DOI:10.24412/2470-1262-2025-1-164-173
УДК (UDC) 004.056

Mariam R. Gevorgyan
French University in Armenia (UFAR),
Yerevan, Armenia,
Institute for Physical Research, NAS (IPR NAS),
Yerevan, Armenia.
Svetlana M. Minasyan
Ijevan Branch of Yerevan State University,
Ijevan, Armenia.
Lilit M. Manukyan
Brusov State University (BSU),
Yerevan, Armenia.

For citation: Gevorgyan M.R., Minasyan S.M., Manukyan L. M. M., (2025). Exploring the Role of Cybersecurity: Interdisciplinary Perspectives and Strategies. Cross-Cultural Studies: Education and Science, Vol. 10, Issue I (2025), pp. 164-173 (in USA)

Manuscript received 06/02/2025
Accepted for publication: 25/03/2025
The author has read and approved the final manuscript.

EXPLORING THE ROLE OF CYBERSECURITY: INTERDISCIPLINARY PERSPECTIVES AND STRATEGIES

ИЗУЧЕНИЕ РОЛИ КИБЕРБЕЗОПАСНОСТИ: МЕЖДИСЦИПЛИНАРНЫЕ ПЕРСПЕКТИВЫ И СТРАТЕГИИ

Abstract:

We have been presenting the pervasive threat of cybersecurity. The article explores interdisciplinary perspectives, such as information technology discipline, types of cybersecurity. Through an in-depth analysis of cybersecurity types, this paper aims to raise awareness about the evolving threat landscape and provides actionable strategies for effective prevention. Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. They also expect the financial impact of ransomware is expected to reach approximately $265 billion annually by 2031. This forecast is based on an anticipated annual growth rate of 30% in ransomware-related damage costs over the next decade.

The conclusion emphasizes that although technology can help mitigate the effects of social engineering attacks, the real vulnerability lies in human behavior, impulses, and psychological tendencies.

Nowadays cybersecurity analyses are incredibly important for all users. Social engineering assaults are still a common and developing concern. Beyond all mentioned, one can also be proactive about privacy and security. Keeping your devices themselves is just as

important as all your other digital behaviors. 90 % of cyber-attacks involve social engineering.

In this paper we have been presenting pervasive cybersecurity, interdisciplinary perspectives, thoughts and analyses. Therefore, in the paper we have been studying types of cybersecurity and ways of using it in a conscious way.

Keywords: Cybersecurity, Social Engineering Attacks, Human Error, Human-Computer Interaction, Security Awareness, Prevention Strategies

Аннотация:

Мы представили все проникающую угрозу кибербезопасности. В статье рассматриваются междисциплинарные перспективы, такие как дисциплина информационных технологий, типы кибербезопасности. С помощью глубокого анализа типов кибербезопасности эта статья направлена на повышение осведомленности о меняющемся ландшафте угроз и предлагает действенные стратегии для эффективного предотвращения. Cybersecurity Ventures ожидает, что глобальные расходы на киберпреступность будут расти на 15 процентов в год в течение следующих пяти лет, достигнув 10,5 триллионов долларов США в год к 2025 году по сравнению с 3 триллионами долларов США в 2015 году. Они также ожидают, что финансовое воздействие программ-вымогателей, как ожидается, достигнет приблизительно 265 миллиардов долларов США в год к 2031 году. Этот прогноз основан на ожидаемом ежегодном темпе роста расходов на ущерб, связанный с программами-вымогателями, на 30% в течение следующего десятилетия.

В заключении подчеркивается, что, хотя технологии могут помочь смягчить последствия атак социальной инженерии, настоящая уязвимость заключается в поведении человека, его импульсах и психологических тенденциях.

В настоящее время анализ кибербезопасности невероятно важен для всех пользователей. Атаки с использованием социальной инженерии по-прежнему являются распространенной и растущей проблемой. Помимо всего вышеперечисленного, можно также проявлять инициативу в отношении конфиденциальности и безопасности. Сохранение самих устройств так же важно, как и все ваше другое цифровое поведение. 90 % кибератак связаны с социальной инженерией.

В этой статье мы представили всеобъемлющую кибербезопасность, междисциплинарные перспективы, мысли и анализы. Поэтому в статье мы изучили типы кибербезопасности и способы ее осознанного использования.

Ключевые слова: кибербезопасность, атаки с использованием социальной инженерии, человеческая ошибка, взаимодействие человека и компьютера, осведомленность о безопасности, стратегии предотвращения

1. Introduction

Information Technology (IT) security encompasses a broad array of cybersecurity techniques aimed at reducing the risk of unauthorized access to organizational resources, which include computers, networks, and sensitive data repositories. It is crucial for ensuring the integrity and confidentiality of sensitive information while defending against sophisticated cyber threats. This paper explores the complex landscape of IT security, delving into its core principles, evolving strategies, and its critical importance in today's organizational settings. This paper aims to provide a comprehensive understanding of IT security by exploring key topics like threat mitigation strategies, encryption technologies, and incident response mechanisms. It seeks to explain how these elements work together to protect against unauthorized access and enhance the resilience of organizational systems.

The contemporary literature on cybersecurity reflects a sophisticated and multi-dimensional field that has evolved significantly from its initial technical foundations. Early

research predominantly concentrated on the development and refinement of cryptographic protocols, network security architectures, and intrusion detection mechanisms.

In recent years, the scope of cybersecurity research has broadened substantially. Researchers now examine the intersection of technical, human, and organizational factors in cybersecurity based on social engineering.

The literature also addresses emerging challenges and innovations, including the implications of artificial intelligence, machine learning, and quantum computing for cybersecurity. The evolving state of cybersecurity research underscores a transition towards a more holistic understanding of security that integrates technical, behavioral, and systemic perspectives to address the dynamic nature of cyber threats.

Methodology

This article adopts a comprehensive and interdisciplinary approach to analyze the pervasive threat of cybersecurity, with a particular focus on social engineering attacks and the broader cybersecurity landscape. The methodology employed in this paper includes the following key components:

Literature
Data analysis
Interdisciplinary perspectives
Case studies
Expert interviews
Prevention strategies evaluation
Future projections

This methodology ensures a thorough and multifaceted exploration of the cybersecurity landscape, integrating quantitative data, qualitative insights, and interdisciplinary perspectives to provide a comprehensive analysis of current and future threats.

This methodology outlines a structured approach to analyzing cybersecurity threats, incorporating diverse sources and methods to provide a well-rounded understanding of the topic.

Types of IT security

Network security is used to prevent unauthorized or malicious users from getting inside the network. This ensures that usability, reliability, and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users' ability to access or use the network. Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to the public cloud [1, 2].

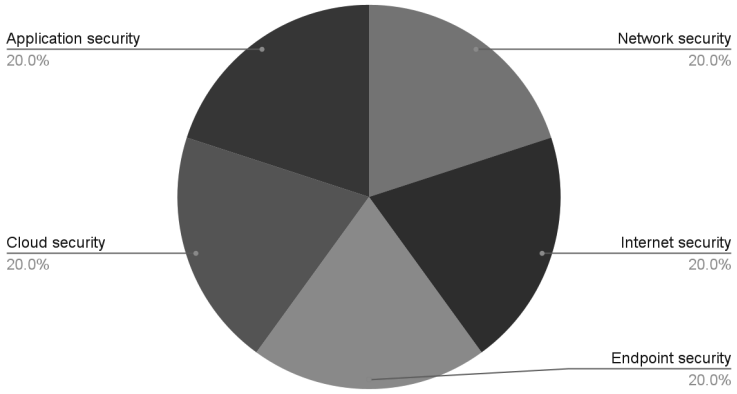
Internet security: Internet security involves protecting data transmitted through web browsers and securing the network infrastructures that support web-based applications. This includes monitoring and filtering incoming internet traffic to detect and block malware and other unwanted content. Key components of internet security include firewalls, antivirus software, and antispyware tools. Together, these tools defend against online threats and help ensure a secure browsing experience.

Endpoint security provides protection at the device level. Endpoint security protects devices such as cell phones, tablets, laptops, and desktop computers. It helps prevent these devices from connecting to malicious networks that could threaten your organization. Examples of endpoint security include advanced malware protection and device management software.

Cloud security: Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. Cloud security can help secure the usage of software-as-a-service (SaaS) applications and the public cloud. A cloud-access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

Application security: Application security involves incorporating security measures throughout the software development lifecycle to proactively address vulnerabilities and defend against potential cyber threats. This practice includes assessing the application's code to identify and rectify weaknesses, ensuring that the software is fortified against potential attacks from the outset. By integrating security into the development process, application security aims to build robust defenses and enhance the overall resilience of the software.
The visual representation of the above five types of IT security is shown in Fig. 1.

Fig. 1. Types of IT security.



2. Human-Computer Interaction

History: Early computers were extremely difficult to use. ENIAC (Electronic Numerical Integrator and Computer) was released in 1945. It was the first programmable electronic and general purpose digital computer.

In the mid 1960‘s command line interface (CLI) was used to interact with computers. CLI is light weight and requires little memory consumption.

1980‘s were the booming phase for HCI. Some of the market leaders like Apple and Microsoft play a crucial role for the modern development of HCI. GUI (Graphic User Interface) application was created that was easy to use, understand and visualize. XEROX STAR was released in 1981. It had a mouse driven graphical user interface and built-in ethernet network and protocol. It also had a laser printer. This was considered far ahead of its time.In 1983 Apple Lisa was released, it offered a document-centered graphical interface based on the metaphor of desktop.

In 1984 the first Macintosh was released and it was revolutionary. It has a good graphic user interface and a variety of fonts that makes your document more appealing to readers.

In the 1990's the internet started its journey. Communication between people becomes very easy through social networking like Email. The World Wide Web (WWW) was created by Tim Berners-Lee. It is a way for people to share information.

In 2000 mobile, laptop, tablet was a buzz word in this period. These gadgets provide more flexibility to users. Users can connect with anyone at any place. Smart phones come into picture. Users don’t need any mouse or pointing device to select anything. They can use their fingers to interact with devices. It provides more features like built-in music player, camera, weather forecast, Internet, GPS, games, video conferencing and many more.

In 2006 NINTENDO released Wii. It was famous for its rear remote controller, a handheld pointing device that detects movements in 3D. It enables users to simulate real world sports and activities through different games. This paved the way for gaming consoles like XBOX

Windows 10, released by Microsoft in 2015, is a series of operating systems designed to provide a consistent user experience across a variety of devices. With the growing popularity and diverse range of laptops and computers, Windows 10 was engineered to be adaptable to different hardware configurations, ensuring a seamless and versatile operating environment across multiple types of systems.

VR oculus rift was a revolution in virtual reality. It was launched in 2016. The rift is primarily a gaming device. However it is also capable of viewing conventional movies and videos from inside the virtual cinema environment. It is increasingly used in universities and schools as an educational tool.

Using psychology to create new models

The earliest use of computers was to solve specific problems, in mathematics, engineering, ballistics, logic. Accordingly, the research psychology of problem-solving was applied and adapted to the study of computer use. **Newell and Simon's "Information processing psychology" (1972)** described human problem solving in information-processing terms and was applied to the study of problem solving with computers. It led directly to the development of cognitive models of problem solving, from high-level descriptions of the writing process to a keystroke-level model of interaction **(Card, Moran, & Newell, 1983)**. These models have been used to predict the behavior of users solving problems with computers, and to inform the design of more effective and comprehensive computer systems. More recently, it has been recognised that people use computers for tasks that do not easily fit the problem-solving mold, such as design, exploration, and communication. New models are being developed which draw on studies of human creativity, exploration, and social interaction [3].

Human-Computer Interaction, Changes and Information Technology

Social changes are rising, as also the HCI is more and more significantly engaged in society. Trends of global society changes in HCI, it makes the distribution of information fast in all directions and has a prompt response system. For this reason, the impact on economic, political, and social changes, the result of advances in HCI, also has caused so many major changes in trends. Society had changed from industrial society to information society. The world society has changed tremendously. From agricultural society that has cultivated and created agricultural products, causing the building of houses as primary sources. Later, it is necessary to produce many products at cheap costs. Therefore, having to turn production into industrial designs, causing the living conditions of humans to change into urban society.

There is a group of residents in the city. There is an industry as a production base. Industrial society has operated and changed into the information society. Business operations use information widely. There is a new word that cyberspace has conducted various activities such as talking over the internet, buying products and services, HCI is a discipline that responds to the needs of individual users, such as communication, watching television, radio. In the past, when we turned on the television or radio receiver, we could not choose according to what we needed. If we are not satisfied, just select the new station. The trend from now on will change in a manner called on-demand. We will choose television programs to watch, and choose to listen to the radio program as needed. HCI is the discipline that plays an important role in every industry. Therefore, affecting social, cultural, moral, educational, economic and political changes, imagine that now we can watch news, watch TV programs that are distributed via satellite of various countries around the world. We can receive news immediately.

We use the internet to communicate with each other. Besides, it connects with people around the world. Therefore, the trend of cultural, economic, social and political changes has become a more global society. The status of the development of chat bots has not yet reached its goal: software that can emulate human behavior completely has not yet arrived. Nonetheless an interesting question has arisen: what can we do with a program that meets all conditions to appear as humans? Will this situation respond the same to us? We will continue to respond to society, will we remain polite, and will we continue to use our social conventions? Will we dare yell at it or show our offense?

3. Security and Privacy Engineering: The what, why and how

The mission is to support the development of trustworthy information systems by applying measurement science and system engineering principles to the creation of frameworks, risk models, guidance, tools, and standards that protect privacy and, by extension, civil liberties [2].

Privacy engineering will be central to the privacy profession going forward.That is an easy assertion to make. Privacy professionals have long discussed the importance of building privacy in rather than bolting it on - aka privacy by design. But as technology has raced ahead, the need for privacy engineering has evolved and intensified.

Privacy engineering initiative - i.e. better define what it is, why it matters and how we can support the professionals doing it. I want to share some of what I have learned from leading practitioners and renew our call for continued engagement from those working in this exciting field.

What is it?

In short, privacy engineering is the technical side of the privacy profession. Privacy engineers ensure that privacy considerations are integrated into product design. The longer answer is that it depends who you ask. Some practitioners view it as process management and others see it more as technical knowhow. Both views seem equally valid and integral. Privacy engineers today work as part of product teams, design teams, IT teams, security teams, and yes, sometimes even legal or compliance teams. It describes the need for practitioners who "understand technology and are able to integrate perspectives that span product design, software development, cyber security, human computer interaction, as well as business and legal considerations" [4].

Regardless of where they sit, privacy engineers must serve as translators between these teams, turning privacy requirements into technical realities.

Why does it matter?

Privacy engineering matters not only because it leads to better products, but because it can significantly influence a company's bottom line.

Increasing lawyers' technical knowledge, helping engineers understand the "why" behind privacy requirements, and ensuring that everyone considers user experience will lead to better products from a consumer perspective. Consumer trust can be a market differentiator so that is clearly one good reason to invest in privacy engineering. Increasingly, though, it is only one of many [5]. Today, it matters because laws, regulators, and automation demand it.

4. Approaches for Addressing Risks in Cybersecurity

Cybersecurity risks that target human psychology and manipulation to accomplish their goals are known as social engineering attacks. Creating efficient counters and solutions requires understanding these attacks' theoretical underpinnings and pertinent concepts. The section thoroughly examines the theoretical underpinnings and essential ideas in social engineering assaults based on various academic research and sources. The skill of psychological manipulation lies at the heart of social engineering attacks. The basis of this idea is the knowledge that people are prone to various cognitive biases and weaknesses. Points out that psychological manipulation generally targets emotions, trust, and cognitive shortcuts in order to take advantage of these biases. To grasp the effectiveness of social engineering assaults, one must first understand the cognitive and emotional factors that influence human decision-making [6].

One of the most common types of social engineering assaults is phishing. In order to deceive receivers into disclosing sensitive information, it entails the use of false communication and have studied phishing in great detail [7]. Attackers frequently use emails, websites, or even phone calls to give the impression that they are legitimate. Phishing attacks work well due to the manipulation of victims' perceptions and the use of persuasive language. Social engineers usually prey on emotional triggers, including fear, uncertainty, and hurry. Social engineers construct

situations that elicit fear or urgency, causing people to behave without carefully considering their actions. These emotions precede logical thought processes, leaving victims more open to deception. Understanding human weaknesses and cognitive biases is a fundamental idea in social engineering.

The literature, such as [8-10], emphasizes the significance of these biases in social engineering since they may be used to influence others. There are several established theoretical frameworks to comprehend social engineering attacks. As described by [11-13], the Extended Parallel Process Model (EPPM) Attackers frequently use emails, websites, or even phone calls to give the impression that they are legitimate. Phishing attacks work well due to the manipulation of victims' perceptions and the use of persuasive language. Social engineers usually prey on emotional triggers, including fear, uncertainty, and hurry. Social engineers construct situations that elicit fear or urgency, causing people to behave without carefully considering their actions. These emotions precede logical thought processes, leaving victims more open to deception. Understanding human weaknesses and cognitive biases is a fundamental idea in social engineering:

Financial loss
Data breaches and loss of sensitive information
Reputation damage
Psychological damage
Legal and regulatory consequences

Preventing the impact of social engineering attacks

It is evident that regardless of how technologically secure a network seems the human element will always be a vulnerability. The success rate and the number of cybercrimes are steadily on the rise due to the level of anonymity social engineering offers malicious actors. As businesses navigate this landscape, it becomes imperative for them to maintain a vigilant awareness of the diverse threat actors and their extensive array of attack vectors. By doing so, organizations can enhance their preparedness and responsiveness to these evolving cyber security challenges. There are technical and non-technical safeguards that can be implemented to lower the risk associated with social engineering to a tolerable level. Technology, education, and the enforcement of policies are all necessary components of a multipronged strategy to mitigate the effects of social engineering attacks. By implementing these tactics, people and organizations will be better equipped to ward against these persistent and changing dangers. [5, 14]. Between 2020-2021 Skybox found that there was a 106% increase in new ransomware, and RiskIQ estimates that six organizations were victimized by ransomware per minute [15-16].

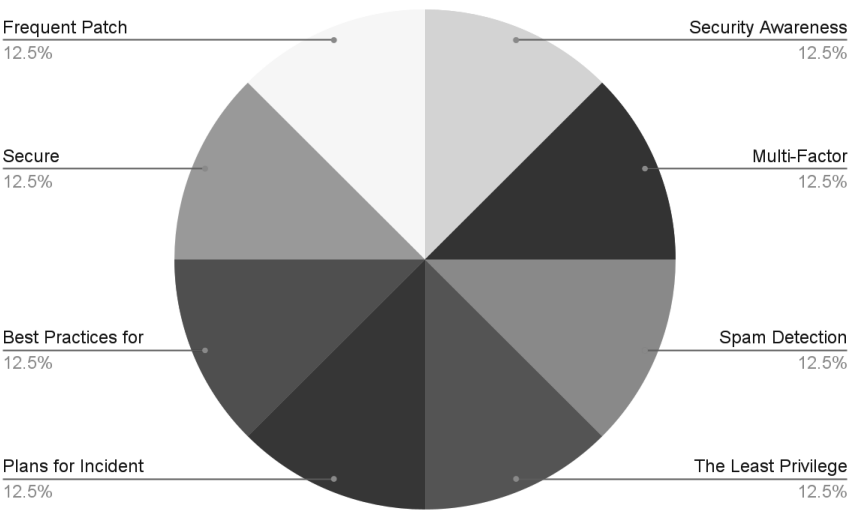


Fig. 2. Comprehensive Strategies for Enhancing Cyber Security. Addressing Cyber Security Challenges through Awareness, Technology, and Strategy.

Key Strategies for Mitigating Cyber Threats and Enhancing Security

1. Security Awareness Training

- ➢ **Description:** Equips individuals with knowledge to recognize and respond to suspicious activities.
- ➢ **Key Points:**
  - Recognize phishing attempts.
  - Real-world examples of social engineering.
  - Confirm authenticity of requests.

2. Multi-Factor Authentication (MFA)

- ➢ **Description:** Adds an extra layer of security by requiring multiple forms of identity verification.
- ➢ **Key Points:**
  - Protects against unauthorized access even with compromised passwords.
  - Should be used for email, vital systems, and sensitive data access.

3. Spam Detection and Email Filtering

- ➢ **Description:** Utilizes software to recognize and quarantine phishing emails.
- ➢ **Key Points:**
  - Analyzes sender behavior, attachments, and content.
  - Invest in reliable email filtering solutions.
  - Use spam filtering capabilities in email clients.

4. The Least Privilege Principle and Access Control

- ➢ **Description:** Restricts access to only what is necessary for job functions.
- ➢ **Key Points:**
  - Reduces risk of insider threats and unauthorized access.
  - Regularly review and adjust access rights.
  - Use role-based access control and access control lists.

5. Plans for Incident Response and Security Policies

- ➢ **Description:** Defines acceptable conduct, security measures, and response guidelines.
- ➢ **Key Points:**
  - Create and communicate security policies.
  - Develop incident response plans with steps for handling and recovering from incidents.

6. Best Practices for User Authentication

- ➢ **Description:** Promotes the use of strong, unique passwords and secure password management.
- ➢ **Key Points:**
  - Use and regularly update secure passwords.
  - Employ password managers and consider passphrases.
  - Enforce password policies.

7. Secure Communication Channels and Encryption

- ➢ **Description:** Protects sensitive data during transmission through encryption.
- ➢ **Key Points:**
  - Use secure communication methods like VPNs and encrypted email services.
  - Encrypt data using recognized algorithms.

8. Frequent Patch Management and Software Updates

- ➢ **Description:** Addresses vulnerabilities through regular updates and patches.
- ➢ **Key Points:**
  - Regularly update software, operating systems, and applications.
  - Implement a robust patch management procedure.
  - Enable automatic updates where possible.

5. Conclusion

The aim of the paper is about a huge challenge in today's cyber security efforts, which are the lack of effective information security awareness and training. Many organizations and companies of the public and the private sector continue to believe that cyber security is only a technical, not a strategic and behavioral discipline.

In the article it is shown that multifactor authentication is a common and often effective way for organizations to confirm that the person accessing the systems should actually have that access. The article asserts that integrating education, robust technical safeguards, and stringent policies enables both individuals and organizations to strengthen their defenses and mitigate the risks associated with social engineering attacks. It also illustrates how advancements in Human-Computer Interaction (HCI) have been crucial in transitioning societies from industrial paradigms to information-centric frameworks. This shift underscores the profound impact of technology on societal structures and behaviors, ushering in an era where the flow of information and digital connectivity fundamentally transform how individuals and communities engage, innovate, and progress.

The impact of social engineering attacks is a stark reminder of the potentially severe consequences on financial, reputational, and security fronts. Considering immediate and long-term implications, a comprehensive approach to addressing these attacks is needed.

Mitigation and prevention strategies emphasize the importance of security awareness, multi-factor authentication, and robust incident response plans.

The reviews we found can be used by practitioners in overcoming cyber security problems. They can carry out development based on a collaboration of several approaches to prevent the mentioned problems.

References:

1. URL: https://www.crowdstrike.com/cybersecurity-101/it-security/
2. Manukyan L., Gevorgyan M., "Social engineering attacks: How to prevent", Journal of Digital Science, 2024. DOI: 10.33847/2686-8296.6.1_3.
3. Siricharoen W. V. licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license, 2019. DOI:10.4108/eai.13-7-2018.160762. URL: http://creativecommons.org/licenses/by/3.0/
4. Gurses S., Jose M. Del Alamo, Guitton (1 June, 2020). "Privacy Engineering: Shaping an Emerging Field of Research and Practice". IEEE Security and Privacy Magazine 14(2):40-46, 2016. DOI: 10.1109/MSP.2016.37.
   URL:
   https://www.researchgate.net/publication/300367232_Privacy_Engineering_Shaping_an_Emerging_Field_of_Research_and_Practice
5. Mathieu J. Guitton (1 June, 2020). "Cybersecurity, social engineering, artificial intelligence, technological addictions: Societal challenges for the coming decade". Computers in Human Behavior. **107**: 106307.
   URL: https://doi.org/10.1016/j.chb.2020.106307
6. Mogha M., Sharma R., Tanwar S., Rana A., and Jain V., "Artificial intelligence predictability of human emotion in psychology," in 2021 9th International Conference on Reliability, Infocom Technologies and Optimisation (Trends and Future Directions) (ICRITO), 2021. URL: https://doi.org/10.1109/ICRITO51393.2021.9596210
7. Dhamija R., Tygar J. D., and Hearst M., "Why phishing works," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006. URL: https://dl.acm.org/doi/10.1145/1124772.1124861

8. Noorehbahani F. and Zarein Z., "The impact of demographic factors on persuasion strategies in personalized recommender systems," in 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE), 2018. DOI:10.1109/ICCKE.2018.8566550
9. G. Sofia, S. Marianna, L. George and K. Panos, "Investigating the role of personality traits and influence strategies on the persuasive effect of personalized recommendations", *CEUR Workshop Proc.*, vol. 1680, pp. 9-17, 2016.
10. M. Bilgic and R. J. Mooney, "Explaining Recommendations: Satisfaction vs. Promotion", *Proc. Beyond Pers. 2005 A Work. Next Stage Recomm. Syst. Res. 2005 Int. Conf. Intell. User Interfaces*, pp. 13-18, 2005.
11. Worthington A. K., "Fear appeals: The extended parallel process model", in Persuasion Theory in Action: An Open Educational Resource, 2021. URL:https://ua.pressbooks.pub/persuasiontheoryinaction/chapter/fear-appeals-the-extended-parallel-process-model/
12. Peters, G. J. Y., Ruiter, R. A., & Kok, G. (2013). Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. Health Psychology Review, 7(sup1), S8-S31.
13. Rhodes, R. E., & Dickau, L. (2013). Moderators of the intention-behavior relationship in the physical activity domain: a systematic review. British Journal of Sports Medicine, 47(4), 215-225.
14. "Social Engineering Defined". Security Through Education. Retrieved, 2021. URL:https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/
15. "Vulnerability and Threat Trends Report 2021", Skybox Security, 2021. https://www.skyboxsecurity.com/trends-report/
16. "RiskIQ's 2021 Evil Internet Minute | RiskIQ", RiskIQ, 2021. https://www.riskiq.com/resources/infographic/evil-internet-minute-2021

Information about the Authors:
Gevorgyan Mariam R. (Yerevan, Armenia) - PhD in Physics, Associate Professor
PhD, Institute for Physical Research, NAS /IPR NAS/. Professor, Faculty of Informatics and Applied Mathematics, French University in Armenia /UFAR/.ORCiD, http://orcid.org/-0000-0003-2927-0437
E-mail: mariamgevorgyan89@gmail.com
Minasyan Svetlana M.(Yerevan, Armenia) –*Ph.D., Professor of the Department of Foreign Languages, Ijevan Branch of Yerevan State University, Ijevan, Armenia.*
ORCiD, https://orcid.org/0000-0001-9301-4927
Email: s.minasyanpmesi@gmail.com
Lilit M. Manukyan (Yerevan, Armenia) -The founder of "Bekial" scientific-cultural NGO
Brusov State University /BSU/, Yerevan, Armenia.
ORCiD, https://orcid.org/0009-0002-2621-5053
Email: manukyanlilith@gmail.com

Acknowledgments: *Thanks for the positive feedback Professor Harry Walter, Ernst – Moritz – Arndt University, Greifswald, Germany.*

Author's contribution: *The work is solely that of the author.*