GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 10, Issue 2, Feb. (2022)

SOME OF THE CRIMES COMMITED ON THE INTERNET, LIABILITY AND PREVENTION

Durdubaeva Nargiza
Korakalpok State University, Direction Jurisprudence,
Specialization-Criminal Law Application Theory and Practice 2-Year Master's Degree

ANNOTATION

This article gives you a brief overview on information technology crime. It also provides advice and information on possible criminal activities over the Internet and how to prevent them. The Criminal Code of the Republic of Uzbekistan also contains articles on criminal cases in the field of information technology and their classification.

Keywords: information technology, internet, cybercrime, website, sms, internet payments.

INTRODUCTION

We now live in a time when the Internet has become an integral part of people's lifestyles. People can now access information from the Internet for almost everything they do. Teachers can teach their students online, accept assignments, and provide grading in a transparent manner. In addition, students can learn thousands of world-renowned professions from training and research papers, depending on their field and interests. Now, like many countries, we have e-government, which means that government agencies and non-governmental organizations all use the Internet to work with documents. we are coming. In short, the Internet has taken over and taken over all areas. As a result, some fraudsters have resorted to online fraud. That's because there's a lot of information out there on the Internet. And again, these would mean that you have to spend for these processes. The vast majority of users, who do not understand the Internet very well, make it easier for fraudsters to work. All the crimes we are considering now are crimes that can be committed over the Internet.

The Concept of Crimes in the Field of Information Technology

With the constant development of information technology and the emergence of the Internet, the concept of "Information Technology Crimes" was formed. The main difference between cybercrime is that some of them are committed using a computer (computer crimes), others through the Internet (cybercrime).

There are many forms of cybercrime and it is increasing with the continuous development of technology and the Internet. There are also a number of difficulties in detecting and exposing these crimes, one of which is the reluctance of citizens to report computer offenses to law enforcement agencies and the lack of legal knowledge in the face of computer crimes.

Some Types of Information Technology Crimes Can be Seen in:

- • Distribution of virus software;
- • Theft of confidential user information;
- • Stealing other people's intellectual property products;
- • Hacking other people's accounts on social networks;
- • Spreading false information, slander;

- • Incitement to inter-ethnic conflict or inter-religious hatred.
- • Illegal transactions with bank plastic cards (card details);
- • Internet fraud in the securities market;
- • Financial pyramids on the internet;
- • Crimes related to mobile communication;
- • Other crimes in the field of e-commerce.

Given the above examples, some recommendations can be made for Internet users to prevent unlawful offenses against them:

- - Access the Internet, use devices with special software designed to combat malicious activity, update them in a timely manner;
- - Use an operating system that has security updates installed, current versions of other software;
- - When using sites, pay attention to their appearance, web address: you may have entered a fake copy;
- - Uses personal information only from secure protocols
- Enter websites (usually the browser displays a block icon on a green background next to the address of such a site);
- - Do not use the same login and password on different sites;
- - Do not use passwords that are too light or easily guessed (date of birth, phone numbers, etc.);
- - If possible, in addition to entering a username and password, use double authentication, which requires entering a temporary code, usually sent to your mobile phone in the form of an SMS-message or "PUSH" notification;
- - Beware of unexpected or accidentally received e-mails, even if you know the sender, never open attachments inside or use links to such e-mail addresses;
- - Beware of e-mails that require account information (financial institutions almost never ask for financial information via e-mail), never send financial information through unprotected Internet channels;
- - When you receive messages from your friends encouraging you to make financial transactions or transfer financial information, you can use this information through other communication channels (personal meeting, phone call, voice messenger) check or clarify the identity of your interlocutor by asking control questions whose answers in extreme cases may not be known to third parties;
- - When making payments via the Internet, if possible, use additional payment security technologies such as 3D Secure for international payment systems Visa and MasterCard;
- - Never talk on the phone with strangers who introduce themselves as bank employees and ask you to provide your bank card information;
- - Keep your bank card information in a safe place, do not tell it to anyone, do not report or send via SMS, etc .;
- - Limit the circle of friends and relatives to keep your notes. Never share your personal information with new online friends. Avoid spreading information about birthdays, email addresses, or pet names that can be used as passwords. All of this information can be very useful to a professional hacker;

- - "Attention! Your account has been hacked. You will need to call to confirm your account. Send us a message, we will call you back ";
- - Don't fall victim to click jacking. This is the kind of cyber attack in which they contain hyperlinks that at first glance look like harmless content. However, clicking on a hyperlink can lead to malware that could invade your computer or transfer your personal information;
- - Carefully consider URLs on e-mail addresses and on the website, even if they contain the names of reputable financial institutions with which you work. the most common scam is a combination of a legitimate website name and a fake one. These addresses often lead to copywriting sites that hide the fact that they are legally linked to hacking activities. Sometimes a URL can be legitimate, but when you click on a link, it will take you to another site.

Of course, there is every crime for which punishment is inevitable. The above-mentioned crimes are also punishable under certain articles of the Criminal Code of the Republic of Uzbekistan. Chapter XX of the Criminal Code deals with crimes in the field of information technology. In this chapter, those who violated the law under Articles 278^1, 278^2, 278^3, 278^4, 278^6, 278^7 will be prosecuted. Let's look at some examples of responsibilities for them.

Violation of the rules of informatization, ie the creation, implementation and use of information systems, databases and banks, information processing and transmission systems, and the unauthorized use of information systems without taking the necessary protective measures is a violation of the rights of citizens or the law, causes significant damage or serious harm to the protected interests or the interests of the state or society,

- Is punished by a fine of up to fifty times the amount of the basic calculation or correctional labor for up to one year.

If the actions were committed with a large amount of damage,

• Shall be punished by a fine in the amount of fifty to one hundred times the amount of the basic calculation or correctional labor for one to two years.

Creating computer programs or making changes to existing programs for the purpose of unauthorized deletion, blocking, modification, copying or retrieval of information stored or transmitted on a computer system, as well as special production of virus programs, their intentional use, or their deliberate distribution.

• Is punishable by a fine of 100 to 300 times the basic calculation amount or restriction of liberty or imprisonment for up to 2 years.

In short, everyone is responsible for a criminal case, whether it is public or online. It is not for nothing that the above-mentioned cases are heard or witnessed during the day. So we also need to have enough knowledge and skills to protect ourselves and our information from criminals. If this happens to us, it is the duty of each of us to act in accordance with the Criminal Code. Awareness is the need of our today.

LITERATURE

1. Criminal Code of the Republic of Uzbekistan. Chapter XX
2.https://iiv.uz/news/axborot-texnologiyalari-sohasidagi-jinoyatlar-va-ulardan-himoyalanish-usullari