INTERNET FRAUD: ESSENCE, TYPES, MEASURES OF PROTECTION

Oleg SOMOV
Department of Software Engineering and Automatics, TI-219, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova, Chișinău, Republic of Moldova

Corresponding author: Somov Oleg, oleg.somov@isa.utm.md

Abstract. *This article has a purpose to describe phenomenon of internet fraud, what technical measures and manipulative techniques use internet fraudsters, types of internet fraud that are generally distributed and measure of prevention and protection from internet fraud.*

Keywords: *cybercrime, fraud, information, social engineering, the internet*

Introduction

Nowadays, the Internet became a powerful instrument of making money, where people by virtue of their talents and abilities can earn a fortune, but there is the reverse side of this phenomenon – internet fraud – way of use of the Internet to propose obviously false information to extract benefits, in particular, stealing money or user's personal information. This type of cybercrime became a serious problem for internet users around the world and a terrifying issue for states with developed economy, where processes of computerization and digitalization are done. According to Internet Crime Report made by Internet Crime Complaint Center, in 2019 victims of internet fraud lost over 3.5 billion dollars [1]. Actuality of this theme rises with each year, because with spreading of the Internet, new internet fraudsters with new instrument of tricking appear and it cause increasing of economic losses.

Essence of internet fraud

At the moment, internet fraudsters own a wide range of instruments that give them significant opportunities in their criminal activity, guarantees them anonymity and avoidance of all types of punishment. On the Internet they have no restrictions and can be found everywhere. Internet users can encounter with internet fraudsters in every place of the Internet, where there is a possibility of communication between users: social networks, chats, message boards, messengers, electronic mail. Due to the fact that such types of Internet services daily attract a lot of users and contain a lot of personal information that can help to commit a crime, they have become a prime target for cybercriminals.

It's also important to note the technical measures and instruments of this type of cybercrime. From simple tricks that are based only on victim's trust to very serious program and viruses that even specialist cannot detect: electronic mail, fake websites, "click baits", fake credit cards and charity funds. Most of these services and sites contain various hidden computer viruses like web scripting viruses, that spread through webpages and browser hijacker, that change settings on your browser [2]. All these programs are extremely dangerous not only for user's computers, but and for personal data, especially messages and bank information. Most of internet scammers permanently change their location, preferring place like internet cafes, where computers are used by a large amount of people during the day and prefer make financial operations, using cryptocurrency like Bitcoin, that provide them safety and anonymity for a long period of time, because traditional money operations on the Internet like bank transfer are easy to detect, so police with help of measure of tracking can discover location of cybercriminal with ease. The harder and more complex measure the less it arouses suspicion among ordinary users and create greater chance of successful crime.

Despite the fact, that technical measures of these fraudsters are defining in their activity, the other measure of impact provide them success – social engineering. Social engineering is a manipulation technique that exploits psychological manipulation to achieve goals: click on the link,

mail, giving private information in order to perform a crime [3]. Preparation for act of influence can began long before interaction with the victim: from collection of facts and contacts of victim in order to increase efficiency of manipulative act. Uses of techniques of social engineering depends on not only prepared information, but on the current situation, therefore they prepare some special techniques that founded on human's emotions and concepts: trust, fears, curiosity, excitement, anger. These techniques include: phishing – message that want to create sense of urgency, curiosity for victims [4], baiting - a false promise to pique a victim's greed or curiosity, scareware – permanent message of alerts.

Types of internet fraud

Understanding that message you are reading is an attempt of fraudsters to get your data and money is essential part of protection from internet fraud, so knowing main types of this cybercrime is key to defense. Types of internet fraud are dived based on areas of human life, so most of them are disguised as normal messages that we encounter during our daily life, but always present some detail that reveal true purpose of the message.

1. Email phishing scam – one of the most common type of internet fraud. Around of 22% of all data breaches in 2020 involved phishing attacks, furthermore 97% percent of users are unable to recognize a sophisticated phishing mail [5]. Email phishing scam include massive sending of electronic mails that encourage victims to open link to the website with malicious content. On those websites users are asked to input their contacts and personal information like password, bank information, contacts. Those websites contain a quantity of malicious content like viruses and trojans that begin process of infection of devices from the moment of opening of the website, purpose of this software is stealing data, especially tied with financial information. In those mails scammers tries to recreate sense of urgency, danger that victim's device is infected and they tried to save his information and help him to fix the problem.
2. Online dating scam – type of internet fraud that based more on advanced techniques of social engineering and acting. Main purpose of scammers is to trick victims through creation of false interest in friendship or romantic relationships. Hackers create fake profiles in social networks or in dating site, through communication they weaken vigilance of victim, at one moment they say about financial problems and say that they should solved urgent, so they ask for help and then, after they received money, disappear, deleting all accounts.
3. Online auction – type of internet fraud that is widely distributed on sites of e-commerce like eBay. Fraudsters selling goods that are not exist or selling one item to several people. Once, money for good delivered, fraudsters cut all contacts with victims or refuses to return money
4. Advance-fee scam – one of the oldest type of internet fraud that appeared with services of electronic mail, also known as "the Nigerian prince scam", because most of scammers that prefer this type of fraud are situated in Africa, especially in in large city agglomeration with access to the Internet like Lagos. In this type of scamming victims proposed to invest or borrow amount of money so they later receive a greater amount. Most of these scammers pretended to be bank workers or lawyers that want to help victim to receive access for a large amount of money that is belong to victim for little financial help. In most cases, they don't break contact with victims and continue to ask for money, referring to the fact they have problems in achieving the goal, so they need more money and time to end this.
5. Lottery fee scams – this type of fraud is especially dangerous because it mostly spreads through targeting advertisement, so it can be found even on trusted website. Through message victims is reported that is a winner in lottery or in contest. The prize variety from a small sum of money to expensive items or luxuries: smartphones, cars or even property.

For receiving the prize victim should click on the advertisement with hyperlink on the site where is reported that before receive a prize, user should pass the registration form where he should write sensitive form of data: real name, bank information, address of living.

6. Fake charity fund – this type of fraud based on emotion of victim, making believe that through his donate he can rectify hard situation of other people. These types of fraudsters pretend employees of charity funds that make a company of donations to help people in danger or in plight. In the message they describe all adversities that region or vulnerable part of society are going through causing pity and compassion of victim, said that only urgent donation can solve the situation.
7. Identity theft – on the Internet people don't shy to share personal information, most of website include advanced protection of personal data, but sometimes thought gaps in defense hackers receive access to large database of user's private information that includes: contacts, photos, videos, private messages. Using this information allows fraudsters blackmail and make psychological pressure to the victims, demanding need information, documents and data.

Measures of protection

Despite the fact, that internet fraudsters use latest methods and psychological techniques exist some measure that will help users to keep their financial and private information in safety. The easiest is not to rush, user should analyze content of message and by knowing signs of internet fraud he can avoid danger of leaking data. Most of electronic mail services are tooled up with automatic algorithm that scanning received mail based on determined pattern and defines danger of internet fraud by deleting message or sending it into a category of spam. Brand-new way to protect account data is two-factor authentication that make process of logging into account longer, but safer by using not only login and password to identify user, but the confirmation from the other source: email, telephone message, special application, generated code. If defense of your account breach, this method will stop most of hackers without special preparations. The most of internet frauds are working on the site with malicious or illegal content, so avoiding these websites will help users in avoiding encounters with the most types of internet fraudsters.

Conclusions

Development of the Internet provides a lot of possibilities in communication, storing important information and data, financial operations, but it also challenges its users. Digital literacy became essential part of protection of our personal information and data on the Internet. This discipline received an impetus in development, because of activities of internet scammers. With the promotion of technological progress, fraudsters find new ways to perform their crimes, but through learning signs of danger, through identification of new types of scam we can create more protected and safer place for communication, for spreading new ideas on the Internet and decrease financial and psychological losses from internet fraud.

References

1. Internet Crime Complaint Center IC3, *2019 Internet Crime Report* [online]. [accessed 06.03.2022]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf
2. What is a computer virus? [online]. [accessed 04.03.2022]. Available: https://www.proofpoint.com/us/threat-reference/computer-virus
3. What is Social Engineering? [online]. [accessed 04.03.2022]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
4. Social Engineering [online]. [accessed 05.03.2022]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/
5. MEHARCHANDANI D. *Staggering Phishing Statistics in 2020* [online]. [accessed 05.03. 2022]. Available: https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/