Online-Journals.org

iJEP International Journal of Engineering Pedagogy

iJEP | eISSN: 2192-4880 | Vol. 16 No. 3 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijep.v16i3.61231

PAPER

Enhancing Social Engineering Awareness through Intergenerational Mentoring and Gamified Learning in Engineering Education

Zoltan Marton (✉), Zoltan Rajnai, Gyorgy Molnar

Obuda University, Budapest, Hungary

marton.zoltan@uni-obuda.hu

ABSTRACT

This study examines the awareness of social engineering (SE) and the need for cybersecurity education among undergraduate engineering students at Obuda University in Hungary. A total of 173 participants, primarily from Generation Z and without a formal specialization in cybersecurity, completed a structured questionnaire. The questionnaire assessed familiarity with the SE concept, exposure to manipulation, confidence in detection, and openness to intergenerational mentoring. The results revealed moderate knowledge levels (5.4/10) and high exposure to suspicious messages, primarily through social media and instant messaging platforms. Most participants (92%) expressed a strong need for further cybersecurity education. The preferred formats were practice-oriented and included simulations, expert-led sessions, and hands-on workshops. Students perceived older adults as more vulnerable (61%), yet approximately one-third reported helping or receiving help from other generations regarding digital safety. These results underscore the necessity of a contextualized, participatory approach to cybersecurity education. The study proposes an intergenerational mentoring model that combines the digital fluency of younger learners with the caution and life experience of older users. This approach could bolster cybersecurity awareness in engineering and teacher training programs.

KEYWORDS

social engineering (SE), cybersecurity awareness, cybersecurity education, gamification, mentoring, generation z, human factors, engineering education, educational technology, digital literacy

1 INTRODUCTION

Social engineering (SE) encompasses a range of techniques that exploit psychological manipulation to deceive individuals into revealing confidential information or performing unauthorized actions [1], [2]. In cybersecurity, it targets the

Marton, Z., Rajnai, Z., Molnar, G. (2026). Enhancing Social Engineering Awareness through Intergenerational Mentoring and Gamified Learning in Engineering Education. *International Journal of Engineering Pedagogy (iJEP)*, 16(3), pp. 35–52. https://doi.org/10.3991/ijep.v16i3.61231

Article submitted 2026-01-13. Revision uploaded 2026-03-03. Final acceptance 2026-03-05.

human factoro—ften cited as the most vulnerable element in an organization's defenses [1], [3]. Research shows that susceptibility to SE is not limited by demographics such as age or profession, making virtually all users potential targets [2], [4].

The World Economic Forum reported in 2022 that approximately 95% of cybersecurity incidents involve some form of human error or manipulation, highlighting that technical safeguards alone are insufficient [3]. The education sector is similarly at risk: schools and universities have increasingly become targets of phishing, fraud, and other SE attacks, with documented cases of staff unwittingly disclosing sensitive data or transferring funds to malicious actors [4].

To the existing discussion on cybersecurity awareness in the education sector, it is critical to expand the geographical context to ensure relevancy to Central Europe. Awareness of cybersecurity threats, particularly SE tactics such as phishing, is a paramount concern across various educational institutions. A recent study from Poland emphasizes the importance of raising awareness regarding cybersecurity among university students. In this study, it was revealed that despite the high engagement of students in online activities, their knowledge about cybersecurity risks was limited, underscoring an urgent need for targeted educational programs [5]. This finding is supported by a comparative evaluation conducted at a university in England, which assessed the knowledge and awareness of students regarding cybersecurity threats, revealing strikingly low levels of awareness [6], [37]. The study highlighted that while students are actively involved in digital environments, their preparedness to respond to cybersecurity incidents needs significant improvement. Recent studies confirm this vulnerability; for example, 66% of educational sector respondents in Saudi Arabia lacked prior knowledge of SE, indicating the urgent need for awareness programs [4]. This is further supported by a large-scale survey conducted at the University of Sulaimani, which found that both students and academic staff demonstrated limited awareness of SE threats, including phishing, despite high exposure rates [35].

There is growing interest in how generational differences influence susceptibility to SE. Individuals across age cohorts (e.g., Baby Boomers, Generation X, Millennials, and Generation Z) exhibit distinct technological habits and communication preferences that may shape their vulnerability to deception [19], [20]. A widespread assumption is that older generations, who did not grow up with digital technology, are more prone to online fraud. Supporting this view, empirical studies have shown that older adults are indeed more susceptible to phishing and deception than younger cohorts, often due to emotional and cognitive factors [21], [22].

However, recent findings complicate this perception. According to a 2023 report by Deloitte, members of Generation Z were over three times more likely to fall for online scams than Baby Boomers [7]. While younger users tend to be proficient with digital platforms, their behavioral patterns—such as frequent social media use and preference for mobile apps—may expose them to highly tailored scam techniques. Moreover, younger adults often display higher trust in online content; for example, a Pew Research Center survey noted that adults under 30 are almost as likely to trust information from social media as from traditional news outlets [23]. In contrast, older individuals may be more vulnerable to scams exploiting emotional manipulation (such as phone scams involving relatives in distress), yet they typically approach unfamiliar digital content with greater caution [8]. These intergenerational variations highlight the need for systematic research in educational contexts where multiple generations of educators and students interact.

Educators occupy a critical position in the SE threat landscape. As individuals, teachers can be directly targeted via phishing emails or fraud schemes (for instance,

attackers impersonating school administrators) [9]. As professionals, educators are also expected to guide students in developing safe digital practices and cybersecurity awareness. This dual responsibility requires teachers to both protect their own digital assets and serve as role models for younger generations. Despite this pivotal role, studies indicate many teachers feel insufficiently prepared for cybersecurity threats. Surveys report that a significant proportion of educators have received minimal cybersecurity training and lack confidence in teaching related content [10]. While common threats like phishing are widely recognized (e.g., over 75% of teachers are aware of phishing attacks [11]), more advanced forms of SE—spear phishing, deepfake-based scams, etc,—remain under-recognized by most educators [12]. These findings point to an urgent need for continuous, targeted professional development. Generic one-off training is often ineffective; research shows that programs tailored to user characteristics (age, experience, technical proficiency) are far more successful in changing security behavior [23], [24]. Empirical studies further confirm that customized, data-driven training interventions significantly reduce phishing susceptibility and improve long-term retention of secure digital practices [23], [24].

To address these gaps, the present study explores engineering students' awareness and preparedness regarding SE in an educational context, with particular attention to age-related perceptions within a predominantly Generation Z cohort. We conducted a questionnaire-based study among university students at two faculties of Obuda University, Hungary. The participants were engineering and IT students concurrently enrolled in a pedagogical course related to mentoring, which provided a unique context to examine mentoring dynamics. The survey assessed students' awareness of manipulation strategies, their self-efficacy in digital safety, and their attitudes toward intergenerational mentorship in cybersecurity.

The aim of this study is to provide an evidence-based analysis of how SE awareness and defense education can be improved in engineering higher education. Specifically, the study seeks to

1. quantitatively evaluate students' knowledge, perceptions, and experiences regarding social engineering;
2. examine age-related differences within the student cohort;
3. relate these findings to previous research on cybersecurity education and mentoring; and
4. propose pedagogical considerations that integrate intergenerational knowledge transfer to strengthen cybersecurity awareness.

2 METHODOLOGY

Participants: The sample consisted of N = 173 undergraduate students from the Faculty of Electrical Engineering and the Faculty of Informatics at Óbuda University, Hungary. All participants were enrolled in a pedagogical course on mentoring that included modules on psychological manipulation in digital environments. The cohort was predominantly composed of members of Generation Z (born in 1997 or later), representing the typical age group of Hungarian university students.

A small number of older respondents were present, but their count was too low to enable separate statistical comparisons; therefore, for analysis we treated the group as a single cohort with awareness of generational issues. The group was predominantly male, which aligns with the typical gender distribution in Hungarian engineering education—in Hungary, women account for less than one-third of STEM graduates [26], [27].

Most students were majoring in information technology or electrical engineering, with a few from security sciences or education-related fields. Importantly, none of the participants were specializing in cybersecurity or safety engineering. Thus, their perspectives represent technologically skilled but non-specialist users—individuals who use digital systems frequently but have only basic formal training in cybersecurity. All participation was voluntary and anonymous. Students gave informed consent and could skip any survey question they found uncomfortable, although the vast majority completed every item.

Survey Instrument: We developed a structured questionnaire in Hungarian (with key technical terms also provided in English for clarity). The instrument consisted primarily of closed-ended questions (multiple choice and Likert-scale items), plus one optional open-ended question. The survey content was informed by previous cybersecurity awareness questionnaires (for example, the design drew on elements of the Human Aspects of Information Security Questionnaire (HAISQ) for baseline ideas [28], as well as custom questions tailored to the context of higher education and mentoring. The final questionnaire included five sections:

1. **Background and technology use:** Collected demographic data (age, gender, study program) and self-assessed digital proficiency. It also asked about the frequency of using communication platforms (email, social media, and messaging), as usage habits can influence exposure to manipulation attempts.
2. **Knowledge of SE concepts:** Assessed awareness of common SE terms and techniques. Students were asked whether they had heard of the term "social engineering" in a cybersecurity context and which specific attack techniques they recognized from a list (e.g., phishing, baiting, pretexting). A short scenario-based question described a potential phishing email to test if they could identify it as malicious. Each correct recognition or response contributed to an overall knowledge score (maximum 10 points).
3. **Personal experience and exposure:** Asked whether students had personally encountered suspicious messages or attempts (such as phishing emails, scam messages on social media, fraudulent phone calls) and whether they or someone close to them had ever fallen victim to a SE attack. This section gauged real-world exposure and incident awareness from personal experience.
4. **Attitudes and self-efficacy:** Used a series of statements with 5-point Likert agreement scales (1 = Strongly Disagree to 5 = Strongly Agree) to measure students' confidence in recognizing manipulation and their perceptions of vulnerability. Example statements included: "I am confident I can recognize a phishing attempt," "I believe older individuals are more easily deceived online than younger ones," and "I feel I have received adequate preparation to deal with SE risks." These items captured self-efficacy and any perceived generational differences in susceptibility.
5. **Preventive practices and mentoring willingness:** Explored what security precautions students currently take and their openness to intergenerational knowledge exchange on cybersecurity. Questions asked about practices like using strong passwords, verifying email sources, or enabling two-factor authentication, as well as whether the student had ever helped someone from a different generation (or received help) regarding online safety. Another item asked if they agreed that mutual mentoring between younger and older people could improve cybersecurity awareness. A final open-ended prompt invited suggestions on how intergenerational collaboration could be implemented in practice.

The questionnaire was **pilot-tested** with five students having similar backgrounds to the target sample to ensure clarity and appropriate terminology. Based on their feedback, minor wording adjustments were made. The estimated completion time for the final survey was about 10–15 minutes.

Data analysis: We applied both descriptive and inferential statistics to analyze the responses. For each closed-ended question, we first calculated frequencies (percentages of respondents selecting each option) and computed mean scores where applicable (e.g., average Likert ratings). An overall SE knowledge score (0–10 scale) was computed by awarding one point per correct answer on knowledge-based items (recognizing terms or identifying the phishing scenario). Likewise, a self-efficacy score was derived by averaging the Likert-scale responses related to confidence in recognizing and handling SE threats; higher scores indicated greater perceived competence. The internal consistency of the Likert scale items was acceptable (Cronbach's alpha = 0.79).

For inferential analysis, we explored associations between certain background factors and awareness measures. For example, chi-square tests were used to examine relationships between categorical variables (such as prior exposure to phishing attempts vs. knowledge of SE concepts), and one-way ANOVAs were conducted to test differences in scores across groups (e.g., by study discipline or gender). Statistical significance was set at $p < 0.05$. Given that the sample was overwhelmingly Generation Z, age-group comparisons could not be meaningfully tested. Any observed differences by subgroup (for instance, between IT majors and others) are noted, but overall, the results are interpreted as **exploratory** rather than confirmatory. In addition to quantitative analysis, we performed a qualitative review of the open-ended responses about intergenerational mentoring to contextualize the statistics with real examples and insights.

3 RESULTS

We present the key findings from the survey, organized into thematic categories corresponding to our research focus. Table 1 provides an overview of the questionnaire structure and hypotheses, while subsequent tables summarize detailed results for selected areas. We focus on students' general awareness of SE, their self-confidence and generational perceptions, personal experiences and current security practices, and their training needs and mentoring attitudes.

Table 1. Research hypotheses and corresponding questionnaire sections

Hypothesis/Focus	Survey Items	Description
H1: Familiarity with SE concepts	Items 1–3	Awareness of the term "social engineering" and knowledge of common attack types (phishing, etc.)
H2: Confidence in identifying manipulation attempts	Items 4–6	Self-efficacy in recognizing phishing or other SE tactics (Likert-scale statements)
H3: Perceived vulnerability across generations	Items 7–10	Beliefs about whether older vs. younger people are more susceptible to online manipulation
H4: Attitudes toward education and mentoring adequacy	Items 11–15	Perceived sufficiency of one's cybersecurity training; openness to further training and intergenerational mentoring.

3.1 Awareness of social engineering

Overall, the survey revealed a **moderate level of awareness** of core SE concepts among students, with considerable variation across specific terms. About **38%** of respondents said they had heard the term *"social engineering"* in a cybersecurity context, indicating that the concept itself was not familiar to the majority. In contrast, recognition of the term *"phishing"* was much higher: as shown in Figure 1, roughly **75% recognized phishing as a known attack method**. Awareness of more specialized attack techniques was very low—for example, only **15%** correctly recognized the term *"pretexting,"* and a mere **8%** were familiar with *"baiting"* as a concept (despite these being common SE tactics). This pattern suggests that students are aware of the most basic and publicized form of SE (phishing emails) but lack familiarity with subtler or less-publicized manipulation methods.

When presented with a short realistic phishing scenario (an email asking for account credentials), about **67%** of respondents correctly identified it as suspicious or malicious. However, **18%** were unsure about the email's legitimacy, and the remaining **15%** actually thought the phishing scenario seemed like a legitimate message. In other words, roughly one in three students failed to confidently recognize a blatant phishing attempt in the scenario, highlighting a notable gap in applied awareness.

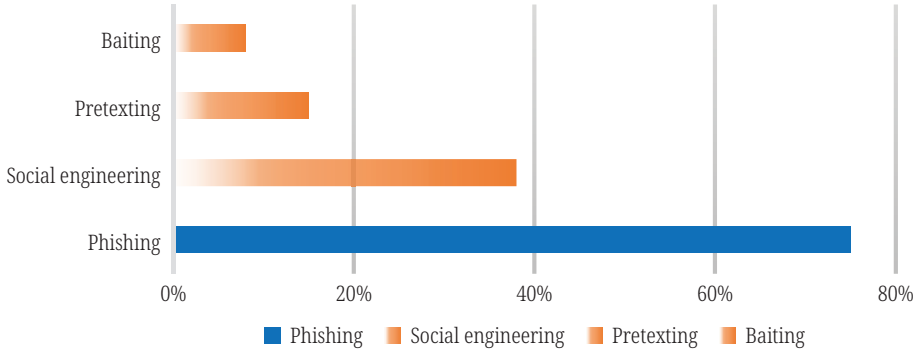

Fig. 1. Awareness of common SE terms among students [14], [15]

When presented with a short, realistic phishing scenario (an email requesting account credentials), **67%** of respondents correctly identified it as suspicious or malicious, while **18%** were uncertain and **15%** considered it legitimate. In other words, nearly one-third of students were unable to confidently recognize a clear phishing attempt, revealing a notable gap in applied cybersecurity awareness.

To assess factual and applied understanding, we calculated an **aggregate cybersecurity knowledge score** based on two components: recognition of SE terminology and correct identification of the phishing scenario. The mean score was **5.4 out of 10** (median = 5), indicating that students, on average, answered about half of the knowledge-related questions correctly. However, the distribution was highly uneven: some participants—particularly those from IT-related programs—scored between 8 and 10, demonstrating strong conceptual familiarity, whereas about 20% scored 3 or below, exposing significant deficiencies in baseline awareness. This disparity suggests that prior exposure, learning experiences, and personal interest in cybersecurity vary greatly among engineering students, as illustrated in Figure 2.

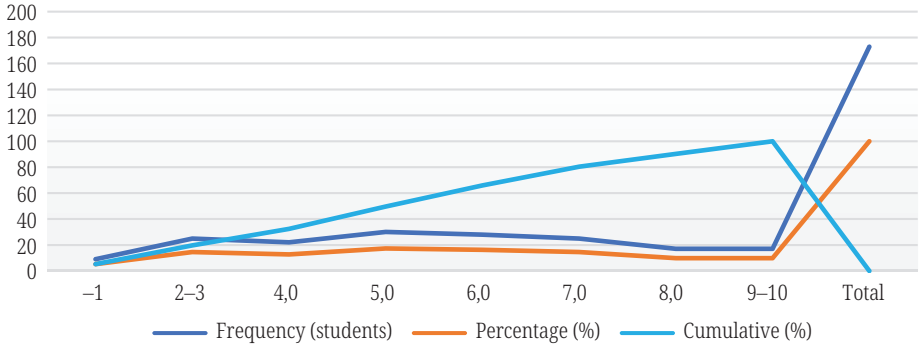

Fig. 2. Cybersecurity knowledge score distribution (N = 173)

3.2 Confidence and generational perceptions

Despite the sample being mostly Generation Z students, participants expressed clear opinions about how **age might relate to cybersecurity savvy**. A majority perceived generational differences in vulnerability: **61%** of students believed that *older adults are more easily deceived online* than younger people. Only **13%** felt that younger individuals (their own age group) might be more at risk, while the remaining ~26% thought that all age groups are equally vulnerable to SE. These perceptions mirror common societal stereotypes that associate older age with lower digital competence. At the same time, many students acknowledged strengths in other generations—for example, in open-ended comments, some noted that older adults tend to be "more cautious" and "skeptical about unsolicited messages," whereas younger users might be "more impulsive" or overly trusting of social media content. Participants thus recognized distinct **behavioral vulnerabilities** across age groups, even if they tended to overestimate the protective role of being digitally native. Notably, our data did not include enough older respondents to test actual age-based differences in awareness; these findings reflect students' *perceptions* rather than a measured generational comparison.

When it came to **self-efficacy**, students reported moderate-to-high confidence in their own ability to identify manipulation attempts. For instance, about **68%** of respondents agreed (somewhat or strongly) with the statement "I am confident I can recognize a phishing attempt," and similarly 59% agreed they can usually detect if someone is trying to manipulate them online. On a 5-point scale, the average self-rated confidence was **around 3.7** (with 5 being "Strongly Agree"), indicating a generally positive self-assessment of their detection skills [36]. However, only **32%** of students agreed that they have received **adequate preparation** to deal with SE risks, which points to a recognized shortfall in formal education or training on this topic (despite their personal confidence). Table 2 illustrates some of these self-assessment results.

Table 2. Self-reported confidence in identifying manipulation attempts (N = 173)

Survey Statement	Mean	SD	Agreement (%)
I am confident I can recognize a phishing attempt.	3,9	0.8	68%
I can usually detect when someone tries to manipulate me online.	3,6	0.9	59%
I believe I can protect myself from most online scams.	3,5	0.9	57%
I feel I have received adequate preparation to deal with SE risks.	2,8	1.0	32%

These results show a mixed picture: students feel somewhat confident in their personal ability to handle threats, but a large majority admit they have not been taught enough about these risks. This gap between **personal confidence and formal preparation** is important. It suggests that while tech-savvy young adults trust their instincts (perhaps due to general digital fluency), they also recognize their education has not fully equipped them for the sophisticated nature of SE attacks.

3.3 Personal experience and security practices

The survey asked students about their **direct experiences** with SE attempts. A striking finding was that exposure is extremely common: about **68%** of respondents reported that they had personally received at least one suspicious message or encountered a likely fraud attempt (such as a phishing email, scam on social media, or fraudulent phone call). Fortunately, very few students reported suffering any actual harm or serious consequence from these attempts—most either ignored or recognized the scams in time. However, a significant minority were uncertain if they had ever been targeted, which could indicate that some incidents went unrecognized. These figures confirm that **the majority of students have already faced SE tactics** in some form, underlining the relevance of SE awareness for all.

We also evaluated students' **current cybersecurity practices** to gauge how they protect themselves in day-to-day digital life. The results were encouraging in terms of basic hygiene: for example, **70%** of students said they routinely check an email sender's address or source before opening links or attachments, and about **65%** use strong passwords or a password manager—indicating fairly widespread adoption of these fundamental precautions. Around half (**50%**) reported using two-factor authentication on at least some of their accounts, and **55%** said they regularly update their operating system or antivirus software. These numbers suggest that a solid foundation of protective behaviors is present in the cohort, likely due to their general tech knowledge. On the other hand, **10%** of respondents admitted that they do not follow any deliberate protection strategies (for example, they might not actively think about security at all). This small but notable subgroup may represent those at higher risk, as they have a more careless online approach despite being in a tech field.

Interestingly, differences emerged among subgroups of students. Those in IT-related majors tended to report slightly better security habits on average (and had higher knowledge scores) compared to those in other engineering programs—likely reflecting greater exposure to IT concepts. However, these differences were not very large, and our sample size limited rigorous statistical comparison. Overall, the **takeaway is that most engineering students do practice basic online safety, yet a lack of comprehensive training means some risks (especially sophisticated ploys) might still catch them off-guard.**

Most students have not received substantial **formal education or training in cybersecurity.** Only about **28%** said they had ever attended any kind of cybersecurity-related course, lecture, or workshop (even a one-off seminar). Similarly, just **18%** had participated in an institutional awareness program (such as a campus-organized phishing simulation or security awareness campaign). Over half of the students (**57%**) indicated they have had **no structured training or instruction** on cybersecurity topics at all—neither in their curriculum

nor through workplace or extracurricular workshops. This finding reveals a considerable gap: despite operating daily in digital environments, many future engineers are essentially self-taught (or not taught) when it comes to security awareness. Only a small fraction (15%) had even tangentially been involved in teaching others or peer mentoring about cybersecurity (e.g., through a project or informally), showing that topics like cybersecurity are not yet embedded in their educational or mentoring activities.

3.4 Training needs and mentoring attitudes

Encouragingly, students demonstrated a strong **desire to learn more** and improve their cybersecurity readiness. When asked if they felt a need for additional cybersecurity education, **92%** of respondents said yes—an overwhelming majority clearly recognizing that their current knowledge is insufficient. In fact, **95%** indicated they would actively attend a cybersecurity awareness training if it were offered to them, which shows exceptional willingness to engage with this subject. This level of interest is a critical opportunity for educational institutions (refer to Table 3).

The survey also probed **how** students would prefer to learn such material. There was a clear preference for active, hands-on learning: **85%** of students preferred interactive workshops or expert-led seminars over simply reading materials or online tutorials. Many also specifically suggested having **simulated phishing exercises or real-case demonstrations**; about 40% mentioned these as desirable training tools, indicating support for gamified or practical learning formats (refer to Table 3). In short, today's engineering students favor *participatory and experiential learning* approaches for cybersecurity—they want to practice recognizing and handling threats in realistic settings, rather than passively absorb information.

Another key focus was attitudes toward **intergenerational mentoring** as a strategy for cybersecurity awareness. Students largely embraced the idea that different generations can help each other. **88%** agreed that intergenerational knowledge exchange (younger and older people learning from one another) could improve cybersecurity awareness for everyone involved (see Table 3: **Mentoring & Intergenerational Exchange**). Importantly, many students have already engaged in such exchange in their personal lives: nearly one-third (**32%**) reported that they have *advised an older person* (such as a parent, grandparent, or older colleague) about some digital safety issue or taught them something about staying safe online. Likewise, about **27%** said they have *received advice from an older adult* about being cautious online (for example, a parent warning them about scams or an experienced mentor giving security tips). These numbers show that informal two-way mentoring between generations is already happening to some extent, even if not formally organized. Students seem to recognize the value of these interactions—younger individuals can contribute technical know-how, while older individuals contribute skepticism and experience. The strong support for intergenerational mentoring signals an untapped resource: **structured programs that connect generations could leverage this mutual learning potential for better cybersecurity outcomes** (refer to Table 3). Table 3 highlights selected metrics from the survey, including current behaviors, training exposure, and attitudes. The "%" columns refer to the percentage of respondents endorsing each item.

Table 3. Summary of key quantitative results (N = 173)

Category	Item/Metric	%	Key Insight
Protective behaviors	Regularly check email sender's address authenticity	70%	High baseline vigilance in verifying sources
	Use strong passwords or a password manager	65%	The majority follow secure password practices
	Use two-factor authentication (2FA) on ≥1 account	50%	Half-implemented multi-factor authentication
	Keep the system and antivirus up-to-date	55%	Moderate adherence to system protection upkeep
	No deliberate protective strategies (none of the above)	10%	Small at-risk group with careless security habits
Cybersecurity education	Ever attended any cybersecurity course/workshop	28%	Formal instruction has reached only a minority
Exposure & training	Participated in an institutional security campaign	18%	Very low institutional engagement so far
	Any form of prior cybersecurity training (formal or informal)	43%	Over half have no prior training experience (57% none)
	Aware of an official university cybersecurity policy	20%	Institutional policies not widely known (if they exist)
	Receive IT security bulletins/alerts from university	44%	Some organizational communication, but not universal
Training needs & preferences	Feel the need for additional cybersecurity education	92%	Very strong demand for more learning opportunities
	Would attend cybersecurity training if offered	95%	Nearly all are willing to participate in training
	Prefer interactive workshops or seminars (vs. reading)	85%	Clear preference for participatory, hands-on learning
	Suggest simulated phishing or real-case demos	40%	Many explicitly support gamified/ practical exercises
Mentoring & intergenerational exchange	Have advised an older person on digital safety	32%	Informal "reverse mentoring" (young → old) already common
	Have received advice from an older person about online caution	27%	Many have learned from older adults' experience
	Agree that cross-generational mentoring can help security	88%	Strong belief in the value of two-way intergenerational learning
Overall indicators	Mean knowledge score (0–10 scale)	5.4	Moderate conceptual knowledge (on average ~50% correct)
	Mean self-efficacy score (1–5 scale)	3.7	Moderate confidence in ability to handle threats
	Personally encountered phishing/ fraud attempt (yes)	68%	High exposure—the majority have faced scams firsthand

Note: Some percentages may not sum to 100% due to questions allowing multiple selections or due to rounding.

4 DISCUSSION

The findings of this study provide empirical evidence that complements existing research on **SE awareness** and human factors in cybersecurity. Prior studies have often focused on working adults or cross-sector populations; by examining engineering students in higher education, our research offers new insights into how future professionals understand and approach SE risks. The results also contribute to the emerging field of **cybersecurity pedagogy**, which integrates technical training with behavioral awareness, critical thinking, and mentoring. In particular, the observed openness to intergenerational knowledge sharing suggests that universities can serve as key environments for cultivating mutual learning, digital responsibility, and resilience across age groups.

Below, we discuss the implications of our results in three thematic areas: (1) generational perceptions and behavioral susceptibility, (2) gaps in students' recognition of SE threats, and (3) strategies for education and mentoring to strengthen cybersecurity awareness.

4.1 Generational perceptions and vulnerabilities: Myth vs. Reality

Our study illustrates that perceptions of generational vulnerability are prevalent among young engineering students, yet the actual patterns of risk are more nuanced than simple age-based stereotypes. As noted, most participants (61%) viewed older individuals as more susceptible to online manipulation, and very few thought their own generation might be at higher risk. This perspective reflects a common narrative that equates older age with lower digital competence. However, our data and existing evidence suggest that **age alone is not a determinant** of vulnerability—instead, different age groups face different types of challenges.

Despite their high digital familiarity, many of our Gen Z respondents recounted close calls with phishing or scam messages, implying that technical fluency does not guarantee immunity to deception. This is consistent with reports in the literature that heavy engagement with online platforms can actually increase exposure to tailored scams [7]. Younger users who spend a lot of time on social media or mobile apps may encounter more frequent and more convincing SE lures (e.g., personalized scam messages) and, due to fast-paced online interactions, might rely on habit and visual cues rather than careful verification. Prior research has shown that individuals who constantly multitask across digital channels often develop automated behavioral responses that reduce critical scrutiny when something unusual (yet superficially plausible) appears [28]–[30]. In our sample, even some tech-savvy students admitted being almost fooled by scam emails, underscoring that overconfidence or habitual clicking can be dangerous.

Conversely, older adults—though often presumed less tech-savvy—might approach digital interactions with more caution. Life experience and a higher skepticism of "too good to be true" offers can make older users pause and double-check, even if they are not as fluent with technology. Students' comments highlighted this: they observed that their parents or elder mentors tend to "**trust but verify**" and avoid impulsive clicking, which can be a protective behavior. On the flip side, younger people's comfort with technology might lead to **lower risk perception**; for example, they might trust familiar app interfaces or common communication formats without suspecting something could be amiss.

Taken together, our findings support a balanced view: **no generation has an absolute advantage** against SE. Younger users' overconfidence and exposure can be as risky as older users' lower technical knowledge. Each group has distinct vulnerabilities—impulsivity and high exposure for the young vs. potential lack of technical understanding (and susceptibility to certain emotional scams) for the old. Therefore, educational interventions should avoid reinforcing simplistic generational stereotypes. Instead, training should emphasize that **everyone** is at risk in different ways and focus on fostering awareness of one's own behaviors and blind spots. Encouraging students to reflect on their personal habits (e.g., "Do I click too quickly? Do I verify sources?") can help them recognize that being young and tech-savvy doesn't exempt them from mistakes. As future mentors and professionals, if students develop this kind of reflective mindset, they will be better equipped to both protect themselves and guide others without bias.

4.2 Recognition gaps in SR awareness

Although most students demonstrated a basic awareness of common SE techniques, we identified significant **recognition gaps** in their knowledge. Many participants struggled with less obvious manipulation tactics: terms like pretexting and baiting were unfamiliar to the vast majority. Additionally, about one-third of students failed to recognize a straightforward phishing scenario, either by misjudging it as legitimate or being unsure. These gaps indicate that **conceptual knowledge does not always translate into practical recognition**. Even digitally skilled students can miss cues if they have not seen examples of certain scams before.

These recognition challenges likely stem from the contextual and psychological nature of SE attacks, rather than purely technical difficulty. University students operate in fast-paced digital environments—juggling learning management systems, university emails, messaging apps, and social networks—which normalize constant communication and quick responses. This habitual rapid interaction can desensitize them to warning signs. For instance, when students are used to clicking links in automated emails from campus services, they might not scrutinize a fake email that closely mimics those routines. Indeed, several respondents remarked that some phishing emails they've seen "**looked just like an official university email**"—blending into the stream of legitimate communications. Such ambiguity between academic or administrative messages and malicious ones makes it harder to tell them apart.

From an educational standpoint, the results highlight the importance of **experiential and scenario-based learning** in improving students' ability to recognize SE threats. Merely teaching terminology or enumerating types of attacks in lectures is insufficient; students need **hands-on practice** to identify manipulation in context. Interactive exercises such as **mock phishing campaigns** (sending simulated phishing emails to evaluate recognition) and **game-based learning activities** that require identifying red flags in realistic digital scenarios can strengthen applied detection skills [36]. This approach aligns with principles of **gamification** and **active learning**, where engagement in authentic, problem-oriented situations helps students internalize cybersecurity awareness. These pedagogical strategies can be conceptualized within a **layered intervention model**, as illustrated in Figure 3.

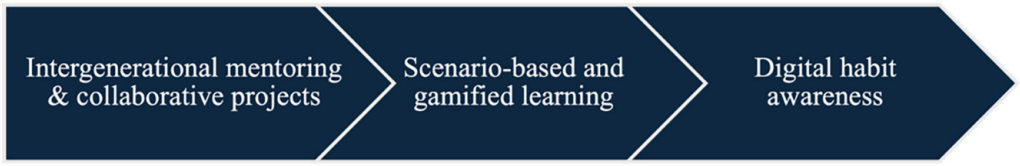

Fig. 3. Layered educational intervention model for enhancing cybersecurity awareness through experiential learning

Furthermore, integrating discussions of real-life examples into regular coursework (not just in a standalone security class) can reinforce critical evaluation habits. If professors occasionally show a suspicious email or a case study in any course and ask students, "Is this legitimate or a scam?" it helps address the gaps that students have not previously filled through formal education, thereby making vigilance a normalized and integrated part of their overall learning process.

It is also important to highlight that **recognition is not purely technical**—it involves critical thinking and skepticism. Students should be encouraged to slow down and analyze communications, especially when requests involve personal data or urgent actions. Training that improves these cognitive skills (like verifying identities, cross-checking information, and noticing inconsistencies) is as crucial as any technical advice.

Our findings reveal a paradox in engineering education: students in technology-related fields exhibit relatively strong digital literacy and personal safety habits, yet **formal cybersecurity education** in their curriculum is sparse. Most have never had a dedicated lesson on SE or cybersecurity basics, even as they progress toward careers where they will inevitably encounter such issues. This gap suggests that universities cannot assume technical familiarity equates to security competence. Being good at programming or electronics, for example, does not automatically teach someone how to recognize a socially engineered scam email. Therefore, higher education institutions should adopt a more structured and integrated approach to developing cybersecurity awareness among first-year students, ensuring that fundamental digital safety competencies are systematically built from the beginning of their studies.

One immediate implication is that institutions should incorporate cybersecurity topics into general engineering education and teacher training programs. This could mean adding modules on cybersecurity awareness into freshman orientation courses, professional ethics classes, or IT fundamentals courses that all students take. These modules should stress the human factor, including SE defense, not just network security or cryptography (which might be taught only to specialists). **Interdisciplinary collaboration** can be helpful here: faculty in computer science/cybersecurity could work with engineering education faculty to create engaging content for non-specialists, ensuring it's accessible and relevant.

The strong **student demand for training** (over 90% want more, and almost everyone is willing to attend a workshop) is a mandate for universities to act. Schools should leverage this enthusiasm by offering interactive workshops, simulations, and even elective courses focused on cybersecurity awareness. Our data show students prefer these to be hands-on; thus, a workshop might involve live demonstrations of phishing techniques, group challenges to detect fake websites, or role-playing exercises where students practice being "penetration testers" of human vulnerabilities. Such participatory formats align with modern pedagogical trends that emphasize learning by doing, and they have been shown to improve long-term retention and behavioral change in learners [32]–[34].

Another promising strategy is to formalize **intergenerational mentoring** within cybersecurity education. Given that many students are already informally exchanging knowledge with family members of different ages, universities could organize programs that pair students with older adults (such as alumni, retired faculty, or community members) for mutual learning sessions. For instance, a workshop on online safety could invite both students and older adults to attend together, creating a dialogue where each group shares their perspective and tips. Younger participants might help older ones set up a password manager or recognize a phishing email, while older participants might share cautionary tales or strategies they use to verify information. This two-way mentorship can reinforce the idea that everyone has something to learn and something to teach regarding cybersecurity. It also humanizes the training process—turning it into a collaborative activity rather than a top-down lecture.

In addition, intergenerational collaboration can be integrated into project-based learning. For example, an assignment in an engineering course could involve students designing a mini "awareness campaign" for a specific demographic (like senior citizens), which would require them to research that demographic's challenges and perhaps pilot their materials with an older relative or mentor. Such projects encourage students to apply their knowledge creatively and consider the user's perspective, thereby deepening their own understanding.

Ultimately, promoting a culture of **cross-generational cooperation** in cybersecurity aligns well with broader educational goals of inclusivity and lifelong learning. It shifts the narrative from "young people are good with tech, old people are bad" to "each generation has strengths; combining them makes everyone safer." This approach is human-centered, emphasizing trust, communication, and shared responsibility. In engineering and IT education, implementing these ideas could involve creating mentorship roles (e.g., "cybersecurity student ambassadors" who run peer and cross-age workshops), incorporating real-world security scenarios into capstone projects, or even leveraging gamified learning platforms that multiple age groups can use together.

By integrating practical cybersecurity modules and intergenerational mentoring opportunities into the engineering curriculum, we can transform students' awareness from a passive understanding into active competence. This not only prepares the students themselves to be more resilient digital citizens but also empowers them as future mentors who can spread cybersecurity awareness in their families, workplaces, and communities.

5 CONCLUSION

In an era where digital threats pervade every sector, the education field must not overlook the growing risk posed by SE. This study—focusing on engineering students and viewed through a generational lens—shows that **psychological manipulation tactics impact all age groups**, and effective countermeasures require nuanced understanding as well as collaborative learning approaches.

Our findings highlight several key points. First, **younger university students (Generation Z) tend to display greater familiarity with technical cybersecurity concepts** and tools, likely due to their digital upbringing and exposure in their studies. However, they can also exhibit overconfidence and habits (like rapid multitasking) that expose them to manipulation in new ways. In contrast, when considering older generations, students acknowledged valuable traits such as skepticism and

cautious behavior developed through life experience. Participants overwhelmingly agreed that no generation is immune: **all age groups can be targets of SE**, albeit through different channels and weaknesses. This underscores that cybersecurity awareness programs should address behavioral factors and avoid one-size-fits-all assumptions based on age.

Second, **overall awareness of SE among these future engineers is not as high as it should be**. Even digitally skilled students failed to recognize certain attack types and fell for basic deception in scenarios. There remains a critical knowledge gap around less common tactics and a need to strengthen practical detection skills. Traditional curricula in engineering currently do little to cover these human-centric security topics, meaning students are entering the professional world underprepared for threats that they will likely face.

Third, the study demonstrates a strong enthusiasm among students to **improve their cybersecurity knowledge and to engage in active learning methods**. Students don't just want more lectures—they want workshops, simulations, and real interactions that make the learning tangible. This is a call to action for educational institutions to invest in more dynamic cybersecurity education interventions. It is also noteworthy that students are very open to **intergenerational collaboration**. They see value in learning from older, experienced individuals and likewise are willing to mentor others on digital topics. This two-way mentoring could be a highly effective and innovative tool in cybersecurity education, leveraging the strengths of each generation.

In practical terms, our research suggests that universities should consider **implementing intergenerational mentorship programs, gamified learning exercises, and integrated curriculum enhancements** to boost security awareness. For example, existing project-based courses could incorporate a cybersecurity challenge that teams of mixed-age participants solve together. By doing so, not only do students refine their technical and social understanding of security, but they also contribute to a culture of shared responsibility and vigilance that can extend beyond the campus.

Future work: This study was exploratory in nature and focused on a single institution's cohort, predominantly young engineering students. Future research should test the proposed educational approaches (such as intergenerational mentoring and gamified training) in practice and evaluate their impact on behavior change. It would also be valuable to include a broader range of age groups and cultural contexts to see how generalizable these findings are. Finally, longitudinal studies could examine how students' attitudes and skills evolve as they receive more training or mentoring and whether they carry those lessons into their professional careers.

By investing in students' cybersecurity awareness now—and fostering cooperation across generations—educational institutions can build a more resilient academic community. This recommendation aligns with recent findings showing that gamified, intergenerational reverse mentorship models significantly enhance digital literacy and learning motivation among older adults [35]. In doing so, they empower not only their students and staff to protect themselves but also enable these future engineers and educators to impart critical digital safety skills to others in an increasingly deceptive online world.

6 ACKNOWLEDGMENT

The authors express their sincere gratitude to all students who participated in the survey and shared their experiences. This study was supported in part by

the Doctoral School on Security and Safety Sciences and by the Obuda University STEAM Office – Hungarian STEAM Platform. The authors also gratefully acknowledge the valuable feedback provided by colleagues during the pilot testing of the questionnaire.

7 REFERENCES

[1] S. Purkait, "Phishing countermeasures and their effectiveness – literature review," *Information Management & Computer Security*, vol. 20, no. 5, pp. 382–420, 2012. https://doi.org/10.1108/09685221211286548

[2] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. New York, NY: Wiley Publishing, 2002.

[3] World Economic Forum, "The Global Risks Report 2022," 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[4] M. Alsulami *et al.*, "Measuring awareness of social engineering in the educational sector in the Kingdom of Saudi Arabia," *Information*, vol. 12, no. 5, p. 208, 2021. https://doi.org/10.3390/info12050208

[5] K. Matyokurehwa, N. Rudhumbu, C. Gombiro, and C. Chipfumbu-Kangara, "Enhanced social engineering framework mitigating against social engineering attacks in higher education," *Security and Privacy*, vol. 5, no. 5, p. e237, 2022. https://doi.org/10.1002/spy2.237

[6] Q. An, W. Hong, X. Xu, Y. Zhang, and K. Kolletar-Zhu, "How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates," *International Journal of Information Security*, vol. 22, no. 2, pp. 305–317, 2022. https://doi.org/10.1007/s10207-022-00637-z

[7] Ponemon Institute, "Generational differences in cybersecurity behaviors," Help Net Security, 2017.

[8] S. Burga, "Why Gen Z is surprisingly susceptible to financial scams," TIME Magazine, 2024.

[9] R. Ravichandran, S. Singh, and P. Sasikala, "Exploring school teachers' cybersecurity awareness, experiences, and practices in the digital age," *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, pp. 1–15, 2025. https://doi.org/10.62915/2472-2707.1214

[10] The Learning Counsel, "The effectiveness of cybersecurity awareness programs in schools," Industry Report, 2023.

[11] Pew Research Center, "The Future of Truth and Misinformation Online," 2017. https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/

[12] G. Bak and A. Kelemen-Erdős, "Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján," *Hadmérnök*, vol. 17, no. 3, pp. 81–95, 2022. https://doi.org/10.32567/hm.2022.3.6

[13] I. Jagadics and Cs. Kollár, "21. századi social engineering támadások, védekezés és szervezeti hatások Európában," *Belügyi Szemle*, vol. 71, no. 1, pp. 113–126, 2023. https://doi.org/10.38146/BSZ.2023.1.6

[14] D. Hauser, "Social engineering awareness in business and academia," in *MWAIS 2016 Proceedings*, 2016, pp. 3–6.

[15] T. Green and L. Donovan, "Pre-service teacher training and cybersecurity: A national analysis," *Journal of Teacher Education and Technology*, vol. 30, no. 2, pp. 85–98, 2020.

[16] K. Jansson and R. von Solms, "Phishing for phishing awareness: A research framework and toolkit for the design of phishing awareness simulations," *Computers & Security*, vol. 62, pp. 117–128, 2016.

[17] R. M. Abdulla *et al.*, "Analysis of social engineering awareness among students and lecturers," *IEEE Access*, vol. 11, pp. 92948–92964, 2023. https://doi.org/10.1109/ACCESS.2023.3311708

[18] K. M. Najmul Islam, M. Mäntymäki, and M. Laato, "Gamification of cybersecurity education: A systematic literature review," *Computers & Security*, vol. 105, p. 102252, 2021.

[19] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts," *IEEE Access*, vol. 9, pp. 121916–121929, 2021. https://doi.org/10.1109/ACCESS.2021.3109091

[20] H. Jones, J. Towse, N. Race, and T. Harrison, "Email fraud: The search for psychological predictors of susceptibility," *PLoS ONE*, vol. 14, no. 1, p. e0209684, 2019. https://doi.org/10.1371/journal.pone.0209684

[21] D. Sarno, J. Lewis, C. Bohil, and M. Neider, "Which phish is on the hook? Phishing vulnerability for older versus younger adults," *Human Factors*, vol. 62, no. 5, pp. 704–717, 2019. https://doi.org/10.1177/0018720819855570

[22] D. Pehlivanoglu *et al.*, "Phishing vulnerability compounded by older age, apolipoprotein E e4 genotype, and lower cognition," *PNAS Nexus*, vol. 3, no. 8, 2024. https://doi.org/10.1093/pnasnexus/pgae296

[23] S. Park and J. Lee, "Incidental news exposure on Facebook and its relation to trust in news," *Social Media + Society*, vol. 9, no. 1, 2023. https://doi.org/10.1177/20563051231158823

[24] W. Gordon *et al.*, "Evaluation of a mandatory phishing training program for high-risk employees at a U.S. healthcare system," *Journal of the American Medical Informatics Association*, vol. 26, no. 6, pp. 547–552, 2019. https://doi.org/10.1093/jamia/ocz005

[25] T. Sutter, A. Bozkır, B. Gehring, and P. Berlich, "Avoiding the hook: Influential factors of phishing awareness training on click-rates," *IEEE Access*, vol. 10, pp. 100540–100565, 2022. https://doi.org/10.1109/ACCESS.2022.3207272

[26] Hungarian Central Statistical Office, "Education and training statistics: Graduates by field of study and gender," 2021. [Online]. Available: https://www.ksh.hu

[27] A. Petrenko and J. Čadil, "Gender disparity in STEM higher education in the European Union: Trends and implications," *Education Sciences*, vol. 14, no. 2, p. 219, 2024.

[28] R. Crowder *et al.*, "Human aspects of information security questionnaire (HAISQ): Development and evaluation," *Journal of Information Security and Applications*, vol. 45, pp. 87–94, 2019. https://doi.org/10.1016/j.jisa.2019.05.009

[29] A. Vishwanath, T. Herath, J. Chen, R. Wang, and H. R. Rao, "Suspicion, cognition, and automaticity model of phishing susceptibility," *Communication Research*, vol. 43, no. 3, pp. 294–319, 2016. https://doi.org/10.1177/0093650215627483

[30] T. E. Gorman and C. S. Green, "Short-term mindfulness intervention reduces the negative attentional effects associated with heavy media multitasking," *Scientific Reports*, vol. 6, no. 1, p. 24542, 2016. https://doi.org/10.1038/srep24542

[31] Y. Zhang, M. Jones, and S. Ekrem, "Multitasking and monetary incentive in a realistic phishing study," in *Proceedings of the 32nd British HCI Conference*, 2018, pp. 1–6. https://doi.org/10.14236/ewic/HCI2018.115

[32] M. Blaak *et al.*, "Effectiveness of simulation with a standardized patient on knowledge acquisition among nursing students," *Healthcare*, vol. 13, no. 3, p. 318, 2025. https://doi.org/10.3390/healthcare13030318

[33] Y. Krishnamoorthy *et al.*, "Gamification-based teaching methods for pandemic and outbreak investigation training," *Simulation & Gaming*, vol. 56, no. 1, pp. 33–49, 2025. https://doi.org/10.1177/10468781251338382

[34] A. J. Loverde, M. G. Adams, and R. D. Phelps, "Comparison of lecture and manipulative teaching methods on learning," *Nursing Forum*, vol. 58, no. 1, pp. 24–33, 2023. https://doi.org/10.1111/nuf.12575

[35] S. Sun, "Designing gamified intergenerational reverse mentorship based on cognitive aging theory," *Multimodal Technologies and Interaction*, vol. 9, no. 6, p. 64, 2025. https://doi.org/10.3390/mti9060064

[36] I. Holik, T. Kersanszki, I. D. Sanda, Z. Marton, "Improving Security and Environmental Awareness through Game-Based Learning with Minecraft," *International Journal of Engineering Pedagogy*, vol. 14, no. 4, pp. 90–107, 2024. https://doi.org/10.3991/ijep.v14i4.48127

[37] E. Karl and G. Molnar, "Development and application of a fuzzy-apriori-based algorithmic model for the pedagogical evaluation of student background data and question generation," *Algorithms*, vol. 18, no. 11, pp. 727–753, 2025. https://doi.org/10.3390/a18110727

8 AUTHORS

Zoltan Marton is Head of the STEAM Office at Obuda University, Director of the Hungarian STEM Platform, and an Assistant Lecturer. PhD candidate in Security and Safety Sciences. Research interests: social engineering, gamified learning, and STEAM-based engineering education. He leads international projects on digital skills and innovative pedagogy (E-mail: marton.zoltan@uni-obuda.hu).

Zoltan Rajnai is a Professor and General Vice-Rector of Obuda University and National Cyber Coordinator of Hungary. A former Colonel, he serves as Head of the Doctoral School on Safety and Security Sciences. Research interests: Cyber Security, Information Security, and info-communication systems (E-mail: rajnai.zoltan@uni-obuda.hu).

Gyorgy Molnar is Professor Head of Teacher Training at Trefort Agoston Engineering Education Centre, Obuda University, and Professor at Szechenyi Istvan University. Research: ICT-based education, digital pedagogy, and engineering teacher training. Recipient of the Bolyai Scholarship and Master Teacher Gold Medal. Senior expert at the Educational Authority (E-mail: molnar.gyorgy@uni-obuda.hu).