Remittances Review
January 2025,
Volume: 10, No: 1, pp. 18-36
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)

Received: 02 August 2024, Accepted: 03 January 2025
DOI: https://doi.org/10.47059/rr.vx9i2.02

Information Security as a Mechanism for Enhancing the Performance of Human Resources in Algerian Banking Institutions

Dr. Mokaddem Tebra [1], Dr. Makhloufi Kenza [2]

Mustapha Stambouli University Mascara, Algeria

Email : m.tebra@univ-mascara.dz , Kenza.makhloufi@univ-mascara.dz

Received: 02/08/2024; Accepted: 03/01/2025

ABSTRACT:

This study aims to examine the information protection methods employed in Algerian banking institutions in light of their use of information networks. The objective is to assess the adequacy of these methods in ensuring information security, highlight their strengths and weaknesses, and contribute to enhancing and reinforcing these measures. The study is divided into two sections: the theoretical framework, which relies on existing academic literature on the subject, and an empirical case study analyzing the state of information security in banking agencies and its impact on improving human resources performance.

To enrich this research, we designed a questionnaire comprising 32 statements distributed across five fundamental dimensions of information security: "**Information security threats, potential threat types, use of modern technology to counter information security threats, obstacles to using modern technology for information security, and ways to enhance banking institutions' capabilities to address information security threats**", in addition to performance improvement indicators. The questionnaire was administered to a sample of banking agencies in the city of Mascara.

Using a descriptive and analytical approach, the study found that most employees in banking institutions lack awareness of information security threats, which, in the context of Algerian banking institutions, primarily manifest as (disrupting computer memory and slowing down processing speed, using viruses to corrupt data, and information theft).

Keywords: Information security, information security threats, performance enhancement, banking institutions.

1. INTRODUCTION:

The advancement of information technology has led to new work patterns where computers have replaced human labor due to the increasing importance of information and the tools that process it, such as technical devices and computing systems. However, alongside these advancements, the negative aspects of technology usage have emerged, allowing for data breaches and information theft. Modern communication technologies have rendered traditional security measures ineffective in the face of rapid technological progress.

Consequently, banking institutions strive to implement the latest IT networks, computer equipment, and databases, establishing data exchange networks among them to create a comprehensive national information system. This system aims to enhance operational efficiency, improve service quality for citizens and other institutions, and leverage IT to optimize human resource performance while reducing service costs. To achieve these objectives, banks must adopt security measures that focus on both human and technological factors to protect against cyber threats and data breaches.

Based on this context, the study raises the following research problem: **What are the various threats to information security in Algerian banking institutions, and to what extent can information security be relied upon as a means to enhance employee performance?**

1.1 Research Questions:

The main research problem leads to the formulation of the following sub-questions:

- To what extent do Algerian banking institutions prioritize information security?
- Can Algerian banks develop a distinctive strategy to address information security threats?
- Is there a relationship between information security and the enhancement of human resource performance?
- What is the current state of modern technology usage in addressing information security threats in Algerian banking institutions?

1.2 Research Hypotheses:

To address the research problem and based on the study variables, the following hypotheses have been formulated:

- **First hypothesis:** There is a statistically significant relationship between information security in Algerian banking institutions and the level of human resource performance development.
- **Second hypothesis:** There are statistically significant differences in the perceptions of study participants regarding information security and its relationship to human resource performance development based on their personal and professional backgrounds.

1.3 Research Objectives:

- Contributing to the enrichment of theoretical and practical knowledge on information security.
- Understanding the concept of information security and its impact on service efficiency in banking institutions.
- Encouraging Algerian banking institutions to adopt modern technology to counter information security threats, which helps reduce operational errors, improve performance levels, and enhance service quality.

2. Theoretical Background of Information Security

Information technology is defined as: "The information revolution associated with the production, possession, marketing, storage, retrieval, display, and distribution of information through the integrated use of electronic computers and modern communication systems. In short, it is the new science of collecting, storing, retrieving, and transmitting modern information automatically via satellites." [1]

On the other hand, the limitless growth of information technology increases the responsibility of regulatory bodies in limiting the negative uses of technology that threaten information security. This requires enhancing protection levels and securing the resources used in information processing, ensuring the security of the organization, its employees, computing devices, and data storage media. This is achieved through the implementation of multiple security measures and protection strategies.[2]

As a result, any institution that owns an information system must be aware of the following:

2.1 Concept of Information Security

Information security is defined as: "The protection of various types of information and the tools used to process and manage it, including organizations, data centers, devices, storage media, and personnel, from theft, forgery, damage, loss, or unauthorized access, through the implementation of preventive measures and security policies." [3]

2.2 Importance of Information Security

Information holds both material and intangible value for individuals, companies, and nations. Its significance is even greater in security, military, and strategically important economic organizations. As a result, confidentiality has become a crucial factor in information security, influencing both the risks associated with data loss and the benefits gained from its protection. Information can play a decisive role in the success or failure of nations. The key reasons for the importance of information security include the following [4]:

- The necessity of integrating with communication and internet systems, as it is no longer feasible to isolate devices from local and wide-area networks while ensuring access to necessary information.

- The reliance of various organizations on the effectiveness of information for decision-making and operations.
- The difficulty of identifying threats, controlling risks, or tracking and prosecuting cybercriminals due to the lack of geographical boundaries in internet and electronic communications, which allow for cross-border intrusions.
- The rapid growth of electronic applications and services, including e-commerce, e-government, and e-administration, all of which require a secure information environment.

2.3 Methods of Information Theft

- **Identity Theft:** This method aims to obtain confidential or security-related information, access financial assets, or infiltrate an organization's database by impersonating another user.[5]
- **Using Viruses for Unauthorized Computer Access:** Viruses are capable of altering a device’s functionality without the owner’s consent or knowledge. They are classified into two types:
    - Benign viruses: These do not destroy software or files but may display messages on the screen or occupy memory space, falsely indicating that the memory is full.
    - Malicious viruses: These aim to cause maximum damage to the system, computer, and stored files. [6]
- **Hacking:** This involves unauthorized access to private or governmental systems and networks using specialized programs that crack passwords and access permissions. The purpose may be to view, corrupt, or steal data. [7]

2.4 Sources of Threats

Threat sources are classified into internal and external threats as follows [8]:

Internal Threats:

These originate from within the organization and include:

- Employees accessing confidential information without authorization to serve personal interests.
- Information leakage by system users or authorized personnel, either intentionally or unintentionally.

External Threats:

The major external threats include:

- **Software Threats:** These involve deleting, stealing, or corrupting software, either by disabling devices or infecting them with viruses.
- **Hardware Threats:** These include theft, tampering, cable damage, and destruction due to fire, water exposure, or electrical surges.

- **Information Threats:** These encompass deletion, erasure, corruption due to hardware and software failures, and ultimately, theft.

2.5 Ways to Enhance the Capabilities of Banking Institutions in Addressing Information Security Threats

- **Use of Smart Cards:** Smart cards store user information, such as their name, personal details, and password, on a magnetic strip. To access the network or its resources, the user must swipe the card through a digital scanner that reads the stored data and compares it with system records. If the credentials match, access is granted; otherwise, it is denied.
- **Biometric Authentication Technology:** This technology identifies users through unique biological traits such as fingerprints, palm prints, voice recognition, or other distinctive personal identifiers. These identifiers are converted into digital signals and stored in a password file. When a user attempts to access the network, they provide their biometric sample (fingerprint, hand scan, eye scan, or voice), which is converted into a digital signal and compared with the stored version. If a sufficient match is found, access is granted.[9]
- **Data Encryption:** Encryption is the process of transforming data using a specific algorithm, known as a key, to make it unreadable without decryption. Data is typically encrypted before transmission over a network to ensure its integrity and protect it from espionage or tampering. The recipient then uses a decryption key to restore the original data[10].
  - **Use of Firewalls:** Firewalls serve as a security system that can be software-based, installed on a server, or part of a more comprehensive solution that includes both software and dedicated hardware equipped with modems and network interface cards[11].
  - **Antivirus Software:** While some viruses may have minimal impact, such as displaying humorous messages, others can cause severe damage, including:
    - Deleting stored information from the hard drive
    - Corrupting software applications
    - Removing programs
    - Generating unexplainable errors
    - Damaging the hard disk [12]
  - **Backup Systems:** Data backups should be performed daily, weekly, or monthly, depending on business needs. For networks that rely entirely on file servers, daily backups are essential, requiring the duplication of all files stored on the server. In cases where users store data locally on personal computers, a full backup may be conducted weekly instead of daily.[13]
    - Regular monitoring of backup systems is necessary to ensure their effectiveness. This can be achieved by retrieving and comparing backup data with the original files.

  - A detailed log of backup operations should be maintained, including information such as backup dates, types, responsible personnel, and storage media used[14].

- **Uninterruptible Power Supply (UPS):** This system ensures the activation of backup power only when the main power supply fails. The backup power source continuously monitors fluctuations in electrical levels, switching to an alternative power supply when needed. During a power outage, there is only a minimal delay before the backup power source starts supplying electricity to the computer. [15]

- **Protection Against Insider Threats:** Employees can be a significant source of risk to information security, whether intentionally—due to malice, boredom, greed, or a desire for recognition or unintentionally, due to inadequate technical training in handling security systems. [16]

3. Field Study

After addressing the theoretical framework of the study variables, we will present, analyze, and interpret the results obtained from the field study. This will help assess the role of information security in enhancing the performance of human resources in Algerian banking institutions from the perspective of the study sample. The analysis is based on several key dimensions, including: Information security threats, Potential threat types ,Use of modern technology to counter information security threats ,Obstacles to implementing modern security technologies ,Ways to enhance the capabilities of banking institutions to address information security threats

This study relies on the statistical analysis of survey data, which was processed using the SPSS software. The following table presents the banking agencies included in the study:

Bank Name	**National Bank of Algeria**	**Algeria**	**External Bank of Algeria**	**Rural Development Bank**
Code	BNA	CPA	BEA	BADR

3.1 Methodological Framework of the Study

Based on the nature of this study, which aims to examine the role of information security in enhancing the performance of human resources in Algerian banking institutions, a descriptive and analytical approach was adopted. This was implemented using the survey method with a sample-based analysis.

3.2 Data Analysis

1 / Reliability Test:

To validate that the questionnaire accurately measures the impact of information security dimensions on human resource performance in banking institutions and to ensure its reliability, we utilized Cronbach’s Alpha coefficient. This method is commonly used to assess the reliability and internal consistency of questionnaires, indicating the strength of correlation between the scale items.

From a practical perspective, a Cronbach’s Alpha value of ≥ 0.60 is considered acceptable for research in management and social sciences. The following table presents the reliability coefficients obtained using the Cronbach’s Alpha method for each dimension:

Table (1): Reliability Coefficients (Cronbach’s Alpha Method) by Dimensions

Dimension	Number of Items	Cronbach’s Alpha Coefficient	Validity
Information Security	20	0.986 / 98%	0.992
Performance Improvement Indicators	12	0.982 / 98%	0.990
Overall Questionnaire	32	0.989 / 98%	0.994

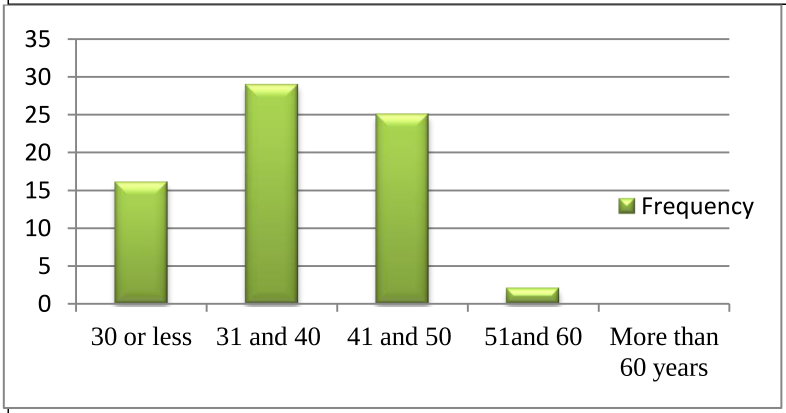
Source: Prepared by the researchers.

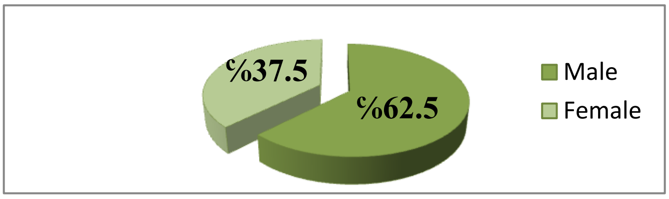
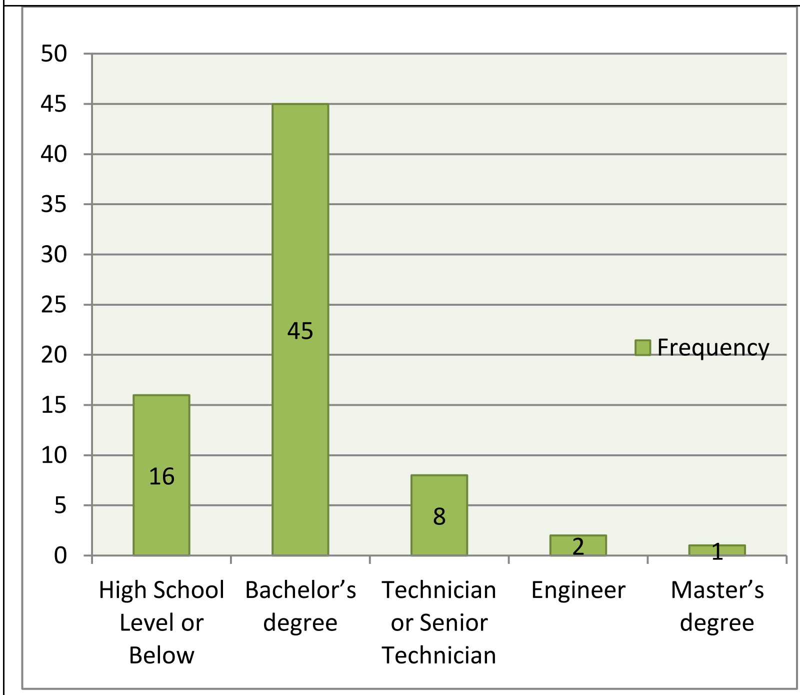
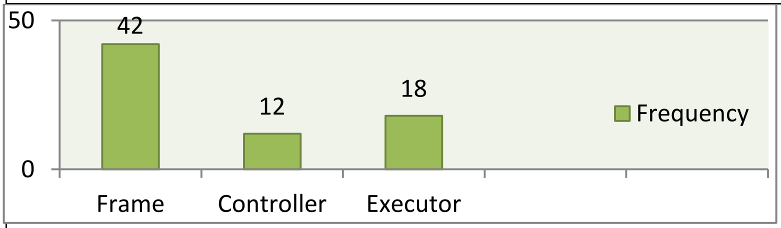
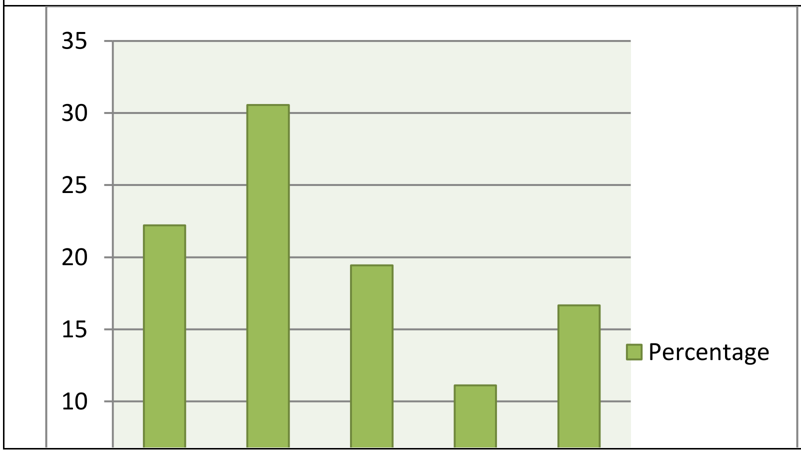
The reliability coefficient was found to be 0.995 (99.5%), which is significantly higher than the statistically acceptable threshold of 60%. Based on this, the measurement tool is considered valid and reliable for obtaining accurate data.

2 / Personal Data

The personal data of the study sample was analyzed based on the following dimensions: age, gender, educational qualification, professional category, and years of experience. After examining the questionnaires, the results were summarized in the following table:

Table (2): Personal Data of the Study Sample

Graph	Percentage		Attribute
1/ Distribution of the Study Sample by Age			
	٪ 22.22	16	30years or less
	٪ 40.27	29	Between 31 and 40 years
	٪ 34.72	25	Between 41 and 50 years
	٪ 2.77	2	Between 51 and 60 years
	٪ 0	0	More than 60 years
2/ Distribution of the Study Sample by Gender			

	٪ 62.50	45	Male
	٪ 37.50	27	Female
3/ Distribution of the Study Sample by Educational Qualification			
	٪ 22.22	16	High school level or below
	٪ 62.50	45	Bachelor's degree
	٪ 11.11	8	Technician or Senior Technician
	٪ 2.77	2	Engineer
	٪ 1.38	1	Master's degree
4/ Distribution of the Study Sample by Professional Level			
	٪ 58.33	42	Frame
	٪ 16.66	12	Controller
	٪ 25	18	Executor
5/ Distribution of the Study Sample by Years of Experience			
	٪ 22.22	16	5 years or less
	٪ 30.55	22	Between 6 and 10 years
	٪ 19.44	14	Between 11 and 15 years
	٪ 11.11	8	Between 16 and 20 years
	٪ 16.66	12	More than

			20 years
	٪100	**72**	**Total**

Source: Prepared by the researchers.

The table indicates that the predominant age group in the study sample is between 31 and 40 years, accounting for 40.27%. No employee in the sample is over 60 years old, suggesting that the surveyed banking institutions focus on a younger workforce. Regarding gender, males constitute 62.5% of the sample. In terms of educational qualifications, the majority hold a Bachelor's degree, representing 62.5%. Additionally, 42 individuals (or 58.33%) are in the executive category, 18 individuals (or 25%) are in the executive assistant category, and 12 individuals (or 16.66%) are in the controller category. The most common experience level is between 6 and 10 years, comprising 30.55% of the sample, followed by those with 5 years or less at 22.22%.

3 / Analysis of Results Related to the Study Dimensions

First Dimension: Information Security Data

Table (3): The Reality of Information Security in Banking Institutions According to the Study Sample

No	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Weighted Arithmetic Mean	Standard Deviation	Trend
		Frequency	Frequency	Frequency	Frequency	Frequency			
		percentage	percentage	percentage	percentage	percentage			
1/ Information Security Threats									
1	Information Security Threats Unsecured Internet Connection	30	25	10	4	3	***3.600***	***1.340***	Strongly Agree
		٪41.66	**٪34.72**	**٪13.88**	**٪5.55**	**٪4.16**			
2	Decreased Employee Efficiency	12	17	11	26	6	***3.080***	***1.226***	Disagree
		٪16.66	**23.61٪**	**٪15.27**	**٪36.11**	**8.33٪**			
3	Poor Operation and Maintenance	14	19	9	17	13	***3.140***	***1.399***	Agree
		٪19.44	**٪26.38**	**٪12.5**	**٪23.61**	**18.05٪**			

4	Connecting to External Networks with Other Information Centers	12	17	22	12	9	***3.240***	***1.187***	Neutral
		16.66	**23.61**	**30.55**	**٪16.66**	**٪12.5**			
2/ Forms of Potential Threats									
5	Hacking and stealing information systems	17	13	8	23	11	***3.060***	***1.476***	Disagree
		٪23.61	**18.05**	**11.11**	**٪31.94**	**٪15.27**			
6	Disrupting computer memory and slowing down its speed	14	26	9	13	10	***3.440***	***1.311***	Agree
		٪19.44	**٪36.11**	**٪12.5**	**18.05٪**	**٪13.88**			
7	Destroying data and deleting information	7	10	7	26	22	***2.100***	***1.199***	Disagree
		٪9.72	**٪13.88**	**٪9.72**	**٪36.11**	**30.55٪**			
8	Altering file locations	6	11	14	26	15	***2.360***	***1.102***	Disagree
		٪8.33	**٪15.27**	**19.44**	**36.11**	**٪20.83**			
3/ Using Modern Technology to Counter Information Security Threats									
9	Using antivirus software	17	18	11	13	13	***3.280***	***1.471***	Agree
		23.61	**25**	**15.27**	**18.05**	**18.05**			
10	Preventing unauthorized access by using strong passwords	40	20	0	6	6	***4.580***	***0.784***	Strongly Agree
		٪55.55	**٪27.77**	**0**	**٪8.33**	**٪8.33**			
11	Using biometric detectors (fingerprint, iris scan, voice recognition)	7	12	13	12	28	***2.180***	***1.350***	Strongly Disagree
		٪9.72	**٪16.66**	**٪18.05**	**16.66**	**38.88**			
12	Implementing an effective encryption system	21	31	9	6	5	***4.160***	***0.817***	Agree
		29.16	**43.05**	**12.5**	**٪8.33**	**٪6.94**			
4/ Barriers to Using Modern Technology to Counter Information Security Threats									
13	Lack of human resources necessary for implementing security measures	14	43	7	8	0	***4.080***	***0.600***	Agree
		٪19.44	**٪59.72**	**٪9.72**	**٪11.11**	**٪0**			
14	Rapid evolution of highly capable viruses that can penetrate information systems, steal, destroy, and alter data and files	16	23	12	9	12	***3.460***	***1.373***	Agree
		22.22	**٪31.94**	**16.66**	**12.5**	**16.66**			
15	Placing devices and control panels in exposed areas accessible to visitors	5	9	9	28	21	***2.000***	***1.010***	**Disagree**
		٪6.94	**٪12.5**	**٪12.5**	**٪38.88**	**٪29.16**			

16	Neglect by senior management in enforcing physical and technical security policies	8	19	14	17	14	***2.780***	***1.282***	Agree
		11.11	**26.38**	**19.44**	**23.61**	**19.44**			
5/ Ways to Enhance the Capabilities of Postal Centers to Counter Information Security Threats									
17	Using biometric and electronic detectors to verify user identity and system access authorization	21	29	7	9	6	***4.020***	***1.039***	Agree
		٪29.16	**40.27**	**9.72**	**12.5**	**8.33**			
18	Recruiting information security experts	21	31	7	8	5	***4.120***	***0.895***	Agree
		٪29.16	**٪43.05**	**9.72**	**٪11.11**	**٪6.94**			
19	Providing the necessary physical infrastructure to protect devices, software, and networks	26	31	8	0	6	***4.320***	***0.740***	Agree
		36.11٪	**٪43.05**	**11.11**	**0**	**8.33**			
20	Equipping banking institutions with advanced security system technologies	35	31	0	6	0	***4.460***	***0.613***	Strongly Agree
		48.61	**43.05**	**0**	**8.33**	**0**			

Source: Prepared by the Researchers

The table shows that the arithmetic means related to the Information Security axis and the statements concerning Information Security Threats were relatively high, reaching (3.600 and 3.140) for statements (1 and 3) respectively. This result indicates that the studied banking institutions attribute information security threats to unsecured internet connections and poor operation and maintenance.

Furthermore, statement 6, under the Forms of Potential Threats dimension, had an arithmetic mean of 3.440, indicating that the surveyed banking institutions consider computer memory disruption and slowdown as a potential threat.

Regarding the Use of Modern Technology to Counter Information Security Threats, the arithmetic means were notably high, reaching (3.280, 4.580, and 4.160), which shows that these institutions strive to protect their information systems. However, they do not keep up with modern technologies, as reflected in statement 11, which had a low arithmetic mean of 2.180, indicating that Algerian banking agencies do not use biometric detectors (fingerprint, iris scan, voice recognition) to secure their information systems.

On the other hand, opinions were somewhat divided regarding the Barriers to Using Modern Technology for Information Security. For instance, statement 13 had an arithmetic mean of 4.080 with a standard deviation of 0.600, while statement 15 had a lower arithmetic mean of 2.000, suggesting that the surveyed agencies suffer from a lack of human resources necessary to implement security measures.

Finally, the Ways to Develop Banking Institutions' Capabilities to Counter Information Security Threats showed significant arithmetic means, ranging between 4.020 and 4.460, indicating that these institutions are actively seeking development.

Second Axis: Aspects of Performance Improvement

Table (4): Aspects of Performance Improvement in Banking Institutions According to the Opinions of the Surveyed Sample

No.	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Weighted Arithmetic Mean	Standard Deviation	Trend
		Frequency	Frequency	Frequency	Frequency	Frequency			
		percentage	percentage	percentage	percentage	percentage			
1	Information security helps overcome work difficulties	26	27	7	6	6	***4.240***	***0.938***	***Agree***
		36.11	**37.5**	**9.72**	**8.33**	**8.33**			
2	Helps reduce work errors	29	24	6	8	5	***4.300***	***0.931***	***Strongly Agree***
		40.27	**33.33**	**8.33**	**11.11**	**6.94**			
3	Allows for improved customer relationships	29	25	8	10	0	***4.220***	***0.932***	***Strongly Agree***
		40.27	**34.72**	**11.11**	**13.88**	**0**			
4	Helps develop work methods	26	32	8	6	0	***4.340***	***0.658***	***Agree***
		36.11	**44.44**	**11.11**	**8.33**	**0**			
5	Ensures information confidentiality	35	28	9	0	0	***4.540***	***0.542***	***Strongly Agree***
		48.61	**38.88**	**12.5**	**0**	**0**			
6	Enables employees to acquire new knowledge by training them in information security procedures and identifying breaches	28	31	5	3	5	***4.060***	***1.095***	***Agree***
		38.88	**43.05**	**6.94**	**4.16**	**6.94**			

7	Provides opportunities for on-the-job training, leading to improved performance levels	24	39	9	0	0	***4.340***	***0.519***	***Agree***
		33.33	**54.16**	**12.5**	**0**	**0**			
8	Keeps pace with rapid changes in modern information and communication technologies	32	40	0	0	0	***4.420***	***0.498***	***Agree***
		44.44	**55.55**	**0**	**0**	**0**			
9	Reduces the cost of errors	27	36	9	0	0	***4.320***	***0.586***	***Agree***
		37.5	**50**	**12.5**	**0**	**0**			
10	Speeds up information access, enhancing work flexibility	34	21	8	9	0	***4.340***	***0.917***	***Strongly Agree***
		47.22	**29.16**	**11.11**	**12.5**	**0**			
11	Facilitates monitoring processes, improving performance levels	32	25	8	7	0	***4.420***	***0.702***	***Strongly Agree***
		44.44	**34.72**	**11.11**	**9.72**	**0**			
12	Enhances the quality of services provided	29	26	7	10	0	***4.300***	***0.863***	***Strongly Agree***
		40.27	**36.11**	**9.72**	**13.88**	**0**			

Source: Prepared by the Researchers

The table indicates that employees of the banking institutions surveyed agree that information security helps overcome work difficulties and develop work methods, as reflected in statements (1 and 4) with arithmetic means of (4.240 and 4.340), respectively.

Additionally, information security provides employees with new expertise, leading to improved performance levels, which is evident in statements (6 and 7) with high arithmetic means of (4.060 and 4.340), respectively.

Furthermore, statement 11 recorded a high arithmetic mean of 4.420, with a strongly agree tendency, highlighting that the information security programs adopted in banking institutions facilitate monitoring processes, thereby enhancing performance levels. This demonstrates one of the positive impacts of information security programs.

4 / Analysis of the Relationship Between Study Variables

Since this study examines the role of information security in enhancing the performance of human resources in banking institutions, it is essential to analyze the correlation between the study variables.

The results of the correlation analysis can be illustrated in the following table:

Table (5): The Relationship Between Information Security and Human Resource Performance Development

Information Security / Performance Development	Information Security Threats	Forms of Potential Threats	Using Modern Technology to Counter Information Security Threats	Barriers to Using Modern Technology to Counter Information Security Threats	Ways to Enhance the Capabilities of Postal Centers to Counter Information Security Threats
Pearson Correlation Coefficient	0.841	0.775	0.668	0.697	0.761

Source: Prepared by the Researchers

The table demonstrates a clear relationship and a high correlation coefficient between information security methods and human resource performance development programs, ranging between (0.668 and 0.841).

5 / Hypothesis Testing: Testing the First Hypothesis

Hypothesis 1:

❬ There is a statistically significant relationship between the prevailing information security in Algerian banking institutions and the level of human resource performance development.❭

Table (6): Results of Simple Regression Analysis to Test the Impact of Information Security Dimensions on Human Resource Performance Development in Banking Institutions

Source of Variance	B	Standard Error	Beta	Calculated T-Value	Significance Level (T)
Information Security Threats	0.307	0.165	0.439	1.864	0.069
Forms of Potential Threats	0.190	0.094	0.298	2.006	0.051
Using Modern Technology to Counter Information Security Threats	0.280	0.132	0.439	2.115	0.040
Barriers to Using Modern Technology to Counter Information Security Threats	0.467	0.134	0.299	3.494	0.001
Ways to Enhance the Capabilities of Postal Centers to Counter Information Security Threats	0.358	0.136	0.396	2.626	0.012

Source: Prepared by the Researchers

The statistical results presented in the table indicate that there is a statistically significant role at a significance level of α ≥ 0.05 for the independent variable (information security) in the dependent variable (human resource performance development). The calculated T-values were significant, reaching (1.864, 2.006, 2.115, 3.494, 2.626), which are greater than their critical table values at α ≥ 0.05, leading to the acceptance of the hypothesis.

Testing the Second Hypothesis

"There are statistically significant differences in the opinions of the study participants regarding information security and its relationship to human resource performance development in postal centers, based on their personal and occupational backgrounds."

To verify this hypothesis, a **One-Way ANOVA** test was conducted, and the summarized results are presented in the following table:

Table (7): One-Way ANOVA Analysis Results for Personal Variables Based on Study Sample Perceptions of the Relationship Between Information Security and Human Resource Performance Development

Variable	Source of Variance	Sum of Squares	Degrees of Freedom	Mean Squares	F-Value	Significance Level
Age	Between Groups	32.335	4	8.084	87.346	0.159
	Within Groups	4.165	45	0.93		
Gender	Between Groups	1.286	4	0.321	1.311	0.280
	Within Groups	11.034	45	0.245		
Educational Qualification	Between Groups	49.530	4	12.382	45.487	0.347
	Within Groups	12.250	45	0.272		
Years of Experience	Between Groups	87.729	4	21.932	36.537	0.259
	Within Groups	2.691	45	0.060		

Source: Prepared by the researchers

The results presented in the table, related to the one-way ANOVA analysis of the responses of the studied sample regarding the dimensions of information security management and their impact on the development of human resource performance in banking institutions according to personal and job-related variables, indicate the following:

- There are no statistically significant differences at a significance level of (0.05 ≥ α) in the study sample's responses regarding the dimensions of information security and their impact on performance development in banking institutions according to age. This is because the calculated significance level (0.159) is greater than the assumed significance level (0.05). This result indicates that the study sample agrees that the dimensions of information security affect performance development in banking institutions.
- There are no statistically significant differences at a significance level of (0.05 ≥ α) in the study sample's responses regarding the dimensions of information security and their impact on performance development in banking institutions according to gender (male, female). This is because the calculated significance level (0.280) is greater than the assumed significance level (0.05). This result indicates that the study sample agrees that the dimensions of information security affect performance development in banking institutions, regardless of gender, as both groups share the same perspective.
- There are no statistically significant differences at a significance level of (0.05 ≥ α) in the study sample's responses regarding the dimensions of information security and their impact on performance development in banking institutions according to educational qualification. This is because the calculated significance level (0.347) is greater than the assumed significance level (0.05). This result indicates that the study sample agrees that the dimensions of information security affect performance development in banking institutions, regardless of their educational level.
- There are no statistically significant differences at a significance level of (0.05 ≥ α) in the study sample's responses regarding the dimensions of information security and their impact on aspects of performance development in banking institutions according to years of experience. This is because the calculated significance level (0.259) is greater than the assumed significance level (0.05). This result indicates that the study sample shares a unified opinion on the role of information security in performance development, regardless of their years of experience.

CONCLUSION

Through the presented discussion, we attempted to address the topic based on the available information and data. The main conclusion we reached is that the subject is highly complex and requires further in-depth exploration. Therefore, we consider this study as a foundational step that can serve as a starting point for other related research, contributing to the enrichment of scientific inquiry in the field of information security and the development of human resource performance. Below, we present the key findings and recommendations derived from the study:

1. Study Findings

- After analyzing the data and drawing conclusions from the interviews conducted with employees of the banking institutions included in the study, the findings were as follows:
- Algerian banking institutions prioritize securing their networks physically by implementing various measures related to infrastructure and wiring.
- The most significant threats to information security in Algerian banking institutions include: (disrupting computer memory and slowing down performance, using viruses to corrupt data, and information theft).
- A major source of information security threats is the lack of certified engineers and IT specialists in banking institutions.
  - Employees of Algerian banking institutions are not adequately trained to handle security-related issues they may encounter.
  - There is a general lack of awareness among employees in Algerian banking agencies regarding information security threats.

2. Recommendations

Based on the study findings, the following recommendations were proposed:

- Separate internet-connected devices from main systems containing critical data such as (passwords, customer information, etc.).
- Utilize software that provides comprehensive reports on device activity and network communications, assigning periodic reviews to a supervisor at short intervals.
- Train employees on new applications before their deployment.
- Foster a culture of teamwork instead of concentrating all privileges and confidential files in the hands of a few individuals.
- Promote a culture of transparency among employees.
- Change passwords whenever an employee leaves the institution.
- Train employees on information security procedures and how to detect security breaches.

REFERENCES

Arabic References:

1. Al-Ghoneimi, Ashraf. Computer Hacker Protection Systems. Dar Al-Farouq Publishing and Distribution, Cairo, 1998.
2. Al-Asimi, Turki bin Ahmed. Protect Your Device: Security Risks and Ways to Prevent Them. Dar Al-Ma’arij, Riyadh, 1420H.
3. Al-Hamdan, Abdulrahman, & Al-Qasim, Mohammed bin Abdullah. Fundamentals of Information Security. Al-Humaidhi Printing Press, Riyadh, 2004.

4. Al-Humeed, Mohammed Debas, & Nino, Marco Ibrahim. Information Systems Protection. Dar Al-Hamed Publishing and Distribution, Amman, 2007.
5. Dodge, Louie. Networking for Beginners. Jadeer Library, Riyadh, 1998.
6. Taher, Dawood Hassan. Computers and Information Security. Institute of Public Administration, Riyadh, 2001.
7. Abbas, Tarek Mahmoud. The Digital Information Society. Al-Asil Center for Publishing and Distribution, Cairo, 2003.
8. Sportack, Mark, & Glenn, Walter. Teach Yourself the Basics of Networking. Arab Scientific Publishers, Beirut, 1998.

Foreign References:

1. Anderson, Christa & Minasi, Mark. Mastering Local Area Networks. San Francisco: SYBEX Network Press, 1999.
2. Grote, Patrik. Network+ Cheat Sheet. Indianapolis: Que Corporation, 2000.

ENDNOTES

[1] **Tariq Mahmoud Abbas**, *Digital Information Society*, Al-Aseel Center for Publishing and Distribution, Cairo, 2003, p. 150.

[2] **Dawood Hassan Taher**, *Computers and Information Security*, Institute of Public Administration, Riyadh, 2001, p. 52.

[3] **Al-Humaid Muhammad Dabbas, Nino Marco Ibrahim**, *Protection of Information Systems*, Dar Al-Hamed for Publishing and Distribution, Amman, 2007, p. 34.

[4] **Abdulrahman Al-Hamdan, Mohammed bin Abdullah Al-Qassim**, *Fundamentals of Information Security*, Al-Humaidi Printing Press, Riyadh, 2004, p. 35.

[5] **Abdulrahman Al-Hamdan, Mohammed bin Abdullah Al-Qassim**, *Previously Cited Reference*, p. 45.

[6] **Al-Humaid Muhammad Dabbas, Nino Marco Ibrahim**, *Previously Cited Reference*, p. 159.

[7] **Abdulrahman Al-Hamdan, Mohammed bin Abdullah Al-Qassim**, *Previously Cited Reference*, p. 46.

[8] **Al-Humaid Muhammad Dabbas, Nino Marco Ibrahim**, *Previously Cited Reference*, pp. 38/40.

[9] **Christa Anderson & Mark Minasi**, *Mastering Local Area Networks*, San Francisco: SYBEX Network Press, 1999, p. 565.

[10] **Patrik Grote**, *Network+ Cheat Sheet*, Indianapolis: Que Corporation, 2000, p. 175.

[11] **Turki bin Ahmed Al-Asimi**, *Protect Your Device: Security Risks and Protection Methods*, Dar Al-Ma'arij, Riyadh, 1420H, p. 236.

[12] **Dodge Louie**, *Networks for Beginners*, Jadir Library, Riyadh, 1998, p. 240.

[13] **Patrik Grote**, *op. cit.*, p. 202.

[14] **Mark Sportack, Walter Glenn**, *Teach Yourself the Basics of Networking*, Arab Scientific Publishers, Beirut, 1998, p. 320.

[15] **Mark Sportack, Walter Glenn**, *Previously Cited Reference*, p. 250.

[16] **Ashraf Al-Ghoneimi**, *Protection Systems from Computer Hackers*, Dar Al-Farouk for Publishing and Distribution, Cairo, 1998, p. 131.