THE ROLE OF DIGITAL CRIMINOLOGY IN FORENSIC COMPUTER EXPERTISE AND LEGAL DOCUMENTS, REFORMS IN THIS FIELD

Medetbayeva Aqsungul Sharapatdin qizi

The Republican Center of Forensic Expertise named after Kh. Sulaymonova under the Ministry of Justice of the Republic of Uzbekistan Scientific research institute of forensic expertise PhD student of 12.00.09- Criminal proceedings. Criminology, investigative law and forensic expertise

Medetbaevaaksungul@gmail.com

Annotation: *This article focuses on digital forensics and technologies, that are becoming the most relevant nowadays, it talks about new technologies and digital forensics, legal documents in computer expertise, also, ensure the justice through digital technologies and the opinions of many scientists and members of international organizations are presented and analyzed in this article.*

Key words: *digital situations, digital forensics, computer crimes, cyber attack, statistics, information technologies, Beklasoft Evidence Center X, Pc-3000 Portable3, modern techniques, tools and legal documents.*

Currently, one of the main trends in the development of society is global digitalization. The relevance of the problem under study is evidenced by the fact that digitalization penetrates into all spheres of social relations, making it commonplace to use various modern information and communication technologies in everyday life. For example, starting with the Face ID scanner for identification of a person by specific characteristics of his/her face, and the fingerprint identification sensor.Touch ID, which not only allows you to quickly unlock your iPhone but also to pay for purchases with apps through a single touch.

After the situation of pandemic and coronavirus, in many countries, the isolation had forced by the government and people used digital products, modern information and telecommunication technologies as internet marketplaces and marketplaces for various online purchases, digital bank cards and bank quick payment systems, personal customer accounts of banks, taxpayers, distance learning platforms, etc [1]. As a result of this, the number of cyber attacks in many countries and the increase in crime through various technologies is one of the global phenomenas are continuing in this day.

People around the world use email for personal and professional communication, making email a target for cybercriminals and the most common vector for malware. In 2023, 35% of malware was delivered via email, and more than 94% of organizations reported email security incidents. The repercussions of cyberattacks are far-reaching and costly. A data breach costs $4.45 million on average. In 2022, compromised business emails accounted for $2.7 billion in losses. These alarming figures emphasize the danger of cyber vulnerabilities and highlight the need for skilled cybersecurity professionals. For example, most common types of identify theft in 2022 is Credit card fraud 440,672 reports,Other identity theft 326,511reports, Bank fraud 156,143 reports, Loan or lease fraud 153,583 reports, Employment or tax-related fraud 103,420 reports. In addition to many types of cyber-attack took place day and night during the peak period of the global COVID-19 crisis. Hackers were busy launching and trying their hands on different variants of cyber-attacks such as phishing, malware, distributed-denial-of-service (DDoS), denial-of-service (DoS), advanced persistent threat (APT), malicious social media messaging (MSMM), business email compromise (BEC), botnet, ransomware amongst many others. In the case of the phishing attack, hackers used harmful links hidden in carefully designed emails to target company employees [2]. Unfortunately, when employees click on such links, they ignorantly download keylogging software onto their computers or devices, giving hostile actors access to their credentials. Hackers can then gain unrestricted access to critical business assets and data of the victim's organization by impersonating a genuine employee. Also, nowadays a lot of cybercesurity attacs are improving, one of them is that spear phishing, whaling, vishing, email phishing and etc.

- Spear phishing: It aims to obtain sensitive information or access computer systems by sending personalized messages via email, text or phone. Attackers using this method frequently leverage information from social media, public databases or previous breaches to enhance their credibility.
- Whaling: Senior or well-known workers, including finance officials and chief executives in targets. Attackers create incredibly convincing, highly persenolized messages to obtain sensitive data and informations.
- Vishing: Making phone calls or leaving voicemails under the guise of a reliable source is known as "vishing." The intent is to obtain bank accounts, take advantage of personal information, and steal money.
- Email Phishing: Mail phishing endeavors to take delicate data by mail. Aggressors posture as true organizations and can target mass gatherings of people.

The aforementioned information indicates the wide range of efforts and methods being used to stop cybercrimes. For instance, "EnCase" Forensic is recognized globally as the standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options. It is built up with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. EnCase Forensic empowers any examiner to seamless complete any investigation, including investigations of mobile devices.

The PC-3000 Portable III System is a hardware-software solution intended for diagnostics, repair and data recovery from almost all storage media devices. Together with the ACE Lab's software products and adapters, the PC-3000 Portable III forms the systems to recover data from SATA/PATA/ USB HDD and PCIe/SATA SSD both in the lab and on-site. At the moment, similar tools are widely spreading in Uzbekistan and other countries like Belksoft Evidence Center X, Mobile Criminal Expert, UFED 4PC Ultimate Kit and others [3].

Of course, the aim of the facts above is to further improvement of this field and the use of information networks. Other variations of these gadgets and equipment are now extensively distributed over the world and contributing to effective outcomes and cyber attack prevention, nevertheless, many reforms have been done in this regard at the moment, because being implemented is vital in all states. But legislations and reforms in this sphere are very important and nowadays in Europe, USA, Asia or Unions and another countries legal documents, conventions, guidelines are available.

For example, The Budapest Convention is more than a legal document; it is a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention [4].

United Nations Convention Against Transnational Organized Crime (2000) as Palermo Convention, Geneva Convention or Declaration for Cyberspace, Cybercrime Convention Negotiations Microsoft's submission to the Sixth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and etc.

Each of the aforementioned agreements, negotiations and legal documents contains measures to prevent cybercrime, to prevent any kind of threats or cyberattacks aimed at disrupting the minds of young people, to ensure the safety of society, the elimination of the economy and the cooperation of the world.

Many reforms have been promoted for the exchange of experiences and knowledge, the understanding and use of new technologies, and the mention of the development of the sector through cooperation to improve the quality of professionals and employees.

Many people around the world use the Internet to keep in touch with business, education, health, etc [5]. This pandemic has tested everyone's burden.

Also, people used the Internet to reduce their stress. This epidemic has shown that people can do their jobs, go to school and participate in other activities from home. However, cybercriminals have seized the opportunity to profit from the widespread public use of the Internet.

However, due to the lack of knowledge about the methods, motivations, complexity and opportunities related to cyber security, cyber security attacks have increased significantly in this age of disease.

The following recommendations are considered complementary solutions to the cybersecurity solutions found primarily for users of digital systems, including primary and secondary prevention strategies.

Today, Some recommendations can useful for everyone and the first step is to prevent cyber attacks [6].

Step 1: Users should ensure that antivirus software is up-to-date on all devices.

Step 2: Make sure your device is powered on.

Step 3: Remove all pirated software.

Step4: Avoid accessing unknown websites that may contain phishing material.

Step 5: Users should not store their username or password in their browser.

Step 6: Users should not click on email links until they are verified as safe.

Step 7: Users find a secure authentication website. This means that anything starting with "HTTPS://" is safe.

Step 8: Users should not store credit/debit card information in their browser.

LITERATURE:

1. http://surl.li/uaelb;

2. Achim, M. V., Vaidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The impact of the development of society on economic and financial crime. Case Study for European Union Member States. Risks, 9(5), 97;

3. https://www.acelab.ru/dep.pc/pc-3000-portable-iii-systems.php;

4. https://www.opentext.com/products/encase-forensic;

5. https://www.coe.int/en/web/cybercrime/the-budapest-convention;

6. https://rm.coe.int/168008160f.