that there may be co-perpetration because, in order to make as difficult as possible the identification, in the early stages, of the illegal interference in cyberspace, but also of measures intended to restore legality, we do not exclude the simultaneous intervention of two or more persons on the computer system that manages the personal data assimilated to the bank account or bank accounts belonging to a natural person or legal entity.

The passive subject

Since this crime belongs to the field of terrorism, the main passive subject is the state as the main holder of the protected value, namely the assurance of national

security, regardless of whether the state's own authorities or an international organization are affected as a result of the offence.

This is also a situation that involves a secondary passive subject, which can be any natural person or legal entity that suffers injuries/damages as a result of the offence being committed.

II.4 Conditions regarding the place, time and the situation favourable to committing the criminal offence

The provisions of the legal rule that criminalize the deed do not provide for the existence of special conditions of place or time, but there is the prerequisite condition of the existence of money in the bank account.

II.5 The constituent elements of the offence

The objective side of the criminal offence

a) The material element of the objective side designating the illegal act provided and sanctioned by the legal rule is achieved by the action of a person whose purpose is to create a false reality in order to obtain for himself or another an undue benefit to be used in order to finance terrorism.

According to the provisions of the criminal rule, the material element consists of commissive activities, performed by the person who is the active subject of the crime, consisting of any activity that meets the constituent elements of crimes against the security and integrity of computer systems and data [article 32 par. 1 letter q of Law no. 535 of 2004].

b) The immediate consequence of the unlawful act consists in the fact that national security has been endangered, including by causing damage to the estate belonging to a natural person or legal entity.

c) The causal relation – results *ex re* (from the materiality of the deed).

The subjective side of the criminal offence

In terms of the subjective side of the offence, considering the behaviour of the active subject, but also the socially dangerous result of the illegal action through the desire to obtain an unjustified benefit, we note that it is characterized by guilt in the form of direct intent.

The guilt manifested in the form of direct intent cannot be questioned because the active subject was aware that he was carrying out an illegal activity, by causing damage, in order to obtain an undue material benefit.

The motive and purpose of the criminal offence

The motive and purpose are the same as for all crimes resulting from the commission of a terrorist act, namely to illegally obtain certain amounts of money in order to finance terrorism.

II.6 Forms of the criminal offence

Attempt and preparatory acts

Just like any crime belonging to the field of terrorism, the crime of cyber terrorism of the phishing type is likely to unfold over the course of time and therefore, most often, there are some preparatory acts. Because of the social danger represented by the criminal offence, along with the attempt, the legislator deemed

it fit to criminalize the preparation of criminal acts, by assimilating them to the attempt [article 37^1 of Law no. 535 of 2004].

Consumption and exhaustion of the criminal offence

The consumption of the offence takes place at the moment when the crime is materialized, creating the state of danger.

Exhaustion takes place either following the intervention of the authorities to restore legality, or following the last illegal act committed through the criminal offence and the voluntary cessation of the illegal act, if it's a situation of continuous offence.

II.7 Sanctions

Taking into account the purposes of the special criminal law criminalizing terrorism [article 1 of Law no. 535 of 2004], the legislator sought to make sure that the sanction applied was in relation to the social danger posed, thus, he considered that, outside the custodial sentence [article 32 par. 1 of Law no. 535 of 2004], the penalty of a fine should not be applied [article 32 par. 2 of Law no. 535 of 2004].

CONCLUSIONS

Even if, at first sight, this criminal act, through its materialization, does not have as a direct effect the loss of human lives, we cannot omit that a crime which helps to finance terrorism will cause chaos and will implicitly lead to terror through the killing of human beings and the destruction of goods.

Therefore, the measures ordered by financial institutions with a view to preventing and combating phishing activities will only become effective if the technology on which the IT field is based are supported by multidisciplinary collaborations between national security experts and IT specialists.

Also, the state authorities, regardless of whether they carry out their activity in the financial or legal field together with specialists in the private financial field, must intensify their efforts to find the best practices in order to implement solutions for the prevention of criminal acts of the phishing type.

BIBLIOGRAPHY

Directive (EU) 2017/541 of the European Parliament and of the Council of 15th March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, published in Official Journal of the European Union, L 88, 31st March 2017, the Romanian version being published in the Official Journal of the European Union L88/6 of 31st March 2017.

Law no. 286 of 17th July 2009 on the Criminal Code, published in the Official Journal no. 510 of 24th July 2009, updated.

Law no. 535 of 25th November 2004 on preventing and combating terrorism, published in the Official Journal no. 1161 of 8th December 2004, with subsequent amendments and additions.

Lascu Ioan, *Incriminarea penală a unor fapte de spălare a banilor* (*The Criminalization of Money Laundering Acts*), Revista Pro-Lege (Pro-Law Journal) no. 4/2001.

Neagoe Visarion, Borşa Silviu-Stelian, *Riscuri şi ameninţări cibernetice la adresa securităţii internaţionale. Terorismul cibernetic - un flagel care ameninţă securitatea globală* (*Cyber Risks and Threats to International Security. Cyber Terrorism – a Scourge Threatening Global Security*), Revista de Ştiinţe Militare (Journal of Military Sciences) no. 4/2016.

Sophie Anderson, *Ce este phishing-ul? Ghid Simplu cu Exemple (What Is Phishing? Simple Guide with Examples*), source: https://ro.safetydetectives.com/blog/ce-este-phishing-ul/, website accessed on 27th October 2021.

Phishing - metoda de furt de identitate - ce este şi cum îl evitam - Banca Transilvania ((Phishing - the Method of Identity Theft – What It Is and How to Avoid It - Banca Transilvania) source: https://www.bancatransilvania.ro/securitatea-informatiilor/despre-phishing/, website accessed on 27th October 2021.