Zharov Matvey Vladislavovich
student
Bychkov Oleg Igorevich
student
Scientific adviser
Filipskaya Anastasia Vadimovna
senior lecturer

MIREA – Russian Technological University
Moscow

DOI 10.31483/r-156021

THE ROLE OF ENGLISH LANGUAGE PROFICIENCY IN ENSURING INTERNET SAFETY

Abstract: *the article examines the relationship between English language proficiency and cybersecurity awareness among non-native English-speaking internet users. The study analyzes common internet safety scenarios-including phishing detection, privacy settings configuration, and security software usage to identify how English competence affects user protection. Recommendations for improving digital safety education for non-English speakers are presented.*

Keywords: *internet safety, cybersecurity, English language proficiency, digital literacy, linguistic barriers, online threats, phishing.*

Жаров Матвей Владиславович
студент
Бычков Олег Игоревич
студент
Научный руководитель
Филипская Анастасия Вадимовна
старший преподаватель

ФГБОУ ВО «МИРЭА – Российский технологический университет»

г. Москва

РОЛЬ ВЛАДЕНИЯ АНГЛИЙСКИМ ЯЗЫКОМ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Аннотация: *в статье рассматривается взаимосвязь между уровнем владения английским языком и осведомленностью о кибербезопасности среди пользователей интернета, для которых английский не является родным. В исследовании анализируются типичные сценарии обеспечения безопасности в интернете, включая распознавание фишинговых атак, настройку параметров конфиденциальности и использование антивирусного программного обеспечения, с целью выявить, как уровень владения английским языком влияет на защищенность пользователя. В заключение представлены рекомендации по совершенствованию программ обучения цифровой безопасности для пользователей, не владеющих английским языком.*

Ключевые слова: *безопасность в интернете, кибербезопасность, владение английским языком, цифровая грамотность, языковые барьеры, онлайн-угрозы, фишинг.*

1. *Introduction.*

In an increasingly interconnected digital world, internet safety has emerged as a fundamental concern for individuals, organizations, and governments. Cybersecurity threats continue to evolve in sophistication and scale, affecting millions of users annually. According to cybersecurity experts, humans are widely recognized as the weakest link in the chain of cybersecurity-a vulnerability that becomes particularly pronounced when users cannot fully understand the safety information provided to them.

The predominance of English in digital spaces is well-documented. English serves as the default language for most operating systems, web browsers, social media platforms, and security software. The most effective cybersecurity educational tools, threat reporting forms, and incident response guides are primarily available on-

ly in English. This linguistic reality creates a significant challenge for the substantial portion of global internet users who possess limited English proficiency (LEP).

The relevance of this topic extends beyond individual user safety to broader societal concerns. As Ngo and colleagues note, «If we want to secure our digital borders, we must ensure that every member in society, regardless of their language skills, is well-informed about the risks inherent in the cyber world." When substantial segments of the population cannot access or understand critical cybersecurity information, the security of entire digital ecosystems may be compromised.

This article aims to analyze how English language competence affects an individual's ability to maintain safety while navigating the internet. Specifically, this study addresses the following research questions. 1. In what ways does English proficiency influence vulnerability to common cyber threats? 2. What linguistic features of cybersecurity terminology pose particular challenges for non-native speakers? 3. How can the security gap experienced by LEP users be addressed?

2. *Literature Review.*

Cybersecurity Terminology as a Specialized Domain.

The field of cybersecurity has developed an extensive and specialized English terminology that poses significant challenges for non-native speakers. Research by Kolesnik has examined the structural-semantic and lexicographic aspects of English computer security terminology, revealing the complexity of this lexical domain. The terminology encompasses numerous subfields, including network security, cloud security, application security, and Internet of Things device security.

Chang has documented that while no unified approach to cybersecurity terminology exists even among English-speaking experts, there is general consensus regarding the classification of cybersecurity into five main types: critical infrastructure security, application security, network security, cloud security, and device security. For non-native English speakers, mastering this terminological system requires not only language proficiency but also conceptual understanding of the technical distinctions these terms encode.

Filatov has argued that the acquisition of key English cybersecurity terms-such as phishing, malware, privacy, cookie, and encryption-serves a dual purpose. Beyond expanding linguistic competence, understanding these terms contributes to deeper conceptual comprehension of digital threats and promotes the development of cyber hygiene skills. This finding suggests that English cybersecurity terminology functions as a linguistic tool for digital safety education.

3. *Language Barriers and Phishing Vulnerability.*

Phishing remains one of the most prevalent forms of cybercrime, accounting for a substantial proportion of successful attacks. Recent research has demonstrated that language proficiency plays a critical role in determining susceptibility to phishing attempts.

Menon and colleagues conducted a comprehensive study investigating linguistic triggers in phishing emails targeting African refugees and immigrant students in the United States. Their research revealed that limited English proficiency, combined with low digital literacy skills, often leads vulnerable populations to ignore or fail to recognize phishing emails as malicious. Notably, even after receiving digital literacy training, recently resettled refugees continued to face significant challenges in identifying phishing attempts due to language barriers.

The study compared three participant groups: African refugees, African immigrant students, and a control group of monolingual US-born students. While both student groups demonstrated greater caution than refugees, instances of data disclosure remained prevalent across all groups. This finding underscores the need for integrated approaches that address both linguistic and educational dimensions of cybersecurity.

4. *Communication Challenges in Multilingual Environments.*

The challenges posed by language barriers extend beyond individual users to professional cybersecurity teams. Falowo conducted a study of 80 cybersecurity professionals working in international organizations, examining how language proficiency, translation tool usage, and cultural diversity affect threat intelligence sharing.

The study's regression analysis revealed three significant findings. First, language proficiency significantly affects the effectiveness of cybersecurity communica-

tion. Second, the use of translation tools has a notable impact on the accuracy of threat intelligence sharing. Third, cultural backgrounds influence collaboration effectiveness. All three models were statistically significant. These findings indicate that multilingual communication barriers can undermine the overall performance and security of global teams.

5. *The Limited English Proficiency Cybersecurity Gap.*

The most direct evidence of the relationship between English proficiency and cybersecurity vulnerability comes from research specifically targeting LEP internet users. Ngo, Holman, and Agarwal conducted what is believed to be the first mixed-method study exploring links among demographic characteristics, cyber hygiene practices, and cyber victimization among LEP internet users, focusing on Spanish and Vietnamese speakers.

Their research yielded two main takeaways. First, LEP internet users share the same concern about cyber threats as any other individual. However, they are constrained by a lack of culturally and linguistically appropriate resources. Second, online guidance that provides the most effective educational tools and reporting forms is only available in English, with the most notable example being the website for the FBI's Internet Crime Complaint Center.

The study documented concerning behavioral patterns. Over a 12-month period, only 29 percent of focus group participants avoided using public Wi-Fi, and only 17 percent reported having antivirus software installed on their devices. These findings indicate that many LEP users engage in risky online behaviors-not due to carelessness, but because they lack access to comprehensible information about appropriate security practices.

6. *Methods.*

This study employs a documentary analysis methodology, synthesizing findings from peer-reviewed research articles and institutional reports published between 2023 and 2026. Sources were selected based on their relevance to the relationship between English proficiency and cybersecurity outcomes. The analysis focuses on three domains: 1) empirical studies measuring cybersecurity behaviors among LEP popula-

tions; 2) linguistic analyses of cybersecurity terminology; 3) intervention studies evaluating digital literacy programs for non-native English speakers.

The research synthesizes findings from multiple national contexts, including the United States, Russia, Ukraine, and Nigeria. This comparative approach allows identification of patterns that transcend specific linguistic or cultural contexts while also revealing context-dependent factors.

7. *Results.*

The synthesis of available research yields several consistent findings regarding the relationship between English proficiency and internet safety.

English Proficiency as a Predictor of Cyber Hygiene.

Multiple studies demonstrate a positive correlation between English proficiency and adoption of recommended cyber hygiene practices. Ngo and colleagues found that LEP users show lower rates of basic security behaviors, including avoiding public Wi-Fi and installing antivirus software. Menon and colleagues documented that refugees with limited English proficiency demonstrated poorer ability to identify phishing emails compared to English-proficient student groups.

These findings persist even when controlling for other factors such as education level. While digital literacy interventions improve awareness of safe practices, LEP individuals continue to face significant challenges that English-proficient peers do not encounter. This suggests that language barriers constitute an independent risk factor for cyber victimization.

8. *Terminology Acquisition as a Protective Factor.*

Filatov's analysis indicates that systematic acquisition of English cybersecurity terminology correlates with improved cyber hygiene outcomes among adolescent learners. Students who mastered key terms such as phishing, malware, and encryption demonstrated better ability to identify online threats and take appropriate protective actions. This finding supports the hypothesis that English cybersecurity terminology functions as a linguistic tool for digital safety.

9. *The Accessibility Gap.*

The most consistent finding across multiple studies is the existence of an accessibility gap-a systematic disparity in the availability of cybersecurity resources in languages other than English. Critical resources, including the FBI's Internet Crime Complaint Center and major educational platforms, provide information only in English. This creates a situation in which LEP users cannot access the same level of protection as English-proficient users, regardless of their motivation or concern about cyber threats.

10. *Discussion.*

The findings synthesized in this article support the conclusion that English language proficiency functions as a significant protective factor in online environments. Several mechanisms mediate this relationship.

First, English proficiency enables direct comprehension of security warnings, privacy policies, and threat notifications. When users cannot understand these communications, they cannot act upon them. Second, English proficiency facilitates access to cybersecurity education resources, which remain predominantly available in English. Third, English proficiency supports effective use of security interfaces, including privacy settings configuration. Fourth, English proficiency enables participation in English-dominant online communities where security information is shared.

These mechanisms interact and reinforce one another. A user who cannot understand security warnings may never learn which behaviors are risky, leading to continued vulnerability. This suggests that language barriers may have cumulative effects.

11. *Implications for Policy and Education.*

The findings have direct implications for cybersecurity policy. If securing our digital borders requires ensuring that all members of society are well-informed about cyber risks, then current arrangements fall short. Policymakers should consider requiring that essential cybersecurity resources be made available in multiple languages.

For education, the finding that English cybersecurity terminology acquisition correlates with improved cyber hygiene suggests that digital literacy education should

integrate language instruction with security training. Educators should explicitly teach English cybersecurity terminology as part of digital safety curricula.

For technology developers, security communications should use clear, straightforward language. Avoiding complex sentence structures and jargon can improve accessibility for LEP users. Additionally, developers should provide security interfaces in multiple languages.

12. *Limitations.*

This study has limitations. First, the available research on LEP populations and cybersecurity remains limited, with few large-scale studies. Second, the mechanisms linking English proficiency to cybersecurity vulnerability require further investigation through experimental designs. Third, the intersection of language proficiency with other vulnerability factors requires further study.

13. *Conclusion.*

This article has examined the relationship between English language proficiency and internet safety. The evidence consistently demonstrates that limited English proficiency is associated with higher vulnerability to cyber threats, including phishing attacks and malware infections. This relationship is mediated by several mechanisms, including direct comprehension of security warnings, access to cybersecurity education resources, and effective use of security interfaces.

The accessibility gap represents a fundamental inequity in current digital environments. Addressing this gap requires coordinated action. Policymakers should consider requiring multilingual access to essential cybersecurity resources. Educators should integrate English cybersecurity terminology into digital literacy curricula. Technology developers should provide security interfaces in multiple languages.

As digital technologies continue to permeate all aspects of modern life, ensuring equitable access to cybersecurity protection becomes a matter of collective security. When substantial segments of the population cannot access comprehensible cybersecurity information, the security of entire digital ecosystems is compromised. Addressing the linguistic dimensions of cybersecurity vulnerability is therefore an essential component of any comprehensive strategy for enhancing internet safety.

References

1. Arslantas T.K. Association between digital literacy, internet addiction, and cyberloafing among higher education students: A structural equation modeling / T.K. Arslantas // E-Learning and Digital Media. – 2022.

2. Bhatnagar N. Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study / N. Bhatnagar. – 2023.

3. Chang V. Cybersecurity for children: An investigation into the application of social media / V. Chang // Enterprise Information Systems. – 2023. – Vol. 17. https://doi.org/10.1080/17517575.2023.2188122. EDN: AHDSHB

4. Díaz-García V. Digitalization and digital transformation in higher education: A bibliometric analysis / V. Díaz-García // Frontiers in Psychology. – 2022. – Vol. 13.

5. Filatov I.A. English-language vocabulary as a tool for developing cyber hygiene in schoolchildren in the digital educational environment / I.A. Filatov. – Cheboksary: Sreda, 2024.

6. Keengwe J. Handbook of Research on Literacy and Digital Technology Integration in Teacher Education / ed. J. Keengwe. – IGI Global, 2023.

7. Khader M. Cybersecurity Awareness Framework for Academia / M. Khader, M. Karam, H. Fares // Information. – 2021. – Vol. 12. No. 10. – P. 417.