



Formation of Cybersecurity Culture in K-12 Schools of Kyrgyzstan: Development and Empirical Validation of the ASMAN Model

G. A. ESENALIEVA, A. D. ONGARBAYEVA, S. K. KALDYBAEV, A. K. KOISHYBEKOVA

ABSTRACT

Introduction. Existing international frameworks (DigComp 3.0, ISTE Standards, UNESCO Global Framework) were designed for resource-rich contexts and do not address AI-generated threats, linguistic specificity or the need for coordinated engagement of students, parents and teachers. Internet access among schoolchildren in the Kyrgyz Republic has expanded rapidly, while cybersecurity education in K-12 schools has lagged behind. *The aim of the study* is to develop and empirically validate the ASMAN model (Awareness, Skills, Monitoring, Assessment, Networking) for the formation of cybersecurity culture in K-12 schools of the Kyrgyz Republic.

Research methods. A mixed-method experimental study with a pre-test / intervention / post-test design was conducted between January 2025 and February 2026 across 727 general educational organisations in Osh, Jalal-Abad and Batken oblasts and the city of Osh. The total sample comprised 23,135 participants: 21,397 parents, 848 students aged 12–16 and 890 teachers. The intervention included a 40-hour Training of Trainers programme, the interactive CyberLab platform (phishing simulator, password trainer, deepfake detector and four further modules) and parent workshops. Data were analysed using descriptive statistics, Pearson's χ^2 , principal component analysis, t-SNE and k-means clustering.

Results. At baseline, 46.3% of parents had never encountered the term "cyber hygiene", 52.4% of students could not define cybersecurity, 72.6% reused weak passwords and only 21.9% of teachers had ever delivered a cybersecurity lesson. After the intervention all indicators improved significantly ($p < 0.001$). Phishing recognition rose by 56.2 percentage points, the share of teachers conducting cybersecurity lessons by 45.9 pp, and belief in the impossibility of video fabrication decreased by 58.3 pp.

Educational implications. The findings show that simulation-based learning outperforms lecture-based approaches in building cybersecurity skills and should be embedded across the curriculum rather than delivered as a stand-alone course. Tri-stakeholder engagement — students, parents and teachers simultaneously — produces larger effects than single-audience interventions and is reproducible at system scale through the existing in-service teacher training infrastructure.

Conclusion. The ASMAN model combined with the CyberLab platform provides an effective and scalable framework for forming cybersecurity culture in K-12 schools of a developing Central Asian country. The tri-stakeholder design and simulation-based training are the key success factors. The results can inform cybersecurity policy in the Kyrgyz Republic and comparable post-Soviet educational systems and provide a baseline dataset for future longitudinal and comparative research in Central Asia.

KEYWORDS

cybersecurity education, ASMAN model, K-12 schools, Kyrgyzstan, teacher training, phishing simulation, Central Asia

For Citation: Esenalieva, G. A., Ongarbayeva, A. D., Kaldybaev, S. K., & Koishybekova, A. K. (2026). Formation of Cybersecurity Culture in K-12 Schools of Kyrgyzstan: Development and Empirical Validation of the ASMAN Model. *Perspektivy nauki i obrazovaniya = Perspectives of Science and Education*, (5), 606–621. <https://doi.org/10.32744/pse.2026.5.39>

Received: 25 April 2026 | Approved: 12 July 2026 | Published: 31 October 2026



This is an open access article distributed under a Creative Commons Attribution-ShareAlike International License (CC-BY-SA 4.0) that allows others to share the work with an acknowledgement of the work's authorship and initial publication in this journal

INTRODUCTION

Education is being reshaped by digital transformation everywhere, but the conversation tends to focus on the opportunities—new tools, new platforms, broader access. Less discussed, though no less real, is that school-age children now navigate a threat landscape that has gotten significantly worse in just the last five years. Phishing and cyberbullying were already problems. What artificial intelligence has added is a layer of sophistication that changes the equation: deepfakes convincing enough to fool adults, voice cloning, scam messages generated by AI that read nothing like the clumsy phishing emails of ten years ago [1; 2]. The scale of the problem is not hypothetical. In the United States, 82% of K-12 schools reported encountering cyber threats between 2023 and 2024 [1]. RAND documented cybersecurity incidents at 60% of schools over 2023–2025 [2]. Central Asia faces the same pressures. Uzbekistan has seen cybercrime surge 48-fold since 2020, with 82% of fraud cases now online [3]; in Kyrgyzstan, 68 citizens lost \$110,000 collectively to fake job advertisements in 2025 alone [3].

Cybersecurity education in Kyrgyz schools is, to put it plainly, almost nonexistent. Earlier research examined the state of information technology and cybersecurity in the Kyrgyz educational system and identified significant gaps in both curriculum and teacher preparedness [4]. This is not for lack of international frameworks. DigComp 3.0 [5], the ISTE Standards [6], UNESCO's Digital Competency framework [7]—all available, all credible. The problem is that they assume things Kyrgyzstan does not have: training infrastructure, dedicated budgets, teacher-preparation pipelines that actually function [8]. And even if those conditions were met, a subtler mismatch would remain. These frameworks are excellent at classification—they can tell you, in considerable detail, what a learner should know. They are far less helpful on the question of how a teacher in a rural school outside Osh, with unreliable internet and zero background in cybersecurity, is supposed to teach any of it.

Research on cybersecurity awareness in Central Asia is thin. One study, conducted at Kyrgyz-Turkish Manas University during COVID-19—when everyone was online constantly—tested university students' cybersecurity knowledge and still found it weak [9]. The OSCE ran a capacity-building project in the region from 2020 to 2024, but it was aimed at law enforcement, not at classrooms [10]. Kazakhstan deserves credit for its CyberShield strategies (2017, 2022) and the UNICEF-partnered CYBER TUMAR campaign in 2024. These are genuine investments. But they rely on broad awareness messaging—posters, social media spots, pamphlets—not on pedagogical programs with measured outcomes [12; 13].

The published literature, taken as a whole, keeps circling back to the same set of problems. Developing countries get studied less—a 2022 meta-analysis reported that 60% of digital literacy interventions had taken place in high-income nations [11]. Tri-stakeholder programs—ones that pull students, parents, and teachers into the same intervention rather than isolating one group—remain the exception [12]. Meanwhile, AI-generated threats are evolving faster than schools can respond. Deepfakes were projected to hit 8 million instances by 2025 [13], and two-thirds of school staff report having had absolutely no training in identifying them [14]. And even when programs do report positive results, what they usually measure is awareness. Did participants learn something? Probably. Did they start behaving differently? That question, which arguably matters more, gets asked much less often [15]. The pedagogical challenge here is not trivial. Teaching cybersecurity is not like teaching history or mathematics, where the content stays relatively stable from year to year. The threats evolve and the platforms change. What was safe advice in 2022 may be outdated by 2025. This means teachers need not just initial training but ongoing support – a framework that helps them stay current without requiring them to become cybersecurity specialists.

This paper is our attempt to do something about those gaps. We set out to build a detailed model for developing cybersecurity culture in Kyrgyz schools—and then to test whether it actually works. The hypothesis was not complicated: bring students, parents, and teachers into the same intervention, rely on interactive simulation-based tools instead of lectures and handouts, and the result should be real, measurable improvement in cybersecurity culture.

LITERATURE REVIEW

International Frameworks for Digital Competence: A Critical Analysis

No shortage of frameworks exists for digital competence education. The question is whether any of them can travel. The European Commission's DigComp-now in version 3.0-maps five competence areas (information and data literacy, communication and joint work, digital content creation, safety, and problem solving) across eight proficiency levels [5]. Within the EU itself, where the framework was born, only 56% of adults had reached above-basic digital skills by 2023 [5]. So DigComp is plainly still needed at home. Whether it can be transplanted to Central Asian classrooms-classrooms where resources are scarce, instruction switches between two or three languages, and teachers' own digital confidence is often shaky-is a genuinely open question.

ISTE Standards foreground digital citizenship and responsible online conduct [6]. UNESCO designed its Global Framework with developing countries in mind-digital competence, in their definition, means the ability to access, manage, understand, and create information safely through digital technologies [7]. Then there are the professional-level instruments: NIST's NICE Cybersecurity Workforce Framework lays out 52 dedicated cybersecurity roles [16]; the ACM/IEEE joint curricula handle the university side [17]. These all serve different populations and aim at different levels of expertise. The underlying problem, though, is the same across the board. They are taxonomies. Sophisticated ones, admittedly-but taxonomies all the same. They describe what a learner should be able to do. They are much quieter on how a teacher, particularly one in Kyrgyzstan with limited internet and no prior cybersecurity training, is supposed to make any of that happen. Implementation blueprints, ready-made assessment tools, K-12 teaching methods that have been field-tested-none of these frameworks provide them.

Put the frameworks side by side and a telling gap opens up. DigComp 3.0 folds cybersecurity into one of five strands without carving out anything specific for school-age learners. ISTE assumes teachers are already digitally ready-an assumption that is flatly wrong in much of the developing world. UNESCO acknowledges infrastructure constraints, yet remains vague about how to teach practical skills, especially regarding newer threats like AI-generated content. And here is perhaps the most important omission: not one of these frameworks treats students, parents, and teachers as a single pedagogical unit. The evidence, though, increasingly suggests that this kind of coordinated engagement is exactly what sustained behavioral change in young people requires [15; 21]. Understanding what already exists is the first step toward building something new. Frameworks matter because they represent accumulated thinking, including years of research, debate, and revision condensed into structured guidance. Reviewing them is not an academic exercise; it is a way of learning from what others have tried, what worked, and what did not.

Table 1 In-depth comparison of international digital competence frameworks

Framework	Developer	Target	Cybersecurity	Tools	Stakeholders
DigComp 3.0	EU Commission	General	Partial	Limited	Not addressed
ISTE	ISTE	K-12	Digital citizen.	Partial	Not addressed
UNESCO DL	UNESCO	Developing	Mentioned	No	Not addressed
NICE	NIST	Professionals	Comprehensive	No	N/A
ASMAN	This study	K-12+parents	Simulation	CyberLab	Core

Cybersecurity Risks Among Minors

What children encounter online today bears little resemblance to the landscape of even 2020 or 2021. Soldatova and Rasskazova [18] studied Russian adolescents and found them regularly exposed to inappropriate content, aggressive messages, and various forms of manipulation. The important finding from their work was not that exposure is common-that much was expected-but that awareness alone does nothing protective. Skills and active adult involvement are what make the difference. Cyberbullying remains pervasive. The reported prevalence ranges from 15% to 40% of teenagers

depending on the country and how the question is asked [23; 24]; anxiety, withdrawal, school avoidance tend to follow. A newer concern showed up in RAND's 2024 survey data: 13% of American school principals were already dealing with deepfake-related bullying, rising to 20–22% in middle and high schools [14]. That was before the latest generation of AI tools became widely accessible.

Phishing, meanwhile, is not going away. If anything it is getting worse. A 2024 meta-analysis of 42 studies showed that simulation-based training—the kind where you get immediate feedback after falling for a fake attack—reduces susceptibility by about 40% [19]. That outperforms video-based instruction and gamified alternatives. The caveat is durability: without periodic refreshers, the gains erode over time [20]. Adolescents are especially vulnerable here, partly because they are less cautious than adults in how they evaluate messages that arrive in their inbox or on their phone [21].

AI-generated threats represent what may fairly be called a qualitative shift. The European Parliament noted that deepfake instances went from 500,000 in 2023 to a projected 8 million in 2025 [13]. In schools specifically, the Thorn Foundation (2024) found AI-generated content being used with growing frequency to produce harassing material aimed at students [14]. UNESCO has called for stronger generative-AI literacy among children, teachers, and parents—noting, in a somewhat embarrassing admission, that even within the EU there are essentially no functioning monitoring indicators for what children encounter online [22]. The implication for anyone designing educational programs is clear enough: treating AI-generated threats as a supplementary topic, something to mention in passing after the "real" cybersecurity content, is no longer defensible. These threats need to be central.

The Role of Parents and Teachers

Parental involvement is, by most measures, one of the strongest mediating factors in children's online safety. Livingstone et al. [12], through the EU Kids Online project, showed a clear correlation: when parents talk openly with their children about online risks, those children report problems and seek help more readily. Wisniewski et al. [23] built on this, finding that preventative mediation—approaches grounded in conversation and skill-building—does measurably better than reactive strategies like installing monitoring software or simply confiscating devices. A persistent blind spot remains, though. Parents routinely underestimate what their children actually encounter online. The focus tends to land on how many hours a child spends on a screen, not on what happens during those hours [12].

Teachers should, in theory, be at the center of cybersecurity education. The reality is messier. ICILS 2018 surveyed 14 countries and found formal professional development in digital safety to be uncommon—teachers mostly figured things out on their own [24]. By 2024, not much had changed: an Education Week survey showed 71% of teachers with no professional development related to AI technologies [14]. None. The picture is not hopeless, however. When teachers do receive structured training—training that involves actual practice and follow-up support, not just a one-day seminar—their confidence rises and cybersecurity topics start appearing in their lessons more frequently [25]. The Training of Trainers model, in particular, has shown its value in resource-constrained environments: train a first cohort, let that cohort train the next, and coverage expands without proportional cost increases [26].

This aligns with prior research conducted in Kyrgyzstan: Esenalieva et al. examined the formation of digital literacy among teachers, identifying key competencies required for effective technology integration and highlighting the importance of online courses, self-education, and peer exchange in developing teachers' digital skills [4]. Related work by Ongarbayeva et al. (2021) similarly demonstrated the need for structured methodological frameworks when preparing computer science teachers to develop electronic educational resources, underscoring the persistent gap between teacher training curricula and practical digital competence demands [27].

Research Gaps and Justification for the Study

The literature points to four gaps that, taken together, explain why we designed the study the way we did.

The geographic one is the most obvious. Central Asia barely registers in the cybersecurity-education research. The e-Governance Academy's 2025 assessment called cybersecurity education

a shared weakness across Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan [8], and when we searched the published record for a large-scale empirical study of school-level cybersecurity instruction in Kyrgyzstan, we found nothing.

Then there is the stakeholder fragmentation. Programs typically pick one audience-students, or parents, or teachers-and work exclusively with that group. Coordinating across all three within a single intervention, and measuring outcomes collectively, is something the field has talked about but rarely done.

Measurement itself is a problem. Plenty of studies show that knowledge went up after training. Far fewer check whether people actually started doing anything differently. The gap between knowing what phishing is and recognizing it when it lands in your inbox is not trivial, and instruments that capture both are uncommon.

Lastly, AI-generated threats-deepfakes above all-have grown faster than educational responses to them. School-level modules addressing these threats specifically are still rare, which is troubling given how rapidly the technology is spreading.

Scientific Novelty

We see the novelty of this work in four areas.

The most straightforward one is scale. With 23,135 participants across 727 schools in four regions of the Kyrgyz Republic, this is-to the best of our knowledge-the first study of its size to address cybersecurity culture in Central Asian schools. We searched. There is nothing comparable in the published literature. This was not a pilot or a convenience-sampled survey of one university; it was a full-scale intervention.

The tri-stakeholder design is the second. Cybersecurity programs overwhelmingly target one group. Students, usually. Sometimes teachers. Rarely parents. We designed the ASMAN model to include all three from the outset, which let us observe interaction effects between the groups-something that single-audience studies are structurally unable to capture.

Third, the CyberLab platform. Researchers have been pointing out for years that schools need practical tools for teaching about AI-generated threats. The tools, however, have mostly not materialized. CyberLab was built to work on mobile devices with poor internet connections (a non-negotiable requirement in rural Osh and Batken), and it includes a deepfake detection module that, as far as we know, is one of very few operational school-level tools of its kind.

Fourth-and this is the part we want to stress-we measured what people actually did, not just what they said they learned. Students who flagged real phishing emails. Teachers who caught cyberbullying incidents they would previously have missed. Password changes that actually happened. Survey scores are useful, but they are not the whole picture. Every field advances through accumulation, what begins as a single data point becomes, over time, a pattern. This study is one contribution among many that will be needed. But it is a necessary one. Without baseline data, there is nothing to compare. Without a tested intervention, there is nothing to improve. The work of future researchers depends on the work done now.

MATERIALS AND METHODS

Study Design and Context

The research project includes pre-test / intervention / post-test design, running from January 2025 through February 2026. The study covered four administrative units in southern Kyrgyzstan-Osh oblast, Jalal-Abad oblast, Batken oblast, and the city of Osh-taking in 727 general educational organizations.

Participants

We recruited three groups. The largest was 21,397 parents whose children were enrolled in grades 5–11. Teachers numbered 890 and included subject teachers, class supervisors, school psychologists,

and social workers. The student sample consisted of 848 adolescents aged 12–16, enrolled in grades 6–30. Female respondents predominated among parents—a pattern well documented in school-based survey research—and the most common age bracket was 36–45 years.

Table 2 Distribution of participants by region

Module	Format	Target	Skills	Assessment
Phishing simulator	Simulation	Students	Threat recognition	Practical
Password trainer	Interactive	Students	Secure credentials	Practical
Deepfake detector	Quiz	Students	AI-content ID	Cognitive
Safe Route quest	Game	Students	Decision-making	Behavioral
Theory modules	Text+quiz	All	Knowledge	Cognitive
Family guides	Reading	Parents	Communication	Motivational

Instruments

Each participant group received its own standardized questionnaire; all were available in Russian and Kyrgyz. The parent version was the longest at 18 items—demographics, how their children use the internet, what parents actually know about online threats, whether they have household rules for digital safety, and whether they would be willing to attend training. For students we kept it shorter: 10 items covering cybersecurity terminology, password habits, and personal experience with cyberbullying. We wanted the student instrument to be completable in a single class period without fatigue effects. The teacher questionnaire (7 items) zeroed in on two things: how teachers rate their own digital competence, and what they have actually done—if anything—to teach cybersecurity in their classrooms.

Table 3 Criteria for measuring cybersecurity culture

Criterion	Indicators measured	Example items
Cognitive	Knowledge of threats, terminology	What is phishing?
Practical	Skills in threat recognition	Identify fraudulent email
Motivational	Willingness to learn	Would you attend training?
Behavioral	Safe practices application	Do you use unique passwords?

Data Analysis

The quantitative side was relatively straightforward. Frequencies and percentages for the descriptive snapshot, Pearson's χ^2 to check whether the before-and-after differences were statistically real. The open-ended parent responses required more work. We started with PCA to bring the dimensionality down to something manageable, ran t-SNE to see whether natural groupings appeared visually (they did, quite clearly), and then applied k-means clustering to formalize those groupings into interpretable profiles.

Intervention Design

The intervention had three simultaneous components.

Training of Trainers program. Teachers took part in a 40-hour professional development course organized around four modules: cyber-threat theory (8 hours), teaching techniques and simulation practices (12 hours), strategies for engaging parents (8 hours), and supervised teaching practice with individual feedback (12 hours). By September 2025, all 890 participating

teachers across the four regions had completed the program and were expected to cascade the training to colleagues in their schools.

CyberLab interactive platform. The platform bundled six modules. The phishing simulator presented students with realistic fraudulent-email scenarios and delivered immediate feedback. A password trainer let users test and improve their password strength interactively. The deepfake detector-which proved to be the most engaging module by far-set authentic images and videos side by side with AI-generated fakes and asked students to tell the difference. Beyond those core modules, there was a Safe Route interactive quest (daily cyber decision-making scenarios presented as a game), theory modules with organized lessons covering threats, terminology, and the legal basics, and family guides designed to give parents a starting point for talking about online safety with their children.

Parent workshops. Schools hosted two-hour sessions that walked parents through the current threat landscape, offered communication techniques for discussing digital safety with children, introduced available parental-control tools, and outlined basic incident-response procedures.

Table 5 CyberLab platform modules and targeted competencies

Module	Format	Target	Skills	Assessment
Phishing simulator	Simulation	Students	Threat recognition	Practical
Password trainer	Interactive	Students	Secure credentials	Practical
Deepfake detector	Quiz	Students	AI-content ID	Cognitive
Safe Route quest	Game	Students	Decision-making	Behavioral
Theory modules	Text+quiz	All	Knowledge	Cognitive
Family guides	Reading	Parents	Communication	Motivational

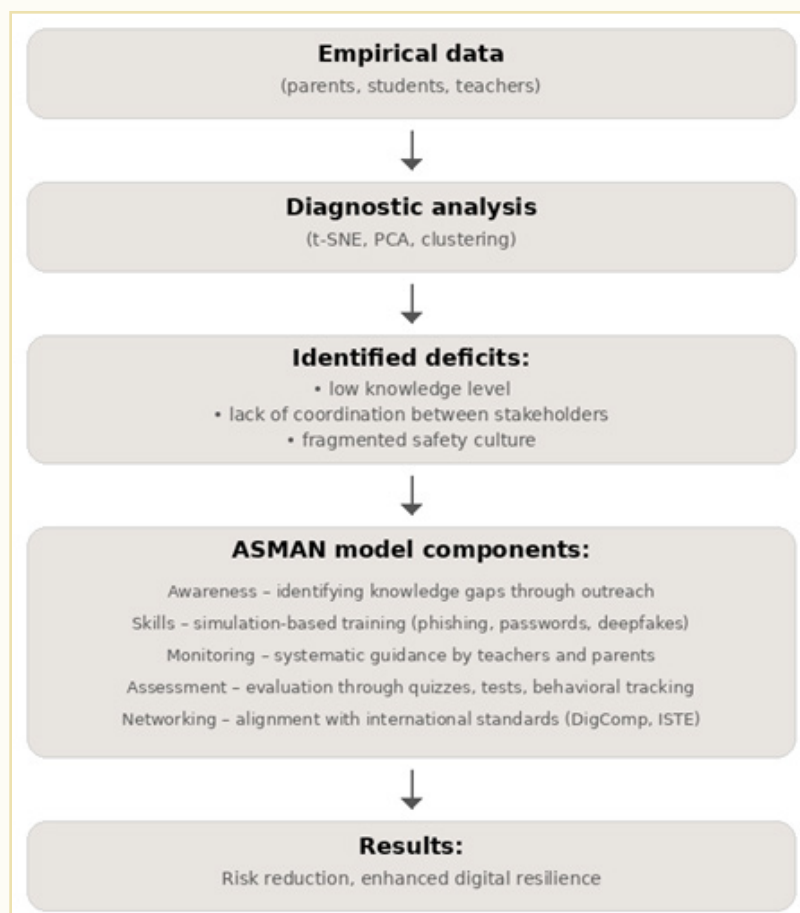


Figure 1 Research design and ASMAN model implementation logic

The overall logic of the study can be summarized as a sequence of connected stages. We began by collecting empirical data from three stakeholder groups—parents, students, and teachers—across 727 schools. This data underwent diagnostic analysis using statistical methods (PCA, t-SNE, k-means clustering) to identify patterns and segment respondents. The analysis revealed three core deficits: low baseline knowledge of cybersecurity concepts, lack of coordination between schools and families, and a fragmented approach to digital safety that treated each group in isolation. These deficits informed the design of the ASMAN model, whose five components directly address the gaps we identified. The intervention was then implemented, and post-test data allowed us to measure results. Figure 5 illustrates this progression from data collection through analysis, model application, and outcome measurement. What matters here, from a pedagogical standpoint, is that the model was not imposed from outside. It grew from the data from what teachers reported they lacked, from what parents said they did not understand, from the mistakes students actually made. This is how educational interventions should work: listen first, design second. A model built on assumptions about what people need will always be less effective than one built on evidence of what they actually lack.

RESULTS

Baseline Assessment

The pre-intervention data were not encouraging. Consider the parents first, since they were the largest group. Nearly half—46.3%—had never come across the term "cyber hygiene." Not "don't understand it well" or "have a vague sense of it." Had never encountered it. More than half (53.2%) reported that they do not regularly discuss online safety with their children. There was an age gradient, predictably enough: younger parents (under 35) showed higher awareness at 53.85%, while parents in the 46–55 bracket were the least informed, with 56.82% unfamiliar with basic cyber hygiene concepts. The older the parent, generally, the wider the knowledge gap.

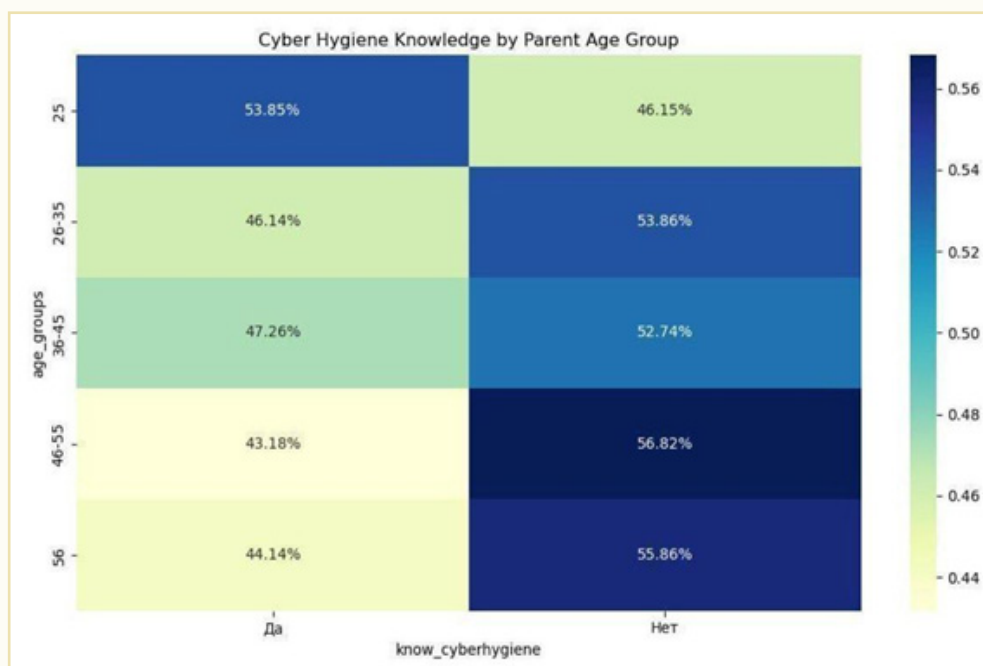


Figure 2 Cyber hygiene knowledge distribution by parent age group

The student data were no more reassuring. Asked to define "cybersecurity," more than half (52.4%) could not. Password reuse was rampant – 72.6% admitted to recycling weak passwords across multiple accounts—and a fifth of the sample (20.1%) had experienced cyberbullying at some point. Teachers, who should in principle be guiding students through this landscape, were themselves struggling: 51.5% put their own cybersecurity knowledge at medium or low, and only 21.9% had ever taught a full lesson on the subject.

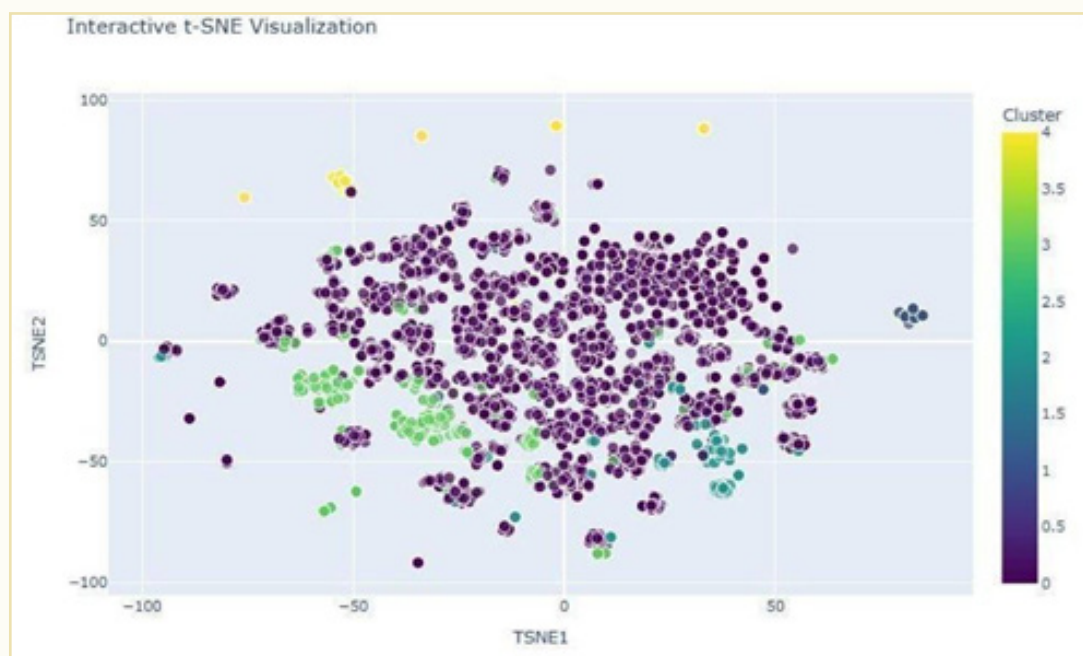
Table 6 Baseline assessment results by participant group

Group	Indicator	Result
Parents	Not familiar with cyber hygiene	46.3%
Parents	Do not regularly discuss online safety	53.2%
Students	Cannot define cybersecurity	52.4%
Students	Reuse weak passwords	72.6%
Students	Have experienced cyberbullying	20.1%
Teachers	Rate knowledge as medium or low	51.5%
Teachers	Have conducted cybersecurity lesson	21.9%

Cluster Analysis of Parent Responses

The open-ended parent responses warranted closer inspection. We ran PCA first; three components surfaced, jointly explaining 67.3% of the variance. Component one (31.2%) sorted respondents by awareness level-essentially, how much they already knew. Component two (21.8%) picked up a parenting-style dimension: strict control at one pole, trust-based communication at the other. Component three (14.3%) had to do with motivation, specifically willingness to invest time in learning more.

K-means clustering then divided the data into four profiles. The largest (41.2%) we labeled "education-seeking": parents who actively asked for workshops, handouts, anything. Next came an "information-deficit" cluster (32.4%)-short answers, vague language, clearly low baseline awareness. A "restriction-oriented" cluster (17.7%) wanted to solve the problem by banning devices or blocking websites. And the smallest group, a "complacent" cluster (8.7%), consisted of parents who saw no problem at all. That last group, though small, may be the most concerning from a program-design standpoint.

**Figure 3** t-SNE visualization of parent respondent clusters

Intervention Implementation

The CyberLab platform was deployed across all participating schools following the completion of the Training of Trainers program. The platform interface is presented in Figure 3.

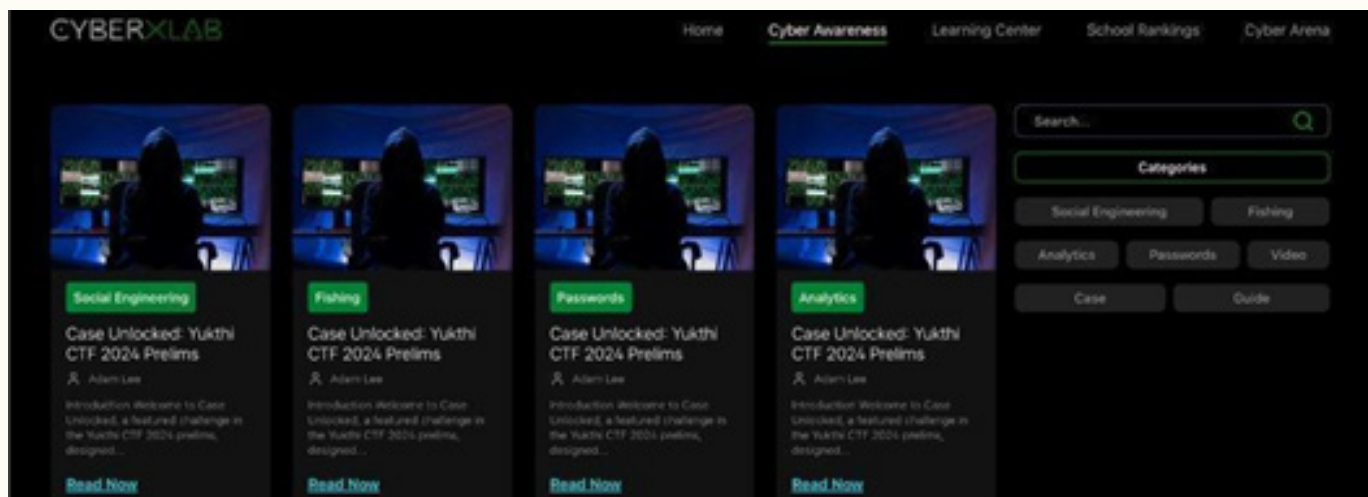


Figure 4 CyberLab platform interface: Cyber Awareness training section

Post-Test Results

We collected post-test data between December 2025 and February 2026. Every indicator moved upward, and the gains were both statistically significant and large enough to matter practically. Table 6 lays out the numbers.

Table 7 Comparison of pre-test and post-test results

Indicator	Group	Pre-test	Post-test	Change	p-value
Aware of cyber hygiene	Parents	53.7%	78.4%	+24.7	<0.01
Discuss safety regularly	Parents	46.8%	67.3%	+20.5	<0.01
Understand cybersecurity	Students	47.6%	84.3%	+36.7	<0.001
Confident in passwords	Students	27.4%	68.9%	+41.5	<0.001
Can recognize phishing	Students	31.4%	87.6%	+56.2	<0.001
Rate competence high	Teachers	43.9%	89.3%	+45.4	<0.001
Conduct cyber lessons	Teachers	21.9%	67.8%	+45.9	<0.001

Behavioral Outcomes and Platform Engagement

Questionnaire scores, of course, tell only part of the story. During the intervention period we also documented concrete behavioral shifts. Fifteen students identified actual fraud attempts and brought them to the attention of a teacher or parent—these were real phishing emails, not simulations. Eight others recognized social-engineering tactics while gaming online and refused to give up personal information. On the teacher side, early detection of cyberbullying jumped 156% relative to the period before the intervention. And after completing the password module, 73.2% of students reported that they had actually gone and changed at least one password.

The deepfake detection module stood out. Its completion rate – 98.4% – was the highest of any CyberLab component. Before training, 72.6% of students believed video content simply could not be faked. Afterward, that number fell to 14.3%: a swing of 58.3 percentage points. This pattern aligns with recent research showing that direct exposure to AI-generated content produces particularly strong shifts in attitudes [28].

DISCUSSION

Interpretation of Key Findings

The short answer to whether the intervention worked is yes. In some areas, by a wider margin than we expected. Every indicator that was measured improved when students, parents, and teachers went through the program together, and several of the improvements were large enough to be practically meaningful, not just statistically significant.

Phishing recognition produced the single biggest swing: 56.2 percentage points ($p < 0.001$). To put that in perspective, a 2024 meta-analysis covering 42 studies found that point-of-error training-feedback right after someone falls for a fake attack-reduces phishing susceptibility by about 40% [19]. Our CyberLab simulator was built on exactly that principle. You click a suspicious link; the system tells you immediately what you missed and why it was dangerous. The students did not just memorize rules about phishing. They developed something closer to pattern recognition, which is a fundamentally different kind of learning. And then fifteen of them went on to catch real phishing attempts outside the platform-in their email, in messaging apps-and reported them to adults. Small numbers, yes. But that transfer from simulation to real life is exactly what educational interventions hope for and rarely achieve.

Teacher development proved critical. Before the program, 21.9% of teachers had taught a cybersecurity lesson. Afterward: 67.8%. That is a threefold increase, and it matches what ICILS data would predict when teachers get structured, hands-on training instead of the usual professional-development fare [24]. The cascade model-890 teachers completing the full ToT program, then taking the material back to 727 schools-works.

The deepfake module was, in some ways, the most striking component. A 98.4% completion rate is unusually high for any educational module-students genuinely wanted to finish it. Before training, nearly three-quarters of participants (72.6%) believed that video content could not be fabricated. That number plummeted to 14.3% afterward. This aligns with research suggesting that direct engagement with AI-generated content is particularly effective for developing critical AI literacy among young people [29]. Naffi et al. reported comparable attitude shifts among 18-to-24-year-olds in North America [28], which is an interesting convergence: our participants were younger, in a completely different cultural and economic setting, and yet the pattern held.

Comparative Study with Regional and International Research

Our baseline numbers look a lot like what other researchers have found in post-Soviet settings. Soldatova and Rasskazova [18] documented the same disconnect among Russian teenagers: heavy daily internet use, minimal understanding of the risks involved. In our sample, 52.4% of students could not even define "cybersecurity"-and these were kids who go online every day. The parallel is hard to miss.

The regional picture is uneven. Kazakhstan has moved furthest, at least on paper. Its CyberShield strategies pushed the country from 103rd to 31st in the ITU Global Cybersecurity Index between 2017 and 2020 [30], which is a remarkable jump. But the investment went mostly into institutional capacity and workforce pipelines, not into classrooms. The e-Governance Academy's 2025 assessment of four Central Asian states-Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan-flagged cybersecurity education as a shared blind spot [8]. Uzbekistan's numbers are frankly alarming: cybercrime reports up 48-fold since 2020, 82% of fraud now happening online [3]. When digital adoption races that far ahead of digital literacy, something has to give.

More recently, Kazakhstan has embedded cybersecurity as a foundational concern in its broader AI development agenda. At the second session of the Presidential Council on Artificial Intelligence held in Almaty in May 2026, President Tokayev emphasized that any digital infrastructure remains vulnerable without fundamental cybersecurity provisions, and directed the government to incorporate security requirements at the architectural level of all digital solutions [31]. This signals a regional shift toward treating cybersecurity not as a standalone domain but as a prerequisite for digital transformation at scale—a direction that aligns closely with the ASMAN model's emphasis on embedding security culture across institutional layers rather than delivering it as an isolated intervention.

Internationally, Shillair et al. [15] looked at cybersecurity education across 80 countries and concluded-unsurprisingly-that wealthier nations with higher internet penetration tend to have more developed awareness programs. Fair enough. But our data complicate that narrative somewhat. You do not necessarily need a large GDP to produce real gains; you need a well-targeted intervention. The improvements we documented in southern Kyrgyzstan happened in schools where bandwidth is spotty and budgets are thin.

The ASMAN Model in Theoretical Context

The empirical data give us some confidence that the ASMAN model works as a practical framework-not just as an idea, but as something that can be deployed in actual schools and produce measurable results. Each of the five components maps onto a specific deficit we found at baseline.

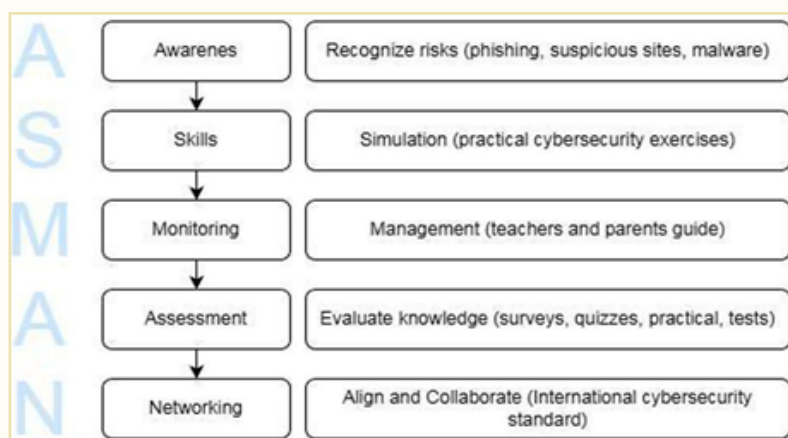


Figure 5 ASMAN model structure and components

Here is what each component does, concretely. Awareness means teaching people to recognize threats-phishing, suspicious websites, malware. Skills takes that recognition and makes it active through simulation exercises and hands-on practice. Monitoring is the ongoing piece: teachers and parents keeping the conversation going through regular dialogue, not just during a training week. Assessment covers the measurement side: surveys, quizzes, practical tasks that test real capability. And Networking ties the model to international benchmarks like DigComp and ISTE, so that it is not a purely local construct. The whole cycle is designed to repeat, because the threats do not stand still.

Theoretically, ASMAN is distinctive because it brings together three things that the literature has mostly kept in separate silos: multi-stakeholder coordination, simulation-based skill development, and rigorous outcome measurement. That combination, taken as a whole, addresses all four of the gaps we identified in the literature review-geography, stakeholder fragmentation, narrow measurement, and the neglect of AI-created threats.

Limitations

This study focused on four regions of Kyrgyzstan: Osh oblast, Jalal-Abad oblast, Batken oblast, and the city of Osh. Together, these regions represent a significant portion of the country's school-age population and provided the scale needed for meaningful statistical analysis. A natural next step would be to extend the research to other regions - Chui, Bishkek, Talas, Naryn, Issyk-Kul – each of which presents its own context and challenges. There was no control group; at 727 schools and 23,000+ participants, withholding the intervention from some schools felt neither practical nor fair. This means we cannot isolate the intervention's effect with certainty, though the consistency of gains across all indicators suggests the program played a real role. Self-report bias remains a possibility-people may overstate their own improvement-and the three-month follow-up window is short. Longer-term tracking would tell us whether these gains hold.

Educational Implications

The clearest lesson from the data is that simulation works. The 56.2-point gain in phishing recognition dwarfed everything else, and it came from hands-on practice, not from reading about threats. For curriculum design, this argues against creating a standalone cybersecurity course and in favor of weaving digital safety into existing subjects-language arts ("analyze whether this email is legitimate"), math (probability exercises using password-cracking scenarios), social studies (media literacy units on manipulated content). That approach is more sustainable and less dependent on finding room in an already crowded timetable.

The Training of Trainers model proved that it could reach 727 schools without importing outside specialists. Kyrgyzstan's IPKPR professional development infrastructure is already in place; the ToT course fits naturally into it. Teachers went from 21.9% conducting cybersecurity lessons to 67.8%-evidence that the cascade mechanism actually delivers.

Parent engagement cannot be one-size-fits-all. Our cluster analysis surfaced four distinct parent profiles, and what works for an education-seeking parent who actively requests workshops is unlikely to reach a complacent parent who sees no problem. Differentiated outreach-targeted messaging, varied workshop formats-is not a luxury here; it is a practical necessity.

At the policy level, the argument is straightforward: cybersecurity competencies belong in the State Educational Standards, and the baseline we built from 23,135 respondents gives the Education Development Strategy 2021-2040 [32] something concrete to benchmark future progress against.

Practical Significance

Different audiences will take different things from this study.

For policymakers, the main takeaway is probably this: the ASMAN model and the CyberLab platform are not proposals on paper. They ran in 727 real schools, with real students and teachers, and the numbers moved. If the Ministry of Education decides to mandate cybersecurity instruction, the question "but does it work?" now has an answer-and the tools to deliver it already exist.

The Training of Trainers structure is where school administrators should look most closely. No outside cybersecurity consultants were needed. We trained 890 teachers at regional centers; they went back to their buildings and replicated the program. That cascade logic keeps the model affordable even at national scale, which matters in a system where money is always tight.

For classroom teachers, the practical modules slot into subjects they already teach. Assignment tools, progress tracking, and assessment features are built in-nothing requires a separate platform or extra software. And everything runs in both Russian and Kyrgyz. Given that some schools teach entirely in one language and the school down the road teaches in the other, bilingual availability is not optional. It is a prerequisite.

Parents tend to get left out of cybersecurity conversations entirely. The workshop format gave them concrete, usable guidance: setting household digital-safety rules, having an age-appropriate conversation about online risks with a twelve-year-old, recognizing the early behavioral signs of cyberbullying. Several parents told us afterward that they had never thought about any of these issues before the workshop.

Finally, for researchers: the baseline dataset-23,135 respondents across four regions-fills a gap that the literature on Central Asia has had for years. Comparative work, longitudinal tracking, country-to-country analysis: the data are there now.

CONCLUSION

This study ran for 14 months, reached 23,135 people in 727 schools, and-we believe-produced findings that matter.

The baseline confirmed what anyone working in Kyrgyz education probably suspected but no one had measured at scale. Cybersecurity awareness is alarmingly low. Close to half of parents had never heard of cyber hygiene. More than half the students could not explain what cybersecurity means. About the same proportion of teachers described their own competence as middling at best. If these numbers sound familiar, it is because researchers in Russia, Kazakhstan, and other developing countries have documented virtually the same pattern: digital adoption racing ahead of digital self-defense.

The ASMAN model-Awareness, Skills, Monitoring, Assessment, Networking-gave us a workable framework. We would not call it a finished product; no model is, in its first iteration. But it did what we needed it to do. Simulation-based components delivered the heaviest gains, which in hindsight makes sense: phishing recognition jumped 56.2 points, password confidence 41.6. Telling someone about phishing is one thing. Making them click a fake malicious link and then showing them why it was fake-that lands differently.

The tri-stakeholder piece is what surprised us most, honestly. There was a real risk that spreading the intervention across students, parents, and teachers would dilute its impact on any single group. The opposite happened. Every group improved, and the anecdotal evidence-parents initiating safety conversations at home for the first time, students warning each other about suspicious links in class group chats-suggests the effects reinforced one another.

All the statistical comparisons cleared $p < 0.1$. Those numbers matter. But we keep coming back to the behavioral data, because survey responses can be inflated by social desirability and self-report bias in ways that actions cannot. Fifteen students spotted real phishing and told an adult. Eight refused to share data with social-engineering bots while gaming. Teachers caught cyberbullying 156% more often. And 73.2% of students went and changed passwords they had been reusing for years. That is not questionnaire noise.

One module deserves special mention. The deepfake detector had the highest completion rate (98.4%) and produced a 58.3-point attitudinal swing. Students were genuinely fascinated by it. AI-threat education, it turns out, resonates with young people in a way that more conventional cybersecurity topics sometimes do not. Future programs should treat it as a priority.

What comes next? The most pressing need is longitudinal data. We measured outcomes three months out; whether those gains survive at six months or a year is genuinely unknown. Running comparative trials in Kazakhstan, Uzbekistan, and Tajikistan would tell us whether the model travels or whether it is too anchored in Kyrgyz specifics to export directly-our instinct is that it will transfer, but instinct is not evidence. Age-adapted versions for younger children (primary school) and older students (upper secondary) are an obvious extension. And somebody-us, hopefully, or another research team-needs to do a serious cost-effectiveness comparison between online-only delivery and the blended model we used. Ministries of education across the region are working with limited budgets, and they need that kind of analysis to make informed allocation decisions.

REFERENCES

1. Center for Internet Security. (2025). 2025 CIS MS-ISAC K-12 cybersecurity report. East Greenbush, NY: CIS. 48 p.
2. RAND Corporation. (2025). Protecting schools virtually (Report RRA3930-6). Santa Monica, CA, RAND Corporation. DOI: 10.7249/RRA3930-6
3. Putz, C. (2026). As cybercrime soars in Central Asia, computer literacy lags behind. *The Diplomat*, March 2026. Retrieved from <https://thediplomat.com/>
4. European Commission. (2024). DigComp 3.0: The digital competence framework for citizens. Luxembourg, Publications Office of the European Union. DOI: 10.2760/115376
5. ISTE. (2016). ISTE standards for students. Arlington, VA, International Society for Technology in Education. 28 p.
6. UNESCO. (2018). A global framework of reference on digital literacy skills for indicator 4.4.2. Montreal, UNESCO Institute for Statistics. 146 p.
7. e-Governance Academy. (2025). Cybersecurity capacity in Central Asia. Tallinn: e-Governance Academy. Retrieved from <https://ega.ee/>
8. Turgunbaev, T., & Dzhumabaev, Y. (2019). Cybercrime risk awareness rate among students in Central Asia. *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, 1–5.

- DOI: 10.1109/ICISCT47635.2019.9011987
9. OSCE. (2024). Capacity-building on combating cybercrime in Central Asia: Phase II. Vienna, Organization for Security and Co-operation in Europe.
 10. 30. Digital Watch Observatory. (2024). Kazakhstan's cyber shield concept. Geneva, DiploFoundation. Retrieved from <https://dig.watch/>
 11. Choudhary, H., & Bansal, N. (2022). Addressing digital divide through digital literacy training programs: A systematic literature review. *Digital Education Review*, (41), 224–248. DOI: 10.1344/der.2022.41.224-248
 12. Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. London, EU Kids Online, LSE. 170 p.
 13. European Parliament. (2025). Deepfakes: Risks, regulation, and combating threats. Brussels, European Parliament, DG EPRS.
 14. RAND Corporation. (2025). Artificially intelligent bullies: Dealing with deepfakes in K–12 schools. Santa Monica, CA: RAND Corporation.
 15. Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, 102756. DOI: 10.1016/j.cose.2022.102756
 16. National Institute of Standards and Technology. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (NIST Special Publication 800-181). Gaithersburg, MD, NIST. DOI: 10.6028/NIST.SP.800-181
 17. ACM/IEEE Joint Task Force on Cybersecurity Education. (2017). Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity. New York, ACM. DOI: 10.1145/3184594
 18. Soldatova, G. U., & Rasskazova, E. I. (2014). Adolescent safety on the internet: Risks, coping with problems and parental mediation. *National Psychological Journal*, (3), 39–51. (In Russian). DOI: 10.11621/npj.2014.0305
 19. SoSafe. (2024). Effectiveness of phishing simulations: Meta-analysis of 42 studies. Köln, SoSafe GmbH.
 20. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 1–31. DOI: 10.1145/1754393.1754396
 21. Ahamed, B., Krishnamoorthy, M., & Prasad, V. (2024). Empowering students for cybersecurity awareness management in the emerging digital era. *SAGE Open*, 14(1). DOI: 10.1177/21582440241228153
 22. UNESCO. (2025). Deepfakes and the crisis of knowing. Paris: UNESCO.
 23. Wisniewski, P., Jia, H., Xu, H., Rosson, M. B., & Carroll, J. M. (2015). "Preventative" vs. "reactive": How parental mediation influences teens' social media privacy behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*, 302–316. DOI: 10.1145/2675133.2675293
 24. Fraillon, J., Ainley, J., Schulz, W., Friedman, T., & Duckworth, D. (2019). Preparing for life in a digital world: IEA International Computer and Information Literacy Study 2018 international report. Amsterdam: IEA. 297 p. DOI: 10.1007/978-3-030-38781-5
 25. Common Sense Media. (2021). The Common Sense census: Media use by tweens and teens, 2021. San Francisco, CA: Common Sense Media. 58 p.
 26. Shirikova, T. S. (2021). Pedagogical support for cybersecurity culture formation among secondary school students [PhD thesis]. Voronezh State Pedagogical University, Voronezh. (In Russian).
 27. Naffi, N., Davidson, A.-L., Patino, A., Brault, N., Duponsel, N., & Beatty, B. (2024). Empowering youth to combat malicious deepfakes and disinformation: An experiential and reflective learning experience. *Journal of Constructivist Psychology*, 37(1), 91–111. DOI: 10.1080/10720537.2023.2244594
 28. Erdolatov, S. S., Ibraev, A. D., Esenalieva, G. A., Bekezhanov, M. M., & Kaldybaev, S. K. (2025). Status and prospects for the development of information technology in the higher education system of Kyrgyzstan. In E. G. Popkova (Ed.), *Bridging the Gap Between the Higher Education and Labor Markets. Education in the Asia-Pacific Region: Issues, Concerns and Prospects*, 73 (pp. 295–305). Springer, Singapore. DOI: 10.1007/978-981-96-1933-7_26
 29. Ministry of Education and Science of the Kyrgyz Republic. (2020). Education development strategy of the Kyrgyz Republic for 2021–2040. Bishkek, MoES KR Publ. (In Russian).
 30. Long, D., & Magerko, B. (2020). What is AI literacy? Competencies and design considerations. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–16. DOI: 10.1145/3313831.3376727
 31. President of the Republic of Kazakhstan. (2026). Second session of the Council on Artificial Intelligence Development [Press release, 4 May 2026]. Akorda. Retrieved from <https://www.akorda.kz/ru/glava-gosudarstva-provel-vtoroe-zasedanie-soveta-po-razvitiyu-iskusstvennogo-intellekta-44481>
 32. Ongarbayeva, A. D., Kaldybaev, S. K., Kasymaliev, M. U., Kozhasheva, G. O., & Yermekova, N. S. (2021). Methodology of preparing future computer science teachers to create electronic educational resources. *World Journal on Educational Technology: Current Issues*, 13(3), 386–396. DOI: 10.18844/wjet.v13i3.5933

Authors

Gulzada A. Esenalieva

(Bishkek, Kyrgyzstan)
Associate Professor
American University of Central Asia
E-mail: esenalieva_g@auca.kg
ORCID: 0009-0000-9135-1671

Aliya D. Ongarbayeva

(Almaty, Kazakhstan)
Cand. Sci. (Educ.),
Senior Lecturer, Department of Informatics, Institute of
Physics, Mathematics and Digital Technologies
Kazakh National Women's Teacher Training University
E-mail: aliaod_80@mail.ru; ongarbayeva.a@qyzpu.edu.kz
ORCID: 0000-0003-0835-4156

Salidin K. Kaldybaev

(Bishkek, Kyrgyzstan)
Dr. Sci. (Educ.), Professor, Vice-Rector
Ala-Too International University
E-mail: salidin.kaldybaev@alattoo.edu.kg

Aizhan K. Koishybekova

(Taldykorgan, Kazakhstan)
PhD, Senior Lecturer, Department of Informatics and
Digitalization of Education, Faculty of Physics and
Mathematics
Zhetysu University named after I. Zhansugurov
E-mail: aizhankym@gmail.com; a.koishybekova@zu.edu.kz
ORCID: 0000-0002-5784-0911

Authors contribution

Gulzada Esenalieva: Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Software, Validation, Writing – Review & Editing, Supervision, Project administration

Aliya D. Ongarbayeva: Writing – Review & Editing, Resources

Salidin K. Kaldybaev: Writing – Review & Editing, Resources

Aizhan K. Koishybekova: Writing – Review & Editing, Resources

© Gulzada Esenalieva, Aliya D. Ongarbayeva, Salidin K. Kaldybaev, Aizhan K. Koishybekova, 2026

Авторы заявляют об отсутствии конфликта интересов

The authors declared no conflicts of interest