Registered in Germany Europa Revue Journal
ISSN: 1862-6564 Vol. 6 No. 5 (2026) Published May 31, 2026

PEDAGOGICAL CONDITIONS FOR DEVELOPING PROACTIVE MALWARE PROTECTION COMPETENCE AMONG SCHOOL STUDENTS

Anvar Kutlimuratov

Teacher of Informatics and ICT, School No. 65, Beruniy District, Republic of Karakalpakstan, Uzbekistan

ABSTRACT

The article substantiates the pedagogical conditions for developing proactive malware protection competence among school students. The study is based on the idea that cybersecurity education should not be limited to recognizing malware names or responding after an incident. Students need to develop the ability to identify early indicators of a potential threat, analyze the situation, make a justified safe decision, perform preventive actions, and reflect on the decision made. The article defines proactive malware protection competence as an integrative competence that enables a student to recognize initial malware indicators, assess associated risks, choose an appropriate preventive decision, act safely, and evaluate the effectiveness of the chosen action. Five structural components are identified: motivational-value, cognitive, diagnostic-analytical, preventive-practical, and reflective-evaluative. A pedagogical mechanism based on the cycle "THREAT → INDICATOR → ANALYSIS → SAFE DECISION → PREVENTIVE ACTION → REFLECTION" is proposed. Five pedagogical conditions are substantiated: a motivational-value environment, indicator-oriented content, problem and situational diagnostic-analytical activity, a safe practical/simulation environment, and a reflective-evaluative environment for independent security decisions. Criteria and three levels of competence development are also proposed. The study has a conceptual and theoretical character and requires further empirical validation.

Keywords: *cybersecurity education, malware protection, proactive competence, school students, threat indicators, preventive action, safe decision-making, digital competence, cybersecurity pedagogy.*

1. INTRODUCTION

The expansion of digital technologies in education has increased the importance of cybersecurity competence among school students. Students increasingly work with web resources, electronic documents, archives, messaging services, cloud platforms, and executable or script-based objects. In such an environment, cybersecurity education cannot be reduced to memorizing the names and characteristics of malicious software. A student may know that an executable file can be dangerous but still fail to identify a suspicious context, evaluate its source, or decide what to do before opening it. Digital competence frameworks explicitly connect digital competence with knowledge, skills, and attitudes for confident, critical, and safe engagement with digital technologies [1].

2. CONCEPTUAL FOUNDATIONS OF PROACTIVE MALWARE PROTECTION COMPETENCE

2.1. Pedagogical Meaning of the Competence

In this study, proactive malware protection competence is considered not simply as a set of technical cybersecurity facts but as the student's ability to apply knowledge in an uncertain or potentially dangerous digital situation. The central educational result is the ability to recognize a possible threat before harmful consequences occur and to choose an appropriate preventive action. This interpretation is consistent with competency-oriented approaches that connect knowledge and skills with the ability to perform cybersecurity-related tasks [2].

2.2. Pedagogical Interpretation of Proactivity

Proactivity in cybersecurity education means acting on the basis of an early warning sign rather than waiting for confirmed damage. The pedagogical object is therefore the student's decision-making process in response to an indicator.

2.3. Author's Definition and Structural Components

Proactive malware protection competence is defined in this article as the student's integrated ability to identify initial indicators of a potential malware threat, analyze the associated risk, make a preventive and justified decision, act safely, and reflect on the result.

The competence includes five structural components:

1. Motivational-value component — awareness of responsibility for digital security and a preventive orientation.

2. Cognitive component — knowledge of threats, their indicators, and basic safe-use rules.

3. Diagnostic-analytical component — ability to identify and analyze threat indicators and contextual evidence.

4. Preventive-practical component — ability to choose and perform safe actions before harm occurs.

5. Reflective-evaluative component — ability to justify a decision, evaluate its effectiveness, and improve future behavior.

3. PEDAGOGICAL CLASSIFICATION OF MALWARE-RELATED THREATS

The proposed classification is intended for educational purposes. Its purpose is not to reproduce a technical malware taxonomy but to organize situations in which students can learn to identify indicators and make preventive decisions. The central pedagogical question is: what observable sign should cause the learner to stop, analyze, and choose a safe action?

3.1. Spam and Phishing

Spam and phishing messages provide accessible situations for developing early-warning skills. Relevant indicators may include an unknown sender, an unusual request, suspicious links, urgency or pressure, inconsistent addresses, or unexpected attachments. The learning objective is to teach students to verify the source and context before following a link, opening an attachment, or providing information [7].

3.2. Archived Objects

Archives can contain executable or script objects and therefore represent an important educational context. Students should learn to examine the source, file contents, expected purpose, and file types before extracting or opening unknown objects. MITRE ATT&CK documents archive-related techniques in which adversaries compress or package data, including through utilities [12]. The related sub-technique specifically describes the use of utilities to archive data [13].

3.3. EXE, COM, BAT, CMD and VBS Objects

Executable and script-related file types provide clear examples for indicator-based instruction. Microsoft documents AppLocker executable rules for executable files and describes the relevant executable-rule behavior [10]. AppLocker rule collections separately distinguish executable files and script types such as .bat, .cmd, and .vbs [11]. The general AppLocker documentation also describes rule collections, enforcement modes, rule conditions, and rule behavior [9].

3.4. Mining Malware and System Behavior

System behavior can also serve as an early indicator. Unexpectedly high CPU utilization, unusual resource consumption, unexplained system slowdown, or other abnormal behavior may require investigation. Students should be taught not to make an immediate conclusion from one symptom, but to consider alternative causes and then inspect the situation systematically.

3.5. General System of Indicators

Situation	Potential indicator	Preventive learning action
Suspicious message or link	Unknown source, unusual request, pressure, unexpected link	Verify sender/source before opening or responding (CISA et al., 2025)
Unknown archive	Unexpected archive or unclear contents	Assess source and contents before extraction (MITRE ATT&CK, n.d.)
EXE/COM file	Executable object from an uncertain source	Check source, purpose, and necessity before execution (Microsoft, n.d.-a; Microsoft, n.d.-b; Microsoft, n.d.-c)
BAT/CMD/VBS file	Script object in an unexpected context	Assess source and intended function before execution (Microsoft, n.d.-a; Microsoft, n.d.-b; Microsoft, n.d.-c)
Abnormal system behavior	Unexpected CPU load, slowdown, or resource consumption	Consider alternative causes and inspect the system

4. PEDAGOGICAL CONDITIONS FOR DEVELOPING PROACTIVE PROTECTION COMPETENCE

The development of proactive competence requires an educational environment in which students repeatedly encounter safe, structured decision-making situations. Five interrelated pedagogical conditions are proposed.

1. Motivational-value environment.

Students need to understand cybersecurity as a personal and collective responsibility. Preventive behavior should be connected with responsibility, caution, and awareness of consequences.

2. Indicator-oriented content.

Learning content should emphasize observable indicators, contextual clues, and relationships between indicators and safe decisions rather than only lists of malware names.

3. Problem and situational diagnostic-analytical activity.

Students should solve cases in which the available information is incomplete or ambiguous. They identify indicators, compare possible explanations, assess risk, and justify their decisions.

4. Safe practical and simulation environment.

Practical learning should model cybersecurity situations without executing real malware, distributing malicious code, or exposing real systems to unnecessary risk.

5. Reflective-evaluative environment for independent security decisions.

Students should explain why they selected an action, evaluate its effectiveness, and identify how their future response could be improved.

5. PROACTIVE PEDAGOGICAL MECHANISM

The central mechanism of the proposed approach is represented as a six-stage cycle:

THREAT → INDICATOR → ANALYSIS → SAFE DECISION → PREVENTIVE ACTION → REFLECTION

At the first stage, a potentially dangerous situation is introduced. At the second stage, students identify observable indicators. At the third stage, they analyze the source, context, file type, message content, or system behavior. At the fourth stage, they select

and justify a safe decision. At the fifth stage, they perform or model a preventive action. At the sixth stage, they reflect on the decision and consider how it could be improved.

The cyclical nature of the mechanism is important because reflection becomes the basis for improving future decisions. Thus, the learning result is not a single correct answer but the development of a transferable decision-making strategy.

6. DIDACTIC PRINCIPLES OF PROACTIVE PROTECTION

1. Preventive and early-warning orientation.
2. Indicator-based learning.
3. Problem-based and situational learning.
4. Safe modeling of cybersecurity situations.
5. Independent decision-making.
6. Evidence- and probability-based reasoning.
7. Gradual increase in complexity.
8. Reflective improvement.
9. Transfer of learned strategies to new situations.

7. CRITERIA AND LEVELS OF COMPETENCE DEVELOPMENT

Competence should not be assessed only through a binary “safe/unsafe” result. Assessment should consider how the student perceives a risk, identifies indicators, analyzes available information, justifies a decision, performs preventive action, and reflects on the result.

Criterion	What is assessed	Expected evidence
Motivational-value	Preventive orientation and responsibility	Recognizes personal responsibility and the need for caution
Cognitive	Knowledge of threats and indicators	Identifies relevant threat indicators and safety rules
Diagnostic-analytical	Identification and analysis of indicators	Connects indicators with context and possible risk
Preventive-practical	Safe preventive action	Chooses and performs an appropriate safe action

Criterion	What is assessed	Expected evidence
Reflective-evaluative	Justification and improvement	Explains the decision and identifies ways to improve

Three levels of competence development are proposed:

Initial level

The student recognizes familiar indicators with teacher support and applies basic safety rules.

Functional level

The student independently identifies indicators, analyzes a situation, and chooses an appropriate preventive action in familiar contexts.

Proactive-reflective level

The student transfers the strategy to new or uncertain situations, justifies decisions using available evidence, acts preventively, and reflects on the effectiveness of the decision.

8. DISCUSSION

The proposed approach is consistent with established cybersecurity and digital competence frameworks while emphasizing a specific pedagogical dimension. DigComp 2.2 provides a framework for safe digital competence [1]. The NICE Framework provides a common structure for cybersecurity tasks, knowledge, skills, and competencies [2], while the NIST K–12 Roadmap identifies educational strategies and priorities for cybersecurity education [3]. The NICE Framework Resource Center separately maintains current framework components, including competency areas and task, knowledge, and skill statements [14]. NIST also provides dedicated K–12 cybersecurity education resources through the NICE initiative [15]. A 2024 systematic review of K–12 cybersecurity education identified 24 eligible academic studies and reported recurring topics and cybersecurity competencies/skills relevant to K–12 learners [4]. Problem-based learning research in cybersecurity education describes the value of using complex, ill-defined problems and hands-on activities to support problem-solving and critical-thinking skills [5]. A systematic literature review of cybersecurity

education papers also mapped covered topics, teaching contexts, evaluation methods, and teaching approaches across the SIGCSE and ITiCSE literature [6].

9. CONCLUSION

The article substantiates proactive malware protection competence as an educational competence focused on the early identification of potential threats, risk analysis, preventive decision-making, safe action, and reflection. The competence is structured through five components: motivational-value, cognitive, diagnostic-analytical, preventive-practical, and reflective-evaluative.

Five pedagogical conditions are proposed: a motivational-value environment; indicator-oriented educational content; problem and situational diagnostic-analytical activity; a safe practical and simulated environment; and a reflective-evaluative environment that supports independent security decisions.

The central pedagogical mechanism is expressed through the cycle THREAT → INDICATOR → ANALYSIS → SAFE DECISION → PREVENTIVE ACTION → REFLECTION. This mechanism connects knowledge with action and reflection and is intended to support the development of security-oriented thinking rather than the simple memorization of malware characteristics.

The proposed approach includes nine didactic principles and three levels of competence development: initial, functional, and proactive-reflective. The framework can be applied to educational situations involving phishing, suspicious links, unknown archives, executable and script objects, and abnormal system behavior.

At the same time, the present study does not claim empirical effectiveness. Further research should experimentally test the proposed conditions and assessment criteria, develop validated diagnostic tools, and compare learning outcomes across different instructional models CISA's #StopRansomware Guide provides prevention, detection, response, and recovery guidance for reducing ransomware risk [8].

For ransomware-related education, CISA's #StopRansomware guidance provides a prevention, detection, response, and recovery perspective that can inform safe instructional scenarios [8].

10. REFERENCES

[1] European Commission, Joint Research Centre. DigComp 2.2: The Digital Competence Framework for Citizens. 2022.

[2] Petersen, R., Santos, R., Wetzel, K. A., Smith, M. C., & Witte, G. Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1. 2020. DOI: 10.6028/NIST.SP.800-181r1.

[3] National Institute of Standards and Technology (NIST). Roadmap for K–12 Cybersecurity Education. 2021.

[4] Ibrahim, A., et al. A Systematic Review of K-12 Cybersecurity Education Around the World. IEEE Access, 12, 59726–59738. 2024. DOI: 10.1109/ACCESS.2024.3393425.

[5] Shivapurkar, A., et al. Problem-based Learning for Cybersecurity Education. Journal of Cybersecurity Education, Research and Practice, 7(1). 2020. DOI: 10.53735/cisse.v7i1.108.

[6] Švábenský, V., Vykopal, J., & Čeleda, P. What Are Cybersecurity Education Papers About? A Systematic Review of Papers Published in Selected Cybersecurity Education Venues. 2019.

[7] CISA, NSA, FBI, & MS-ISAC. Phishing Guidance: Stopping the Attack Cycle at Phase One. 2025.

[8] Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware Guide.

[9] Microsoft. Working with AppLocker Rules.

[10] Microsoft. Executable Rules in AppLocker.

[11] Microsoft. Understanding AppLocker Rule Collections.

[12] MITRE ATT&CK. Archive Collected Data (T1560).

[13] MITRE ATT&CK. Archive via Utility (T1560.001).

[14] National Institute of Standards and Technology (NIST). NICE Framework Components.

[15] National Institute of Standards and Technology (NIST). NICE K–12 Cybersecurity Education Resources.