CYBERSECURITY RISKS IN EDUCATIONAL COMMUNICATION SYSTEMS: ACCOUNT COMPROMISE, SOCIAL ENGINEERING, AND FINANCIAL FRAUD

Nematova Mohigul Bakhtiyor kizi
Uzbekistan State World Languages University
Faculty of English Language No. 2
3rd-year student
Scientific supervisor: Khudoyberganova Nozimakhon Bakhtiyor kizi
Teacher, Uzbekistan State World Languages University

Abstract. *The rapid digitalization of education has improved communication, accessibility, and instructional efficiency. At the same time, it has exposed educational institutions to growing cybersecurity risks, especially those related to phishing, account compromise, social engineering, and financial fraud. Human factors remain central in many cyber incidents, making students and teachers particularly vulnerable in trust-based communication environments. This article examines major cybersecurity threats affecting educational communication systems, with special attention to compromised teacher accounts used to deceive students. It also discusses the causes and consequences of such attacks and proposes preventive measures based on international cybersecurity guidance and current research.*

Keywords: *cybersecurity in education, account compromise, phishing, social engineering, financial fraud, educational communication*

Introduction

Digital platforms have become an essential part of modern education. Universities and schools increasingly depend on messaging applications, learning management systems, and cloud-based services for communication between teachers and students. While these technologies improve academic interaction and administrative efficiency, they also create new security vulnerabilities.

Cybersecurity refers to the protection of digital systems, networks, and data from unauthorized access, misuse, and disruption. In educational settings, cybersecurity is particularly important because institutions process sensitive information, including student records, academic communications, and financial data. Global threat reporting shows that phishing, credential theft, and social engineering remain among the most persistent cyber threats, and many incidents exploit human trust rather than technical weaknesses alone (ENISA, 2023).

A particularly serious issue in educational communication systems is the compromise of teacher accounts. When attackers gain access to an official account, they may impersonate the teacher and send fraudulent messages to students, often requesting money under urgent or deceptive pretexts. Because such messages appear to come from a trusted academic authority, students may comply without verifying authenticity. This study investigates how these attacks occur, what consequences they produce, and what preventive measures educational institutions should adopt.

DOI: 10.5281/zenodo.19781050

Method

This article uses a qualitative analytical approach based on secondary sources. It draws on cybersecurity reports, international guidance, and academic literature to examine common threats affecting educational communication systems. The analysis focuses on four areas: the cybersecurity threat landscape in education, major causes of account compromise, the pattern of social engineering and financial fraud through impersonation, and effective mitigation strategies.

The study also uses descriptive comparison to relate general cybersecurity findings to educational environments, especially higher education contexts in which teacher-student communication depends heavily on digital trust. The selected sources include ENISA's threat landscape reporting, Verizon's data breach investigations, IBM's breach-cost reporting, UNESCO materials on digital safety and education, and Hadnagy's work on social engineering.

Results

The analysis indicates that educational communication systems are vulnerable to both technical and human-centered threats. One major finding is that a large proportion of cybersecurity incidents involve human action or error. Verizon's 2023 Data Breach Investigations Report states that the human element was involved in 74% of breaches, while stolen credentials and phishing remained among the main initial access methods (Verizon, 2023).

Another result is that phishing and social engineering continue to be highly effective because attackers exploit trust, urgency, and institutional authority. ENISA's 2023 threat landscape also identifies social engineering as a major cyber threat category (ENISA, 2023).

In educational settings, these general patterns appear in a specific form: compromised teacher accounts are used to send deceptive messages to students. The attack sequence commonly involves gaining access through weak passwords or phishing, impersonating the teacher, requesting urgent financial support or payment, and then collecting money fraudulently. Because the message comes from a familiar and trusted source, students may respond without suspicion.

The study further shows that the consequences of these incidents extend beyond direct financial loss. Victims may experience stress and confusion, while teachers may suffer reputational damage. Repeated incidents can also weaken trust in digital education platforms and reduce confidence in institutional communication. At the organizational level, continued security failures may damage the credibility of schools and universities. IBM's 2023 reporting also shows that data breaches carry significant financial consequences globally, underlining the broader cost of poor cyber resilience (IBM Security, 2023).

Discussion

The findings suggest that cybersecurity in education should not be treated as a purely technical issue. Instead, it must be understood as a behavioral, institutional, and technological challenge. Even when educational organizations use digital systems effectively, their communication environments remain vulnerable if users are unable to recognize manipulation attempts or follow safe authentication practices.

The educational context is especially sensitive because relationships between teachers and students are built on trust. This trust, while essential for learning, can be exploited by attackers who impersonate legitimate authority figures. Hadnagy (2018)

explains that social engineering attacks succeed because they rely on psychological influence, urgency, and compliance rather than on sophisticated technical intrusion alone.

The discussion also highlights disparities in institutional preparedness. Many institutions in technologically advanced settings implement multi-factor authentication, centralized communication tools, continuous monitoring, and awareness training. In contrast, institutions with limited cybersecurity infrastructure may still rely on informal channels and weak account protection, increasing exposure to fraud. UNESCO's materials on safe digital spaces support the need for safer digital environments and stronger digital literacy across educational systems (UNESCO, 2021).

These findings imply that effective prevention requires a multi-layered response. Technical protections such as multi-factor authentication should be combined with user education, clear communication protocols, and incident-reporting systems. Financial requests should never be made through informal academic accounts or unsecured messaging channels. Awareness campaigns should also teach students how to verify suspicious requests before acting on them.

Conclusion

The digital transformation of education has created important opportunities for communication and learning, but it has also increased exposure to cyber threats. Among the most serious risks are account compromise, phishing, and social engineering attacks that exploit teacher-student trust for financial fraud. These attacks produce financial, psychological, and reputational harm and may undermine confidence in educational institutions.

To address these risks, educational organizations need an integrated cybersecurity strategy that combines technical safeguards, user awareness, and institutional policy. Improving cybersecurity literacy among both teachers and students is essential for building a safer and more resilient digital education environment.

References:

1. ENISA. (2023). Cybersecurity Threat Landscape Report.
2. UNESCO. (2022). Digital Safety in Education.
3. Verizon DBIR. (2023). Data Breach Investigations Report.
4. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking.
5. IBM Security. (2023). Cost of a Data Breach Report.