PHISHING AND E-COMMERCE: AN INFORMATION SECURITY MANAGEMENT PROBLEM

Mircea Constantin SCHEAU*
Adrian-Liviu ARSENE**
Gerald DINCA***

*Romanian Commercial Bank, Romania
** Bitdefender, Romania
***Romanian Banking Association, Romania

Phishing and E -commerce have at least two things in common - cyberspace and money, and the intersection of the two is often built around services and products offered by banking institutions and investment trusts. Nowadays, fraud economy and fraud methods that have been known to be particularly prolific for cybercriminals are hot issues. Attacks have become refined, with time and profit as determining factors. The risks of being discovered are significantly lower as the analysis preceding offenses is more comprehensive. Inside pawns or accomplices increase the chances of success for fraudulent actions. Cyberspace offers boundless possibilities. Technology is accessible to all. Innovation supports developments in all areas. The same device can be used in various areas. Imagination is the final frontier.

Key words: phishing, e-commerce, vulnerabilities, financial institution, browser

1. INTRODUCTION

Phishing is one of the most popular forms of fraud by which an attacker tries to find confidential information specific to an average user, such as authentication credentials or information on login to public infrastructure, through communication channels (e.g. e-mail services Instant messaging, SMS, etc.).

It is an extremely popular tool within communities of cybercriminals because it is easier to try and cheat a ”target” by sending an apparently legitimate e-mail with a link to a resource controlled by the attacker, than attempting to break into a remote and most often advanced protection system. Successfully addressing such an attack is necessary. However, sophisticated marketing techniques are used to identify the most effective types of messages with which one can grab attention, like an account about to expire or an immediate update due to the emergence of a vulnerability.

Thus, true phishing strategies are often built around leading companies, major events, or "News of the Day" topics, all of which can be both true and fictional. For emails to seem credible, they are packaged and presented as coming from a well-known source, including logos and identification information

copied directly from that company's website. The links contained in the message body are designed to create the impression that they're coming from the company. In reality they lead to "a node" controlled by the offender. Similarly, the use of sub very similar domains and URLs is a fairly common trick, just like masking URLs using different logical characters. Some phishing attacks use sophisticated JavaScript code to place a picture of a legitimate URL on top of a browser's address bar.

Another form of fraud is the use of botnet networks to generate profit for attackers. Hackers use infected computers that they directly control in order to access advertising services, to which they are actually affiliated, and thus generate profit from illegitimate clicks.

The aim of this article is to bring some of the economic implications of cybercrime-based phishing and e-commerce to the attention of the specialists and the general public. To control the risk of compromising their image, companies may not report the exact values of their damages. In Romania, the financial segment is not declared a critical infrastructure and state agencies can hardly conduct audits in this field. Furthermore, the article substantiates the theoretical approaches via a few cases that could become the subject of reflection, while also outlining several proposals for incident response.

2. CONCEPTUAL FRAMEWORK

Phishing is a form of cheating in an online environment by using techniques for handling the identity of people/organizations to obtain material or confidential [21] information. By extending the definition above, phishing can be considered a method for obtaining card data by creating fake websites that mimic legitimate banking websites or government institutions. The information thus obtained can be transferred back into the banking circuit by affixing other cards that can be used to either make transactions over the internet or that can be transferred/sold to third parties [21].

Even if it seems hard to believe, according to a specialized study [16], two thirds of domestic attacks are based on sending infected emails, apparently legitimate and as coming from institutions that ask users to renew passwords, download attachments, or change other features, as in **Figure 1.** They consequently exploit misinformation and lack of attention, achieving the desired effect. There are also cases where the malware is installed during the second phase of the attack. The recipient answers so-called business proposals from an unknown sender, providing access to the resources of its computer system.

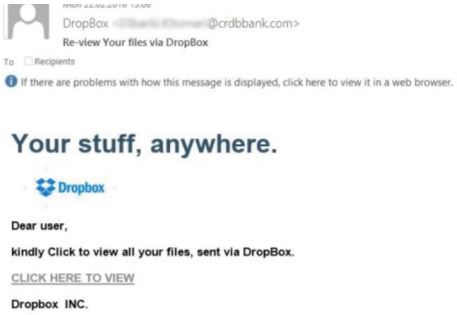

Fig. no. 1. Email example of redirecting victims to phishing websites [8]

Most intrusion procedures are initiated by criminals motivated by greed or by the desire to demonstrate their skills. However, it has become quite difficult lately to make a clear distinction between criminal organized groups and state-sponsored terrorist attacks. In the latter case, phishing actions are in conjunction with money laundering and attacks on critical infrastructure. A criminal group's activity may take place in two ways: redirect a victim to a phishing site - controlled by them - or take control of a legitimate site without its owners' knowledge and collect information from trustworthy buyers. After profiling the latter based on the criminals' own goals, both companies and individuals can become victims.

All this is possible due to the diversity of threats, and existing differences in institutional culture. For example, in Romania in 2014 there were over 710,000 domains registered and over ten million unique IPs allocated to organizations. Out of all these, more than two million reported a cyber security alert [2].

When it is difficult to attack a company directly, vulnerabilities, most of which are the result of human nature, become the target. Even though, as www.cert-ro.eu reveals for 2014, about 54% systems are not properly configured and are thus turned into vulnerabilities - filters can be installed to block daily "robot" assails. Nonetheless, as Kevin Mitnick [5] says, they can only partly prevent negligence or "in-house" criminality. On the other hand, a vulnerability may cause immediate or future damages within the targeted or adjacent systems, depending on the intended victim. Personnel training and public awareness, in conjunction with a significant increase in IT budget used to rapidly detect and respond to incidents, may represent a future solution. According to a Gartner prediction, until 2020 there will be a raise of up to 75% in the IT budgets and that will be reserved for investments in detection and rapid reaction systems.

All of the above considered, the article aims at narrowing down the scope of phishing to the field of electronic commerce, also known as e-commerce.

Consequently, the operational definition provided for this purpose runs as follows: e-commerce is the procedure of buying and selling products and services via the Internet. A simple, fast and convenient payment for goods and services from online stores is represented by the banking card. In this respect, the international security standard 3D-Secure is designed to protect transactions. Card payment acceptance is decided mainly by the owner of the online store and not by the financial institution issuing the card. There are sites that do not accept all types cards, even if issued by an international brand, just as there are instances when sellers decline the transaction or require additional information if they have doubts about the authenticity of the payer. Similarly, purchases are recommended only on secure virtual stores, from traders known for their good reputation and privacy practices. This practice has been widespread, especially after publicizing cases of fraud, one of the most common being the non-delivery of goods, selling stolen goods/counterfeit/prohibited,

fake offers "second chance offers", unauthorized access, phishing, spoofing, etc. Although promoter efforts have increased exponentially since the debut of online trading service, the rise of fraudulent transactions and risks has led to an increase in payment denials and disputes, leading to low profitability and a low utilization rate. The main cause was the lack of secure methods of authentication in conjunction with card forgery. Currently, companies regularly invest in developing new and effective mechanisms for detecting and combating fraud, and the stability of processing platforms is just as important as the security of online trading. Each merchant-supported system is validated under Visa and MasterCard regulations, transactions are processed in 3D secure environment, and each transition is associated with a security level that is decided based on a risk level assessment. When a customer wants to purchase a product and enters data onto a secure platform, the financial institution, following anti-fraud validation, authenticates and authorizes payment, and it is only then that the online store is notified on transaction validity.

3. TYPES OF PHISHING ATTACKS

To understand the scale of the phenomenon, the findings of a report are truly conclusive. Thus, according to this, the damages caused by retailer fraud were estimated [11] at 32 billion dollars in 2014, while in 2015 it was estimated [12] that the same retailers lost about 1.32 % of revenues, which is almost the double of the previous year. As shown in **Figure 2**, the increase recorded for fraudulent transactions in just over two quarters in the area of e-commerce is almost by two and a half of the total transactions, from 0.8% to 2.1%.

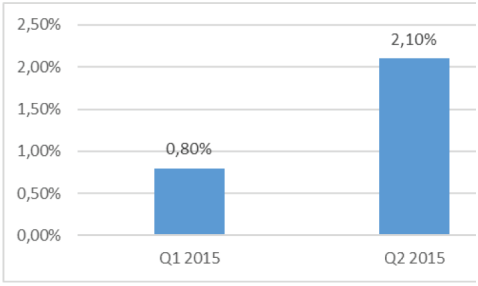

Fig. no. 2. Fraudulent attacks (% from the total number of transactions) [10]

This phenomenon is becoming increasingly worrying to online merchants, even if not all e-commerce segments are equally attacked by hackers. They only target areas of interest that are extremely popular in the online environment, aiming luxury goods (e.g. jewelry, brand products, etc.). Its dynamics is complex and even if there are times when the costs per fraudulent transaction drop, on a general level the losses are significant (see **Figure 3.**).

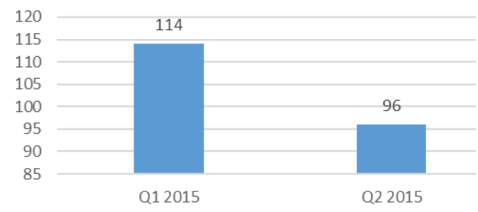

Fig. no. 3. Costs generated by attacks ($ per transaction) [10]

For Romania, **Figure 4** shows an attack distribution, highlighting the peaks and troughs relating to developments in crime.

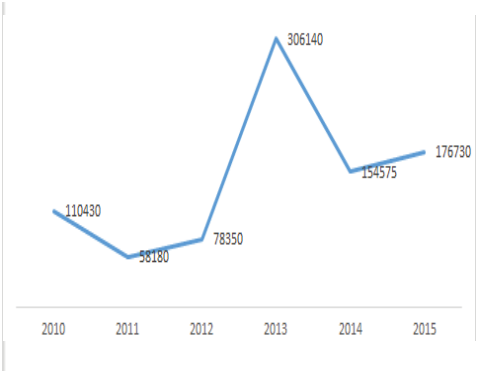

Fig. no. 4. Damages in Romania [5]

According to a survey conducted in Q1 2016 by a security company, and displayed in **Figure number 5**, large companies are among the most affected online service merchants and are particularly impacted by phishing campaigns.

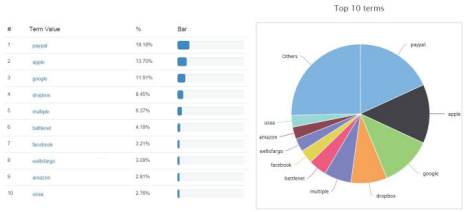

Fig. no. 5. The most affected brands in phishing "campaigns" [8]

So far, many different types of attacks that can be labeled as phishing have been identified. The most relevant can be grouped into the list below.

"Classic" phishing is a term originally referring to stealing data specific to a private account by using instant messaging services that suggested the need for checking account information, unauthorized account modifications, new free services which required quick action, etc. Messages were (and are) broadcasted to a wide group of recipients with the hope that unwary ones will respond by accessing the link to a fake website, where their confidential information can be collected by the offender.

Key loggers and Screen loggers are special varieties of malware that pursue and capture any entry made on the keypad, and send relevant information to the attacker via Internet connection available at that station. They can be incorporated both in users' browsers in the form of small utility programs that run automatically when the browser is started, or as system files and device drivers.

Session hijacking describes an attack in which user activities are monitored. When the latter are connected to a target account or transactional application the malware takes control of the session and performs unauthorized actions, the most commonly encountered one being the transfer of funds without the user's knowledge.

Data handling by installing a Trojan [18] which acts as an invisible pop-up when users try to connect to various resources of interest to criminals (e.g. financial institutions websites). They collect user credentials locally and submit them to the attacker via an active connection to the Internet.

Address list contamination is based on the fact that a user accessing

a URL to visit a website must first associate it with an IP address before the application is submitted via the Internet. Most users run Microsoft Windows, which assumes a mapping between the "hostname" and the IP addresses of the sites. This is the basic functionality of a DNS [19]. By "contaminating" the host's file, attackers associate false addresses to a real website, redirecting users to a website controlled by the attacker.

Phishing using malware [20] refers to misleading users to run a special software on their endpoint. Malware can be introduced via an email attachment, as a file downloaded from a website, or by exploiting security vulnerabilities in the operating system. Statistically, companies are more exposed to this type of attack, as it is very difficult to keep all applications up to date with their latest versions.

As shown in **Figure 6,** according to Q1 2016 statistics from a security company, some of the most used phishing campaigns exploit the file sharing industry (19.70%), retail (19.29%), and online payments (18.79%) and banking industry (18.00%).

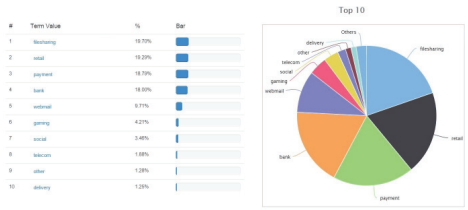

Fig. no. 6. The top 10 most targeted industry sectors for internet phishing [8]

Not even organizations whose security systems are different from those of the financial-banking institutions are protected against computer assaults. The CFO of a company received a mail sent from an address that was already under the control of a hacker. The result was defrauding 5000 Bitcoin, equivalent of 1.85 million dollars and triggering a conflict with the insurer [6].

Attacks that involve reconfiguring the target system are aimed at changing the settings on a user's PC. Favorite URLs stored locally could be modified to direct users to fake websites or false addresses, such as electronic banking applications. For example, instead of "banktest.com" it can lead to "banctest.com".

Injecting content into real sites targets public websites that manage confidential information of interest to attackers. It exploits vulnerabilities in the programming code of the website in question and replaces some of the content segments designed to mislead the user, in order to disclose certain confidential information. For example, attackers can insert malicious code or overlay additional content on the page to capture user credentials.

Man-in-the-middle is the most difficult to detect of all forms of phishing. The attackers manage to position themselves between the user and the legitimate website. Initially, they record network information and even transactions, but without the intention of affecting users. Because of that, man-in-the-middle attacks are very difficult to detect.

Attacks by creating attractive sites involve creating websites that search engines index legitimately. Digital

certificates usually offer a measure of trust on the Internet, but they often end up being used to sign malicious web applications. Such websites appear to be signed by a root certificate authority and are seen as "trusted" by browsers. Hence, more malware variants have begun to use false or stolen digital certificates [1] from different certification authorities. Users access these sites by looking for information needed in certain context (e.g. travel offers). Filling out the required fields (e.g. email, password, data cards, etc.) actually ends up delivering the information to the attackers. A far more dangerous example of such an attack is when fake banking websites display lower than regular credit costs and interest rates. Victims "interested" in the offering are encouraged to transfer their accounts to these "banks", the end result being fairly easy to predict.

4. IDENTIFYING A PHISHING ATTACK

There have been many statistics that reference the matter. People are often curious to know what percentage of Internet users are the target of attacks, especially how many fall prey to these, but one of the most credible sources in this area [13] detailed a study showing that such information is counterproductive. However, another company [9] says that 97% of people around the world were unable to correctly identify phishing emails. The sources for these statistics were the results of an online questionnaire testing over 19,000 people from 144 countries.

Since only 3% of respondents correctly identified all 10 phishing emails presented to them, by way of contrast it can be concluded that 97% of people cannot identify phishing attacks. The issue is quite questionable as most people detect a potential attack from the analysis of the context and not the technical elements. Should these statistics represent a warning to companies? Absolutely yes! But are people really so gullible and incompetent in identifying phishing emails? We believe there is sufficient evidence to doubt such a statistic. Even if many emails appear to come from a source trusted or familiar to the user, these attacks often betray themselves by using a different language than the real sender. An email from the personnel administration department, which began with "Dear Mr. X", is immediately suspect because HR never uses this tone to address employees. Cultural elements are equally important in identifying phishing attempts. For example, if the recipient receives an email with data relevant to the financing department but s/he works in IT, or information about the weather in a country when s/he lives in another one, or useful information for parenthood when s/he has no children, identifying such attacks becomes simple. On the other hand, the ability to distinguish legitimate URLs will not necessarily prevent a phishing attack. Numerous cases of attackers who took control of legitimate websites, using them to host malware, have been investigated.

The 97% statistic was classified as controversial. If a user correctly identifies 8 or 9 out of 10 emails, it is

thought to be wrong, if not biased to consider 97% of cases as a "failed" qualitative. When evaluating the effectiveness of a technical solution, we expect it to detect 100% of threats. A person who can correctly identify the majority of phishing attacks is an important resource for the general security of a company or a financial institution in particular, and awareness can help the company protect itself from future threats. Based on the experience of those studying the phenomenon, there have emerged a number of methods by which an attack can properly be identified and its effects mitigated/ canceled:

a) Checking the displayed name

A favorite tactic among phishing attacks is to fake the displayed name of the one sending the e-mail. Many fake e-mail threats display the name incorrectly. The only effective method is to check the "real" address from which the mail comes, and if it is unknown, the message should not be opened.

b) Reading the message without opening it

It is recommended to hover the mouse over any embedded links in the message. If the address of the link looks odd or suspicious, it is not recommended to "click" on it. To test the link, a new window can be opened and thus the address can be checked. Most often, the domain is unknown, and its authenticity cannot be verified.

c) Checking for spelling errors

Large companies care about the content of the messages they send to clients. They cannot afford major grammar or spelling mistakes. Reading e-mails carefully and checking that everything looks proper in terms of grammar or semantics, may relieve the user of much misery.

d) Analyzing how the e-mail is addressed

Is the message addressed generically, such as "Dear Customer"? Companies often prefer directly addressing the customer by including a personalized name and surname.

e) Privacy of personal information

Most companies will not ask to email confidential data related to credentials or credit card/debit card information. Any such request deserves maximum attention from the recipient.

f) Usage of the words "urgent" or "danger" in the subject line

Creating a sense of fear is a fairly common tactic for phishing. E-mails having subject lines claiming that the "account has been suspended" or that there was "an unauthorized login attempt" should be treated with caution.

g) Examining the signature of the one who sent the email

The lack of detail about how to contact the one who sent the e-mail might suggest a phishing attempt. Companies always provide real contact details.

h) Analyzing attachments

Attachments are commonly used for disseminating threats. These can damage computer files and even steal passwords or other confidential data. It is not recommended opening any e-mail attachment if it has not been correctly identified.

i) Verifying the header information of an e-mail

Attackers falsify not only display names, but also the email addresses placed in the message header.

According to statistics almost 30% out of 760,000 emails contain changes to the email address in the message header [3] [14].

j) "Don't believe everything you see!"

In most cases, attackers are highly trained in what they do. Just because an email has convincing logos of a well-known company, it is written in a valid way, and comes from an apparently valid e-mail address, which does not mean it is legitimate.

5. MEASURES FOR COUNTERACTING PHISHING ATTACKS

Security management aims to prevent crisis situations, minimize losses, and ensure the safety and stability of a company's activity. It also consists of a complex set of legal, organizational, economic, physical and information technologies capable of preventing the action of destructive factors threatening activity, and thus of weakening or annihilating their consequences by:

- securing access routes by implementing firewall solutions, using strong passwords and certificate authentication, and periodically renewing them; limiting access only to authorized locations;
- VPN (Virtual Private Network) solutions for securing information transfer between multiple locations or remote connections within the IT infrastructure;
- Applying access rights to sensitive company information;
- Establishing employees' access levels to company documents;
- Encrypting confidential data;
- Using Anti-Virus and Anti-Spam security solutions for data security;
- Allocation of responsibilities;
- Ensuring continuity of provided support;
- Increasing the capacity for incident response;
- Periodic security audit and review;
- Staff training in ICT and sub-domain security;
- Investigating staff activities;
- Installing a licensing and re-licensing system;
- Implementing a system of risk assessment.

Depending on each specific phishing attack, as well as on the resource it employees to reach its goal (i.e. the user or centralized infrastructure that processes confidential information), there are several safeguards that can be adopted, each with advantages and disadvantages. The list below is not exhaustive and can be updated at any time.

a) Automatically generating passwords for each domain

Specific mechanisms have been developed lately, by which any typed credentials are altered with the domain name, through a transparent method. The basic idea is to obtain a password hash with a secret key, along with the domain name of the website. That is very important because it tells the user that the entered password is for accessing that domain. Even if the user employs the same password for every account, it will be changed due to the mechanism in question, making it very difficult for the attacker to obtain the password for a particular area. It is a user-friendly method and

works well in theory, but its practical application is quite difficult because companies use multiple domains and sub domains;

b) Maintaining a database with dynamic passwords

In this case, random passwords are generated and stored in the user's browser. For example, if the password for the www.banktest.com website are saved, the credentials will be considered valid only if that URL is displayed. If anything is changed in the URL, credentials will not be validated. There are engines that have this option available (e.g. Firefox), storing passwords by encrypting them, but this feature is not enabled by default.

c) Using virtual keyboards

This procedure was preferred in the 1990s. Instead of a traditional hardware keyboard, users use a virtual keyboard that appears on the screen, assuming that attackers will not be able to capture their activity. Currently, the method was abandoned because of several "effective" variants of intercepting a screen and a virtual keyboard.

d) Educating staff

Most companies carry seminars and workshops with specific security issues, in order to increase the educational level of employees. It can be a step towards a culture of security awareness, even if some employees do not treat seriously such a step. In response to criminals having begun writing in almost perfect English, a method of education should consist of teaching instructions in English. Knowledge testing frequency is is a key factor in raising employees' education and security levels.

e) Building website extension

Several companies (e.g. Internet Explorer, Mozilla, Chrome, and Opera) have built toolbars for browsers to determine if a URL is fake or not. When a visited website is reported as "phishing", the user is warned about this risk on a red background. If the site is only under suspicion, yellow is the warning color. Currently some sites use so-called "extended validation" which implies a new type of certificate sold only after the information is checked very carefully. If a toolbar in the browser finds this type of website, the color is green.

f) 2FA-two factor authentication

This method requires a two fold authentication: identifying the name with a password, and using information that only the user knows. This can be generated by a physical token as unique codes that are valid only for a short period of time and non-reusable. In Europe, most banks use this technology to authenticate customers for online services. To connect to an online account, a username and a code generated by the device, which in its turn is protected by a PIN, are required. Authorizing the payment is also handled by introducing a code that is based on transaction details. Lately, token hardware has been replaced by software versions available on mobile operating systems. (e.g. Andoid, iOS, Blackberry sau Microsoft Windows) Although it is a very secure authentication and authorization method, users may find tedious and time-consuming.

However, there are banks that invest in security to increase their customer's trust in online

transactions. For example, a pilot [7] project intends to replace the card's allocated CVV area required for online payments, with a small screen that provides a security code that can automatically change with some frequency - dynamic CVV.

g) Exchange of encryption keys to prevent dictionary-based attacks

Many researchers have proposed as a solution to the avalanche of attacks a new authentication protocol for exchanging keys, involving combining common public keys. This process occurs in such a way that, if the attacker is the middle man s/he cannot guess the information being exchanged. However, these protocols are difficult to implement and are considered time consuming.

6. CONCLUSIONS

Attackers are becoming more intelligent and versatile, using information from social media. They know who to target, what the weak links are, which elements are missing, and how to effectively set a trap. They have demonstrated that there is always an alternative. In a Salesforce case study from November 2007 [15], the attacked received the password from a staff member. Subsequently, customers began to receive bills and false bills. Consequently, if an attack on a target may fail, it can be redirected towards the latter's stakeholders, in the example above - the company's suppliers.

How does the future look like when such attacks are taken into consideration? It is difficult and very dangerous to make such predictions without a solid background and understanding of how such threats behave and without understanding the attackers' psychology. It is clear that attackers will generate never ending ways to get the information they need. Unfortunately, countermeasures generating industry will always be forced to take defensive measures and hence adopt a reactive stand. The best approach is to communicate clearly the premises of such an attack and the risks associated without the use of technical terms, so that everyone can understand. But what is the economic and social impact? What are the "real" losses registered by institutions, what is the number of aggregated attacks against users? What are the measures that must be implemented to limit them? Could the involvement of relevant bodies that could declare the financial and banking sector a critical infrastructure bring added value to the fight against crime and what would be the effects of such a decision? What other solutions are intended to be adopted? How to harmonize domestic proposals with European law? These are questions that require a very thorough analysis since they can seriously affect several of the current practices. Divergent points of view may converge or may provide alternative solutions and that is the way ahead in future research and studies on the field.

NOTES AND REFERENCES

I. Books, articles

[1] Ghid Amenințări generice la adresa securității cibernetice (Romanian for *Guide on Generic Threats to Cyber Security)*, www.cert-ro.eu/ecsm.php;

[2] Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2014 (Romanian for *Report on*

Cyber Security Allerts Processed by CERT-RO in 2014),www.cert-ro.eu;

[3] The Travel Guide to Email Fraud, returnpath.com;

[4] Adaptation after Bogdan Adrian Turliu's presentation,Cards Investigations Team, Investigations Department, 2015;

[5] Analysis made by Mircea Constantin Scheau and Bogdan Adrian Turliu for the period Q1 2010 – Q3 2015;

II. Internet Resources

[6] http://www.finextra.com/news/fullstory.aspx?newsitemid=27865&topic=security, last retrieved January 2016;

[7] http://www.finextra.com/news/fullstory.aspx?newsitemid=27917 last retrieved January 2016;

[8] http://www.hotforsecurity.com/blog/phishing-surges-file-sharing-takes-lead-as-most-targeted-industry-of-q1-13472.html, last retrieved March 2016;

[9] http://newsroom.mcafee.com/press-release/97-people-globally-unable-correctly-identify-phishing-emails - Intel Security, last retrieved February 2016;

[10] www.pymnts.com, last retrieved March 2016;

[11] Pymnts, 2014 Fraud Spike Cost US Retailers $32 Billion, 2015, http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/, last retrieved March 2016;

[12] Pymnts, "Global Fraud Attack Index",2016, http://www.pymnts.com/fraud-prevention/2016/benchmarking-hackers-and-their-attack-methods/, last retrieved March 2016;

[13] http://phishme.com/the-danger-of-sensationalizing-phishing-statistics/, last retrieved February 2016;

[14] https://returnpath.com/webinars/how-cybercriminals-cheat-email-authentication/, last retrieved February 2016;

[15] www.salesforce.com, last retrieved February 2016;

[16] Verizon,,,2015 Data Breach Investigations Report", 2015, last retrieved 2016;

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf, last retrieved January 2016;

[17] https://en.wikipedia.org/wiki/Kevin_Mitnick, last retrieved January 2016;

[18] https://en.wikipedia.org/wiki/Trojan_horse_(computing), last retrieved February 2016;

[19] https://en.wikipedia.org/wiki/Name_server, last retrieved February 2016;

[20] https://en.wikipedia.org/wiki/Internet_safety#Malware, last retrieved February 2016;

[21] www.cert.ro, last retrieved January 2016.