INNOVATIVE DEVELOPMENT OF SCIENCE, TECHNOLOGY AND EDUCATION

Proceedings of X International Scientific and Practical Conference

Vancouver, Canada

4-6 July 2024

Vancouver, Canada

2024

UDC 001.1

The 10th International scientific and practical conference "Innovative development of science, technology and education" (July 4-6, 2024) Perfect Publishing, Vancouver, Canada. 2024. 405 p.

ISBN 978-1-4879-3792-8

The recommended citation for this publication is:
Ivanov I. Analysis of the phaunistic composition of Ukraine // Innovative development of science, technology and education. Proceedings of the 10th International scientific and practical conference. Perfect Publishing. Vancouver, Canada. 2024. Pp. 21-27. URL: https://sci-conf.com.ua/x-mizhnarodna-naukovo-praktichna-konferentsiya-innovative-development-of-science-technology-and-education-4-6-07-2024-vankuver-kanada-arhiv/.

Editor
Komarytskyy M.L.
Ph.D. in Economics, Associate Professor

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine and from neighbouring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: vancouver@sci-conf.com.ua

homepage: *https://sci-conf.com.ua/*

PHILOLOGICAL SCIENCES

UDC 378.147*: 81'24*

THE IMPORTANCE OF LEARNING ENGLISH FOR CYBER SECURITY STUDENTS

Melnyk Oksana
Senior Instructor
Borys Grinchenko Kyiv
Metropolitan University
Kyiv, Ukraine
Tereshchuk Mariia
Instructor
Borys Grinchenko Kyiv
Metropolitan University
Kyiv, Ukraine
Huryna Nataliia
Senior Instructor
Borys Grinchenko Kyiv
Metropolitan University
Kyiv, Ukraine

Abstract. In the rapidly changing field of cyber security, knowledge of the English language is not just an additional skill, but a fundamental requirement. It facilitates access to critical information, enables effective global communications and collaboration, promotes professional development through training and certification, and ensures compliance with international standards. As the challenges of cyber security grow, the ability to work effectively and work in English will remain a key success factor for professionals in this important field.

Keywords: education, high-school level, collaboration, information, success, cyber security challenges.

Introduction

Cybersecurity has increasingly become a headline feature in news media in recent years, generally prompted by spectacular breaches of various information systems, including airlines, health organizations, credit agencies, administrations, financial institutions, telecoms, and many others [1, p. 23]. Until recently, cybersecurity was considered an information communication technology (ICT) challenge rather than a business risk.

Aim. This finding is now driving long-term changes in the approach to the methods used to teach cybersecurity skills. The importance of cybersecurity awareness for sustainable society development is now recognized widely, but how to build an educational ecosystem that will include all target audiences that need to develop cybersecurity skills is not clear yet. In that context, skills are understood to represent a combination of abilities, knowledge, and experience that enable an individual to complete a task when working in a digital environment and using digital services [2. p. 44]. The failure to address the missing cybersecurity skills of the European labor force hurts the capacity of a modern, digitized society to successfully react to the rising number of cybercrime cases. Cybersecurity skills are becoming especially important as most experts in economic development claim [3, p. 77-84] that the digital economy's winners and losers will be determined by who has these skills. Another problem in this area is that the skills required are changing at a faster pace than usual within advanced-technology fields, due to the changes introduced by the new digital technology and fast digitalization of society.

Review of Literature. According to several authors [4, 5 pp. 232-248, pp. 49- 65], only a sustainable education for sustainable social development aims at giving people the skills and knowledge that enable them to face the challenges of the fast development of the digital economy [6 p. 77-84]. Sustainability in that context is defined as "the ability to continue an activity continuously and by pursuing the adopted goals for sustainable development". In that context, the sustainability of education focuses on the implementation of practices through educational development, leadership, and innovation [7 p. 77-84]. According to Allan Friedman

and P.W. Singer [8 p. 13-23], the interest in sustainable education is focused on students and innovative pedagogies that bring those involved in the educational process closer to social reality and its main conflicts. The main goal is to enable the students to better understand the environments where they will act every day or where they will work.

Social and economic changes have now made the issue of sustainable development more pressing than ever. As several studies have found [9 p. 22-34], education and training in universities in several areas including ICT are very technocratic, and the educational approach is not promoted in line with sustainability requirements [10 p.4-8]. According to recent studies carried out in Europe [3], education for developing sustainable skills is not sufficiently integrated with European High Educational Level programs (HEI). The active pedagogical activities that help strengthen this vision are not yet included in the majority of HEI cybersecurity programs. Actions for addressing the increased cybersecurity skills shortage have been launched in Europe in the last few years [11, 12] but as reported by the European Cyber Security Organization (ECSO) [12 p.3 7-42], and by other organizations [13 p. 77-84], they are not sufficiently viewed by the European HEI as an emerging discipline important for developing the sustainability of the digital society. This finding comes from the analysis [9 p. 77-84] of the contents of European HEI programs; it was found that these programs focus mainly on traditional cybersecurity topics as part of classical academic courses. Modern learning methodologies with hands-on training and range platforms that help in building skills have been left behind in the European HEI [5, 9]. However, several actions and efforts have recently been taken and launched by the EUC, through the activities of funded Competence Centers for Cybersecurity [13 p. 95-98], to help restructure cybersecurity programs in the HEI and among professional educational providers to overcome the existing skill gap.

Materials and methods. In the conditions of globalization and the rapid development of technologies, cyber security is becoming one of the key aspects of protecting information systems and data. The number of cyber threats and attacks that

require a high level of training of specialists in this field is increasing every year. One of the most important skills, the last one for a successful career in cyber security, is the knowledge of the English language. Consider why learning English is enough for cybersecurity professionals.

Access to the latest information and research

English is the main language of scientific research and technical documentation. State-of-the-art research, scholarly articles, and analytical reports in the field of cybersecurity are published primarily in English. Knowing English, specialists can:

Keep up with new trends: Get access to the latest developments, research, and technological innovations in the field of cyber security.

Participate in conferences: Attend international conferences and seminars where English is the main language of communication and presentations.

Global communication and cooperation

Cybersecurity is a global issue that requires international cooperation. Knowledge of the English language allows specialists to:

Work in international teams: Cooperate effectively with colleagues and experts from different countries.

Serve international customers: Communicate with customers and partners from all over the world, understand their needs, and propose appropriate solutions.

Training and certification

Many of the most popular and recognized cybersecurity certifications and training programs are available in English. This includes:

Certifications: such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security+.

Online courses and resources: access to quality online courses, webinars, and other educational resources, mostly offered in English.

Cyber threats and intelligence

Understanding and neutralizing cyber threats requires access to comprehensive threat information, most of which is documented in English. Knowledge of the

English language allows specialists to:

Monitor Global Threats: Follow the latest emerging cyber threats, vulnerabilities, and attack methods in English.

Participate in forums and communities: Participate in international cybersecurity forums and communities to share knowledge and best practices.

Documentation and reporting

Effective cybersecurity management ensures thorough documentation and reporting, often required in English. This includes:

Technical documentation: Creation and understanding of technical documentation, user manuals, and standard operating procedures.

Incident Reports: Writing clear and accurate incident reports and security assessments.

Career growth

Knowledge of the English language significantly improves the career prospects of cyber security specialists:

New job opportunities: Many top cybersecurity positions in international companies require fluency in English.

Networking: Building professional networks at international conferences and through professional associations where English is the primary language of communication.

Regulatory and regulatory requirements

Many international regulatory acts and standards in the field of cyber security are documented in English. Understanding these rules is key to compliance:

International standards: such as the General Data Protection Regulation (GDPR), ISO/IEC 27001 standards, and NIST guidelines.

Documentation of compliance: Preparation and understanding of documentation of compliance with international standards.

Access to open tools

A large part of the open tools and resources on cybersecurity are documented

in English. Knowledge of the English language allows specialists to:

Use open-source programs: Effectively use and contribute to projects such as Wireshark, Metasploit, and Snort.

Community Participation: Participate in discussions, bug reports, and changes to open projects.

Discussion.

Teachers, and students, are more vulnerable to cyberattacks due to the increased reliance on digital tools and platforms for teaching and learning. The teaching-learning process participants must be adequately trained because a lack of awareness can result in risky online behaviors that make them more susceptible to cyber threats. It should also be considered that inappropriate safety-conscious behavior can affect individuals and an entire educational institution. This research was prepared only for a small group of students from a single institution. Among the findings, the two most problematic areas are password management and not performing sensitive activities other than our computers. A further research opportunity is to compare the obtained results with data collected in a broad sample. On the other hand, the security awareness of instructors and the information security organization of educational institutions.

Conclusion

For cybersecurity students, proficiency in English is essential and far-reaching. It is the gateway to accessing comprehensive resources, participating in professional development programs, and obtaining industry-recognized certifications. English is critical for effective communication in a globally interconnected field, understanding technical terminology, and broadening career opportunities. Additionally, it enables students to contribute to research and innovation, stay informed about emerging threats, and engage in practical skills development through hands-on labs and simulations. Therefore, mastering English is not just advantageous but imperative for anyone aspiring to excel in the dynamic and rapidly evolving domain of cybersecurity.

REFERENCES

1. Caulkins, B.; Marlowe, T.; Reardon, A.C. Cybersecurity Skills to Address Today’s Threats. In Advances in Human Factors in Cybersecurity, Proceedings of the International Conference on Applied Human Factors and Ergonomics, Orlando, FL, USA, 21–25 July 2018; Ahram, T., Nicholson, D., Eds.; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2018; pp. 782–788.
2. Castro, M.P.; Zermeño, M.G.G. Challenge Based Learning: Innovative Pedagogy for Sustainability through e-Learning in Higher Education. Sustainability 2020, 12, 4063. [Google Scholar] [CrossRef]
3. Oliveira, P.M.; Gomes de Souza, K.; Reis, C.; Souza, W.M. Gamification in E-Learning and Sustainability: A Theoretical Framework. Sustainability 2021, 13, 11945. [Google Scholar] [CrossRef]
4. Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip Craig, and Donald
5. CompTIA Security+ All-in-One Exam Guide, Fifth Edition (Exam SY0-501)" by Darril Gibson
6. The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security" by Allison Cerra
7. Hacking: The Art of Exploitation" by Jon Erickson
8. **Cybersecurity and Cyberwar: What Everyone Needs to Know"** by P.W. Singer and Allan Friedman
9. The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski
10. The Impact of Language Barriers on Cybersecurity" by Megan L. McBride and Samantha E. Subin
11. Global Cybersecurity Index (GCI)" by the International Telecommunication Union (ITU)
12. Cyber Threat Intelligence: The Importance of English Proficiency" by SANS Institute

13. Douglas, D. and Selinker, L. (1993). Performance on a General Versus a Field- Field-specific test of Speaking Proficiency by International Teaching Assistants. In Douglas, D. and Selinker, L.(ed.). A New Decade of Language Testing Research (pp. 235-256). Alexandria, VA: TESOL, Inc.

14. Farkas I. et al (2014). Wireless Sensor Network Protocol Developed for Microcontroller-based Wireless Sensor Units, and Data Processing with Visualization by LabVIEW. In 2014 IEEE12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). pp.95–98.