# The Growing Global Threat of Cyber-crime given the Current Economic Crisis: A Study regarding Internet Malicious Activities in Romania

**Ana Maria Tuluc, PhD in progress**
*Academy of Economic Studies, Bucharest, Romania*
*anamaria.tuluc@yahoo.com*

**Abstract**: Computer crime, also referred as cyber-crime, is considered today one of the main leading problems in the ongoing global economic crisis and an impediment in the development of many countries. **Objectives** of this work are: to determine the evolution of cyber-crime during the current economic crisis, to emphasize the severity of this problem and the urgent need to limit its impact worldwide, to determine consumers perceptions regarding this phenomenon in Romania. **Prior Work** related to this issue was conducted by the Computer Security Institute in United States, International Computer Protection Agency, Symantec and Ponemon Institute. In their studies, these institutions have revealed many of cyber-crime features and proposed valuable solutions for decreasing its impact. The **Approach** used in this paper was a survey among Romanian consumers regarding cyber-crime. A total number of 110 respondents participated in this survey. **Results** showed that almost 80% of respondents were victims of cyber-crime at least once and more than 87% of respondents never reported these crimes to the police. As regards **Implications,** the study can offer support to specialized institutions, while academics can use these findings for further research. The **Value** of this paper consists of relevant findings regarding cyber-crime issue in Romania.

**Keywords:** Computer crime; economic decline; Internet security; web-attack victims

**Jel Classification:** H12; L86; C89

## 1. Introduction

In a vulnerable economic context, computer crimes have become an important issue to be addressed by specialized institutions and private companies. Studies show that, nowadays, attack toolkits can be not only easily purchased but also can be installed by anyone, no matter his level of skill. As the economic crisis rapidly spreads worldwide, cyber-attacks increased, causing damages to businesses and households. Another factor which favoured the spread of Internet malicious activities was the increasing number of Internet users, which is today more than 360 million. As a result, fast Internet penetration represents for cyber-criminals just another opportunity to attack markets. The good side of this issue is that, as computer crimes continue to grow, businesses and end-users can gain a better understanding of the problem and develop counter attack solutions. In this paper, the author expresses the urgent need for reducing the evolution of cyber-crime phenomenon while emphasizing the current state of the economy. As a result, the paper brings to attention the consequences of further development of cyber-crime and its impact on the end-users. The article carries a population-based, cross-sectional survey, using a sample of 110 respondents. The survey was conducted in Romania, during October-December 2010. The purpose of this survey is to analyse the features of cyber-crime in Romania, while questioning the victims on several aspects: types of cyber-crimes, most common malicious activities initiated through Internet, the estimated time for solving the damages, the generated costs and, of course, the feeling aroused by these attacks. A second section of the survey analyses the response of cyber-crime victims as regards the reporting of these crimes to law enforcement. The final section describes the relationship between the response of cyber-crime victims and the socio-demographic characteristics of participants. The survey shows that people often encounter such problems, and choose not to do anything about it. The reasons are diverse, most of them considering the crime not serious enough to report it to the police while others choose to put the blame on themselves.

## 2. Basic Considerations regarding Cyber-Crime

Cyber-crime or computer crime is considered to be any crime that uses a computer and a computer network (Matthews, 2010). A basic definition describes cyber-crime as a crime where computers have the possibility of playing an important part (Thomas and Loader, 2000).

The main factor in cyber-crime increase is the Internet. By use of Internet, cyber-criminals often appeal to images, codes or electronic communication in order to run malicious activities. Among the most important types of Internet crimes we can mention: identity theft, financial theft, espionage, pornography, or copyright infringement. The cyber-crimes can be divided into two categories: the crimes where a computer network attacks other computers networks – e.g. a code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, intrusions (Svensson, 2011).

For identity theft, cyber-criminals often use phishing, a tool which facilitates internet fraud through detection of usernames, passwords or credit card information (Matthews, 2010). Phishing can be used in e-mails or instant messaging, which is why it is most frequently detected in online payments, Internet auctions or social networks.

Issues revolving around cyber-crime have become more and more complex. Computer criminal activities have grown in importance and institutions are more interested than ever in putting an end to these attacks. Progressions have been made in the development of new malware software, which can easily detect criminal behavior (Balkin et al., 2007). Moreover, high quality anti-virus systems are offered for free now in many countries at every purchase of a computer or an operating system.

## 3. The Impact of Economic Crisis on Cyber-Crime

The current economic crisis affected many financial institutions around the world, creating the premises for the development of the underground economy, also known as cyber-crime. According to Symantec, in 2009, the most targeted sectors by phishing attacks were: the financial sector and the Internet service providers sector. In the financial sector, more than 74% of the brands were used in phishing campaigns while in the Internet service providers sector only 9% of the brands were compromised through malicious online campaigns.

Globally, cyber-crime statistics have reached staggering proportions and many countries consider the Internet malicious activities as being one of the leading problems of the current economic crisis (Barnetson, 2009). In fighting the spread of cyber-crimes, Symantec is an important software provider, which enables confidence wherever information is used or stored. According to Symantec statistics, in 2009, more than 100 computer attacks were initiated every second (Fossi, 2010). In the report "State of Enterprise Security Report", Symantec places malicious codes among the most frequently used methods by cyber-criminals. Thus, statistics show an increase of 100% in 2009, comparing to 2008, of malicious code use worldwide.

Cyber-crimes not only affect households, but also large companies. These institutions deal almost every day with espionage, financial theft attempts or information leakage. According to the "Symantec State of Enterprise Security Report" in 2009, almost 75% of the companies surveyed had experienced some sort of cyber attacks a year before (Fossi, 2010).

Figure 1 presents the evolution of attack tool kits, as stated in the 2010 "Symantec Report on Attack Kits and Malicious Websites". There were considered for analysis only the last 3 years of economic crisis: 2008, 2009 and 2010. According to the statistics, in 2009 and 2010 there were developed more attack tool kits then ever before (Storey, 2010). This explains the severity of Internet malicious activities and encourages society' involvement in stopping the spread.

The image shows the development of only 2 attack tool kits in 2008: Fire Pack and 31.Fiesta, while in 2009 there were developed almost 15 attack tool kits. Among them we can mention: Crimepack, Siberia, Fragus or Liberty. A slight decrease was registered in 2010, when almost 7 attack tool kits were created: Zeus 2.0, Golod, Spy Eye, etc.

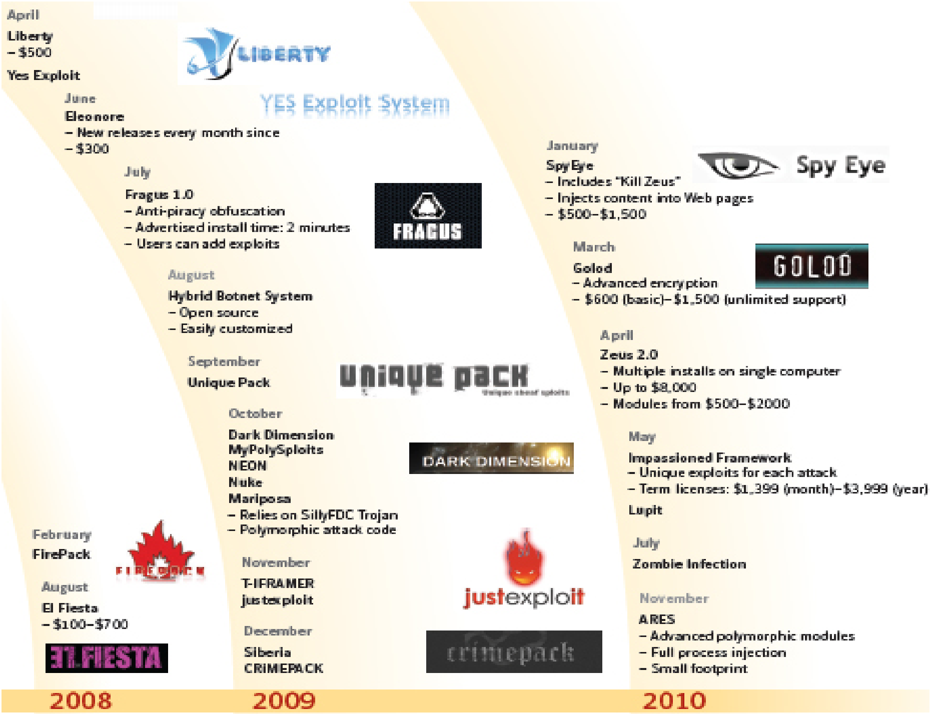


**Figure 1 Evolution of attack tool kits**

Figure 2 presents the evolution of malicious web pages per month. The information is extracted from the 2010 "Symantec Report on Attack Kits and Malicious Websites" and reflects the fluctuations of cyber-crimes during July 2009-June 2010. The period considered is marked by an important decrease at the beginning at the July 2009, followed by small increases and decreases. The evolution of malicious websites ends with another important decrease, emphasizing a possible ending of the economic crisis or a development of new software which prevents cyber-attacks.

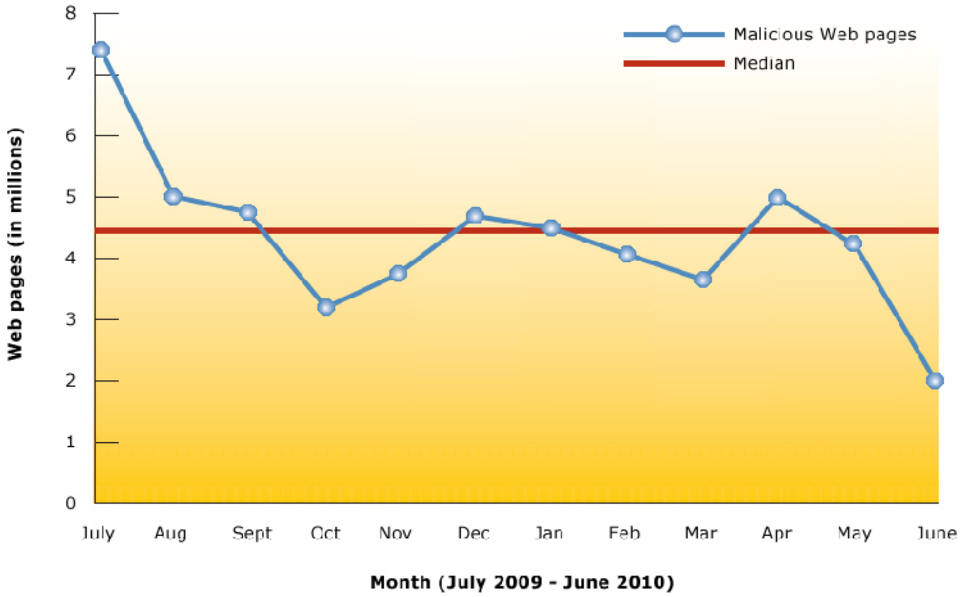


**Figure 2. Malicious web pages by month**

Figure 3 represents the result of a survey carried by Symantec and described in the 2010 “Symantec Report on Attack Kits and Malicious Websites”. The data consisted of a collection of unique search terms that resulted in visits of malicious websites. The top 100 search terms were ranked and ordered by their logical meaning.

The results show that an important number of malicious websites are in adult entertainment category, summing up to 44% of the search terms. This does not come as a surprise considering people attraction towards these movies. Studies show that more than 28.000 people visit these websites every second, which explains cyber-criminals interest in them.

The second category of malicious websites is video streaming, with 21% of the total. In the third category, other, there were included generic terms, not specific to one category in particular. This category reflects the variety of web pages found on the Internet.

Other categories considered in the study were: file sharing, software/technology, social networking, games, news/information and celebrities.

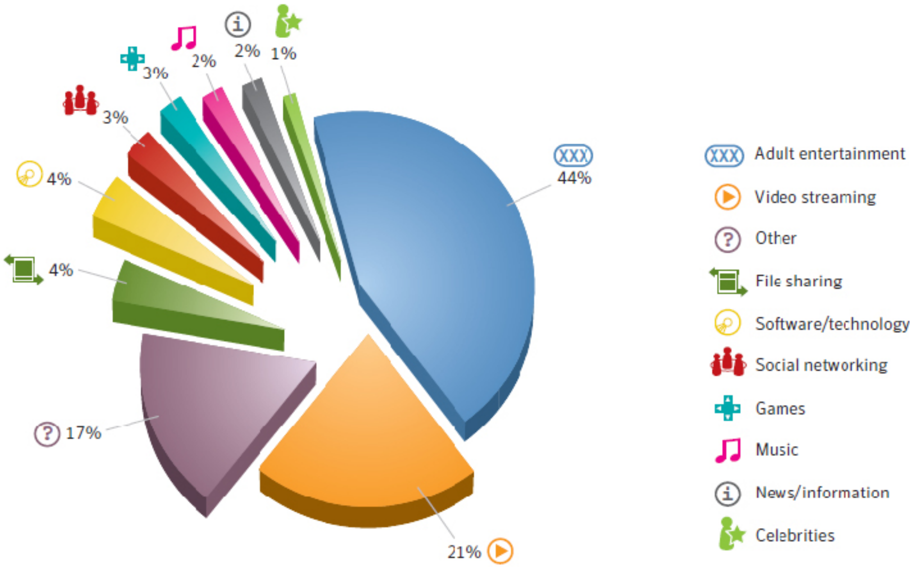


**Figure 3. Malicious websites by search term type**

The statistics presented indicate that web-based attacks have become one of the most common mechanisms for installing malicious code on computers. Usually installed through malicious advertisements, computers which host these codes can easily affect other users, regardless of their location.

As Internet has developed into a popular medium of communication, users tend to ignore its limitations regarding law enforcement procedures. This makes the Internet an easy target for cyber-crime on a global scale. Fighting against cyber-crime can only be done together, and therefore, countries need to establish international Internet laws while private companies need to cooperate with nonprofit organizations in order to develop strong communication campaigns (Şerban, 2011).

According to the ”Symantec Internet Security Threat Report” malicious activities tend to develop easier in Third World Nations because of the robust IT conditions and broadband infrastructure in these countries. Recently, even big countries like Brazil, India, Russia or China have had problems as concerns Internet security (Broadhurst and Grabosky, 2005).

Statistics say that Brazil and India represent nowadays the main source of web-based attacks, a more reason for countries worldwide to increase cooperation and establish strong relationships.

However, cyber-crime solutions need to address not only the governmental side but also the possibility of carrying sophisticated campaigns through world’s largest corporations and international institutions. Attackers will only stop if serious measures are taken globally, therefore discouraging malicious Internet practices.

## 4. Study Regarding Cyber-Crime in Romania

### 4.1. Purpose

The purpose of this study is to describe the current situation of Internet malicious activities in Romania, by studying consumer's perceptions through face-to-face interviews.

### 4.2. Objectives

The main objectives of this study are:

a. Determine the percent of cyber-crime victims.
b. Identify the types of cyber-crimes.
c. Determine the estimated time for solving cyber-crime damages.
d. Determine the cost of cyber-crimes.
e. Identify the feelings aroused by cyber-crimes.
f. Determine the response of cyber-crime victims.

### 4.3. Methods

A population-based, cross-sectional survey was conducted among Romanians, during October-December 2010. The method used to collect data was the questionnaire. In order to assure the relevance and correctness of the data, the questionnaire was at first conducted on 5 persons, which were not included in the final sample. Their purpose was to test the level of understanding of the text.

The questionnaire had a number of 13 items: the first two questions were preliminary, the following 7 questions regarded cyber-crime dimensions and the last 4 questions were demographic ones.

Having been a victim of malicious Internet activities was evaluated through the following question: "Have you ever been a victim of cyber-crime?" The questions regarding cyber-crime were related to the 6 objectives described above. The answers to the questions were measured through enclosed options.

### 4.4. Participants

A total number of 110 persons were involved in this study. Because the research focused mainly on the victims of cyber-crime, a final sample of 78 respondents was considered in the survey. In building the sample, the author used the random sampling method.

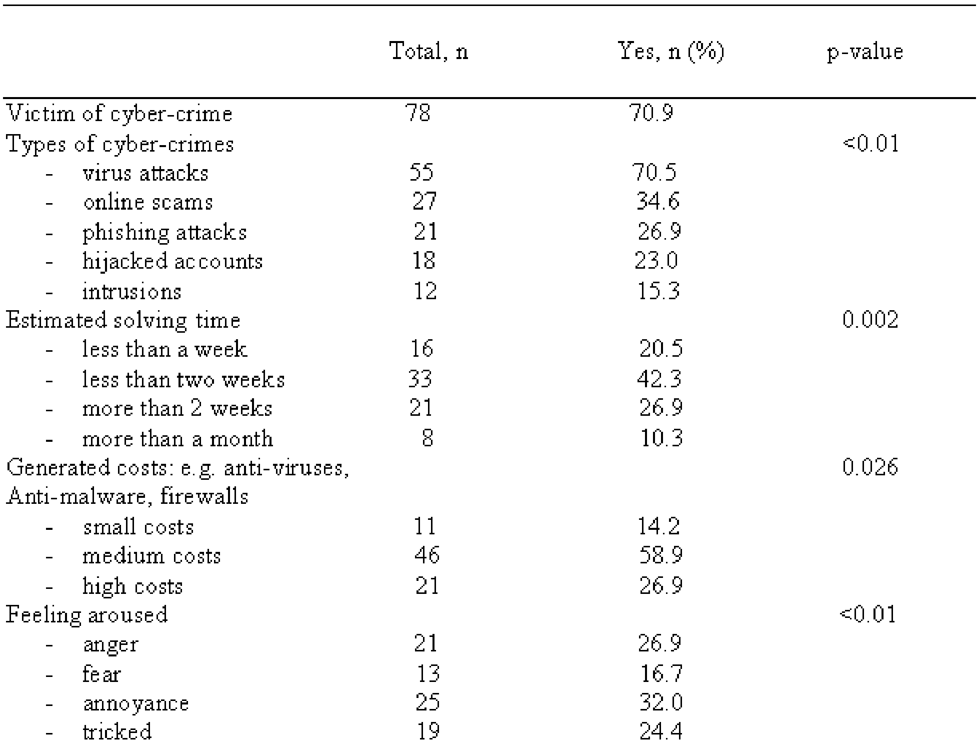
Data was obtained through interviews in public places and self-administrated questionnaires. Still, most of the interviews were carried in academic institutions.

The participants were encouraged to express their opinions freely, by given explanations and offering examples. Most of the respondents were young people, who used the Internet for entertainment and communication with others. Their IT knowledge was medium, but they all navigated the Internet at least once a day.

### 4.5. Data Analysis and Results

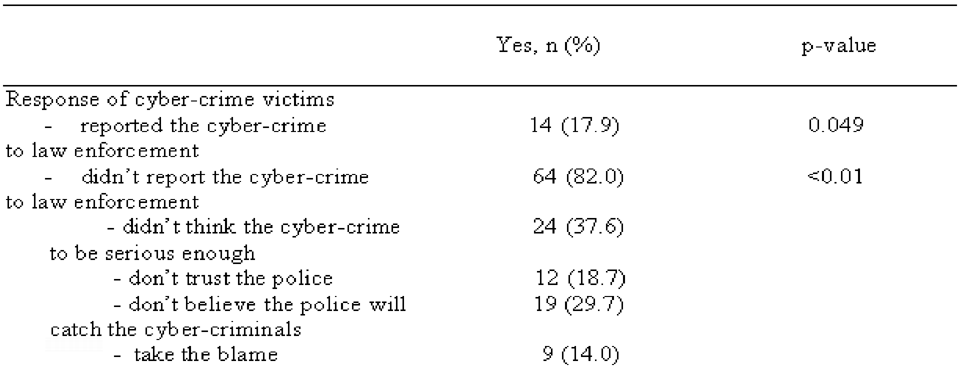
In conducting the research, the author used SPSS 13.0 software program. The findings revealed the number of persons who responded the question with a certain answer and their percent in the total population. The level of significance, p-value, was also determined. Afterwards, p-value was compared with the theoretical value of 0.05 in order to test the relevance of variables.

Figure 4 presents the characteristics of cyber-crime victims as they resulted from the survey. 70.9% of respondents admitted having been victims of cyber-crime at least once. Most frequently encountered cyber-crimes in Romania are the virus attacks (70.5%), followed by online scams (34.6%) and phishing attacks or identity theft (26.9%). The estimated time required for solving cyber-crime damages is less than 2 weeks (42.3%), the generated costs are medium (58.9%) and the most reported feelings were annoyance (32%) and anger (26.9).



| | Total, n | Yes, n (%) | p-value |
|---|---|---|---|
| Victim of cyber-crime | 78 | 70.9 | |
| Types of cyber-crimes | | | <0.01 |
| - virus attacks | 55 | 70.5 | |
| - online scams | 27 | 34.6 | |
| - phishing attacks | 21 | 26.9 | |
| - hijacked accounts | 18 | 23.0 | |
| - intrusions | 12 | 15.3 | |
| Estimated solving time | | | 0.002 |
| - less than a week | 16 | 20.5 | |
| - less than two weeks | 33 | 42.3 | |
| - more than 2 weeks | 21 | 26.9 | |
| - more than a month | 8 | 10.3 | |
| Generated costs: e.g. anti-viruses, Anti-malware, firewalls | | | 0.026 |
| - small costs | 11 | 14.2 | |
| - medium costs | 46 | 58.9 | |
| - high costs | 21 | 26.9 | |
| Feeling aroused | | | <0.01 |
| - anger | 21 | 26.9 | |
| - fear | 13 | 16.7 | |
| - annoyance | 25 | 32.0 | |
| - tricked | 19 | 24.4 | |

**Figure 4. Characteristics of cyber-crime victims**

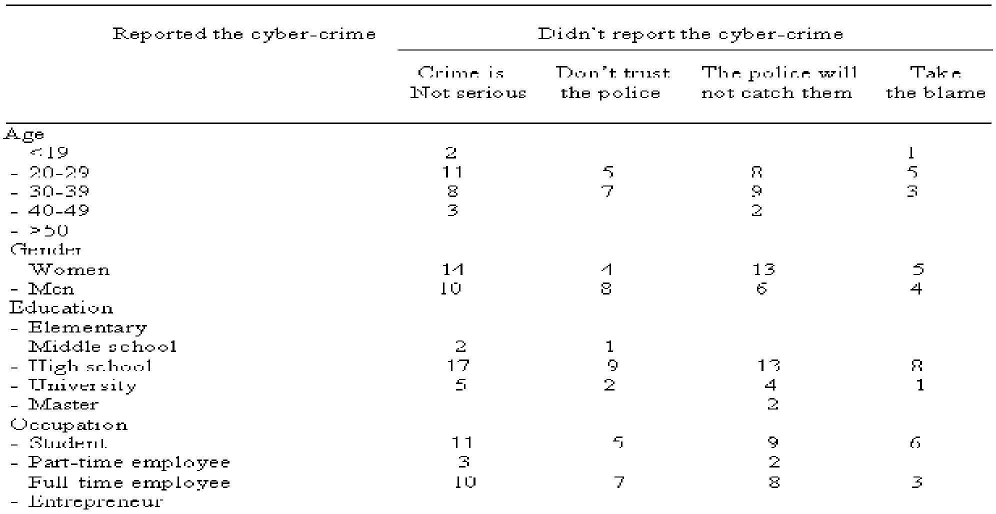


| | Yes, n (%) | p-value |
|---|---|---|
| Response of cyber-crime victims | | |
| - reported the cyber-crime to law enforcement | 14 (17.9) | 0.049 |
| - didn't report the cyber-crime to law enforcement | 64 (82.0) | <0.01 |
| - didn't think the cyber-crime to be serious enough | 24 (37.6) | |
| - don't trust the police | 12 (18.7) | |
| - don't believe the police will catch the cyber-criminals | 19 (29.7) | |
| - take the blame | 9 (14.0) | |

**Figure 5. Response of cyber-crime victims**

In figure 5, it is described the response of cyber-crime victims to web-attacks. Surprisingly, less than 20% of respondents chose to report the cyber-crime to the police. The reasons are various and mostly regard the importance of the crime and the relationship with the police.

Thus, most respondents consider cyber-crimes not serious enough to be reported to law enforcement (24%). They are followed by respondents who don't believe the police will catch the cyber-criminals (29.7%) and the respondents who don't trust the police (18.7%). Though the percent is small, 9% of respondents use to take the blame on themselves. They consider themselves to be guilty for not hading installed a Internet security software or for navigating on web pages they had suspected to be malicious.



| Reported the cyber-crime | Didn't report the cyber-crime | | | |
|---|---|---|---|---|
| | Crime is Not serious | Don't trust the police | The police will not catch them | Take the blame |
| Age | | | | |
| <19 | 2 | | | 1 |
| - 20-29 | 11 | 5 | 8 | 5 |
| - 30-39 | 8 | 7 | 9 | 3 |
| - 40-49 | 3 | | 2 | |
| - >50 | | | | |
| Gender | | | | |
| Women | 14 | 4 | 13 | 5 |
| - Men | 10 | 8 | 6 | 4 |
| Education | | | | |
| - Elementary | | | | |
| Middle school | 2 | 1 | | |
| - High school | 17 | 9 | 13 | 8 |
| - University | 5 | 2 | 4 | 1 |
| - Master | | | 2 | |
| Occupation | | | | |
| - Student | 11 | 5 | 9 | 6 |
| - Part-time employee | 3 | | 2 | |
| Full time employee | 10 | 7 | 8 | 3 |
| - Entrepreneur | | | | |

**Figure 6. Relationship between the response of cyber-crime victims and demographic characteristics**

The last figure, figure 6, presents the relationship between the response of cyber-crime victims to the web-attacks and their socio-demographic characteristics. According to the survey, most respondents -24 people- consider cyber-crimes not to be serious enough. These persons age is 20-29 and 30-39, they are mostly women, and they have graduated high school. Their occupation is learning, as 11 persons are students, and the others are full-time employees.

The second category, the respondents who don't trust de police, consists of mostly men, who graduated high school and work as full-time employees.

The third category includes the persons who think the police won't catch the cyber-criminals. This category consists of women – 13 persons, which are students – 9 persons or full-time employees – 8 persons. The last category is smaller, only 9 respondents, and includes persons who prefer taking the blame for cyber-crimes. They are mostly students, with ages 20-29.

## 5. Conclusions

The study presented shows that cyber-crime is an important issue for population. Its rapid increase is generated by the current economic crisis and the fluctuating social conditions. Although cyber-criminals are becoming more sophisticated every day, measures can be taken in order to prevent their development. Together, business and consumers can employ best practices to reduce risk and ensure Internet security. The latest technologies are implemented and new software is discovered daily. Companies can take advantage of these opportunities and include anti-viruses, firewalls and intrusion detection equipment among their security measures. Such strategies can educate the end user and discourage the spread of Internet malicious activities.

## 6. Acknowledgement

The author would like to thank all the respondents who participated in the study.

## 7. References

Balkin, J. M. et al. (2007). *Cybercrime: digital cops in a networked environment*. New York: New York University Press (NYU).

Barnetson, D. (2009). *Economic crisis 'to boost cyber crime':Microsoft*. Retrieved from http://news.theage.com.au/breaking-news-technology/economic-crisis-to-boost-cyber-crime-microsoft-20090417-a92m.html

Broadhurst, R. G., and Grabosky, P. N. (2005). *Cyber-crime: the challenge in Asia*. Hong Kong: Hong Kong University Press.

Fossi, M. (2010). *Cybercrimes's financial and geographic growth shows no slowdown during the global economic crisis*. Retrieved from http://www.techrepublic.com/blog/security/cybercrimes-financial-and-geographic-growth-shows-no-slowdown-during-the-global-economic-crisis/3653

Fossi, M. (2009). *Symantec Global Internet Security Threat Report. Trends for 2008*. Cupertino: Symantec enterprise security.

Fossi, M. (2010). *Symantec Global Internet Security Threat Report. Trends for 2009*. Cupertino: Symantec enterprise security publishing.

Fossi, M. (2010). *Symantec Report on Attack Kits and Malicious Websites*. Mountain View: Symantec enterprise security publishing.

Matthews, B. (2010). *Computer Crimes: Cybercrime Information, Facts and Resources*. Retrieved from http://www.thefreeresource.com/computer-crimes-cybercrime-information-facts-and-resources

Serban, C. (2011). Partnership in social marketing programs. Socially responsible companies and non-profit organizations engagement in solving society's problems. *Amfiteatru Economic*, XIII (29), pp. 104-116.

Storey, R. O. (2010). *Black Hats are Winning, Symantec Says*. Retrieved from http://www.pcworld.com/article/203287/black_hats_are_winning_symantec_says.html

Svensson, P. (2011). *Nasdaq hackers target service for corporate boards*. Retrieved from http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers;_ylt=AkCZAisq.eg0IMS_mDfpc4MjtBAF;_ylu=X3oDMTJpNmI1OW8xBGFzc2V0A2FwLzIwMTEwMjA1L3VzX25hc2RhcV9oYWNrZXJzBGNwb3MDMQRwb3MDMwRzZWMDeW5fdG9wX3N0b3J5BHNsawNmdWxsbmJzcHN0b3I-

Thomas, D., and Loader, B. (2000). *Cybercrime: law enforcement, security and surveillance in the information age*. London: Routledge.