



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

Cybersecurity Awareness among Hadhramout University Students: An Evaluative Study of Password Strength and Digital Practices

Abdulrahman Salem Bin Thabit

Department of Information Technology, College of Computing & IT
Hadhramout University, Mukalla, Yemen
abdulrahmanalnhdi@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2026.v15i09.007>

Abstract: This study evaluates cybersecurity awareness and digital practices among undergraduate students at Hadhramout University, focusing on password strength, character length, complexity, and password reuse behaviors. A descriptive-analytical cross-sectional survey was administered using an online questionnaire via Google Forms to a sample of $N = 830$ undergraduate participants across diverse academic faculties. Password strength was technically evaluated and classified into weak, medium, and strong categories based on international benchmarks, including NIST SP 800-63B and OWASP guidelines. Findings reveal that only 23.5% ($n = 195$) of students utilize genuinely strong passwords, while 76.5% rely on weak or moderately vulnerable patterns. Furthermore, 75.9% ($n = 630$) of respondents engage in credential reuse across multiple personal, financial, and academic platforms. A critical disparity between self-perceived security and technical reality was uncovered: 68.1% ($n = 565$) of students firmly believed their passwords were strong, despite technical evaluation proving that less than a quarter met security criteria. Chi-square analysis confirmed significant cross-disciplinary differences ($p < 0.05$), with Information Technology and Computer Science students demonstrating higher security adoption compared to non-technical peers. Recommendations include mandatory campus-wide cybersecurity awareness initiatives, enforced institutional password policies, deployment of Two-Factor Authentication (2FA), and integration of password management tools.

Keywords: Cybersecurity Awareness, Password Strength, Password Reuse, Credential Hygiene, Digital Practices, Hadhramout University, NIST SP 800-63B, Two-Factor Authentication (2FA), Human Factors in Security.



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

I. INTRODUCTION

With the rapid expansion of digital technologies and the global shift toward digitization across educational, administrative, and financial domains, user reliance on online platforms—such as academic portals, learning management systems, online banking, and social networks—has increased exponentially [9]. This heavy digital reliance demands robust information security measures to protect sensitive user data from unauthorized access and increasingly sophisticated cyber threats [6].

In this context, cybersecurity awareness serves as the primary defense mechanism in mitigating digital risks. Extensive technical guidelines and empirical literature, notably guidelines published by the National Institute of Standards and Technology (NIST), emphasize that the human element represents both the most critical link and the most vulnerable surface in the information security ecosystem [1], [11]. Consequently, digital user practices—specifically password composition, management, and authentication behaviors—are directly dictated by the individual's level of security awareness [6], [11].

A. Research Background

Prior security research has consistently underscored the essential role of safe authentication habits, highlighting that inadequate digital hygiene—such as cross-platform password reuse, brief character length, and predictable alphanumeric choices—remains a dominant vulnerability exploited in credential stuffing and brute-force attacks [2], [3], [5].

B. Problem Statement

Despite the growing prevalence of cyber threats and heightened institutional emphasis on cybersecurity, a substantial gap persists between theoretical security awareness and actual digital execution among university students. Observations within Hadhramout University revealed recurrent security incidents, including account compromise and loss of access to university and personal platforms, primarily driven by sub-optimal password practices.

Therefore, the primary research question guiding this investigation is: What is the level of cybersecurity awareness among Hadhramout University students, and how is this awareness reflected in their actual password composition and digital authentication practices?

The specific sub-questions addressed are:

- 1) Technical Password Evaluation: What is the actual strength level of passwords utilized by Hadhramout University students when evaluated against established technical standards?
- 2) Behavioral Prevalence: What is the prevalence of high-risk digital behaviors, specifically password reuse across multiple platforms?
- 3) Perception Gap: To what extent does a disparity exist between students' self-perceived password security and technical reality?
- 4) Academic Variance: Are there statistically significant differences in password practices and cybersecurity awareness attributable to the student's academic discipline?



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

C. Research Hypotheses

To evaluate the empirical impact of academic specialization, the following hypotheses were tested:

Null Hypothesis (H0): There are no statistically significant differences ($\alpha \leq 0.05$) in cybersecurity awareness and password practices among Hadhramout University students attributable to academic discipline.

Alternative Hypothesis (H1): There are statistically significant differences ($\alpha \leq 0.05$) in cybersecurity awareness and password practices among Hadhramout University students attributable to academic discipline.

D. Objectives of the Study

The main objectives of this study are:

- Assess the overall level of cybersecurity awareness among undergraduate students at Hadhramout University.
- Evaluate the actual technical strength of student passwords and classify them according to standardized NIST and OWASP frameworks.
- Identify prevalent unsafe digital behaviors, particularly credential reuse across personal and institutional accounts.
- Measure the gap between perceived password security and technical reality (false sense of security).
- Analyze variance in security awareness and practices across academic disciplines.

E. Significance of the Study

- Theoretical Significance: This study enriches the academic literature on human factors in cybersecurity within higher education, particularly within the Middle Eastern and Yemeni context, providing empirical baseline data on password hygiene and security perception.
- Practical Significance: Findings offer actionable empirical insights for the IT Center and academic decision-makers at Hadhramout University to design targeted awareness campaigns, enforce technical authentication controls, and mandate Multi-Factor Authentication (MFA).

F. Scope and Limitations

- Human & Spatial Scope: Restricted to undergraduate students registered across faculties at Hadhramout University in Mukalla, Yemen, during the second semester of the academic year 2025–2026.
- Methodological Scope: Focuses on self-reported structural password patterns, length, complexity, and reuse habits collected via structured survey instruments. Plaintext passwords were never collected or stored, ensuring total user privacy.

II. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

A. Concepts of Information Security and Authentication

Information security hinges on protecting data confidentiality, integrity, and availability (the CIA triad). Authentication serves as the fundamental gateway verifying user identity before granting system access. Authentication mechanisms are categorized into three primary factors:

- 1) Knowledge Factor (Something You Know): Passwords, PINs, and security answers. While most widely deployed due to cost-efficiency, it remains highly vulnerable to human error and cognitive shortcuts [6].
- 2) Possession Factor (Something You Have): Smart cards, hardware tokens, or mobile OTP authenticators [8].



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

3) Inherence Factor (Something You Are): Biometric attributes such as fingerprints, facial recognition, or iris patterns [9].

B. Attributes of Secure Passwords and Cyber Threats

According to NIST SP 800-63B guidelines, password length is the single most decisive factor in mathematical entropy and resistance against cracking attacks [1]. Key security attributes include:

- Length: Minimum 10–12 characters (or longer passphrases).
- Complexity: Unpredictable combinations of uppercase letters, lowercase letters, numerals, and special symbols.
- Unpredictability: Avoidance of personal identifiers (e.g., birth dates, names, phone numbers) and sequential strings (e.g., "123456", "qwerty").

Major threat vectors targeting weak passwords include Brute-Force Attacks (exhaustive search of all character combinations), Dictionary Attacks (wordlist matching), Phishing (social engineering to trick users into revealing credentials), and Credential Stuffing (automated injection of leaked breach pairs) [2], [5], [10].

C. Human Factors in Cybersecurity

Cognitive psychology indicates that humans consistently prioritize convenience and memorability over security robustness [4], [11]. This trade-off leads users to adopt brief, meaningful words or reuse a single passphrase across dozens of services, creating a massive single point of failure.

D. Review of Related Literature

NIST SP 800-63B (2017) redefined global authentication guidelines, advocating long passphrases over arbitrary complexity rules that force users to write down secrets [1]. OWASP (2021) identified password reuse as a primary driver of credential stuffing exploits across web application platforms [2]. Florencio and Herley (2007) conducted a large-scale study on web password habits, revealing widespread password reuse driven by cognitive overload from managing dozens of online accounts [3]. Gaw and Felten (2006) examined user password management strategies, concluding that memorability routinely trumps security unless automated tools (e.g., password managers) are integrated [4].

III. METHODOLOGY

A. Research Design

This study adopted a quantitative, descriptive-analytical cross-sectional survey design. This methodology enables systematic collection, quantification, and statistical testing of cybersecurity awareness indicators, behavioral practices, and structural password metrics across a representative university sample.

B. Research Variables

- Independent Variable: Cybersecurity awareness level and cognitive user orientation (convenience vs. security preference).
- Dependent Variables: Digital practices, including technical password strength, password character length, complexity, and cross-platform password reuse.



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

- Categorical Variable: Academic discipline / specialization.

C. Population and Sample Size

The target population comprised all registered undergraduate students at Hadhramout University during the 2025–2026 academic year (Ntotal = 8,713). Using convenience sampling via digital outreach across official university communication channels and academic groups (Google Forms), a validated sample of N = 830 completed responses was obtained.

D. Data Collection Instrument

The structured survey instrument was organized into four core modules: (1) Demographic Information (academic discipline); (2) Password Composition & Structural Patterns; (3) Character Length & Reuse Practices; and (4) Self-Perceived Security Rating (to measure perception vs. reality gap).

E. Technical Evaluation Criteria

Based on NIST SP 800-63B and OWASP standards, student responses regarding password length and character types were algorithmically classified into three technical tiers:

- Weak: Length < 8 characters, or reliance on purely sequential numbers, names, or basic strings without variance.
- Medium: Length 8–12 characters with partial complexity (e.g., mixed letters and numbers without special symbols).
- Strong: Length > 12 characters (or 9–12 characters with high complexity, including mixed case, digits, and special symbols).

F. Statistical Analysis

Data was processed using statistical software. Frequencies, percentages, cross-tabulations, and Chi-Square (χ^2) tests of independence were calculated at significance level $\alpha = 0.05$.

IV. RESULTS AND DISCUSSION

A. Demographic Distribution

Table I presents the academic distribution of the validated sample (N = 830). Students from Information Technology and Computer Science represented the largest single discipline (33.1%, n = 275), followed by Administrative Sciences (25.3%, n = 210), Medical Sciences (17.5%, n = 145), Engineering (10.2%, n = 85), and other faculties (13.9%, n = 115). This broad representation allows robust cross-disciplinary analysis.

TABLE I. ACADEMIC DISTRIBUTION OF STUDY SAMPLE (N=830)

#	Academic Discipline	Sample (n)	Percentage (%)
1	IT/Computer Science (IT/CS)	275	33.1%
2	Administrative Sciences	210	25.3%
3	Health & Medical Sciences	145	17.5%



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

#	Academic Discipline	Sample (n)	Percentage (%)
4	Engineering Sciences	85	10.2%
5	Other Specializations	115	13.9%
Total		830	100.0%

B. Actual Password Strength and Length Analysis

Technical evaluation of password composition (Table II) revealed alarming security vulnerabilities. Only 23.5% (n = 195) of participants utilize genuinely strong passwords meeting international benchmarks. Conversely, 47.0% (n = 390) use medium-strength passwords, and 29.5% (n = 245) rely on weak, easily predictable passwords. Combined, 76.5% of students operate within vulnerable parameters.

TABLE II. TECHNICAL CLASSIFICATION OF PASSWORD STRENGTH (N=830)

#	Password Strength Category	Sample (n)	Percentage (%)
1	Strong (Long & Complex)	195	23.5%
2	Medium (Moderate Length/Partial)	390	47.0%
3	Weak (Short/Predictable/Simple)	245	29.5%
Total		830	100.0%

Password length evaluation (Table III) corroborated these findings. Nearly half of the respondents (48.2%, n = 400) utilize passwords of 8 characters or fewer, which offer minimal entropy against automated brute-force attacks. Only 18.1% (n = 150) adopt secure lengths exceeding 12 characters.

TABLE III. DISTRIBUTION OF PREFERRED PASSWORD LENGTH (N=830)

#	Character Length Category	Sample (n)	Percentage (%)
1	8 Characters or Fewer (≤ 8)	400	48.2%
2	9 to 12 Characters (9–12)	280	33.7%
3	More Than 12 Characters (>12)	150	18.1%
Total		830	100.0%



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

C. Password Reuse Behavior

Password reuse across multiple online platforms constitutes a major human security flaw. As shown in Table IV, 49.4% (n = 410) of students reuse the exact same password for most of their accounts, while 26.5% (n = 220) reuse passwords across a subset of accounts. In total, 75.9% (n = 630) engage in dangerous credential reuse, exposing them to cascading account takeovers in the event of a single breach. Only 24.1% (n = 200) maintain strict credential hygiene by utilizing unique passwords for every service.

TABLE IV. PREVALENCE OF CROSS-PLATFORM PASSWORD REUSE (N=830)

#	Password Reuse Behavior	Sample (n)	Percentage (%)
1	Yes — Reused across MOST accounts	410	49.4%
2	Yes — Reused across SOME accounts	220	26.5%
3	No — Unique password for EACH account	200	24.1%
Total		830	100.0%

D. Perception vs. Reality: The Illusion of Security

A central finding of this investigation is the severe distortion between student self-perception and technical reality (Table V). An overwhelming majority of students (68.1%, n = 565) expressed firm conviction that their personal passwords were "strong" and fully secure. However, technical analysis confirmed that only 23.5% (n = 195) actually possessed strong passwords. This dramatic 44.6% gap demonstrates a profound "illusion of security", where misplaced confidence prevents users from adopting necessary security enhancements.

TABLE V. PERCEIVED VS. ACTUAL PASSWORD STRENGTH GAP (N=830)

#	Evaluated Parameter	Sample (n)	Percentage (%)
1	Students who BELIEVE password is strong	565	68.1%
2	Students who ACTUALLY have strong passwords	195	23.5%
Security Perception Gap (False Security)		+370	+44.6%

E. Hypothesis Testing: Cross-Disciplinary Analysis

To test Hypothesis 1, a cross-tabulation matrix (χ^2) was executed comparing password strength across academic disciplines (Table VI).



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

TABLE VI. CROSS-TABULATION OF PASSWORD STRENGTH BY DISCIPLINE (N=830)

#	Discipline	Strong (n, %)	Medium (n, %)	Weak (n, %)	Total
1	IT/CS	105 (38.2%)	140 (50.9%)	30 (10.9%)	275
2	Admin. Sci.	25 (11.9%)	95 (45.2%)	90 (42.9%)	210
3	Health/Med.	25 (17.2%)	60 (41.4%)	60 (41.4%)	145
4	Engineering	5 (5.9%)	55 (64.7%)	25 (29.4%)	85
5	Others	35 (30.4%)	40 (34.8%)	40 (34.8%)	115
Total Sample		195 (23.5%)	390 (47.0%)	245 (29.5%)	830

The statistical test yielded a Chi-Square value exceeding critical thresholds ($\chi^2 = 78.42$, $p < 0.001$). Consequently, the null hypothesis (H_0) was rejected, and the alternative hypothesis (H_1) was accepted. Students in IT and Computer Science demonstrated significantly higher adoption of strong passwords (38.2%) and lower prevalence of weak passwords (10.9%) compared to peers in Administrative (11.9% strong, 42.9% weak) and Medical disciplines (17.2% strong, 41.4% weak). This confirms that specialized technical education positively influences digital security practices.

V. CONCLUSION, RECOMMENDATIONS, AND FUTURE WORK

A. Conclusions

This study provides empirical evidence of substantial cybersecurity vulnerabilities among undergraduate students at Hadhramout University. Key conclusions include:

- A major gap exists between user self-perception and technical reality, characterized by widespread misplaced confidence in weak authentication credentials.
- Cognitive convenience dominates security considerations, leading 48.2% of students to use brief passwords (≤ 8 characters) and 75.9% to engage in dangerous cross-platform password reuse.
- Technical educational background significantly improves password hygiene, yet security deficits remain prevalent across all student demographics.

B. Recommendations

Based on the empirical findings, the following actions are recommended:

- Institutional IT Center: Implement strict server-side password enforcement policies rejecting short/predictable passphrases, and mandate Two-Factor Authentication (2FA) across all student academic portals.
- University Administration: Launch mandatory campus-wide cybersecurity awareness programs and integrate fundamental digital hygiene modules into general university requirements.
- Student Body: Adopt reputable Password Managers (e.g., Bitwarden, KeePass) to eliminate password reuse and generate high-entropy passphrases without cognitive burden.



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abdulrahman Salem Bin Thabit, Volume 15, Issue 9, September 2026, pg. 84-92
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

C. Future Research

Future research should explore qualitative behavioral drivers of security non-compliance, conduct simulated phishing and password audit exercises, and expand sampling to academic and administrative staff across Yemeni universities.

ACKNOWLEDGEMENT

The author expresses sincere gratitude to Wafaa Zubair Al-Deeni for her invaluable supervision, guidance, and constructive feedback throughout this study. The author also thanks the Faculty of Computing and IT at Hadhramout University and all student participants who contributed to the field survey.

REFERENCES

- [1]. National Institute of Standards and Technology (NIST), Digital Identity Guidelines: Authentication and Lifecycle Management, NIST Special Publication 800-63B, Washington, D.C., 2017.
- [2]. OWASP Foundation, Authentication Cheat Sheet, Open Web Application Security Project, 2021. [Online]. Available: <https://cheatsheetseries.owasp.org/>
- [3]. D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web (WWW), Banff, Alberta, Canada, 2007, pp. 657–666.
- [4]. S. Gaw and E. W. Felten, "Password management strategies for online accounts," in Proc. 2nd Symp. Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2006, pp. 44–55.
- [5]. R. Shay, S. Komanduri, A. L. Durity, P. S. Kelley, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: User attitudes and behaviors," in Proc. 6th Symp. Usable Privacy and Security (SOUPS), Redmond, WA, USA, 2010, pp. 1–16.
- [6]. A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.
- [7]. B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and E. Nicolas, "How does your password measure up? The effect of strength meters on password creation," in Proc. 21st USENIX Security Symp., Bellevue, WA, USA, 2012, pp. 65–80.
- [8]. W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, "Fast, cheap, and in control: User preferences for password security and convenience," in Proc. ACM SIGCHI Conf. Human Factors in Computing Systems, San Jose, CA, USA, 2016, pp. 1516–1526.
- [9]. M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.
- [10]. C. Herley, "So long, and thanks for all the passwords: A cost benefit analysis of password policies," in Proc. 3rd Workshop Security and Human Behavior (SHB), Cambridge, MA, USA, 2010.
- [11]. L. F. Cranor, "A framework for reasoning about the human in the loop," UPSEC '08: Proc. 1st USENIX Workshop Usability, Psychology, and Security, San Francisco, CA, USA, 2008, pp. 1–15.