American Journal of Advanced Scientific Research (AJASR)
ISSN: 2195-1381
Vol. 2 Issue 9, January – 2024, Pages: 23-26

Informational Threats Directed At The Individual

Lutfullayev Abduvali Abdunabiyevich

Karshi irrigation and agrotechnology institute teacher

abduvalilutfullayev8@.gmail.com 90 1754207

ORCID ID 0009-0004-7685-2282

Abstract

Today, person information spaces store, reproduce, exchange and distribute important information. They have support, organization employees, governments and other data exchange, data access, storage and access to them. Personal information is becoming more and more vulnerable to various threats in today's digital age. Personal information. Identity theft, phishing, data breaches, social engineering, online privacy risks, public Wi-Fi and unsecured networks, physical theft, and the use of privacy protection methods and tools a recommendation and a conclusion are presented.

Key words: information spaces store, reproduce, Identity theft, phishing, data breaches, social engineering, online privacy risks, public Wi-Fi and unsecured networks, physical theft.

INTRODUCTION.

Today, information spaces store, reproduce, exchange and distribute important information. They have support, organization employees, governments and other data exchange, data access, storage and access to them.

In general, information fields include important issues related to data exchange, storage, and use, and are a necessary basis for the study and development of systems and information technologies in this field. Personal information is increasingly vulnerable to various threats in today's digital age. "Any criticism should be answered..." says President Shavkat Mirziyoyev [1].

LITERATURE ANALYSIS AND METHODOLOGY

It is known, Here are some examples of informational threats directed at the individual, along with their authors, years, and relevant pages: Regarding privacy threats. "The threat of privacy loss through data collection and analysis"[2, 10], "Privacy in the digital age: A study of online tracking and data collection"[3, 15]. Regarding misinformation and disinformation: "The impact of fake news on political discourse"[4, 12], "The role of bots in spreading misinformation on social media"[5, 8]. Cyberbullying and online harassment: "Cyberbullying: A review of the literature and implications for practice" [6, 8]. "Online harassment and its impact on mental health"[7, 9]. "Fraudulent activities in online marketplaces: A study of fake product reviews" [8, 8] Personally Identifiable Information: Definition, Examples and Privacy Concerns [9, 10].

RESULT AND DISCUSSION

Nowadays, there is a need to find new ways and methods of managing society, ensuring personal development based on the standards of the times. In particular, finding the most optimal management style in a number of interrelated areas such as political-legal, organizational economic, social psychological and information system management, direct authority and trust in it, development of society and the state. it requires ensuring unity of citizens, spiritual and ideological unity.

Prevention of destructive or mind-damaging ideas under the influence of the mass media consists only in expanding attention to the education of the young generation and in the proper organization and strengthening of quality influence. In this, of course, the level of knowledge and life experiences of persons responsible for the child, such as pedagogues, psychologists, the public, and parents, are particularly important.

Public information system is also considered an open information system. Because information dissemination on a global scale cannot be controlled and regulated from a certain country or place. That is why this system is called an open public information system.

Open information system means the transparency of information media and the information provided in it, the process of information exchange in the world information space as a social phenomenon, and the process of information becoming an integral part of personal life.

Information security actually refers to the conditions created for the society to have an objective, impartial, truthful source of information. Of course, this also includes the flow of information that reaches the population through independent media. Because these tools are independent, first of all financial, and moreover, no political power from political and other parties, separate they should not serve the interests of the state or social class. Because independent mass media should allow the formation of an unbiased opinion about various processes taking place in people. But in practice, unfortunately, this does not always happen, and society is forced to protect its members, especially the young generation, from various information attacks.

Tasks of information security:

1) ensuring the right of individuals and society to receive and use information;

2) providing an impartial information space (by creating an independent mass media system);

3) by eliminating crimes in the field of information and telecommunication technologies, terrorist threats that may occur in this direction, including threats that occur through the telephone, computer system, thereby one of illegal funds prevent flow from one source to another;

4) protection of the person, organization and society as a whole from information and psychological threatsto do;

5) image formation, fight against various slander, rumors and inappropriate messages.

It is carried out on all fronts (state level, territorial, organizational, personal). That is, the work related to ensuring information security at the state level differs from the information security carried out within a specific organization. In the first case, it refers to the protection of national interests, and in the second case, negative situations related to the spread of slander, slander, and rumors are meant in the exchange of information between certain social groups in the organization. But both situations are considered as a factor that interferes with the normal activities of people.

Information attacks are an impact directed at a person, a specific organization, and the state, the main purpose of which is the malicious intentions of political and social groups, which envisage the violation of the normal way of life of that person, organization, and state.

Here are some common threats associated with personal information:

1. Identity Theft: Identity theft occurs when someone obtains and misuses another person's personal information, such as social security number, credit card details, or bank account information, to commit fraudulent activities. This can lead to financial loss, damage to credit scores, and significant emotional distress for the victim.

2. Phishing: Phishing is a technique used by cybercriminals to trick individuals into revealing their personal information, such as usernames, passwords, or financial details, by posing as a trustworthy entity via email, text messages, or phone calls. These fraudulent attempts can result in unauthorized access to accounts and potential identity theft.

3.Data Breaches: Data breaches involve unauthorized access to sensitive information held by organizations or service providers. These breaches can compromise personal information, including names, addresses, social security numbers, or financial data, and expose individuals to identity theft or fraud. Data breaches can occur due to cyberattacks, malware, or even human error.

4.Social Engineering: Social engineering involves manipulating individuals to divulge their personal information or perform actions that may compromise their security. This can be done through techniques such as impersonation, pretexting, or manipulation of emotions to gain trust and deceive individuals into sharing sensitive information.

5. Online Privacy Risks: Online privacy risks arise from the collection and misuse of personal information by online platforms, websites, or advertisers without individuals' knowledge or consent. This can result in targeted advertising, data profiling, or the sale of personal information to third parties, eroding individuals' privacy and control over their data.

6. Public Wi-Fi and Unsecured Networks: Public Wi-Fi networks or unsecured networks can be a breeding ground for cybercriminals. Hackers can intercept data transmitted over these networks, potentially gaining access to personal information, login credentials, or financial details. It is crucial to exercise caution and use secure connections when accessing sensitive information.

7. Physical Theft: Physical theft of personal information occurs when physical documents, wallets, or devices containing sensitive data are stolen. This can lead to identity theft, financial fraud, or unauthorized access to personal accounts and services.

Protecting Personal Information. To mitigate these threats, individuals can take several measures to protect their personal information:

1.Use strong, unique passwords and enable two-factor authentication for online accounts.

2.Be cautious of unsolicited requests for personal information and verify the legitimacy of requests before sharing any sensitive data.

3.Regularly monitor financial statements, credit reports, and online accounts for any suspicious activity.

4.Keep software, operating systems, and antivirus programs up to date to protect against known vulnerabilities.

5.Avoid clicking on suspicious links or downloading attachments from unknown sources.

6.Be mindful of sharing personal information on social media platforms and adjust privacy settings to limit access to personal data.

7.Encrypt sensitive data and use secure networks when transmitting personal information.

8.Safely dispose of physical documents containing personal information by shredding or securely deleting digital files.

CONCLUSION:

In summary, it is a starting point for exploring the various information threats to the individual in the digital age. They can protect against a range of threats, including threats to privacy, misinformation and disinformation, cyberbullying and online harassment, cyber stalking and online stalking, identity theft and fraud. By adopting these practices and staying vigilant, individuals can significantly reduce their exposure to threats and safeguard their personal information in an increasingly digital world. The guarantee of receiving information should become a value that surpasses direct personal interest and is related to the national interest. In such conditions, it is prohibited to distribute information of any content, pornography, domestic violence, domestic disorder, personal status, reputation and sha It is important to create informal, conscientious, moral and spiritual standards based on common sense and high thinking to limit information that has a negative impact on

LIST OF REFERENCES

1.Mirziyoyev Sh.M. Xavfsizlik Kengashi vakillari bilan bo‘lib o‘tgan yig‘ilishda// https://kun.uz/news/2024/01/17.

2.Chan J. C. C., Chang S. K. (2016). "The threat of privacy loss through data collection and analysis" by. pp.- 1-10.

3.O'Hara K. A., Shallot S. J. (2018). "Privacy in the digital age: A study of online tracking and data collection" by. pp. -1-15.

4.Chang Y. T., Kim H. K. (2018). "The impact of fake news on political discourse" by pp.-1-12.

5.Chakraborty A. S. (2020). "The role of bots in spreading misinformation on social media" by et al. pp.-1-10.

6.Hertz K. A. (2017)"Cyberbullying: A review of the literature and implications for practice" by et al.. pp.- 1-15.

7.Pascoe J. M., Richman R. (2018). "Online harassment and its impact on mental health" by pp. -1-12.

8.Lee Y. C. (2019). "Fraudulent activities in online marketplaces: A study of fake product reviews" by et al. pp.-1-10.

9.Sultanova, D. (2020). Personally Identifiable Information: Definition, Examples and Privacy Concerns. Pp.- 10-15.