EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
IF = 7.899 www.in-academy.uz

MAIN INTERNET THREATS AND WAYS TO PROTECT AGAINST THEM

Shoyqulov Shodmonkul Qudratovich
Acting Associate Professor, department of Applied Mathematics, Karshi State university, Karshi, Republic of Uzbekistan
https://doi.org/10.5281/zenodo.13991390

ARTICLE INFO

Received: 18th October 2024
Accepted: 24th October 2024
Online: 25th October 2024

KEYWORDS

Cyber threats, Internet attacks, data protection, phishing, DDoS, encryption, VPN, two-factor authentication, cybersecurity, Internet of Things, artificial intelligence.

ABSTRACT

The article covers the main types of Internet threats and methods of protection against them. The study analyzed the most common types of threats, such as phishing, malware, account hacking and DDoS attacks. Particular attention is paid to the possible consequences for private users and organizations, as well as effective ways to protect data. The proposed solutions include the use of antivirus software, data encryption, VPN and two-factor authentication. The article also touches on new challenges, such as the security of Internet of Things devices and the use of artificial intelligence in cyberattacks. Examples of the practical application of protective measures are given and conclusions are made about future trends in the field of cybersecurity.

INTRODUCTION

The Internet is an integral part of people's lives today, providing a wide range of opportunities for communication, data exchange and business. At the same time, with its development, the number of cyber threats has increased significantly, posing a danger to both private users and organizations. These threats can cause serious damage, affecting both the financial sphere and the reputation of the victims.

Cyberattacks on the network are becoming increasingly sophisticated, ranging from malware and phishing to DDoS attacks and identity theft. The risks increase every year, especially in the context of an increasing volume of digital information transmitted over the Internet. Thus, the need to develop and apply reliable methods of information protection is becoming especially relevant.

The purpose of this article is to analyze the main Internet threats and consider existing methods of protection against them.

RESULTS and DISCUSSIONS

Internet threats can be classified by their nature and the methods by which they affect users and systems. The main types of Internet threats include the following:

1. Malware

2. This category includes viruses, Trojans, worms, spyware, and ransomware. These programs are designed to infiltrate systems and perform malicious actions, such as stealing data, destroying files, or locking the system and demanding a ransom.
3. Phishing
4. Phishing is an attempt to fraudulently obtain confidential data, such as passwords or banking information. This is achieved by creating fake websites or sending fraudulent emails that look like legitimate requests from trusted organizations.
5. Denial of Service (DDoS) attacks
6. DDoS attacks are aimed at overloading servers by sending mass requests, which can lead to the shutdown of web resources and the unavailability of services to legitimate users.
7. Account Hacking
8. Account hacking is done by guessing passwords or exploiting vulnerabilities in authentication systems. Once hacked, attackers gain access to personal data and can use accounts to conduct further attacks or steal information.
9. Social Engineering Techniques
10. Social engineering involves psychologically influencing people to gain access to confidential information or to encourage them to perform dangerous actions, such as disclosing passwords or installing malware.
11. Internet of Things (IoT) Threats
12. With the increase in devices connected to the internet, such as smart cameras and home appliances, the risk of hacking increases. Hackers can exploit vulnerabilities in these devices to access other systems or carry out attacks.
13. Mobile Device Threats
14. Mobile malware poses a significant threat. These threats can include programs that collect data from devices, spyware, or viruses that attack mobile systems such as Android and iOS.
15. Crypto-malware
16. Ransomware encrypts data on devices and demands a ransom to restore it. This type of threat is especially dangerous for organizations and corporations, where data loss can lead to serious consequences.
17. Social Media Threats
18. Social media threats can allow attackers to collect personal data from users for further use in fraudulent activities, such as phishing or account hacking. Social media is a popular platform for social engineering.

These threats continue to evolve, becoming more complex, which requires the use of multi-layered approaches to information protection.

The consequences of Internet threats can be extremely serious and affect various areas of life, both for individuals and for companies. One of the most dangerous outcomes is identity theft, which can lead to fraud, identity theft, or financial losses. This creates risks not only for users, but also for businesses, where the consequences can be devastating to the company's reputation[1,3].

Financial losses are often a direct result of cyber attacks. Attackers can gain access to financial systems and banks, which can lead to the theft of funds, damage to assets, and loss of

confidential information. Attacks on banks and financial institutions are especially dangerous, where data compromise leads to major losses for customers and companies.

In addition, system failures are a serious consequence of Internet threats. For example, DDoS attacks can temporarily disable websites, services, and even entire control systems, which causes significant financial losses and reduces user confidence in the company. In the case of attacks on critical infrastructures, such as energy systems or healthcare, the consequences can be even more significant, up to and including a threat to human life and safety.

Another important aspect is legal and regulatory liability. Companies that do not ensure adequate data protection can face large fines and lawsuits for violating personal data protection requirements, such as the GDPR or other international standards. Thus, the consequences of Internet threats include data leakage, significant financial losses, infrastructure failures, legal sanctions and loss of customer trust, which together lead to serious risks and costs for businesses and users.

Methods of protection against online threats include many approaches aimed at preventing attacks and minimizing their consequences. The main methods include the following.

1. Using antivirus programs and firewalls: Antivirus software helps detect and remove malware such as viruses and Trojans. To improve protection, it is important to regularly update antivirus software. Firewalls block unauthorized connections to the network by monitoring incoming and outgoing traffic, which helps protect your computer from external threats.
2. Data encryption: To protect confidential information, encryption methods are used to transform data into a form inaccessible to third parties. Using security protocols such as SSL or TLS ensures secure data transmission over the Internet and protects it from interception.
3. User authentication and access control: Multi-factor authentication (for example, using a password and a one-time code) is an important measure to protect access to accounts. Access control helps limit who has access to sensitive data or resources and prevents unauthorized access.
4. Software Updates: Regularly updating operating systems and applications is essential to eliminate vulnerabilities that attackers can use to infiltrate the system.
5. Backing Up Data: To minimize the damage from ransomware, it is important to regularly back up your data. This will allow you to restore it in case of damage or loss, reducing risks and ensuring uninterrupted operation of the system.
6. User Training: Cyberattacks often target the human factor. Training employees in the basics of Internet security, such as how to safely handle email and suspicious links, helps reduce the likelihood of phishing attacks.
7. Monitoring Network Activity: Regularly monitoring network traffic helps to promptly identify suspicious activity and promptly respond to potential threats. This helps protect data and systems from hacker attacks.

The integrated use of these methods can significantly increase the level of protection against Internet threats, minimizing the risks of hacking, data theft, and attacks on systems.

1. Phishing attacks

2. Phishing is a method of deceiving users by sending fake emails or creating fake websites to obtain confidential data, such as passwords and bank card details.
3. Example: In 2020, there was a large-scale phishing attack on users of Google and Microsoft services, when hackers collected personal data under the guise of official messages.
4. Prevention:

- Using spam filters to filter out phishing emails.
- Using two-factor authentication to improve security.
- Carefully checking links before opening them and providing personal information.

5. Ransomware
6. Ransomware blocks access to data or systems, demanding a ransom to restore them. They can cause serious data loss and financial damage.
7. Example: One of the most well-known attacks was the WannaCry virus in 2017, which affected many computers, blocking access to data[2,4].
8. Prevention:

- Update software and operating systems to protect against vulnerabilities.
- Use antivirus software and backup data.
- Restrict access through ports and use firewalls.

9. DDoS attacks
10. DDoS attacks are aimed at overloading a server by sending a large number of requests, which makes it unavailable.
11. Example: In 2016, a large DDoS attack on Dyn servers disrupted the operation of sites such as Twitter and Netflix.
12. Prevention:

- Use cloud solutions to protect against DDoS attacks.
- Set up traffic filtering via QoS.
- Regularly test for resistance to attacks.

13. Brute Force Attacks
14. This method involves systematically trying possible password combinations, which can lead to account compromise.
15. Example: In 2021, thousands of Google and Microsoft accounts were compromised through brute force attacks.
16. Prevention:

- Use complex passwords.
- Set up two-factor authentication.
- Limit the number of login attempts.

17. SQL Injections
18. SQL injections allow malicious code to be injected into database queries, which can lead to data theft or modification of database information[5,6].
19. Example: In 2019, British Airways was attacked using SQL injections, which resulted in the theft of data on over 500,000 users.
20. Prevention:

- Use parameterized queries to protect against injections.

- Regular code audits and vulnerability checks.
- Using specialized tools to protect against

Modern Internet threats are rapidly evolving, constantly acquiring new forms and becoming more complex. This is due to the widespread use of digital technologies and the increase in the volume of data transmitted over the Internet. Let's consider the main modern trends in the field of Internet threats and methods of protection against them.

1. Sophistication of attacks. Today's cyberattacks are becoming more sophisticated due to the introduction of advanced technologies such as artificial intelligence (AI) and machine learning. These technologies allow attackers to develop more precise, targeted attacks, bypassing traditional defense systems. Such threats include complex phishing attacks, advanced persistent threats (APTs), and attacks on vulnerable APIs.
2. Attacks on cloud services. With the increasing use of cloud technologies, there has been an increase in attacks on cloud service infrastructure. Attackers try to access confidential information by exploiting configuration flaws and vulnerabilities in APIs. This can lead to serious data leaks and compromise the security of user accounts.
3. Internet of Things (IoT). With the proliferation of smart devices in everyday life, such as surveillance cameras, smart home appliances, and sensors, the number of attacks on the IoT is increasing. These devices are often not sufficiently protected, making them vulnerable to hacker attacks, such as massive DDoS attacks using IoT botnets.
4. Using AI for attacks. Artificial intelligence and machine learning are also actively used by attackers to analyze system vulnerabilities and carry out more accurate attacks. On the other hand, AI is used to strengthen security, for example, to detect abnormal activity on the network and respond to threats in real time.
5. Attacks on cryptocurrencies. With the growing popularity of cryptocurrencies such as Bitcoin, the number of attacks aimed at stealing digital assets is increasing. Hacking of cryptocurrency wallets, exchanges, and platforms is becoming more common, especially due to the high level of anonymity of these technologies.
6. Attacks on supply chains. One of the new types of threats is supply chain attacks. Attackers hack into the infrastructure of software vendors, allowing them to inject malicious code before the products reach end users. An example of such an attack is the SolarWinds incident, where hackers gained access to the networks of multiple organizations.
7. Deepfakes and cyberattacks. The use of deepfakes to create fake videos and audio recordings is gaining momentum. Such technologies can be used for blackmail or disinformation. For example, deepfakes can be used to create fake videos for the purpose of fraud.

These trends show that online threats are becoming more diverse, requiring cybersecurity professionals to apply new protection methods and countermeasure strategies. It is important to constantly improve security tools, raise user awareness, and implement modern technologies to protect information on the Internet.

The future of cybersecurity is a complex and ever-changing field, where innovative technologies will play a key role. As digital technologies continue to expand, so does the need to protect data and information systems. One of the most promising areas is the implementation of artificial intelligence (AI) and machine learning in cyber defense systems.

These technologies will be able to automatically detect and respond to threats in real time, analyzing the behavior of systems and users to more accurately predict attacks.

Quantum computing will also have a significant impact on cyber security, especially in the field of cryptography. The advent of quantum computers can make existing encryption systems vulnerable, which will require the development of new quantum-resistant encryption methods[7,8].

The growth in the number of devices connected to the Internet of Things (IoT) creates additional challenges for protecting the data transmitted through these devices. Future cyber security solutions are expected to include security standards specifically designed for the IoT.

Another area is the use of blockchain technologies to protect networks and ensure data integrity. Due to its distributed structure, blockchain can prevent attempts to forge data and increase transparency in security systems.

With the development of deepfake technologies aimed at creating realistic fakes, means are needed to detect such fakes in order to prevent fraud, blackmail, and other forms of abuse. In addition, an important trend will be the expansion of interaction between humans and machines in the process of ensuring cybersecurity. This will help to increase the effectiveness of protection by combining automated systems with the professional skills of specialists.

Data privacy will also become a key issue of the future, with stricter regulations and laws to protect user information.

In the context of globalization of cyberspace, states and corporations will be forced to develop powerful defense systems to prevent cyber wars and ensure national security.

Overall, the future of cybersecurity requires continuous improvement of protection methods and the introduction of advanced technologies to successfully counter new and increasingly complex threats.

CONCLUSIONS

With the rapid growth of digital technologies and the increase in the volume of data transmitted over the Internet, Internet threats are becoming an increasingly significant challenge to information security. This article covered the main types of threats on the Internet, such as viruses, phishing, DDoS attacks, and cyber espionage. Modern protection methods were also analyzed, including antivirus programs, firewalls, data encryption, and multifactor authentication. These tools play a crucial role in protecting personal and corporate data.

It is important to emphasize that, despite the development of protection tools, Internet threats continue to evolve, becoming more complex and sophisticated. This requires constant improvement of security methods and increasing user awareness of current threats.

To effectively combat Internet threats, it is necessary to implement both technical means of protection and strategies for raising user awareness. Updating software, using modern protection systems, and following safe online behavior rules will help reduce risks and minimize losses from cyber attacks.

Thus, Internet threats will continue to evolve, which dictates the need for constant monitoring of new challenges and the development of innovative solutions in the field of cybersecurity.

References:

1. Shoykulov Sh.K. (2024). USING PYTHON PROGRAMMING IN COMPUTER GRAPHICS. https://doi.org/10.5281/zenodo.13926022
2. Shoyqulov, S. (2024). DATA VISUALIZATION IN PYTHON. B EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (Т. 4, Выпуск 10, сс. 15–22). Zenodo. https://doi.org/10.5281/zenodo.13892777
3. Shoyqulov, S. (2024). GRAPHICAL PROGRAMMING OF 2D APPLICATIONS IN C#. B EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (Т. 4, Выпуск 10, сс. 7–14). Zenodo. https://doi.org/10.5281/zenodo.13892766
4. Bozorov, A., & Shoyqulov, S. (2024). COMPUTER GRAPHICS IN TECHNICAL DISCIPLINES. B EURASIAN JOURNAL OF ACADEMIC RESEARCH (Т. 4, Выпуск 10, сс. 21–27). Zenodo. https://doi.org/10.5281/zenodo.13898180
5. Bozorov, A., & Shoyqulov, S. (2024). COMPUTER GRAPHICS IN THE NATURAL SCIENCES. B EURASIAN JOURNAL OF ACADEMIC RESEARCH (Т. 4, Выпуск 10, сс. 12–20). Zenodo. https://doi.org/10.5281/zenodo.13898146
6. Shoyqulov Sh. Q.METHODS FOR PLOTTING FUNCTION GRAPHS IN COMPUTERS USING BACKEND AND FRONTEND INTERNET TECHNOLOGIES. European Scholar Journal (ESJ). Vol. 2 No. 6, June 2021, ISSN: 2660-5562. P.161-165, https://scholarzest.com/index.php/esj/article/view/964/826
7. Sh.Q. Shoyqulov. (2021). Methods for plotting function graphs in computers using backend and frontend internet technologies. European Scholar Journal, 2(6), 161-165. Retrieved from https://scholarzest.com/index.php/esj/article/view/964
8. Sh.Q. Shoyqulov. (2022). The text is of the main components of multimedia technologies. Academicia Globe: Inderscience Research, 3(04), 573–580. https://doi.org/10.17605/OSF.IO/VBY8Z