Primakov Nikita Alexandrovich
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

UNAUTHORIZED ACCESS TO INFORMATION WHILE WORKING IN THE NETWORK

Abstract: *The article is devoted to one of the most common crimes in the field of computer information - identity theft. This paper investigated the behavior of e-Commerce users in order to detect identity theft.*

Keywords: *Information system, identity theft, e-Commerce, crime, security.*

Примаков Никита Александрович
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ПРИ РАБОТЕ В СЕТИ

Аннотация: *Статья посвящена одной из самых распространенных преступлений в сфере компьютерной информации - кража личных данных. В данной статье было исследовано поведение пользователей электронной коммерции с целью выявления кражи личных данных.*

Ключевые слова: *Информационная система, кража личных данных, электронная коммерция, преступление, безопасность.*

Introduction

One of the fastest growing cybercrime which could causes large indispensable costs and financial loss is identity theft. The cybercrime occurs due to failing of protection measures to meet the ends. Also there are some psychological and emotional impacts on the people which are attacked by identity theft.

Many companies and governments play a big role in preventing theft, but there is still a significant gap that consumers can fall victim to. This leads to consumers having to become defenders of their property. In other words, consumers need to be educated to understand the key factors that can have a big impact on identity theft. Since they are the owners of the certificates, each online user must protect his identity. Identity card holders are responsible for using their identity legally for everyday purposes. Recently, there has been a rapid increase in the crime of identity theft, which tells us about the Rationale of the study of this problem. Proper care must be taken to protect the identity of consumers and it is also their responsibility to take action to prohibit any data breach.

Identity theft as a fast-growing problem

One of the rapidly developing problems of cybercrime, which can lead to large costs and financial losses, is identity theft.

In order to detect identity theft, it is necessary to analyze the behavior of users on different web platforms. «Electronic commerce (e-commerce) is a business paradigm which evolve very fast recently» [1, p.1]. Due to the widespread use of e-Commerce and banking services, which leads to the accessibility of large quantities of important data, there has been a significant increase in identity theft and fraud. There are several large online databases that store sensitive user data with their Bank and credit accounts. These databases are susceptible to hacker attacks. Due to the Increase in Internet banking and shopping sites, where there is a transfer of confidential, personal and financial data over the Internet, are prone to hacker attacks. However, each user of such information systems should be aware of the possible risks associated with cybercrime. Most of the cybercrimes related to identity theft occur among students because they use the Internet more frequently than the general population. For example,

many educational institutions have their own information systems with personal information about all students who are also prone to identity theft.

The main purpose of the study [1] was to identify factors that contribute to the prevention of identity theft among e-Commerce users. Comprehensive, understandable and applicable models are included to estimate the prevention of identity theft among the e-commerce users. Therefore, each holder of an identity card is obliged to protect their data. A user, holding an identity card, may apply for an identity card, which may be used in a variety of financial and social activities. Thus, one of the main duties of the identity card holder is to keep it safe. Figure 1 shows a conceptual model of identity theft where one can see the independent variables like physical security, online security, account monitoring, offline risk, online risk and victimization.

Figure 1 - Identity theft conceptual model

As the author notes in the article [1], physical security is a security action aimed at blocking the access of users who do not have the authority to physically access data. Thus, physical security has a negative impact on the frequency of identity theft, which is the first hypothesis in the study.

Online security is closely related to the behavior of users on the Internet. Therefore, every user should be aware of threats and fraud on the Internet, as well as how it can damage the privacy of personal data. This means that every user should be aware of the protection measures. In that way, Internet security has a negative impact on the frequency of identity theft. Account monitoring is one way to prevent identity theft or other online threats. Regular account monitoring may help users identify some fraudulent activities. Account monitoring has a negative impact on the frequency of identity theft. In the absence of physical security, offline risk can lead to identity theft

or other fraud. Any risk behavior could lead to likelihood of identity theft despite it is offline behavior. Offline risk has positive influence on the crime frequency. Online risk is always active when users are online. Identity theft is one of the common phenomena during online shopping or e-Commerce. Online risk has positive influence on the crime frequency.

Victimization is a way to make absolutely any e-Commerce user a victim of data theft or fraudulent activity. Therefore, in order to reduce the likelihood of victimization, it is necessary to study the main threats to users of data leakage. Victimization has positive influence on the crime frequency.

Unfortunately, students are very prone to fraudulent behavior and identity theft, so the author in his study [1] examines them in relation to the behavior of e-Commerce. In his research, the author used data sets, which based on world Bank databases and EuroStat databases. The main goal is to eliminate all kinds of factors that could lead to fraud and identity theft of students in the field of e-Commerce. Moreover, among the six independent variables dependent variable-identity theft may be distinguished.

Object-oriented approach is an approach to the analysis and modeling of information systems [2]. The standard object-oriented modeling language is Unified Modeling Language (UML). UML is used to define, visualize, build and document an information system at the development stage. There are also various object-oriented concepts that may be used to design and model information systems. In the study [2], the authors simulate the e-Commerce system with a detection module data theft on the basis of the diagrams of cases.

As a model evaluation the standardized regression weight is used. On the basis of the results presented below in Figure 2, it may be concluded that the above hypotheses are confirmed. The first three hypotheses have a negative impact on identity theft, and the other three have a positive impact.

As the results in Figure 2 that at a higher level of physical security theft of personal data from the user of e-Commerce is reduced. Users of e-Commerce who follow the rules of Internet safety, less prone to identity theft. It is also important to note that the user of e-Commerce, which monitors good safety offline, are also less

prone to identity theft. The main conclusion of the results is that users need to reduce careless behavior when working in the electronic Commerce system, to prevent identity theft.

Hypotheses summary.

Hypothesis	Standardized regression weights
1. Physical security	−0.159
2. Online security	−0.151
3. Account monitoring	−0.275
4. Offline risk	0.197
5. Online risk	0.138
6. Victimization	0.172

Figure 2 – Hypotheses summary

Here is an example of the use of electronic Commerce with the module identity theft based on object oriented approach (Figure 3). We can see that the user can perform the purchases and payment using e-Commerce systems. However, you have to be logged to the e-Commerce system that may lead to identity theft. This model realized one identity module to prevent hacker attacks (Figure 3 The [3] shows an example of using the module identity theft. We see that the module may manage the user account. If it detects a suspicious behavior of the user, the module should prevent it.

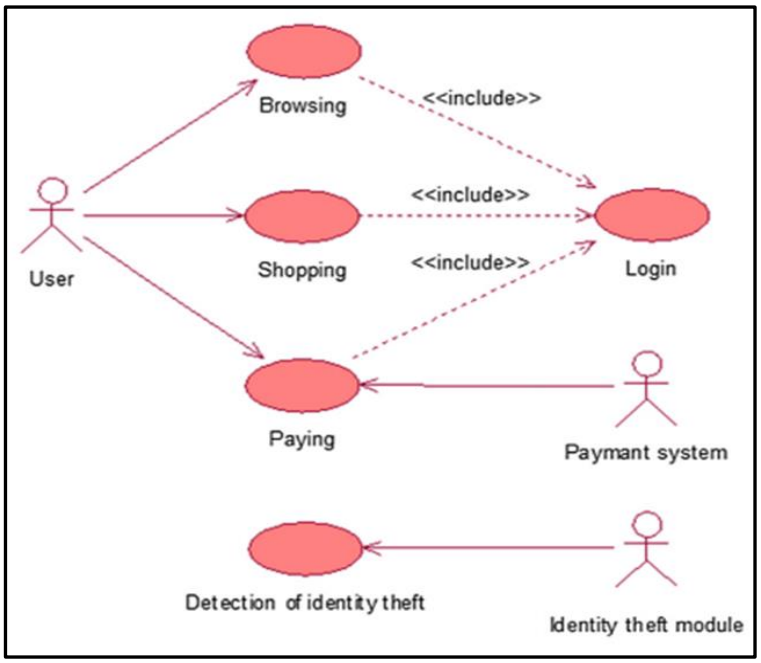

Figure 3. Use case diagram of e-commerce system with identity theft module

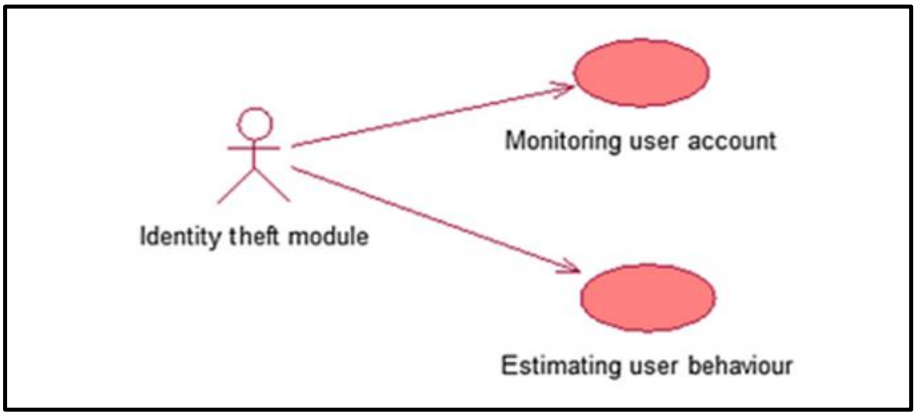

Figure 4. Use case diagram of identity theft module.

Conclusion

One of the main goals of the researches' overview is to contribute to the reduction of identity theft for users of electronic commerce. One of the most important aspects to prevent identity theft is careless behavior of users in information systems. However, unsafe user behavior associated with the level of education of users. Based on the results, a user needs to exert more effort to protect their identity in information systems. The information system presents the object-oriented approach which involves monitoring module of the identity theft. The module should track and evaluate user behavior in the electronic Commerce system. Based on the user behavior, the module should prevent the manipulation of data and identity theft.

REFERENCES

1. Analyzing of e-commerce user behavior to detect identity theft: site ScienceDirect. [Electronic resource]. – URL: https://ezproxy.urfu.ru:2123/science/article/pii/S0378437118309312 (date of issue: 16.12.2019).

2. Object-Oriented Modeling (OOM): site techopedia. [Electronic resource]. – URL: https://www.techopedia.com/definition/28584/object-oriented-modeling-oom (date of issue: 16.12.2019.)

3. Conceptual framework: site Wikipedia. [Electronic resource]. – URL: https://en.wikipedia.org/wiki/Conceptual_framework (date of issue: 16.12.2019).

4. Identity Theft: site Investopedia. [Electronic resource]. – URL: https://www.investopedia.com/terms/i/identitytheft.asp (date of issue: 16.12.2019).