UOT: 342.7.

Nargiz HAJIYEVA
"Information Law" specialization, master's degree Faculty of law, Baku State University
e-mail: haciyeva.nargiz00@gmail.com

CYBERCRIMES AND WAYS TO PREVENT THEM

Açar sözlər: kibercinayət, kompüter, kibertəhlükəsizlik, tənzimləmə, bəyannamə, məhkəmə təcrübəsi, qanunvericilik, müdafiə.

Ключевые слова: киберпреступность, компьютер, кибербезопасность, регулирование, декларация, судебная практика, законодательство, защита.

Keywords: cybercrime, computer, cybersecurity, regulation, declaration, case law, legislation, protection.

After the most recent advancements in networks and the computer sector, the word "cybercrime" was coined. "The unauthorized use of any communication equipment to commit or enable the commission of any illegal act" is the definition of cybercrime. In the Criminal Code of AR, there is a separate chapter on cybercrimes. Illegal access to electron-computer information; creation, use and distribution of nocuous programs for electron-computers; infringement of service regulations on electron-computers, computer systems or their network are considered cybercrimes due to national legislation and they all have their responsibilities [3].

I. Ways to Prevent Cyber Crime Targeted at Personal Property

There can be many types of cybercrimes, and one of them can be phishing. Phishing is a common cybercrime that involves the creation of bogus websites and the transmission of fraudulent emails and text messages that look to be from a legitimate source [4; 300]. Through phishing, hackers attempt to gain sensitive information from victims such as online banking user names and passwords, email IDs and passwords, and other similar credentials by impersonating a trustworthy institution over electronic communication. The majority of computers have two or three 90-day trial versions of antivirus software. This is a need, not a choice. Make sure you are using a tool to prevent viruses from infecting your computer system. Damage caused by viruses is sometimes referred to as the "payload." The majority of computer viruses travel from one host to another like a bacterium. These self-replicating viruses are often programmed to attack as many hosts as they can, and they may also be told to remove, transfer, or delete your data, along with your operating system, leaving your computer useless. You risk damaging your machine if you don't utilize anti-virus software. You will ultimately require a variety of programs, most notably antivirus software.

Another way is called a program to detect spyware which is very new and can be spread through a number of different techniques. A spyware program's main objective is to enter your computer without your knowledge or consent. Once installed, spyware gives the computer instructions to send data about your internet use to another system or to reroute you to a website. Some spyware, possibly a manual for marketing, is comparatively safe. By repeatedly rerouting your browser and/or displaying pop-up windows, other malware is more bothersome. It is quite terrible that certain individuals and computer code may install instructions without your consent. We must all have anti-spyware software on our com-

puters as a result of these efforts.

As personal property, intellectual property rights can be infringed. There are two methods for intellectual property rights safeguarding on the Internet. According to the first viewpoint, there is no need to defend intellectual property rights in cyberspace, which might stifle Internet development. At most, acknowledging a person's non-property rights suffices. The second approach, on the other hand, believes that it is vital to defend intellectual property rights in cyberspace, and it suggests the method of "collective administration of rights" to that end. When individual protection of copyright and associated rights is challenging, this strategy is utilized. In this instance, intellectual property objects are exploited, and the right holders are compensated in accordance with the established method [6; 4].

To resolve the aforementioned conflicts, the legal acts governing intellectual property rights must be revised. Because it would be more appropriate to establish a separate regulating system for material published on the Internet in order to safeguard the copyright on such work.

II. Ways to Prevent Cyber Crime Targeted at a Business

Every organization, business, and/or corporation has rules or processes for installing and maintaining software to secure its intellectual property, employee information, and employee communications, or at least they should. Firewalls, anti-virus software, anti-spyware software, and email spam filters are a few of these technologies that have been covered. In addition, a lot of companies use network intrusion detection software (NIDS). Corporate users, however, are the victims of malware or harmful software, unlike individual or family users. Malware is damaging software with malicious purpose. It can be viruses, trojan horses, worms, spyware, or other forms of malicious software. These unwanted and unwelcome software applications are made to infiltrate and harm computer systems, or, to put it another way, to bring a network or website server offline.

One of the several websites on the Internet that was impacted by a group of cyberterrorists in February 2000 that broke into the site and changed the program code was Amazon.com. Due to the severity of the issue, Amazon was compelled to suspend operations in order to rectify the harm and halt the illegal conduct. Program modifications were implemented as a result of the site shutting to aid in preventing future breakins [7; 7].

The Slammer infection, which appeared in January 2003, is one of the most notorious examples of malware. Including the Code Red, Blaster, Klez, and Nimda worms, the Slammer virus propagated more quickly than any other documented attack. Beginning with millions of copies, this Microsoft SQL malware multiplied roughly every 8.5 seconds. Almost 300,000 cable modem subscribers in Portugal were without service by the time the rest of the internet community started to notice the issue. The cell phone and Internet service providers in South Korea were in complete disarray, with several of them shut down for more than 24 hours. Flights on other airlines, including Continental, had to be canceled. Around $1.2 billion was predicted to be the cost of the global recovery.

Many think there are more losses than are disclosed. Too many companies decide not to disclose cybercrime out of concern about losing clients, receiving negative news, or losing employees. It is time for business executives who choose to conceal cybercrimes to face harsher punishments. Organizations that assist safeguard our online boundaries, such as the Association of Certified Fraud Examiners (ACFE—www.acfe.org) or the InfraGard group (www.infragard.net), require increased attention and engagement.

III. Ways to Prevent Cyber Crime Targeted at an Organization and Government Agency

Nonprofit and academic organizations, like corporations, must have rules and procedures in place to safeguard the rights of the organization, its staff, volunteers, students, and members. The best approach to stop cybercrime is to inform members about the specific policies and procedures that apply to your company. Companies must recognize potential weaknesses and potential exploitation.

According to estimates made by the American Justice Department in 2001, up to 85% of American businesses and government organizations had experienced hacking and other penetration attempts. Whether or whether that estimate is accurate, all governments are currently and will continue to be targets of cyberattacks. As a result, stringent regulations and guidelines must be put in place and followed. This must take place proactively, not after the fact.

The Veteran's Association's recent data leak serves as an illustration of how easily private information may get into the wrong hands. Each agency is in charge of what is necessary and needed, and the majority of them follow the rules set down for their particular agency. The ability to save data on the following devices is something that many agencies are learning. Hence, these tools are employed to replicate private, sensitive, or classified material.

IV. Recommendations on the prevention of cybercrime

Information security has traditionally been defined as the protection of information and the infrastructure that supports it against impermissible, natural or manufactured, accidental or purposeful threats that might harm the participants in the information interaction [1; 397]. In a nutshell, this idea encompasses the protection and defense of the subjects of information connections.

One of the most important forms of protection is through security software, which includes firewall and antivirus applications. All applications must be updated and patched. According to a Be Secure Online poll, users only update their security software every 8.5 months.

The second option is to use strong passwords. Passwords of eight characters or more with a mix of upper and lower case letters, numbers, and symbols are considered strong. Maintain passwords in a secure location and avoid using the same one for several services and accounts. Passwords should be changed every 90 days for maximum safety.

The next system preventative measure is to avoid using public Wi-Fi. While utilizing public Wi-Fi, one never makes online payments, transfer sensitive information, or enter critical account passwords. Cyber crooks set up networks that appear to be free internet but offer them access to your data.

Unsolicited emails and SMS communications should be avoided. Never click on a link, picture, or video sent to you by an unknown source. Verify to see whether emails are real; red flags include spelling errors, bad language, unusual phrasing, and urgent requests for money or action. Contact the sender directly to confirm communication. Verify the legitimacy of websites as well. Malicious websites may appear identical to normal sites, however, the URL frequently differs in spelling or uses a different domain.

Personal information should be kept private on social media. Social media is used by identity thieves to gather personal information that they may subsequently use in phishing schemes. Consider sharing personal information such as your name, home address, phone number, and email address with others.

Physical access to sensitive information should be restricted. While you are not present, turn off your computer. To keep private data safe, lock mobile devices and encrypt confidential data. Restrict who in your workplace has access to certain network drives.

Next way is using caution when using any equipment. Cell phones and other mobile gadgets are popular targets. Always keep an eye on your mobile gadgets and never leave them alone and visible.

Examine your bank and credit card statements on a regular basis. Identity theft and internet crimes can be mitigated by discovering them early, according to research.

Do not accumulate computers or digital data. Keep digital data organized and up to date by frequently purging files. In your office, have obsolete or useless computer hard drives securely destroyed.

In addition to these initiatives, the Council of Europe passed the Budapest Agreement on Cybercrime as a worldwide defense in 2001. The Convention states that its main objective is to persuade parties that the current Convention is necessary in order to prevent actions taken to compromise the confidentiality, integrity, and availability of computer systems, networks, and

data, as well as the misuse of such systems, networks, and data, by criminalizing such conduct and adopting measures sufficient to effectively combat such criminal crimes.

As an alternative, bear in mind the need to strike a proper balance between law enforcement objectives and observance of fundamental human rights, as outlined in the 1966 International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm everyone's right to hold beliefs without restraint. The 1981 Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data may also be included.

Taking into account the current Council of Europe conventions on cooperation in the criminal justice system, as well as comparable treaties between Council of Europe member states and other States, and emphasizing that the Budapest Convention is intended to supplement those conventions in order to improve the effectiveness of criminal investigations and proceedings involving crimes involving computer systems and data as well as the ability to gather evidence electronically [2; 2].

V. Case Law

A person gained illegal access to a nation's National Institute of Health network in 1999 [5; 5]. He gained access to the network by exploiting a backdoor he installed on the machine while working for the NIH. He downloaded papers including medical dosage recommendations for patients. A subpoena was issued for the computer's Internet Protocol address that connected to the NIH network. A search warrant for the individual's home was obtained. During the search, three computers were discovered and confiscated as evidence. Examination of the three computers revealed that he had unlawfully obtained material from the NIH, as well as child pornography. His attorneys attempted to suppress evidence at his trial based on search warrant processes. The evidence was permitted by the judge, and this person was found guilty.

List of used literature:

1. A. Aliyev, G. Rzayeva, A. Ibrahimova, B. Maharramov, S. Mammadrzali, Information Law, Textbook, Baku: Nurlar, 2019, 448 p.
2. Budapest Convention on Cybercrime, 2001, 22 p.
3. Criminal Code of Azerbaijan Republic, https://www.e-qanun.az/framework/46947#_Toc89058526
4. C. S. Biswal1 and S. K. Pani, Cyber-Crime Prevention Methodology, 2020, 312 p.
5. Cyber Crime: Its Impact on Government, Society and the Prosecutor, 29 p.
6. K. Imanov, Internet and Copyrights: Clash of Interests and Compromise Search, Baku, 2016, 59 p.
7. S. Kratchman, J. L. Smith, L. M. Smith, Perpetration and Prevention of Cyber Crimes, 2008, 22 p

Наргиз Гаджиева

Киберпреступления и способы их предотвращения

Каждый, у кого есть подключение к Интернету, рискует стать мишенью и/или жертвой киберпреступления. Другие утверждают, что интернет-угрозы, издевательства, убийства или «грабежи» более распространены, чем инциденты на углу улицы. Имея это в виду, вы должны принять упреждающие меры, чтобы защитить себя от эмоциональных, денежных или телесных повреждений. Вы должны защищать свое благополучие, личность, репутацию и себя. Вы тот, кто раскроет информацию о вас другим, либо напрямую через ваши ответы, либо косвенно из-

за вашего несоблюдения правил здравого смысла. В этой статье описаны шаги, которые вы можете предпринять, чтобы обезопасить себя и предотвратить личные киберпреступления.

Nərgiz Hacıyeva

Kiber cinayətlər və onların qarşısının alınması yolları

İnternet bağlantısı olan hər kəs kibercinayətin hədəfi olmaq və yaxud qurbanı olmaq təhlükəsi ilə üzləşir. Digərləri iddia edirlər ki, internet təhdidləri, zorakılıq, sui-qəsd və ya "soyğunçuluq" küçə küncündəki insidentlərdən daha çox olur. Bunu nəzərə alaraq, özünüzü emosional, pul və ya bədən xəsarətlərindən qorumaq üçün qabaqlayıcı tədbirlər görməlisiniz. Siz öz rifahınızı, şəxsiyyətinizi, reputasiyanızı və özünüzü qorumalısınız. Ya birbaşa cavablarınızla, ya da dolayısı ilə sağlam düşüncə qaydalarına əməl etmədiyiniz üçün haqqınızda məlumatı başqalarına açan sizsiniz. Bu məqalə özünüzü qorumaq və şəxsi kibercinayətkarlığın qarşısını almaq üçün edə biləcəyiniz addımları təsvir edir.