



University of Ghardaia

Faculty of Economic, Commercial, and Management Sciences

In collaboration with the Laboratory for Research on Digital Infrastructure, Artificial Intelligence, and their Applications in the Digital Transformation of Economic Sectors.

And in partnership with the Research Team on the Requirements for Implementing Corporate Governance and Auditing in Algerian Economic Institutions at the Laboratory of Applied Studies in Financial Sciences.

And in partnership with the National Independent Union of Higher Education Employees - Ghardaia Branch, they are organizing:

The First National Forum (in person and remotely) on: Governance of Higher Education Institutions

In light of digital transformation and modern legislation.

: Title of the research paper

Digital transformation as a tool to support social re-engineering in university management - an analytical study -

Prepared by:

Axis number:

*Dr. Kheira Zeguieb (Senior Lecturer - A-) University of Ghardaia (Algeria)

zeguieb.kheira@univ-ghardaia.edu.dz

Prof. Dr. Mohamed ADJILA (Professor of Higher Education), University of Ghardaia

m.adjila@univ-ghardaia.edu.dz

Abstract:

This study aims to highlight the role of Digital Transformation in reducing the risks of Social Engineering within university administration. Higher education institutions face increasing threats targeting human vulnerabilities to gain unauthorized access to sensitive information. The study analyzes the relationship between adopting digital technologies and enhancing information security, emphasizing the importance of awareness and training in mitigating such risks. It concludes that digital transformation, when supported by effective security measures and a strong organizational culture, can serve as a powerful tool for protecting data and improving administrative efficiency.

Keywords: Digital Transformation, Social Engineering, Information Security, University Administration, Cyber Risks, Data Protection.

المخلص:

تهدف هذه الدراسة إلى إبراز دور التحول الرقمي في الحد من مخاطر الهندسة الاجتماعية داخل الإدارة الجامعية، حيث تواجه المؤسسات الجامعية تهديدات متزايدة تستهدف العنصر البشري بهدف اختراق الأنظمة والوصول إلى معلومات حساسة. تعتمد الدراسة على تحليل العلاقة بين تبني التقنيات الرقمية وتعزيز الأمن المعلوماتي، مع التركيز على أهمية التوعية والتدريب في تقليل هذه المخاطر. وتخلص إلى أن التحول الرقمي، إذا تم دعمه بإجراءات أمنية فعالة وثقافة تنظيمية واعية، يمكن أن يشكل أداة قوية لحماية البيانات وتحسين كفاءة العمل الإداري.

الكلمات المفتاحية: تحول الرقمي، هندسة اجتماعية، أمن المعلوماتي، إدارة جامعية، مخاطر سيبرانية، حماية بيانات،

1. Introduction:

In recent years, the world has witnessed rapid developments in digital transformation, which has become a fundamental element in improving the efficiency and performance of institutions. This transformation has encompassed various sectors, including higher education, which seeks to adopt digital systems to enhance the quality of administrative and academic services.

Conversely, increasing security threats have emerged, most notably social engineering, which targets human beings by exploiting their psychological and behavioral vulnerabilities to access sensitive information.

University administrations are fertile ground for such attacks due to their handling of diverse data (students, faculty, and staff).

Therefore, the importance of digital transformation is highlighted not only as a means to improve performance but also as a tool to enhance information security and mitigate the risks associated with social engineering.

1.1 Problem Statement:

Despite the expansion of digital transformation applications within university administrations, the risks of social engineering persist and may even be exacerbated in some cases due to weak security awareness or misuse of technology.

Accordingly, the main research problem can be formulated as follows:

To what extent does digital transformation contribute to reducing the risks of social engineering within university administration?

This leads to the following sub-questions:

- What is the nature of threats associated with social engineering in the university environment?

- How can digital systems enhance information security within university administration?
- What role do awareness and training play in supporting the effectiveness of digital transformation in this field?

1.2 Study Significance :

The significance of this study stems from several aspects:

Scientific Significance: It contributes to enriching the literature related to information security in the higher education sector.

Applied Significance: It helps university administrations adopt effective digital solutions to reduce security risks.

Awareness Significance: It highlights the role of the human element in protecting information and promotes a culture of cyber security.

Strategic Significance: It supports the efforts of educational institutions in achieving a secure and sustainable digital environment.

1.3 Study Objectives:

This study aims to:

- Analyze the concept of digital transformation and its role in university administration.
- Identify the most common social engineering techniques in educational institutions.
- Evaluate the extent to which digital transformation contributes to reducing these risks.
- Propose mechanisms and strategies to enhance information security within university administrations.
- Raise awareness among employees about the importance of cyber security.

2. Digital Transformation – A Comprehensive Vision

Digital transformation refers to the use of computer and internet technology in the process of creating more efficient and effective economic value. In a broader sense, it refers to the changes that new technology generally brings about in how we work, interact with it, and create wealth within this system.

2.1 Definition of Digital Transformation:

Digital transformation is defined as a new business model based on the use of digital technologies to create new products and services, their distribution methods, and a focus on the customer or user. (Ghraissi, Reda, & Ali, 2021)

It has also been defined as the process of transforming information from the physical to the digital level, a fact reflected in the accelerating global trends of technological adaptation by individuals, companies, societies, and nations. (Basba, 2020)

It can also be defined as a comprehensive transformation process resulting from a combination of three phenomena: automation, dematerialization, and the reorganization of mediation patterns. This transformation affects all internal operations, activities, and processes within an organization. (Taqawa & Shawam, 2023)

The digital transformation process must include three main requirements: (Sharqi & Safih, 2024)

First: A suitable strategy for digital transformation.

Second: Understanding the existing operational mechanisms within the organization and the degree of importance and effectiveness of each.

Third: Providing appropriate training to all stakeholders to demonstrate the best approach to the transformation and ensure adherence to the correct methodology through effective steps.

From the above definitions, it is clear that despite the multiple definitions of digital transformation, they all converge on one meaning that refers to the integration of digital technology with all areas of business, with the aim of improving processes and services. Digital transformation includes a wide range of technological technologies, including applications and programs, adoption of digital platforms, data analytics, internet-based services, network capabilities, artificial intelligence, machine learning, augmented and virtual reality, sensing technology, video-based analytics, and others, thus ensuring the selection of the appropriate technology to achieve the desired results.

2.2 Digital Transformation Objectives

Adopting digital transformation aims to achieve the following: (Mohammed Abdel Ghani, 2022)

- Promoting the development of more innovative and collaborative technological systems and financial culture at the institutional and societal levels.
- Transforming the education system to provide new skills and future-oriented guidance for individuals, enabling them to excel in digital work and society.
- Establishing and maintaining digital communications infrastructure, ensuring its management and accessibility, and balancing service quality with delivery costs.
- Enhancing digital data protection and transparency, guaranteeing independence requirements, and fostering trust.

- Improving access to services and establishing controls, mechanisms, and quality standards for digital services provided to the community.
- Implementing new and innovative business models and improving the regulatory framework and technical standards. The implementation of digital transformation is of great importance, including the following benefits (Ashouri & Ashouri, 2023):
- Significantly reduces costs, effort, and time.
- Improves and streamlines operational costs.
- Creates new and innovative opportunities that are far removed from traditional methods of providing various services.
- Reaching a wider segment of the public, customers, consumers, and competitors.
- Ensuring transparency in transactions.
- Creating an information society capable of handling technological data and keeping pace with the information age.

2.3 Risks and Challenges of Digital Transformation

The digital transformation process is not without risks. Among the reasons that have led to an increase in digital risks are the following (Chaouchi & Khalouf, 2023):

- Heavy reliance on digital technologies
- Increased number of targeted sites due to the proliferation of connected devices
- Digital innovation outpacing cybersecurity measures
- The convergence of information technology systems, operational technology, and the Internet of Things (IoT). To overcome these risks, the following challenges must be addressed (Ghraissi, Reda, & Ali, 2021):
- Lack of technical skills among the organization's employees is a fundamental factor that must be considered when formulating and revising the digital strategy
- Organizational culture, which is a blend of beliefs, values, and norms, is a problem that hinders the digital transformation process unless it is based on openness to change
- Coordination: If there is no good communication between the strategic leadership and the individuals, the digital transformation process will fail. Therefore, roles, responsibilities, and objectives must be clearly defined.
- Conflicting goals and roles, coordination and leadership problems, and a lack of vision and clarity for the key players. Weakness in the infrastructure related to information and communication technology equipment and technologies.

3. Social Engineering

3.1 Definition of Social Engineering:

Social engineering is defined as: "A set of techniques and skills used to manipulate people and exploit their psychological, emotional, and social weaknesses in order to obtain sensitive information or facilitate access to systems, networks, or programs. Social engineering relies on the principles of trust and persuasion, exploiting curiosity, fear, greed, desire, compassion, affiliation, or other human emotions. It uses various means of communication with victims, such as mobile phones, email, text messages, social media, personal visits, gifts, or rewards. Social engineering is considered One of the most serious threats to cybersecurity is cyberattacks, as they target the human element, which is considered the weakest link in the security chain. (Abdul-Ilah Saeed and Arwa Ahmed, 2025)

It has also been defined as: "The exploitation of human instincts, which are considered vulnerabilities in human nature, such as fear, trust, greed, curiosity, the desire to help, and attraction to like-minded individuals, among others, through various methods, most notably the internet, including emails, fake websites, and social networks." (Banking Studies Institute, 2019)

3.2 Stages of Social Engineering:

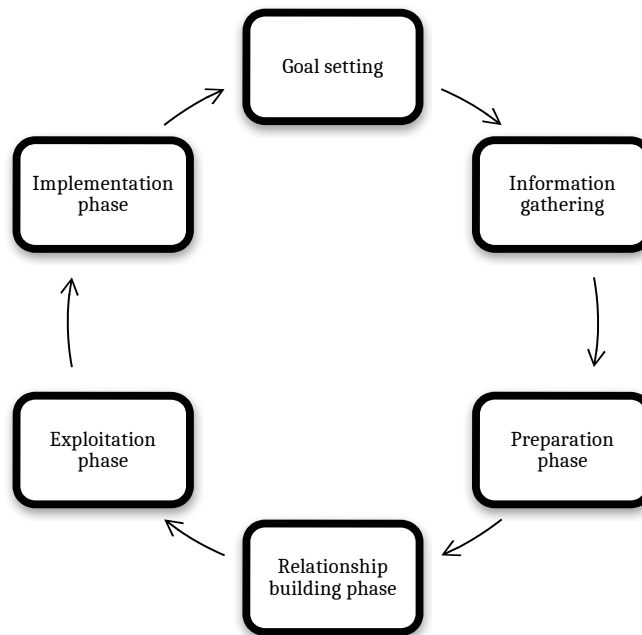
Social engineering requires several steps, which can be summarized as follows:

- **Target Identification:** This is the first stage of social engineering, where the attacker identifies the target they wish to attack and the information they want to obtain.
- **Information Gathering:** Once the target is identified, the attacker begins gathering various information related to that target. Attackers invest significant time and resources in collecting diverse information about their targets. The better the information, the easier the attack. (Dahmani, 2023)
- **Preparation Stage:** The preparation stage is the third stage of social engineering. In this stage, the attacker begins analyzing the information they have obtained about the target and develops a plan to establish a relationship with them.
- **Relationship Establishment Stage:** The relationship establishment stage is the fourth stage of social engineering. In this stage, the attacker begins to establish, improve, and strengthen their relationship with the target. This is done using social media, email, phone calls, or text messages. The stronger the relationship between the attacker and the target, the greater and faster the attacker can achieve their objective. The attacker will utilize all available means to solidify and strengthen this relationship. (Al-Shaboul, 2023)
- **Exploiting the Relationship:** Once the relationship with the targeted victim is established and developed, the attacker exploits it to their advantage.

- **The Implementation Phase:** Reaching the Objective: In this phase, the attacker actually carries out the planned actions and attempts to reach the final objective. If the attacker fails to achieve the desired results, they may repeat the previous steps. (Kamal & Abdel Raouf, 2018)

The stages can be summarized in the following figure:

Figure 1: Social engineering techniques:



Source

: Prepared by the researchers

The spread of social engineering is due to several factors, including: (Banking Studies Institute, 2019)

- The lack of policies and laws to protect the system and its users.
- The ease of access to any information, especially with the proliferation of social networks and search engines.
- Insufficient training in information security.
- The division of the institution or country into separate units.
- Its ease compared to other technical methods, as it can be achieved simply by exploiting human relationships and may not require extensive technical expertise.
- Security equipment and technology do not prevent its occurrence because it relies on the human element.
- The attacker does not need specialized equipment or skills; it is an inexpensive method.
- Victims' tendency to conceal errors and thefts that occur to them.

- A lack of awareness of its importance and severity among information security specialists and computer users
- The difficulty in detecting and tracing its effects.

3.3 Social Engineering Methods:

- **Human Methods:** This is one of the most commonly used methods in social engineering. Social engineers employ psychological techniques and methods to persuade their targets by building relationships and influencing them once they gain control.
- **Technological Methods:** These methods rely on digital technology. Various digital media are important sources of information, and social engineers often use digital search engines to gather as many victims as possible.
- **Human-Technical Methods:** These represent the most powerful methods and techniques of social engineering because they combine the human and technical elements. The social engineer takes into account societal cultures, human behaviors, values, and goals of the victims. This combination of methods increases the social engineer's chances of success in their desired tasks. (Hussein Ibrahim Hammadi, 2025)

4. The Role of Digital Transformation in Reducing Social Engineering Risks in University Administration

Digital transformation plays a crucial role in mitigating social engineering risks within university administration. This is because it reorganizes processes and enhances information security by utilizing modern technology instead of relying heavily on human resources (which are the primary target of social engineering attackers). (“Impact of Digital Transformation on Information Security in Higher Education”, p. 1)

4.1 Social Engineering Risks in University Administration: These include data breaches targeting students and faculty, hacking administrative accounts, manipulating results or documents, financial losses, or damaging the institution's reputation.

4.2 The Role of Digital Transformation in Reducing These Risks

Table (1) illustrates: Digital Transformation and its Role in Reducing Risks

Table (1) illustrates: Digital Transformation and its Role in Reducing Risks

Steps:	Digital transformation and its role in reducing risks -
Adopting advanced verification	Two-factor authentication (2FA) - Biometric verification This reduces the risk of account theft even if the password is compromised.
Digitalizing administrative processes	replacing paper documents with secure electronic systems – minimizes direct contact that can be exploited for fraud – thus reducing opportunities for manipulation
Utilizing threat detection	artificial intelligence systems to monitor abnormal behavior – and anti-phishing software helps detect attacks before damage occurs.
Digital awareness and training	- Training employees to recognize fraud attempts and promoting a cybersecurity culture within the university; the human element is the weakest link, so raising
Access and permissions management	- Defining user privileges and implementing the "least privilege" principle to prevent unauthorized access to sensitive information.
Using secure cloud computing	Storing data in secure environments and performing regular backups protects data from loss or breaches.

Source: Prepared by the researchers

Here is a comprehensive explanation of the role it can play

First: Reducing reliance on direct human interaction.

Social engineering relies primarily on deceiving people (such as identity theft or requesting sensitive information).

Digital transformation contributes to:

- Automating procedures (registration, document retrieval, approvals)
- Reducing paper-based or verbal communication.

This reduces opportunities for exploiting employees or students.

Second: Enhancing authentication and verification systems.

By implementing technologies such as:

- Multi-factor authentication (MFA)
- Single sign-on (SSO) system
- Biometric verification (fingerprint or facial recognition). - Even if a user is deceived, it is difficult for an attacker to access the system.

Third: Tracking processes and recording activities (logging).

Digital systems allow for:

- Recording all processes (Who logged in? What did they do? When?)
- Rapidly detecting abnormal behavior.

This helps in early detection of attacks and mitigating their impact.

Fourth – Digital Awareness and Training

Digital transformation is not limited to tools but also includes:

- Online training platforms for employees and students
- Phishing attack simulations

Raising awareness reduces the likelihood of falling victim to scams.

Fifth – Using Artificial Intelligence to Detect Threats

Modern systems can:

- Analyze messages and emails
- Detect phishing or fraud attempts
- Monitor abnormal behavior patterns

This provides proactive protection.

Sixth – Strict Access Control

Digital transformation allows for:

- Granting each user the lowest possible privileges (Principle of Least Privilege)
- Separating permissions among employees

This reduces damage even in the event of an account breach.

Seventh – Reducing Paper Documents

Paper documents:

- Are easily forged or lost
- Can be exploited in social engineering

This shift to secure digital systems reduces these risks.

Eighth - Unifying Official Communication Channels

Through:

- Official platforms (university portals, corporate email)

- Reducing reliance on unofficial channels

This facilitates message verification and reduces plagiarism.

Therefore, we conclude that digital transformation does not completely eliminate social engineering, but it:

- Reduces its chances of success
- Accelerates its detection
- Limits its impact. However, its success depends on two key elements:
 1. Secure technology
 2. User awareness

5. Conclusion:

Digital transformation significantly contributes to reducing the risks of social engineering, but its success depends not only on technology but also on user awareness and the implementation of strict security policies.

5.1. Results and Recommendations:

- Enhance information security
- Reduce cyber attacks
- Improve university management efficiency
- Increase trust in digital services
- Develop an integrated digital cyber security strategy
- Invest in modern protection technologies
- Mandate continuous training for staff
- Establish a dedicated information security unit within the university

6. References:

1. Asma Sharqi and Sadiq Safih. (December 2024). Evaluating the Algerian Experience in Digital Transformation: Reality and Challenges. *Journal of Studies in Economics and Business Administration*, 06(02), pp. 127-147.
2. Al Mahya Abdel-Ilah Saeed and Makin Arwa Ahmed. (2025). The Impact of Social Engineering on Cybersecurity Risks in Banks in Riyadh, Saudi Arabia. *Journal of Economic, Administrative and Legal Sciences*, 09(01), 06.
3. Al Anbaki Hussein Ibrahim Hammadi. (2025). Digital Social Engineering and its Impact on the Value System of Society. *Wasit Journal for Human Sciences*, 21(1), 635.
4. Amna Kharroubi and Marwa Attafi. (2022). The Role of Digital Transformation in Developing E-commerce in Algeria during the Period 2016-2021. Guelma: University of Guelma.
5. Amina Badr Eddine and Nassima Khadir. (2023). Digital Transformation in Algeria: Between Reality and Challenges. *International Conference: The Digital Revolution: What Opportunities for Growth?* (p. 17). Koléa: Higher School of Management and Digital Economy.
6. Badr Eddine Achouri and Ibrahim Achouri. (2023). The Impact of Digital Transformation on the Development of the Information and Communication Technology Sector for Integration into the Digital Economy. *Journal of Finance, Investment, and Sustainable Development*, 08(02), 219.
7. Ben Chaib Kamal and Ben Guida Abdelraouf. (2018). The Dangers of Social Engineering. *Third National Conference on the Consumer and the Digital Economy: The Necessity of Transition and the Challenges of Protection* (p. 3). Mila: Abdelhafid Boussouf University Center.
8. Khira Chaouchi and Zahra Khalouf. (August 25, 2023). Digital Transformation in Algeria. *Journal of Accounting, Auditing, and Finance*, 05(01), 21.
9. Rania Takaoua and Bouchama Chouam. (April 1, 2023). Digital Transformation as a Strategic Option in Light of the Transition to a Digital Economy in Algeria: An Exploratory Study. *Journal of Economics and Environment*, 06(01), 422.
10. Zina Al-Shaboul. (August 15, 2023). Stages of Social Engineering. Retrieved from: https://mawdoo3.com/%D9%85%D8%B1%D8%A7%D8%AD%D9%84_%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9_%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9
11. Sanaa Mohamed Abdel-Ghani. (April 2022). The Impact of Digital Transformation on Enhancing Economic Growth in Egypt. *Journal of the Faculty of Political Science and Economics*, 15(14), 56.
12. Sondos Obeidi Saad. (2023). The Impact of Digital Transformation on Financial Performance in Economic Institutions: A Case Study of the Regional Directorate of Mobilis. Ouargla: University of Ouargla.
13. Sadouki Ghraissi, Si Tayeb El Hachemi Reda, and El Absi Ali. (December 31, 2021). The Reality and Importance of Digital Transformation and Automation. *Araa Journal for Economic and Administrative Studies*, 03(02), 90-109.

14. Abdelkader Besbaa. (December 31, 2020). Evaluating the Digital Transformation Experience in Saudi Arabia According to the 2020 Digital Economy Index During the Coronavirus Pandemic. Research Journal, 07(02), 401.
15. Mohamed Dahmani. (2023). Cyber Threats: Social Engineering as a Model. Academic Journal of Legal and Political Research, 07(02), 695.
16. Institute of Banking Studies. (2019). Social Engineering. Kuwait: Institute of Banking Studies.
17. Institute of Banking Studies. (2022). The Future of the Caught in the Digital Age. Kuwait: Insights.