How best to protect the user-individuals in Moscow from cyber crime attacks;

Imran Askerniya (PhD research student),
Hamid Jahankhani, Chrisina Draganova (Supervisors)
University of East London
School of Computing, Information Technology and Engineering
London, UK

Abstract:
This research which is still at it’s initial stages will examine the potential impacts of cyber attacks on Russian society and will determine a framework for pattern recognition from Russian cyber space to identify the major clusters of people’s knowledge and skills in protecting themselves against cyber crime.

The main aim of this research is to create the map of Russian society showing the more and less educated districts of the country. The researcher will identify what initiative is being employed to secure user-individuals.

The objectives of the research are therefore:
• To determine how best to protect the user-individuals from cyber crime attacks.
• To determine more specifically how such incidents are perceived and the possible effects this may have.
• To identify the clusters of people and explaining the similarities, differences and how the different clusters of people can be connected.

1. Introduction
Cybercrime is the world’s biggest growth industry and is now costing an estimated €180 billion loss to organisations and individuals, every year. The creation of ‘virtual identities’ gives a greater anonymity to the activities of organised criminals.

E-security is an issue of global importance and the methods cyber-criminals use are far-reaching, cunning and technologically advanced. Criminals search out the services of thrill-seeking hackers and ‘script kiddies’ to provide the expertise they need, which can be seen as a modern form of child labour.

The concern about cybercrime prevention has increased significantly among politicians, security specialist, academic institutions and legal professionals, with a staggering array of methods in an attempt to reduce the level of cyber criminal activities in the society.

In the EU and USA, the decision to focus on implications of technical methods for fighting cyber criminal is not arbitrary but comes from the need to do so after the 9/11 attacks. According to Suleyman Anil, who is in charge of protecting NATO against computer attacks, “Cyber defence is now mentioned at the highest level along with missile defence and energy security. We have seen more of these attacks and we do not think this problem will disappear soon”.

International money laundering is a particular concern in the arena of cybercrime as it can be used to finance and support criminal activities. Internet banking and digital cash are the most common ways of washing dirty money. Criminals try to hide and cover the sources from which their money comes by creating complex layers involving ‘social engineering’ - tricking innocent parties into divulging sensitive information. Phishing, Pharming, Spyware, Bin Raiding and Public Records Access are just some of the common techniques used by the criminals. Also, money
launderers are moving to exploit other poorly defended message transmission systems and emerging technologies, such as Voice over Internet Protocols (VoIP).

Phishing is an effective means of gathering valuable personal and organisation information. Phishing is one end of a two-ended criminal enterprise in that it is the gathering of the information and the second part is the utilisation of that information for criminal purposes. Phishing is mainly conducted through the medium of email given the ease of use and the relative anonymity of email use. Criminals are able to ‘mass email’ potential victims masquerading as their bank or other party who might have a legitimate interest in contacting them about financial matters. The emails are crafted in such a way as to appear as though the request for the information e.g. names, dates of birth, mother’s maiden name, account details etc. is being legitimately made. In reality it is not and many willingly provide this information only later to discover that they have unwittingly passed them to an identity thief. Once in possession of this information the thief can use it to steal an individual’s or organisation’s identity and divert money away from them.

Bin Raiding is a method of obtaining information applies equally to individuals and organisations. As the name suggests, a criminal can rout through dustbins to obtain valuable information about an organisation. This includes obtaining bank account and credit card details, computer passwords, letterheads, signatures and other information which either on their own or added to other information allow a criminal to gain access to an organisation’s accounts or those of its clients, trading partners, or suppliers. In a survey commissioned by the security company, Fellowes, it was estimated that 97% of households, approximately 21 million homes, disposed of information that could be exploited by identity thieves by throwing it in their household refuse, [1].

The internet is used for many purposes including paying bills, booking tickets and e-banking, Figure 1.

![Internet Users in the World](image)

**Internet Users in the World**  
**Growth Between 2000 and 2007**

Note: Total World Internet Users estimate is 1,319,672,109 for year-end 2007.  
Copyright © 2008, Miniwatts Marketing Group - www.internetworldstats.com  
Figure 1, Internet users Growth, Source, [2]
According to the general-colonel Boris Miroshnikov, chief of bureau for special technical undertakings at the RF Ministry of the Interior, only in 2007 about 12 thousand computer crimes were recorded, and more than 600 resources containing 'undesirable content' were closed. More than half are sites with child pornography and that is only the top of the iceberg [4].

The anonymous nature of the internet makes it possible for many individuals to engage into a variety of criminal activities in cyberspace. Hollinger (1988) conclude that individuals were more likely to be involved in illegal computer activity if they had friends who also were engaged in the activity.

These trends of crime could:

- Have grave social consequences for the society.
- Be of immediate concern to national government.
- Have a serious impact on the national economy.

![Figure 2, Internet users in UK; Source, [3]](image)

![Figure 3, list of services used, Source [3]](image)

<table>
<thead>
<tr>
<th></th>
<th>2004 Feb</th>
<th>2004 April</th>
<th>2004 July</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding information about goods or services</td>
<td>79%</td>
<td>73%</td>
<td>82%</td>
</tr>
<tr>
<td>Searching for information about travel and accommodation</td>
<td>69%</td>
<td>68%</td>
<td>68%</td>
</tr>
<tr>
<td>Using email</td>
<td>83%</td>
<td>86%</td>
<td>85%</td>
</tr>
<tr>
<td>Telephoning over the Internet/video conferencing</td>
<td>*</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>General browsing</td>
<td>63%</td>
<td>65%</td>
<td>62%</td>
</tr>
<tr>
<td>Finding information relating to education</td>
<td>35%</td>
<td>37%</td>
<td>33%</td>
</tr>
<tr>
<td>Buying or ordering tickets/goods or services</td>
<td>47%</td>
<td>50%</td>
<td>49%</td>
</tr>
<tr>
<td>Selling goods or services</td>
<td>5%</td>
<td>10%</td>
<td>8%</td>
</tr>
<tr>
<td>Personal banking and financial services</td>
<td>34%</td>
<td>37%</td>
<td>36%</td>
</tr>
<tr>
<td>Playing or downloading games</td>
<td>11%</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Using chatrooms</td>
<td>17%</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>Playing or downloading music</td>
<td>25%</td>
<td>27%</td>
<td>22%</td>
</tr>
<tr>
<td>Reading or downloading on-line news</td>
<td>24%</td>
<td>32%</td>
<td>26%</td>
</tr>
<tr>
<td>Listening to web radio/watching web television</td>
<td>12%</td>
<td>15%</td>
<td>17%</td>
</tr>
<tr>
<td>Downloading other software</td>
<td>20%</td>
<td>24%</td>
<td>20%</td>
</tr>
<tr>
<td>Downloading images</td>
<td>22%</td>
<td>27%</td>
<td>21%</td>
</tr>
<tr>
<td>Looking for a job/sending job application</td>
<td>20%</td>
<td>22%</td>
<td>23%</td>
</tr>
</tbody>
</table>

[Source: National Statistics, 2004, UK data]
In the face of these challenges, the criminal code of Russian Federation have produced the first piece of law, which includes the articles against cyber crime (The Criminal Code of the Russian Federation, Chapter 28, Federal Law No. 64-FZ of June 13, 1996 on the Enforcement of the Criminal Code of the Russian Federation).

Chapter 28. Crimes in sphere of the computer information

- Article 272. Illegal Accessing of Computer Information
- Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses
- Article 274. Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks

However despite the numerous attempts, there is a lack of an agreement in frameworks for either understanding or responding to these issues, their impacts and their interrelationships in Russia.

2. Cybercrime Profiling

Researchers from different disciplines have attempted to explore different dimensions of the issues surrounded cybercrime behaviour. To date however, despite numerous attempts, there is a lack of agreement on frameworks for either understanding and/or responding to these issues, their impacts and their interrelationships [5]. The lack of classification system is significant handicap and may be due to the considerable confusion that occurs around the very notion of what constitutes “Cybercrime” or computer – related crime and indeed whether it is new or old crime in a new bottle [6].

In order to develop useful profiles of different offender categories, a large amount of data is required and in order to improve the reporting of cybercrime, there are needs to increase the trust between the public and private sectors, which will result in reporting of cybercrimes when they occur. This will allow researchers to more precisely identify whether or not any unique patterns and characteristics actually exist.

In order to understand the new trends of the cybercrime and also establishing the appropriate framework that will be the foundation stone to investigate and prosecute the cybercriminals, there is an urgent need for cooperation and harmonisation of public and private sectors to encourage cybercrime reporting. Understanding the steps in the process of committing crime, and understanding the conditions that facilitate its commission, helps us to see how we can intervene to frustrate crime”[7].

Criminal profiling is the process of Investigating and examining criminal behaviour in order to help identify the type of person responsible [9]. The FBI’s Hayelwood and Douglas 1980, sited in Johnson 2005, [8], defined profiling as - *An educated attempt to provide...specific information as to the type of individual who committed a certain crime.... A profile based on characteristics patterns or factors of uniqueness that distinguishes certain individuals from the general population.*

To date, all the national security organisations depend on data and text mining techniques to detect and predict criminal activities, while data mining refers to the exploration and analysis of large quantities of data to discover meaningful patterns
and rules, [10]. Text mining, sometimes refers to as text data mining, is the process of analysing naturally occurring text for the purposes of extracting and non trivial patterns or knowledge from unstructured text [10]. The objective of many intelligence data analysis projects is to use data mining to find association and/or discover relationships among suspect entities based in historical data, while data mining analysis data from structured database, there is a large volume textual data (e.g e-mail, telephone conversation and text messages), which crime investigators have to examine which are unstructured.

Data mining is a powerful tool that enables criminal investigator who may lack extensive training as data analysts to explore large database quickly and efficiently. The following are some of the very common techniques;

a) **Entity extraction:** the process of identifying names, places, dates, and other words and phrases that establish the meaning of a body of text—is critical to software systems that process large amounts of unstructured data coming from sources such as email, document files, and the Web. By locating certain types of phrases and associating them with a category, applications such as text analysis software can perform functions such as concept extraction.

b) **Clustering technique:** group data Items into classes with similar characteristics to maximise or minimise interclass similarity- for example, to identify suspects who conduct crimes in similar ways or distinguish among groups belonging to different gangs [11].

c) **Deviation detection:** researcher deploy this technique to detect fraud, network intrusion detection, and other crime analysis that involve tracing some activities which can be appear sometimes to be abnormal.

d) **Classification:** finds common properties among different crime entities and organises them into predefined classes. This technique has been used to identify the source of email spamming based on the senders linguistic patterns and structural features.

e) **Social network analysis:** describes the roles of and interaction among nodes in a conceptual network. Investigator can use the technique to construct a network that illustrates criminal’s roles, the flow of tangible and intangible goods and information [11].

In the case of cybercrime as there is a rapid change of the technology, therefore, cyber criminal’s behaviour may become dynamic. This change in behaviour will require a reclassification of the typology being currently used. Essentially, cyber criminal’s behaviour is evolving and changing overtime with experience where they learn from their actions, or from their friend’s experience, which will enhance their skills. The offender signature which is a repetitive ritualistic behaviour that the offender usually displays at every crime scene provides police an appropriate profiling tool, [8]. This will give the investigator the opportunity to understand the motivations that drives the offender to perpetrate such crime. This finding will result in assisting the researcher in the classifying of the type of perpetrator that is being sought.
It is important that we consider some of the more prominent theories of criminal behavior if we are to understand trends and patterns in criminal activity and if we are to understand the behavior of those sought by profilers. It would be naive to presume that the reason why most people commit crime can be found in just one theory [12].

3. Cyber attacks on Moscow internet society

Nowadays, the Russian Federation is a member of world web space. Moscow as a capital of the country is a pioneer in Runet by the web services in RF. Moscow users could use many services, such as online banking and online shopping, pay for the utilities and mobile phones, etc. Survey shows that the majority of banks from the list of Interfax agency (13) provide online banking. Moreover, around 30 payment systems such as "WebMoney", "Yandex Money" etc., provides the facilities for payment for goods and services. Surely, all these services where circulating the huge sums of money are under the strict attention of cyber criminals and that is why users should know how to protect themselves and their money.

This research aims to help to improve the security policy and show the weakest link in users’ knowledge about cyber crime and how to fight against it and by understanding legal system to protect themselves.

The main part of the research will be heavily rely on grouping (clustering and mapping) the Moscow cyber society through a questionnaire which is directed to all types of people from no IT knowledge to people within the IT industry. In this study Moscow is divided into four parts, by districts (East, West, North and South) and the internet society into the groups of knowledge and opportunity to countermeasures the cyber crime. The aim is to collect over 400 questionnaires which would provide a sound analysis through an Artificial Intelligent (AI) tool.

The questionnaire is divided into 4 sections to identify various aspects of the recipients;

1. General Information. This section identifies the recipients’ gender, age, location and the qualification

2. The security tools. Here we are identifying the recipients knowledge about the security tools and theirs operating skills. The data obtained in this section would help the researcher to create the conception of spread of the security tools in Moscow cyber society.

3. Legislation system. In this section the researcher needs to identify the basic recipient’s knowledge in the Russian legislation system and users’ rights.

4. Cyber crime behavior. The 4th sections, identifies the users’ experience and knowledge in cyber criminal behavior including the understanding of Internet frauds and the methods of cybercrime countermeasures.

The questionnaire consists of 28 questions in 4 sections and different types of questions are employed as follow;
Open questions [14]
These are useful in getting another person to speak. Sometimes they are statements: “tell me about”, “give me examples of”. Quest.6, II sec: We will be very appreciating, if you could explain why you DO or DO NOT prefer using a public computer in 2-3 sentences.

Closed questions [14]
These are questions that require a yes or no answer and are useful for checking facts. Quest. 4, IV sec: In you opinion the people in Moscow face the cyber crime more often, than people from other parts of Russia?

Specific questions [14] These are used to determine facts. Quest.10, I sec: Have you or your friends been the victim of one of the cyber crime, listed in the question 9?

Hypothetical questions [14]
These pose a theoretical situation in the future. Quest.4 III sec: Unfortunately your computer was infected by any malicious code and you lose some important data. What is the main purpose of filling the application form to the police?
[ ] The fact of infection.
[ ] The harm had been done by virus.
[ ] The virus writing is not prosecuted by Russian laws.

This mixed type of questions will be more effective in achieving the project aims. Also it will give us wider look to investigating problem.

Conclusions

This investigation is quite new and progressive, because nowadays the internet is wildly used for work, shopping and entertainment and the enormous amount of data transmitting all over the world every day. In this case even the single user has had some skills about the cyber crime and cyber legislation. This research project allows finding out the different clusters of people and analyzing their knowledge in cyber crime and legislation system.

References


