Social engineering as a component of professional competence in information security of future computer science teachers

Bohdan M. Oliinyk[1] [0000-0003-3670-2605]
and Vasyl P. Oleksiuk[2,1] [0000-0003-2206-8447]

[1] Institute for Digitalisation of Education of the NAES Ukraine,
9 M. Berlynskoho Str., Kyiv, 04060, Ukraine
[2] Ternopil Volodymyr Hnatiuk National Pedagogical University,
2 Maksyma Kryvonosa Str., Ternopil, 46027, Ukraine
olijnyk_b@iitlt.gov.ua, oleksyuk@fizmat.tnpu.edu.ua

Abstract. The article considers the actual problem of information security – social engineering. The authors investigate what social engineering is and its main methods, including phishing, vishing, baiting, and pretexting, and analyze the educational programs of the speciality "014.09 Secondary Education (Informatics)" regarding the availability of relevant competencies. The article analyzes data on the components of professional competencies in information security and social engineering of the leading educational institutions of the USA, the EU, and Ukrainian higher education institutions; based on the analyzed data provided in general, the relationship between training in cyber security and social engineering. The authors also explore the role of future computer science teachers in protecting students from the threats of social engineering. They note that a critical factor in this protection is teaching students to recognize and eliminate social engineering threats and how to protect their sensitive information.

Keywords: social engineering · types of social engineering attacks · information security · professional competence in information security

1 Introduction

In the modern digital world, where technologies are becoming not only an integral part of our daily lives but also a dominant factor in many aspects of our existence, information security issues are becoming critically important. With each advancement in technology, not only does the amount of digital data we generate and process increase, but also its significance for our personal lives, business, and even national security. "Information security threats carry great risks that can turn into significant losses not only for organizations that have not implemented an information protection system but also for the whole country", writes Platonenko [28].

Every day, the volume and importance of digital data containing personal and commercial information increases. As Lupton [19] notes: "People's interactions online, their use of mobile and wearable devices, and other 'smart' objects and their movements in sensor-embedded spaces all generate multiple and constant flows of digital data, often about intensely personal actions and preferences, social relationships, and bodily functions and movements" [19, p. 1599]. Therefore, proper provision and protection of this data becomes a critical task for everyone who uses digital technologies. Along with this, many threats to digital systems arise as a result of the activities of their users or administrators. That is, the problem of protection is not only a technical problem but also concerns personality, views, beliefs, attitudes and activities. In this regard, these aspects should be taken into account when training specialists working with digital technologies.

When it comes to cybercrime cases, one can hear about technical vulnerabilities. However, in reality, in most cases of cybercrime, the human element is used as the most vulnerable link in cyberattacks. These attacks use social engineering mechanisms; the statistics on this practice are staggering. As Reed [29] notes, "In the broad world of cyber attacks, 98% involve social engineering on some level. It could involve masquerading as a trusted contact to encourage an employee to click a malicious link or email, pretending to be a reliable banking institution to capture login credentials, or similar activities designed to gain entry into target systems."

So, the question lies in studying the reasons for the effectiveness of social engineering methods and technologies for attackers. As is known, modern digital systems are developed taking into account security rules that are constantly updated to ensure the elimination of vulnerabilities and the actualization of protections. The same cannot be said about people. The thinking of many users is usually scattered and occupied by many things that (with the exception of those working in the field) negatively affect the level of security of computer systems. Hadnagy and Fincher [12] explores the psychological manipulation involved in phishing and other forms of social engineering, demonstrating that human error can bypass even the most sophisticated security systems. The authors focus on how the human factor remains the weakest link in cybersecurity, reinforcing the idea that no system with human interaction is completely secure from manipulation.

Lack of knowledge and not paying special attention are the main reasons why social engineering attacks are so successful. In addition, a person's general information, such as name, city of residence, address, and even names of relatives, can be publicly available and easily found on the Internet. This personal information is the key to building trust and establishing relationships with victims in order to obtain other, more useful information. "Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system", notes Gragg [10, p. 6].

Modern social engineering technologies, such as deepfake videos and voices, are becoming more realistic every day, making it difficult to distinguish between a real conversation or request for specific information and an attempt at violation.

As the analysis of scientific literature shows, the study of social engineering issues in educational programs for training future computer science specialists is a new area of research. Aycock's [7] article highlights an approach to teaching social engineering using improvisation techniques. It aims to improve students' understanding of basic concepts of social engineering by engaging them in interactive and improvisational activities. The author's exercises help students understand the peculiarities of human behaviour and manipulation tactics used by attackers in attacks.

Hermosilla et al. [14] investigate how the implementation of social engineering methods affects the preparation of communication skills of future computer science specialists. As a result of the experiment, the researchers conclude that students need to study effective communication strategies that can be demonstrated based on social networks.

Another aspect of social engineering training is the consideration of ethical issues of network interaction as a value component of the professional competencies of computer science specialists. Relevant issues are present in several Computer Science Curricula documents, starting from 2013 [15]. García-Holgado et al. [9] discusses the experience of integrating ethical issues of using computer technologies into the curriculum of "Software Engineering" and "Human-Computer Interaction" disciplines. The authors state that their approach helps students understand the social, legal, ethical and cultural issues related to social engineering and broader computer science topics.

Research by Hazzan and Har-Shai [13] focuses on the importance of soft skills in computer science education. They emphasize that communication skills, teamwork, emotional intelligence, communication and ethical behaviour are as necessary as algorithmic and technical competencies. Training in the author's course prepares students' ability to counter cyber and social engineering threats effectively.

Other studies concern the creation of a digital environment for social development, research on its impact on students' communication and cooperation [8], studying the role of generative artificial intelligence for social engineering attacks [30], using game and flipped classroom techniques in the process of studying social engineering technologies [26].

The purpose of the article is to study social engineering as a content and activity component of the training of a modern computer science teacher. To achieve the goal, it is necessary to solve the following tasks:

1. Review the concept of "social engineering" and systematize its main methods.
2. Analyze foreign experience and domestic educational programs for training future computer science teachers regarding the presence of competencies related to social engineering.
3. Provide recommendations for future computer science teachers and their students on preventing the harmful effects of social engineering on their professional and educational activities.

2 Social engineering and its main methods

Considering the concept of "social engineering", directed manipulation of a person is highlighted in order to perform specific actions and provide certain information. Mouton et al. [21] writes that the "art" of influencing people to disclose confidential information is known as social engineering, and the process of doing this is known as a social engineering attack. Social engineering methods are diverse and usually aimed at the victim, using their feelings and personal qualities—for example, negligence, greed, trust, and sympathy.

The concept of "social engineering" was introduced into cybersecurity by Kevin Mitnick, who was a famous hacker in the 1990s [20]. He used social methods to gain access to information and systems, using not technical but human weaknesses. Such illegal actions increased attention to this problem and popularized the concept of social engineering in cybersecurity. Now, most crimes of this kind occur in cyberspace due to the fact that social engineering technologies are constantly developing and are complemented by new schemes and types. Let us consider the most common of them.

2.1 Phishing

One of the most popular types of social engineering is phishing attacks, which consist of sending emails and SMS messages in order to create a sense of urgency, curiosity or fear in victims [11]. Then, they encourage users to disclose confidential information, click on links to dangerous sites or open attached files that may contain viruses.

An example may be an email sent to users of an online service, notifying them of a policy violation that requires immediate action, such as changing a password. The letter contains a link to a fake website almost identical to the official version, which forces an unsuspecting user to enter their own credentials or even change the password. After submitting the form, the information is sent to the attacker.

Since identical or almost identical messages are sent to all users in phishing campaigns, their detection and blocking are much easier at the mail server level. As Aleroud and Zhou [6] emphasize, the widespread use of social media creates a favourable ground for phishing attacks due to the increase in the volume of personal information exchange but insufficient awareness and actions to protect information.

2.2 Vishing

This is one of the forms of phishing, which also uses social engineering methods, but already uses phone calls [16]. Now, this form has gained particular popularity, and quite often, one can receive such calls.

A typical scenario of actions of attackers known as "vishers" is as follows: a call comes to a mobile phone from a bank employee, and the operator warns that if complete information about the bank card is not provided by phone now, the card will be blocked. A gullible user, hearing such a "threat", immediately panics and can give away all personal data, including the verification code from SMS.

Also, during vishing, a profitable purchase with a significant discount may be offered, or information about winning in some promotion may be announced.

2.3 Baiting

This method uses a false promise to evoke the victim's greed or curiosity. Fraudsters "bait" users into a "trap" to steal their personal information or infect their computers with malicious software.

The most common means of this method is the use of physical media to spread malware. For example, attackers leave electronic media [18], usually flash drives, infected with malware in prominent places where potential victims will definitely see them (for example, in toilets, elevators, in the parking lot of the target company). Victims pick up this medium out of curiosity and insert it into a work or home computer, which leads to the automatic installation of malware.

Baiting attacks do not necessarily have to be carried out in the physical world. Online forms consist of attractive advertisements that lead to malicious sites or that encourage users to download a file infected with malware.

2.4 Pretexting

Using this method, an attacker tries to obtain information using a series of skillfully fabricated deceptions. Fraudsters invent plausible stories or pretexts to force victims to provide personal information or access to an account. Such schemes present a false but plausible scenario to gain the victim's trust and make them feel comfortable disclosing certain information. The effectiveness of this method lies in the attacker's ability to convince a person that their actions or requests are legitimate and require an immediate response [5].

Fraudsters using this social engineering method collect various types of information, such as bank card data, phone numbers, addresses, and even security information related to a physical enterprise.

3 Cybersecurity as a technological basis of social engineering

Today, social engineering receives not only large amounts of confidential information about people, networks and devices but also more attack channels with the widespread use of social networks, the Internet of Things (IoT), the industrial Internet, mobile communications and smartphones. Analysis of scientific publications shows that social engineering research can be conditionally classified in conceptual, methodological and experimental directions. In particular, Chinese scientists have developed a conceptual model that provides an understanding of how social engineering attacks work [34]. It is based on human vulnerabilities (such as influence, persuasion, deception and manipulation) that attackers use to violate cyberspace security goals (for example, confidentiality, integrity, and availability).

Wang et al. [33] proposes a domain ontology for social engineering in cybersecurity. The authors identified the basic concepts of social engineering and the types of relationships between these concepts. The ontology provides a formal knowledge scheme for understanding, analyzing, reusing and sharing knowledge about social engineering. In the security ontology, social engineering, social engineering attack, person and human vulnerability were respectively aligned as child classes of attacker, attack, asset and vulnerability; two more concepts were also added to the model, such as the media through which attacks are carried out and social engineering methods. Pilkevych et al. [27] conclude that increasing user competence is the most effective method of countering internal threats. They proposed a method for assessing the impact of personnel competence on the information security of the institution. The author's method takes into account models of violators and models of information threats that are developed for a specific institution. The method proposes to assess the competence of the institution's personnel according to three components: the level of knowledge, skills and character traits (personal qualities).

Currently, social engineering is a set of methods that attackers use to study the human psyche in order to gain access to confidential data or systems [31]. In the context of this study, it is vital to know the features of the functioning and protection of digital tools, which is the subject of cybersecurity study. In view of this, let us consider the components of professional competencies of future bachelor or master of computer science related to the protection of digital systems. To do this, we will briefly analyze the experience of teaching relevant disciplines in leading universities in the USA and the EU (table 1).

As the analysis of the websites of the universities listed in the table from the USA and Europe shows, their training programs emphasize a wide range of skills, research abilities and practical applications, which reflects the diversity of modern digital technologies. Summarizing this list, we can distinguish the following groups of disciplines:

- *Mathematical foundations of cyber defense.* The mentioned universities offer fundamental training starting from the basics of cryptography, on the basis of which training is carried out to solve urgent problems of network security, cyber-physical systems, etc. Training in the field of cryptography, formal methods, and data confidentiality is offered by bachelor's and master's programs at the University of Oxford, ETH Zurich, and others.
- *Computer systems and networks.* Here, the main emphasis is on security tasks in the design, implementation, and administration of computer networks and systems. Institutions such as the University of Cambridge and the Technical University of Munich focus on understanding computer architectures, networks, and cybersecurity, teaching students to design and manage secure systems.

Table 1. Components of professional competencies in cybersecurity and social engineering of educational institutions in the USA, Europe [4, 23, 32].

Educational institution	Higher education level	Competency	Learning outcomes	Disciplines in which competencies are developed or formed
University of California, Berkeley	Bachelor	Knowledge of computer systems and networks	Ability to design, implement and administer information systems and computer networks	Computer networks, operating systems, cybersecurity
Massachusetts Institute of Technology	Master	Deep understanding of software engineering	Develop complex software systems and ensure their security	Software engineering, system security, data structures and algorithms
Stanford University	Bachelor	Proficiency in programming languages	Ability to write effective and secure code	Introduction to computer science, programming methodologies, database systems
Harvard University	Master	Expertise in Data Science and machine learning	Application of Data Science methods to solve real problems	Data science, machine learning, Big Data systems
New York University	Bachelor	Proficiency in social engineering methods	Ability to understand and mitigate social engineering threats	Cybersecurity, social engineering, information security awareness
University of Cambridge	Bachelor	Understanding of computer architectures and networks	Design and management of computer networks	Computer architecture, Network systems, Information security
Technical University of Munich	Master	Deep knowledge in software development and IT security	Develop secure software applications and systems	Software engineering, IT security, cryptography
University of Oxford	Bachelor	Proficiency in theoretical computer science and algorithms	Solving complex computational problems	Algorithms, theory of computation, data structures
ETH Zurich	Master	Expertise in artificial intelligence and machine learning	Implement artificial intelligence and machine learning solutions	Artificial intelligence, machine learning, data analysis
University College London	Bachelor	Understanding of social engineering and security policies	Development of strategies to prevent social engineering attacks	Social engineering, cybersecurity policy, information security

- *Software engineering and data science.* Research and innovation. Universities emphasize software engineering, system security, data science, and machine learning, preparing students to work with complex software systems and make data-driven decisions. Educational programs provide for mastering achievements in the fields of artificial intelligence, machine learning, and big data. The University of Oxford and ETH Zurich focus on both theoretical computer science (algorithms, computation theory) and practical applications (artificial intelligence, machine learning).
- *Cybersecurity and social engineering.* The training programs highlight competencies in understanding and mitigating social engineering threats. For example, New York University and University College London integrate courses on cybersecurity and social engineering. This is done so that future specialists can develop strategies for preventing and responding to social engineering attacks.

Since information security is an interdisciplinary field, leading universities often work to create close ties with industry partners and other educational institutions. Another trend in student training in the USA and Europe is the in-depth study of AI and machine learning to prepare students to use these technologies as tools for protecting digital systems.

The Ukrainian experience of forming competencies of future specialists in social engineering and cybersecurity is also interesting. Let us consider the educational-professional programs (EPP) of Ukrainian higher education institutions that train students in the speciality 014.09 Secondary Education (Informatics). Although these specialists are not professionals in the field of cybersecurity, they conduct the educational process, work in educational environments with the personal data of students, and are also directly responsible for their training and development of skills in information and cybersecurity. As the review of university websites shows, the relevant disciplines are educational components of both bachelor's and master's programs (table 2).

Table 2: Components of professional competencies in cybersecurity and social engineering of Ukrainian higher education institutions (based on [1–3]).

Educational institution	Higher education level	Professional (special) competency	Program learning outcomes	Disciplines in which competencies are developed or formed
Zhytomyr Ivan Franko State University	Bachelor	Proficiency in technologies of debugging, maintenance and operation of a computer network; ability to	Ability to design information web resources with integration of external data and software products, using information	Methods of teaching informatics, Use of digital technologies in the educational process, Computer architecture and configuration of

Continued on next page

Table 2 – continued from previous page

Educational institution	Higher education level	Professional (special) competency	Program learning outcomes	Disciplines in which competencies are developed or formed
		implement a set of measures aimed at ensuring information security; ability to form skills of safe work of students in a computer network.	protection methods based on knowledge of basic Internet protocols, models and structures of Internet servers. Knows and understands the legal principles of using information and communication technologies; is able to implement means and methods of information protection and security on the Internet.	computer systems
Ternopil Volodymyr Hnatiuk National Pedagogical University	Bachelor	Ability to apply methods and means of ensuring information security, develop and operate special software for protection of information resources of critical information infrastructure objects.	Knowledge of basics of computer architecture and computer networks, server technologies of web application creation, and ability to apply them in the process of substantiation of technical support of information systems.	Computer networks, Operating systems, Basics of cybersecurity, Information security of computer systems, Cryptographic protection technologies
Ivan Franko National University of Lviv	Master	Knowledge and understanding of general principles of functioning and architecture of computer systems and basics of operating systems, mastery of system and application software.	Knowledge of technologies for building computer networks, including wireless; knowledge of data transmission protocols and rules of information security. Ability to apply this knowledge in practice to support the network at school.	Information technologies in education, Client-server architecture, Technologies of computer system modelling

Continued on next page

Table 2 – continued from previous page

Educational institution	Higher education level	Professional (special) competency	Program learning outcomes	Disciplines in which competencies are developed or formed
Kremenchuk Mykhailo Ostrohradskyi National University	Master	Ability to organize the work of a team of performers, make appropriate and economically justified organizational and managerial decisions, ensure safe working conditions	Demonstrate knowledge of basic Internet protocols, models and structures of Internet resources, organization of information web-resources with integration of external data and software products, methods of information protection	Computer-information technologies in education and science, Computer virology, Information and communication technologies in higher education
Izmail State Humanitarian University	Bachelor	Professional mastery of computer and communication equipment; use of data protection tools	Ability to organize students' activities in the lesson in compliance with rules and recommendations for preserving students' health; implement means and methods of information protection and security on the Internet.	Computer networks and Internet, Computer architecture and configuration of computer systems, Use of ICT in management and educational process of educational institution, Protection of information in information systems
Zaporizhzhia National University	Bachelor	Ability to debug, maintain, operate computer network and ensure safe work of students in it.	Provides information protection and security in local and global networks.	Computer networks and Web-programming

As can be seen from the table 2, the professional competencies of future computer science teachers combine technical knowledge, practical skills and pedagogical abilities. The professional competencies from table 2 can be classified as:

- *Technical competence.* The programs stipulate that teachers should have a deep understanding of the architecture of information systems, computer networks, and the Internet and in particular, be able to configure, maintain and operate these systems. For this, they need knowledge of the capabilities of data protection tools and methods of ensuring information security.

- *Competencies in integrating educational technologies for the use of digital technologies in education.* Modern computer science teachers should be able to select and integrate digital technologies (ICT) into the educational process. In the educational context, the protection of data and personal information of students is also provided for in the EPP.
- *Competencies in teaching computer science.* Mastery of computer science teaching methods is the key to ensuring that future teachers will be able to convey complex technical concepts to students effectively. Educators should monitor compliance with health and safety standards for students' activities in the classroom. In particular, this also applies to activities in the digital environment. To do this, they need to understand and apply methods of preventing and countering social engineering attacks, contributing to raising students' awareness of information security.

So, in the analyzed EPPs, the relationship between training in cybersecurity and social engineering is generally reflected. For example, Izmail State Humanitarian University, Zaporizhzhia National University and Zhytomyr Ivan Franko State University offer separate normative disciplines for the development of relevant competencies. Other universities may form these competencies within elective courses, the names of which are not reflected in their educational programs.

4 The role of the computer science teacher in protecting students from social engineering threats

Given the relevance and prevalence of social engineering, it is especially important that future computer science teachers are skilled in the technical aspects of digital technologies and understand the social aspects of information security, particularly social engineering.

The best way to protect against social engineering attacks is to teach students to recognize and eliminate threats. For example, when a person receives an email saying that their account has been hacked, they panic and experience a rush of adrenaline and fear. That is, there is a physical reaction to what the person has just read, and this is what the attackers' plans are focused on. Scammers want you to act quickly and thoughtlessly while under this internal influence. It is important to teach students not to act impulsively, even if they are in an elevated emotional state. Teach them to know about signs of social engineering and what they should do if they think they have received a fraudulent message; for example, tell a teacher or parent.

In addition, all students should be reminded not to post personal information online. This information helps attackers research potential victims and create more plausible attacks. Teachers and students should also use different passwords for each of their accounts, which will prevent credential substitution if scammers obtain one of their passwords.

Despite the human factor, some technologies can help protect the school from social engineering attacks. Endpoint protection and spam filters can prevent phishing emails from reaching recipients, and they can also protect the network if a user accidentally clicks on a malicious link. Multi-factor authentication is another solution that can protect against social engineering. Kamiński et al. [17] notes that an account without two-factor authentication cannot be considered secure. It needs to be enabled everywhere – it greatly enhances the security of the account. This "second factor" can come both as an SMS message and as a confirmation code that is generated on the user's smartphone in an application, for example, Google authenticator [22].

Based on the analysis of the above sources and educational programs, as well as our own experience, we will describe the competencies that future computer science teachers should master in order to be able to teach the topics "Cyber defence" and "Information security" at the highest professional level:

1. Technological competencies in:
   - Basics of cybersecurity, which involve understanding threats, vulnerabilities, risks and countermeasures.
   - Network security, which requires students' awareness of network security principles, protocols and technologies.
   - Cryptography, in particular knowledge of cryptographic algorithms, key management skills and digital signatures.
   - Operating system security regarding understanding of relevant mechanisms, vulnerabilities and protection methods.
   - Application security, which includes knowledge of application security principles, their vulnerabilities and requirements for secure use of third-party code.
   - Incident response through detection, localization, and elimination of threats, as well as system recovery and incident analysis.
2. Pedagogical competencies regarding:
   - Curriculum development, as the ability to create interesting and interactive learning materials using various teaching methods and technologies.
   - Assessment is the ability to conduct assessments to measure student learning outcomes in information and cybersecurity.
   - Differentiated learning is the ability to adapt teaching methods for conducting differentiated learning for students with different needs and abilities.
   - Technology integration, which involves the ability to integrate technological tools and resources into cybersecurity training effectively.
   - Emotional intelligence and critical thinking, which are necessary for the effective development of problem-solving and critical thinking skills in students during cybersecurity training.
3. Professional competencies and personal qualities:
   - Practical knowledge of ethical hacking methods and tools for vulnerability assessment and penetration testing.
   - Ability to assess and manage cybersecurity risks in the educational environment.
   - Understanding of relevant laws and regulations in the field of cybersecurity.

– Effective communication and collaboration with students, colleagues and parents on cybersecurity issues.
– Desire for continuous professional development in the field of cybersecurity.
– Ability to collaborate with other educators, IT professionals and external stakeholders to improve cybersecurity education.
– Desire to learn about new cybersecurity threats and technologies.
– Ability to adapt to the rapidly changing cybersecurity landscape.
– Ability to effectively respond to cybersecurity incidents and challenges.
– Adherence to ethical principles of safe use of digital technologies.

In our opinion, the training of students in the speciality 014.09 Secondary Education (Informatics) should be interdisciplinary and carried out within the disciplines of general and professional training. In-depth development of the above competencies should be carried out within elective disciplines, which can be devoted to issues of automation of protection processes, social issues of cyber defence, testing of digital systems for penetration, etc. To increase the effectiveness of training future computer science teachers, it is advisable to deploy and use cloud-oriented learning environments [24, 25].

5 Conclusions

Nowadays, social engineering has become one of the most common and effective attacks in cyberspace. Attacks of this type use the person as the weakest component of cyberspace. Since people have their flaws and weaknesses, they can be easily manipulated, which allows attackers to carry out various fraudulent actions, from stealing personal information to using computers to send malware.

However, it should be noted that increasing user awareness of social engineering methods and skills in recognizing attacks can significantly reduce their effectiveness. It is important to teach students to distinguish suspicious situations, recognize threats, and understand how to protect their confidential information.

In school information security training, attention should be focused on the importance of caution when receiving unsolicited electronic messages or phone calls, checking the authenticity of websites, and using reliable passwords. Students should also be taught to identify signs of social engineering, such as unknown or suspicious links, requests for immediate action, or provision of confidential data.

Mastering the competencies defined in the study will contribute to the fact that computer science teachers will be able to form the necessary knowledge and skills in students in order to educate the future generation as informed and responsible citizens of the digital society who are able to protect themselves and others from cyber threats. However, verification of this hypothesis requires quality organization and the conduct of one or more pedagogical experiments, which may be a promising stage for the continuation of this study.

References

[1] Osvitno-profesiina prohrama “Serednia osvita (Informatyka)” druhoho (mahisterskoho) rivnia vyshchoi osvity za predmetnoiu spetsialnistiu 014.09 - Serednia osvita (Informatyka) spetsialnosti 014 - Serednia osvita haluzi znan 01 – Osvita/Pedahohika (2020), URL https://ami.lnu.edu.ua/wp-content/uploads/2020/10/OP_Serednia_osvita_informatyka_2020_proekt.pdf

[2] Osvitno-profesiina prohrama “Serednia osvita (Informatyka)” pershoho (bakalavrskoho) rivnia vyshchoi osvity za predmetnoiu spetsialnistiu 014.09 Serednia osvita predmetnoii spetsialnosti 0.14.09 - Serednia osvita (Informatyka) haluzi znan 01 – Osvita / Pedahohika (2021), URL https://www.znu.edu.ua/opp/bak/math/opp_so-inform_21.pdf

[3] Osvitno-profesiina prohrama “Serednia osvita (Informatyka, matematyka, osnovy STEM-navchnnia)” Pershoho (bakalavrskoho) rivnia vyshchoi osvity za spetsialnistiu 014 Serednia osvita haluzi znan 01 Osvita/Pedahohika (2022), URL https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni_prohramy/bakalavr/fizmat/014.09_2022.pdf

[4] Technical University of Munich: The Entrepreneurial University - TUM (2024), URL https://www.tum.de/en

[5] Abdulla, R.M., Faraj, H.A., Abdullah, C.O., Amin, A.H., Rashid, T.A.: Analysis of Social Engineering Awareness Among Students and Lecturers. IEEE Access **11**, 101098–101111 (2023), https://doi.org/10.1109/ACCESS.2023.3311708

[6] Aleroud, A., Zhou, L.: Phishing environments, techniques, and countermeasures: A survey. Computers & Security **68**, 160–196 (2017), https://doi.org/10.1016/j.cose.2017.04.006

[7] Aycock, J.: Teaching Social Engineering Using Improv. In: Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 2, p. 629–630, ITiCSE ’21, Association for Computing Machinery, New York, NY, USA (2021), https://doi.org/10.1145/3456565.3460037

[8] Bani-Salameh, H., Hjeela, F.A., Bani-Salameh, D.: Using Social Development Environments in Introductory Computer Science Classrooms: A Case Study on SCI. In: 2017 Second International Conference on Information Systems Engineering (ICISE), pp. 22–26 (2017), https://doi.org/10.1109/ICISE.2017.15

[9] García-Holgado, A., García-Peñalvo, F.J., Therón, R., Vázquez-Ingelmo, A., Gamazo, A., González-González, C.S., Gil Iranzo, R.M., Frango Silveira, I., Alier Forment, M.: Experiencia piloto para incorporar la ética informática de forma transversal en el Grado de Ingeniería Informática - [Pilot experience to mainstream computer ethics in the Computer Science Degree]. In: Innovaciones docentes en tiempos de pandemia, p. 431–436, CINAIC 2021, Servicio de Publicaciones Universidad (2021), https://doi.org/10.26754/cinaic.2021.0082

[10] Gragg, D.: A Multi-Level Defense Against Social Engineering. White paper, SANS Institute (2022), URL https://sansorg.egnyte.com/dl/AbCFV3mA3o

[11] Gupta, S., Singhal, A., Kapoor, A.: A literature survey on social engineering attacks: Phishing attack. In: 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 537–540 (2016), https://doi.org/10.1109/CCAA.2016.7813778

[12] Hadnagy, C., Fincher, M.: Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Wiley (2015)

[13] Hazzan, O., Har-Shai, G.: Teaching Computer Science Soft Skills (Abstract Only). In: Proceedings of the 46th ACM Technical Symposium on Computer Science Education, p. 704, SIGCSE '15, Association for Computing Machinery, New York, NY, USA (2015), https://doi.org/10.1145/2676723.2678289

[14] Hermosilla, P., Boye, N., Roncagliolo, S.: Teaching Communication Strategies in Social Networks for Computer Science Students. In: Meiselwitz, G. (ed.) Social Computing and Social Media. User Experience and Behavior, Lecture Notes in Computer Science, vol. 10913, pp. 57–66, Springer International Publishing, Cham (2018), https://doi.org/10.1007/978-3-319-91521-0_5

[15] Joint Task Force on Computing Curricula, Association for Computing Machinery (ACM), IEEE Computer Society: Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. Association for Computing Machinery, New York, NY, USA (2013), https://doi.org/10.1145/2534860

[16] Jones, K.S., Armstrong, M.E., Tornblad, M.K., Siami Namin, A.: How social engineers use persuasion principles during vishing attacks. Information & Computer Security **29**(2), 314–331 (Dec 2020), https://doi.org/10.1108/ics-07-2020-0113

[17] Kamiński, K.A., Dobrowolski, A.P., Piotrowski, Z., Ścibiorek, P.: Enhancing Web Application Security: Advanced Biometric Voice Verification for Two-Factor Authentication. Electronics **12**(18), 3791 (2023), https://doi.org/10.3390/electronics12183791

[18] Lawson, P.A., Crowson, A.D., Mayhorn, C.B.: Baiting the Hook: Exploring the Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. In: Bagnara, S., Tartaglia, R., Albolino, S., Alexander, T., Fujita, Y. (eds.) Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018), Advances in Intelligent Systems and Computing, vol. 822, pp. 401–406, Springer International Publishing, Cham (2019), https://doi.org/10.1007/978-3-319-96077-7_42

[19] Lupton, D.: Feeling your data: Touch and making sense of personal digital data. New Media & Society **19**(10), 1599–1614 (2017), https://doi.org/10.1177/1461444817717515

[20] Mitnick Security Consulting LLC: The History of Social Engineering & How to Stay Safe Today (2024), URL https://www.mitnicksecurity.com/the-history-of-social-engineering

[21] Mouton, F., Leenen, L., Venter, H.: Social engineering attack examples, templates and scenarios. Computers & Security **59**, 186–209 (2016), https://doi.org/10.1016/j.cose.2016.03.004

[22] Nash, A., Studiawan, H., Grispos, G., Choo, K.K.R.: Security Analysis of Google Authenticator, Microsoft Authenticator, and Authy. In: Goel, S., Nunes de Souza, P.R. (eds.) Digital Forensics and Cyber Crime, pp. 197–206, Springer Nature Switzerland, Cham (2024), https://doi.org/10.1007/978-3-031-56583-0_13

[23] New York University: NYU (2024), URL https://www.nyu.edu

[24] Oleksiuk, V.P.: Yedyna systema avtentyfikatsii yak krok do stvorennia osvitnoho prostoru zahalnoosvitnoho navchalnoho zakladu. Scientific Journal of the Mykhailo Dragomanov Ukrainian State University. Series 2. Computer-oriented learning systems (13 (20)), 188–193 (Feb 2012), URL https://sj.udu.edu.ua/index.php/kosn/article/view/343

[25] Oleksyuk, V.P.: Designing of university cloud infrastructure based on Apache Cloudstack. Information Technologies and Learning Tools **54**(4), 153–164 (Sep 2016), https://doi.org/10.33407/itlt.v54i4.1453

[26] Olivindo, M., Veras, N., Viana, W., Cortés, M., Rocha, L.: Gamifying Flipped Classes: An Experience Report in Software Engineering Remote Teaching. In: Proceedings of the XXXV Brazilian Symposium on Software Engineering, p. 143–152, SBES '21, Association for Computing Machinery, New York, NY, USA (2021), https://doi.org/10.1145/3474624.3476971

[27] Pilkevych, I.A., Boychenko, O., Lobanchykova, N., Vakaliuk, T.A., Semerikov, S.: Method of Assessing the Influence of Personnel Competence on Institutional Information Security. In: Hovorushchenko, T., Savenko, O., Popov, P.T., Lysenko, S. (eds.) Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 24-26, 2021, CEUR Workshop Proceedings, vol. 2853, pp. 266–275, CEUR-WS.org (2021), URL https://ceur-ws.org/Vol-2853/paper33.pdf

[28] Platonenko, A.: Techodology of providing functional security for wireless communication systems based on the improvement of the password policies. The dissertation is for the degree of a candidate of technical sciences in specialty 05.13.06 - Information technologies, Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv (2019), URL https://itgip.org/wp-content/uploads/2019/10/dis-1.pdf

[29] Reed, C.: 30 Social Engineering Statistics – 2023 (2023), URL https://firewalltimes.com/social-engineering-statistics/

[30] Schmitt, M., Flechais, I.: Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing (2023), URL https://arxiv.org/abs/2310.13715

[31] Siddiqi, M.A., Pak, W., Siddiqi, M.A.: A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Applied Sciences **12**(12), 6042 (2022), https://doi.org/10.3390/app12126042

[32] The President and Fellows of Harvard College: Harvard university (2024), URL https://www.harvard.edu

[33] Wang, Z., Zhu, H., Liu, P., Sun, L.: Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecurity **4**(1), 31 (Aug 2021), https://doi.org/10.1186/s42400-021-00094-6

[34] Wang, Z., Zhu, H., Sun, L.: Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access **9**, 11895–11910 (2021), https://doi.org/10.1109/ACCESS.2021.3051633