

CYBER HYGIENE: KEY THREATS AND COUNTERMEASURES

Vinnytsia National Technical University

Анотація

З розвитком технологій зросли також і ризики роботи з ними. Кожен день мільйони людей стають жертвами кібератак, а компанії зазнають випадки кібертероризму. Саме тому кібергігієна стала важливим елементом безпеки в сучасному Інтернет-середовищі. У роботі розглянуто основні кіберзагрози, зокрема фішинг, шкідливе ПЗ та DDoS-атаки, а також методи їх запобігання. Особливу увагу приділено практичним заходам захисту. Підкреслено значення обізнаності користувачів для зниження ризиків у кіберпросторі.

Ключові слова: кібергігієна, кібератака, захист, антивірус, кіберобізнаність.

Abstract

As technology has advanced, so too have the risks associated with its use. Every day, millions of people fall victim to cyberattacks, and companies face incidents of cyberterrorism. This is why cyber hygiene has become a crucial element of security in today's online environment. This paper examines the main cyber threats, including phishing, malware, and DDoS attacks, as well as methods for preventing them. Particular attention is paid to practical security measures. The importance of user awareness in reducing risks in cyberspace is emphasized.

Keywords: cybersecurity, cyberattack, protection, antivirus, cyber awareness.

Introduction

It is no secret that every environment poses threats and dangers; just as real life is full of unpredictable situations, the Internet is not entirely safe either. The global spread of information and communication technologies in society has led to the emergence and development of a fundamentally new form of terrorism – information terrorism or cyberterrorism. Every day, thousands of users face both usability issues and various malicious actions targeting them and the information they possess. Cyberspace today is an integral part of life for the entire population. For simplicity's sake, it's best to imagine the internet as a separate world with its own rules, laws, and, of course, those who break them. To this end, black-hat hackers resort to phishing (tricking users) and social engineering (psychological manipulation to gain access to information). Cyber hygiene begins when we pick up our phones and tag our favourite coffee shop in social media posts, reply to messages from strangers without thinking, or fail to notice when our friends are messaging us in a way that's out of character for them.

Research results

By examining various types of threats, we can identify effective methods for countering and eliminating them. For a long time, cybersecurity specialists have been developing various measures and services to verify security and prevent threats through cyber hygiene practices. Cyber hygiene refers to security measures designed to protect users' devices from malware infection and the potential theft of confidential information.

Among the threats on the Internet, the main ones include: phishing (information theft), BotNet, DDoS attacks, malware, hacker attacks, false information, suspicious links, etc. Various cyber hygiene methods and services exist for the timely detection of threats. Various websites and software allow you to check other websites, links, information sources, or software for reliability and security. The main methods used to prevent threats include using antivirus software (ESET, Avast, Norton), creating complex and strong passwords (services for checking password strength: PasswordMonster), updating software, avoiding open Wi-Fi networks, checking links using specialized services (VirusTotal, NordVPN LinkChecker, URLVoid), verifying the reliability of information sources, using two-factor authentication, exercising caution with emails and attachments, and so on. All of these practices have become essential for reducing the risk of cybercrime and enhancing the protection of personal data.

Conclusion

Cyber hygiene is an integral part of every internet user's life. Cyber hygiene practices not only help users navigate the internet safely but also prevent the leakage of personal information or even unauthorized access to user accounts. It is important for users to continue learning and staying informed about new threats and ways to counter them, which will help improve overall cybersecurity.

REFERENCES

1. Cyber Hygiene. URL: <https://www.enisa.europa.eu/topics/cyber-hygiene>.
2. What Is Cyber Hygiene? Introduction, Best Practices, & Next Steps for Organizations. URL: https://www.splunk.com/en_us/blog/learn/cyber-hygiene.html.
3. Cyberterrorism as a threat to the cyber security of Ukraine: A discussion of theoretical aspects. URL: <https://amazoniainvestiga.info/index.php/amazonia/article/view/1599/1672>.
4. Ibrahimova L. V., Nykyporets, S. S. Information security in the global context: linguistic perspectives and the role of English. *International security studies: managerial, technical, legal, environmental, informative and psychological aspects*. International collective monograph. Volume II. ISAP, Research and Education. 2025. 436 p., P. 321-345. DOI: <https://doi.org/10.5281/zenodo.15356365>.
5. Nykyporets, S. S., & Kukharchuk, H. V. (2025). Intercultural communication in information security: Risks, conflicts, and educational opportunities for English language teachers. In *International security studies: Managerial, technical, legal, environmental, informative and psychological aspects* (Vol. II, pp. 398-420). ISAP, Research and Education. DOI: <https://doi.org/10.5281/zenodo.15356424>.
6. Nykyporets S. S., Herasymenko N. V., Chopliak V. V. Developing digital language competence as a factor of competitiveness of future master's degree holders in power engineering in the digital economy. *Artificial intelligence as a tool to protect the economy disinformation: innovative solutions and international practices: collective monograph* / edited by O. H. Cherep. Riga, Latvia : Baltija Publishing, 2025. 258 p. P. 140-193. DOI: <https://doi.org/10.30525/978-9934-26-586-0>.
7. Kot S. O., Nykyporets, S. S. Activating students' cognitive engagement in technical English learning with AI tools. *Science and education in the third millennium: information technology, education, law, psychology, social security and work, management*. International collective monograph. Volume I. Institute of Public Administration Affairs. Lublin, Polska, 2025. 532 p., Pp. 295-332. DOI: <https://doi.org/10.5281/zenodo.16942267>.

Заліський Владислав Сергійович – студент групи ІБС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vladzaliskiy686@gmail.com.

Науковий керівник: **Чопляк Вікторія Володимирівна** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Vladyslav S. Zalyiskii – a student of ISS-24b group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vladzaliskiy686@gmail.com.

Scientific Supervisor: **Victoriia V. Chopliak** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.