

PIXEL CONFERENCES  
NEW PERSPECTIVES IN SCIENCE EDUCATION  
FLORENCE 19-20 MARCH 2026

# **IMPROVING THE SAFETY POSTURE OF ITALIAN RESEARCH SECTOR IN LIGHT OF NEW EUROPEAN REGULATORY FRAMEWORKS.**



Serena Montefusco  
Matteo Bernardini  
Paolo Micozzi

PIXEL CONFERENCES  
NEW PERSPECTIVES IN SCIENCE EDUCATION  
FLORENCE 19-20 MARCH 2026

# OVERVIEW



- Introduction
- Objective
- Research Questions
- Literature Review
- Research Design
- Data Collection & Analysis
- Key Findings
- Discussion
- Conclusion
- Recommendations

PIXEL CONFERENCES

NEW PERSPECTIVES IN SCIENCE EDUCATION

FLORENCE 19-20 MARCH 2026

# INTRODUCTION



Research institutions are particularly **vulnerable** because they **manage high-value data**, including scientific research results, intellectual property, and personal data.

At the same time, universities and research institutions operate in **highly interconnected digital environments**, often collaborating internationally.

For this reason, **cybersecurity** must be considered **not only a technical issue but also a strategic governance challenge**.

Several regulatory instruments have been introduced, including the **NIS Directive**, the **GDPR**, and more recently the **NIS2 Directive**.

PIXEL CONFERENCES

NEW PERSPECTIVES IN SCIENCE EDUCATION

FLORENCE 19-20 MARCH 2026

# OBJECTIVES



- Analyze how training and awareness initiatives improve cybersecurity posture
- Evaluate the Cyber Sapere program
- Assess cybersecurity awareness levels in the research sector
- Support NIS2 implementation

PIXEL CONFERENCES

NEW PERSPECTIVES IN SCIENCE EDUCATION

FLORENCE 19-20 MARCH 2026

# RESEARCH QUESTIONS



**1** How does cybersecurity training influence organizational security posture?

**2** What is the current cyber awareness level within the Italian research sector?

**3** Do phishing simulations and training programs influence user behavior?

**4** Which strategies can strengthen cyber resilience in research institutions?

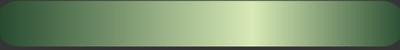
PIXEL CONFERENCES  
NEW PERSPECTIVES  
IN SCIENCE EDUCATION  
FLORENCE 19-20 MARCH 2026

# LITERATURE REVIEW

## Key Themes in Cybersecurity Research

- De Zan, Tommaso, Giampiero Giacomello, and Luigi Martino. "Italy's Cybersecurity Architecture and Critical Infrastructure." *Routledge Companion to Global Cyber-Security Strategy*, edited by Mary Manjikian and Scott Romaniuk, Routledge, 2021, pp. 121–131.
- European Cyber Security Organisation, "NIS2 Implementation: challenges and priorities.", 2025.
- Wenbo, G., Yujin, P., Tianneng, S., Zhun, W., Andy, Z., Dawn, S., "Frontier AI's Impact on the Cybersecurity Landscape.", Arxiv, 2025
- Tolossa, N. D., "Importance of Cybersecurity Awareness Training for Employees in Business. Vidya", *A Journal of Gujarat University*, 2023, 2. 104-107.
- Micozzi, P., Montefusco, S., "Digitalization of Services and the Creation of New Barriers: Upskilling and Reskilling as a Way to Mitigate the Digital Divide." In *Firenze Pixel, The Future of Education Conference Proceedings 2025*. Filodiritto Publisher, 2025, 561-567

# RESEARCH DESIGN



## Case Study Approach

Our research design is based on the analysis of the Cyber Sapere program, which represents a large-scale cybersecurity initiative within the Italian research sector.

## Empirical approach

Analyzing data generated through training activities and awareness initiatives.

# DATA COLLECTION & ANALYSIS

---

## Cyber Skill Assessment

Evaluation of participants' initial cybersecurity knowledge.

## Training Programs

- Asynchronous e-learning
- Synchronous online courses
- In-person workshops

## Phishing Simulations

Conducted to observe user behavior

# KEY FINDINGS



## Program Participation

- Cyber Skill Assessment:
  - 233 institutions involved
  - 12,853 participants

Average awareness level: Intermediate

- Training participation:
  - Nearly 2,000 participants in synchronous courses
  - Positive satisfaction levels

## Phishing Simulation Results

- Click rates:
  - Campaign 1 → 9% average
  - Campaign 2 → 14% average
  - Campaign 3 → 10% average

Trend → Gradual improvement in awareness

# DISCUSSION



- The results confirm that the human factor plays a crucial role in cybersecurity.
- Training initiatives appear to improve awareness and reduce risky behavior.
- Upskilling and reskilling as enabling factors for a proper security posture
- Differences between institutions suggest that organizational culture and internal practices also influence cybersecurity awareness.

PIXEL CONFERENCES

NEW PERSPECTIVES IN SCIENCE EDUCATION

FLORENCE 19-20 MARCH 2026

# CONCLUSION



The results of the initial **Cyber Skill Assessment** indicate an **overall medium level of security posture** for both **universities** and **AFAM institutions**, while a **significant difference emerges** in the outcomes of **phishing campaigns** between **universities** and **AFAM institutions** on the one hand and the **Ministry** on the other, in favor of **greater awareness among the former**. Assuming the statistical sample to be reliable, this result is, at present, difficult to explain other than by considering endogenous factors that generate distinct sensitivity toward the proposed campaigns.

PIXEL CONFERENCES

NEW PERSPECTIVES IN SCIENCE EDUCATION

FLORENCE 19-20 MARCH 2026

# RECOMMENDATIONS



- Investing in skills and awareness is essential
- Continuous cybersecurity training
- Strong security culture
- Development of specialized skills
- Replication of the Cyber Sapere model



# THANK YOU

F O R T H E A T T E N T I O N

## Q&A

Serena Montefusco: [serena.montefusco@hspi.it](mailto:serena.montefusco@hspi.it)

Matteo Bernardini: [matteo.bernardini@hspi.it](mailto:matteo.bernardini@hspi.it)

Paolo Micozzi: [paolo.micozzi@mur.gov.it](mailto:paolo.micozzi@mur.gov.it)

