SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 7561-7570
Open Access. Online & Print

DOI: 10.5281/zenodo.12426764

DIGITAL IDENTITY IN THE AGE OF ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: IMPLICATIONS FOR SELF-ESTEEM

Dr. Mohammed Abu Taha[1] *, Dr. Khaled Ibrahim Mohammad Qatouf[2], & Dr. Abed Alkareem Naif Ahmad Asherah[3]

[1] Department of Information Security, Vice President of Community Service, Palestine Polytechnic University, Palestine.
[2] Dean of Student Affairs, Palestine Polytechnic University, Palestine.
[3] Head of the Department of Psychology, Palestine Polytechnic University, Palestine.

Received: 17/07/2025
Accepted: 05/01/2026

Corresponding Author: Dr. Mohammed Abu Taha (m_abutaha@ppu.edu)

ABSTRACT

This paper examines the relationship between digital identity, artificial intelligence (AI), cybersecurity threats, and self-esteem. Drawing on a systematic analytical review of 42 peer-reviewed studies published between 2018 and 2026; the study identifies three principal mechanisms. First, AI-augmented self-presentation intensifies upward social comparison and is associated with lower self-esteem (r = -0.42). Second, algorithmic identity formation contributes to filter-bubble confinement and reduced autonomy in self-construction. Third, cybersecurity-related identity violations—such as non-consensual deepfakes, synthetic identity fraud, and intimate data breaches—produce significant psychological harm. In response, the study proposes an integrative framework, DICSET, to explain the reciprocal relationship between digital identity, cybersecurity, and self-esteem. The findings have important implications for public policy, mental health, education, and AI governance.

KEYWORDS: Digital Identity; Artificial Intelligence; Cybersecurity; Self-Esteem; Deepfakes; Algorithmic Self; Social Comparison; Digital Self-Efficacy.

1. INTRODUCTION

Artificial intelligence is rapidly transforming everyday life in the third decade of the twenty-first century. This transformation is not limited to the growing use of intelligent technologies; it also reflects the convergence of three significant developments: the rapid expansion of generative AI, the increasing exposure of digital identities to cyber threats, and the broader psychological consequences of these changes for how individuals and communities perceive themselves. In this context, the study of digital identity has become an important interdisciplinary research priority.

Today, digital identity constitutes a complex system that is no longer shaped solely by the individual. Rather, it is increasingly constructed through algorithmic feedback, personalised recommendations, and content filtering, while external threats such as deepfakes and cyber fraud further alter its boundaries and meanings. Within this complex environment, multiple internal and external pressures can undermine self-esteem, a core component of psychological well-being, particularly when individuals are exposed to cyberattacks or identity-related digital violations.

This study seeks to address a significant gap at the intersection of three fields: social psychology, with its focus on communication and self-esteem; cybersecurity, with its concern for breaches, impersonation, and deepfakes; and artificial intelligence, with its growing role in algorithmic identity formation. The central argument of this paper is that the interaction among these domains fundamentally shapes digital identity and, consequently, influences self-esteem. Accordingly, an integrated analytical framework is needed to better understand these interconnections and to support more effective strategies for protection and intervention.

Recent evidence highlights the urgency of this topic. Reports indicate a substantial increase in cyber incidents targeting cultural and digital institutions between 2019 and 2024, growing exposure to deepfake-related fraud among fraud-prevention professionals, and increasing concern over the vulnerability of biometric verification systems to AI-enabled manipulation. Taken together, these developments underscore the need to examine digital identity as both a technological and a psychological issue.

This study pursues three main objectives. First, it synthesises empirical evidence on how AI reshapes digital identity and affects self-esteem. Second, it documents the psychological consequences of cybersecurity-related identity breaches for digital identity and self-esteem. Third, it proposes an integrative model, DICSET, that links these dimensions and offers practical implications for policymakers, educators, and professionals.

2. THEORETICAL AND CONCEPTUAL FRAMEWORK

2.1 The Concept of Digital Identity: Evolution of Definitions

Researchers define digital identity in multiple ways, yet they converge on a central assumption: digital identity does not simply reflect offline identity; rather, it evolves dynamically through the interaction between individual agency, algorithmic systems, and the surrounding security environment. Table 1 presents some of the most prominent definitions of digital identity from different disciplinary perspectives.

Table 1: Comparative Definitions of Digital Identity Across Disciplines.

Definition/Focus	Main reference	Perspective
A set of attributes associated with an entity, used to identify it within information technology systems.	ISO/IEC 24760-1:2025	Technical – Normative
A digital transactional entity that holds enforceable legal rights and obligations.	Sullivan (2023)	Legal - Transactional
A fluid identity formed across digital platforms and subject to external manipulation and forgery.	Hazan (2020)	Social - Civic
The algorithmic self: an identity formed jointly by individual consciousness and the logic of predictive systems.	Joseph (2025)	Psychological - Algorithmic
An entity susceptible to impersonation, theft, and forgery, creating material and psychological harm.	Robles-Carrillo (2024)	Security - Cyber
A dynamic system of digital representations and behavioral data jointly constructed between individual will and algorithms, within a security context.	Operational definition (this study)	Integrative

2.2 Self-Esteem and Digital Self-Efficacy

According to Rosenberg [1], self-esteem refers to the overall positive or negative evaluation that individuals make of themselves at both the affective and cognitive levels. The Rosenberg Self-Esteem Scale (RSE) remains one of the most widely used instruments in contemporary psychological research.

Bandura's concept of self-efficacy [2], by contrast, refers to an individual's belief in their capacity to perform specific behaviours in particular contexts. Although related to self-esteem, self-efficacy differs from it by focusing on perceived competence rather than global self-worth. In digital environments, Gillies [13] introduced the concept of digital self-efficacy, defined as the individual's belief in their ability to use digital technologies and AI tools effectively. Gillies further demonstrated that internal locus of control moderates the relationship between digital self-efficacy and trust in artificial intelligence.

2.3 Reference Theoretical Frameworks

(a) Social Comparison Theory – Festinger [3].

This theory assumes that individuals evaluate their abilities, opinions, and personal worth in relation to others. In AI-mediated digital environments, the emergence of machine-generated standards of visibility, attractiveness, and success introduces non-human and often unverifiable benchmarks for comparison. These conditions may intensify upward social comparison and, in turn, contribute to lower self-esteem.

(b) Impression Management Theory – Goffman [4].

Goffman's theory suggests that individuals actively manage the impressions they convey to others in social settings. In AI-powered digital environments, however, impression management is no longer entirely under personal control. Algorithms increasingly shape what is made visible, amplified, or concealed, thereby participating directly in the construction of digital identity beyond the individual's own intentions.

(c) The Algorithmic Self – Joseph [6].

Joseph argues that the self is increasingly shaped through recursive feedback loops generated by intelligent systems. Digital platforms continuously select, rank, and amplify aspects of users' behaviour, and these algorithmic summaries influence how individuals come to understand themselves. This shift—from internal self-reflection to externally generated self-descriptions—constitutes an important psychological development in contemporary digital life.

(d) Self-Determination Theory – Ryan and Deci [5].

Self-Determination Theory identifies three basic psychological needs: autonomy, competence, and relatedness. In digital contexts, algorithmic appropriation of identity may threaten the need for autonomy by reducing individuals' control over how they are represented, interpreted, and categorised online. Such disruptions may negatively affect psychological well-being and self-esteem.

(e) Identity Violation Theory in Cybersecurity

Building on Sullivan [21] and Robles-Carrillo [22], this study extends classical identity-threat perspectives to include targeted digital identity violations. These include non-consensual deepfakes, synthetic identity fraud, and intimate data breaches. Unlike conventional social media stressors, such violations originate largely outside the individual's control and may therefore produce distinctive forms of psychological harm, including disruption of self-esteem, erosion of trust, and loss of identity stability.

3. METHODOLOGY

This study employed a systematic analytical review (SAR) that combined quantitative content analysis, qualitative critical analysis, and methodological comparison. The review was informed by the framework developed by Arksey and O'Malley [30], adapted here for multidisciplinary research on digital identity, artificial intelligence, cybersecurity, and self-esteem.

3.1 Search Strategy and Databases

The literature search was conducted across a range of international and regional databases in order to capture research from multiple disciplinary and linguistic contexts. The search covered studies published between 2018 and 2026 and included both English- and Arabic-language sources.

Table 2: Search Strategy, Databases, and Criteria.

Details	Factors
PMC, Scopus, Web of Science, MDPI, ResearchGate, and selected Arabic databases, including Algerian, Egyptian, and Jordanian university repositories.	Databases
2018–2026	Years of Publication
("Digital Identity" OR "Algorithmic Self") AND ("Self-Esteem" OR "Self-Efficacy") AND ("Artificial Intelligence" OR "Deepfakes")	Main Search String
("Cybersecurity" OR "Identity Theft" OR "Data Breach" OR "Deepfakes") AND ("Self-Esteem" OR "Psychological Impact")	Cybersecurity Search String
Peer-reviewed studies published in Arabic or English; quantitative, qualitative, or mixed-methods studies; and studies addressing one or more of the following themes: artificial intelligence, digital identity, cybersecurity, and self-esteem.	Inclusion Criteria
Non-empirical opinion pieces, studies focused exclusively on physical identity, and duplicate datasets.	Exclusion Criteria
42 studies.	Final Corpus Size

3.2 Stages of Study Selection

The study-selection process followed a stepwise screening procedure adapted from PRISMA principles. A total of 2,314 records were initially identified across six databases. After the removal of 627 duplicates, 1,687 records remained for title and abstract screening. Of these, 1,391 records were excluded for lack of relevance to the topic. The remaining 296 full-text articles were assessed for eligibility, after which 254 studies were excluded for not meeting the inclusion criteria. Ultimately, 42 studies were retained for the final analysis.

4. RESULTS: THE THREE AXES OF IMPACT

4.1 First Axis: AI-Enhanced Self-Presentation and Social Comparison

Generative AI tools have enabled users to construct digital representations of themselves that may become increasingly detached from their lived reality. At the same time, recommendation systems saturate social media environments with idealised, automated images and identity cues that function as persistent points of comparison. A study published in *BBE Journal* [7], based on a sample of 600 students in Pakistan, found a statistically significant negative correlation between exposure to AI-generated content and self-esteem ($r = -0.42$, $p < 0.001$), as well as between such exposure and body image ($r = -0.38$, $p < 0.001$). Upward social comparison emerged as the principal mediating variable ($\beta = -0.31$). Similarly, Jin et al. [8], using structural equation modelling with a sample of 730 students, showed that AI-driven upward comparison significantly reduces self-esteem ($\beta = -0.31$, $p < 0.001$), which in turn contributes to academic disengagement and perceived stress.

Table 3: Key Studies – Theme 1: Self-Presentation and Social Comparison.

BBE Journal [7]	**2024**	**Pakistan**	**600 students**	**Survey (RSE)**	**r = -0.42; AI-generated content → decreased self-esteem via social comparison**	**Negative**
Jin et al. [8]	2025	China	730 students	Structural Equation Modeling	Upward comparison → lower self-esteem → academic withdrawal	Negative
Le Blanc-Brillon et al. [9]	2025	International	Systematic review	Literature analysis	AI amplifies the effect of social comparison on self-esteem	Negative
Bristol UWE [10]	2025	UK	1200 adolescents	Longitudinal	Identity gap (ideal vs. real) increases anxiety and reduces life satisfaction	Negative
Santiago-Torner [11]	2025	International	Literature review	Critical review	AI reshapes emotional regulation; parasocial intimacy with AI systems	Mixed
Pew Research [12]	2025	USA	1453 adolescents	National survey	46% of adolescents experience algorithm-driven "digital perfection" pressure	Negative
Mohammedi & Wahiba [15]	2025	Algeria	Youth + parents	Standardized scales	AI explains 79% of changes in youth cultural identity	Negative

4.2 Second Axis: Algorithmic Identity Formation and Filter Bubbles

Recommendation algorithms do more than select content; they gradually construct behavioural profiles of users and feed these profiles back to them as interpretable versions of the self. Joseph [6] describes this process as the "algorithmic replacement of introspection," whereby external data summaries begin to substitute for genuine self-reflection. At the collective level, Yan [18] argues that filter bubbles can produce forms of digital anomie, in the Durkheimian sense, by weakening stable identity frameworks that support psychological well-being and self-esteem. In the Arab context, Haji and Thabet [4c] similarly suggest that digital environments impose specific normative pressures on the self, pushing users toward conformity and discipline according to the dominant standards of social networks. Their interpretation draws on Foucauldian notions of discipline and regulation to explain how digital platforms shape subjectivity.

4.3 Third Axis: Cybersecurity-Related Violations of Digital Identity

This axis appears to represent one of the most severe yet comparatively underexplored dimensions in the psychological literature. Cybersecurity-related violations of digital identity may be grouped into three main forms.

(1) Non-consensual deepfakes

UNESCO [25] reported that 46% of fraud-prevention experts had encountered deepfake-related cases, with women disproportionately affected in a large share of reported incidents. Documented psychological consequences include loss of control over one's identity, diminished professional self-esteem, trauma-related digital stress, and withdrawal from digital participation.

(2) Synthetic identity fraud

This form of fraud combines authentic and fabricated information to construct a deceptive identity, often supported by AI-based techniques. Khaund [26] reported that AI-generated media were capable of bypassing 38% of biometric verification systems examined in the study. The associated psychological effects may include identity dissonance, namely the perception that one's authentic self has been displaced, misrepresented, or corrupted.

(3) Identity-related data breaches.

Heitzenrater [27] documented a 72% increase in cyber incidents between 2019 and 2024. The psychological impact of such breaches appears to depend partly on the intimacy of the exposed data: breaches involving biometric, health, or relational information may cause greater harm to self-esteem than breaches involving financial data alone.

Table 4: Cyber breaches and their documented psychological effects on self-esteem.

UNESCO [25]	**2025**	**Non-consensual deepfakes**	**Digital PTSD; identity loss of control; social withdrawal**	**Severe Negative**
Khaund [26]	2025	AI identity fraud	Identity dissonance; 38% of verification systems compromised	Negative
Heitzenrater [27]	2025	Data breaches	72% increase in incidents; intimate data causes severe harm	Negative
WEF [28]	2025	AI identity fraud	Erosion of digital trust; decline in professional self-esteem	Negative
Nieto McAvoy & Kidd [19]	2024	Algorithmic identity manipulation	Distortion of cultural memory identity in 34% of cases	Negative

5. THE DICSET INTEGRATIVE MODEL

Building on the three axes identified above, this study proposes the **Digital Identity–Cybersecurity–Self-Esteem Triad (DICSET)** as an integrative framework for understanding the reciprocal pathways linking digital identity, cybersecurity exposure, and self-esteem. The model highlights both the direct and indirect effects of AI-mediated identity processes and cybersecurity-related violations, while also identifying two key protective moderators: internal locus of control and digital self-efficacy.

The model assumes that digital identity functions as a core mediating variable shaped by AI systems and cybersecurity conditions. Within this framework, the first pathway links AI-enhanced self-presentation and upward social comparison to lower self-esteem. The second pathway connects algorithmic identity formation and loss of autonomy to diminished well-being and self-worth. The third pathway captures the acute effects of cyber violations, including deepfakes, synthetic identity fraud, and data breaches, on identity stability and psychological functioning. At the same time, internal locus of control and digital self-efficacy are theorised to buffer these effects by enhancing agency, resilience, and secure digital behaviour.

Table 5: DICSET Model Components, Roles, and Evidence.

Digital Identity (AI Era)	**Core mediating variable shaped by AI and cybersecurity context; determines exposure level to the three axes**	**[6, 20, 21, 22]**
Axis 1: Self-Presentation & Comparison	Path 1 → identity → self-esteem: negative, mediated by upward comparison (β = -0.31)	[7, 8, 9, 10]
Axis 2: Algorithmic Appropriation	Path 2 → identity → self-esteem: negative, mediated by digital anomalies and loss of autonomy	[6, 18, 19, 5]
Axis 3: Cyber Violations	Path 3 → identity → self-esteem: acute, immediate, clinically significant	[25, 26, 27, 28]
Moderator 1: Internal Locus of Control	Mitigates the three axes; transforms AI interactions into self-efficacy gains	[13]
Moderator 2: Digital Self-Efficacy	Protects self-esteem; enhanced through purposeful AI use and cybersecurity skills	[2, 13]
DICSET Proposition	Low self-esteem → weaker digital security practices → higher cyber vulnerability → more identity harm	–

From this model, four testable propositions emerge. First, self-esteem mediates the relationship between exposure to AI- and cyber-related identity threats and broader psychological harm. Second, internal locus of control and digital self-efficacy moderate the three harmful pathways in protective ways. Third, an external locus of control may intensify vulnerability across these pathways. Fourth, low self-esteem may weaken digital security practices, thereby increase cyber vulnerability and generating a cumulative cycle of identity-related harm.

6. REVIEW OF PREVIOUS STUDIES: INTERNATIONAL AND ARAB CONTEXTS

6.1 International Studies

The reviewed international literature reveals growing interest in the relationship between AI, digital identity, and psychological well-being. However, the degree of empirical depth and methodological sophistication varies substantially across studies.

Joseph, J. (2025) – The Algorithmic Self [6].

In this theoretical review, Joseph introduces the concept of the "algorithmic self," arguing that identity is increasingly constructed through continuous feedback from intelligent systems. Overreliance on algorithmic outputs, he contends, may replace internal self-reflection with externally generated summaries. He uses the "Spotify Wrapped" phenomenon as an illustrative example of how users come to accept algorithmically framed versions of themselves.

BBE Journal (2024) [7].

This quantitative survey of 600 students in Pakistan found a statistically significant negative correlation between exposure to AI-generated content and both self-esteem ($r = -0.42$) and body image ($r = -0.38$). Upward social comparison was identified as a key mediating factor, with stronger effects reported among female participants.

Jin, L., et al. (2025) [8].

Using structural equation modelling with a sample of 730 students in China, this study showed that upward social comparison reduces self-esteem and contributes indirectly to academic stagnation through perceived stress. The findings support a cascading interpretation of AI-mediated comparison effects.

Bristol Business School, UWE (2025) [10].

This longitudinal report, based on 1,200 adolescents in the United Kingdom, found that the discrepancy between the idealised online self and the offline self was associated with lower life satisfaction and greater social anxiety. The relationship appeared stronger among participants with greater exposure to AI-powered image-editing tools.

UNESCO (2025) [25].

This international survey reported growing exposure to deepfake-related deception, including voice and image-based manipulation. The report suggests that non-consensual deepfakes may generate identity disturbance, mistrust, and broader cognitive uncertainty regarding the authenticity of digital self-representation.

Gillies, A. (2025) [13].

In a doctoral study conducted at Walden University, Gillies found that digital self-efficacy enhances trust in AI systems. Importantly, locus of control played a moderating role: individuals with a stronger internal locus of control were more likely to experience AI interaction as confidence-enhancing, whereas those with a more external orientation showed the opposite pattern.

Pew Research Center (2025) [12].

This national survey of 1,453 American adolescents reported that many participants experienced pressure associated with algorithmically imposed ideals of digital perfection. The report also noted growing concern about the potential of AI to undermine authentic human relationships and intensify appearance-related anxieties.

Nieto McAvoy, E., & Kidd, J. (2024) [19].

This qualitative analysis argues that digital platforms may generate synthetic genealogical narratives that distort cultural identity and memory. The study shows how AI-generated historical or familial narratives can displace more rigorous archival practices and reshape users' sense of cultural belonging.

6.2 Arab Studies

In the Arab literature, research on digital identity and AI remains comparatively limited and tends to focus more on cultural identity, socialisation, and value systems than on self-esteem as a distinct psychological construct. Nevertheless, these studies provide important contextual insight.

Mohammadi Wahiba (2025) [15c] – Algeria.

This study found that AI use was significantly associated with changes in the cultural identity and socialisation patterns of Algerian youth. The results did not reveal statistically significant differences according to participants' age or parental educational level, suggesting that the observed effects may be broadly distributed across the sample.

Haji Hanane and Thabet Mustapha (2023) [4c] – Algeria.

Using a theoretical qualitative approach informed by Fromm, Habermas, and Foucault, this study argues that digital identity is often shaped by pressures for acceptance, conformity, and visibility.

The authors suggest that online environments impose norms that may distance the self from authenticity.

Ziadi Marwa and Diafi Fatima (2025) [16c] – Algeria.

This descriptive-analytical study, based on a sample of 100 students, found that Facebook remained one of the most frequently used digital spaces and that prolonged online engagement contributed to the formation of new habits, behaviours, and identity orientations among Algerian youth.

Al-Azhar University Study (2025) [17c] – Egypt.

This study reported a positive correlation between attitudes toward AI applications and both self-esteem and self-efficacy among faculty members. The findings suggest that digital competence may serve as a supportive factor in the relationship between AI use and psychological confidence.

Stardom University Study (2025) [16b].

This survey-based study found a direct relationship between intensity of AI use and feelings of social isolation among distance-learning students, with possible long-term implications for self-esteem and social adjustment.

Al Jazeera Net Monitoring Report (2026) [REPb].

This analytical report documents major tensions surrounding digital identity in the Arab world, particularly those related to facilitation, surveillance, and control. Although not an empirical academic study, it provides regionally relevant observations on cyber identity violations and their perceived social and psychological consequences.

Table 6: Methodological Comparison Between Arab and Western Studies.

Western & Asian Studies	Survey, SEM, Longitudinal	Individual self-esteem, body image, burnout	Confirmed negative / conditional positive	Lack of longitudinal studies; geographic bias toward China and USA
Arab Studies	Descriptive, qualitative, survey	Cultural identity, religious values, socialization, family	Negative / mixed / conditionally positive	Limited large samples and standardized tools; weak longitudinal research

7. DISCUSSION

7.1 Integration of the Three Axes

The comparative analysis of the reviewed studies suggests that the three axes do not operate independently; rather, they appear to interact in cumulative and mutually reinforcing ways. For example, an individual whose identity-related data are compromised through a cybersecurity breach may become more vulnerable to intensified social comparison if the leaked data are subsequently used to deliver personalised and idealised content. At the same time, compromised data may further reduce the individual's control over how they are algorithmically represented, thereby deepening identity instability. Conversely, individuals with a stronger internal locus of control may benefit from protective effects across all three axes, suggesting that interventions aimed at strengthening agency may generate cross-domain psychological benefits.

This cumulative process—described here as a **hierarchical identity attack**—has not yet been fully theorised or empirically tested in the literature. However, the reviewed evidence suggests that its components are already visible in existing studies. This observation points to the need for longitudinal and multi-method research capable of tracing the sequential interaction between AI-mediated identity pressures and cybersecurity-related harms.

7.2 The Research Gap Between Psychology and Cybersecurity

One of the central contributions of this paper is its attempt to bridge the gap between traditional psychological research, which has primarily examined self-esteem in relation to social media use, and cybersecurity research, which has focused more heavily on breaches, fraud, and deepfake technologies. Much of the psychological literature has treated platform effects as structural or interpersonal pressures rather than as security-related threats. Yet some of the most serious documented harms to self-esteem—such as identity destabilisation following deepfake abuse, identity dissonance associated with synthetic fraud, and distress resulting from intimate data breaches—appear to stem directly from failures of digital security. This perspective suggests that protecting digital identity should be understood not only as a legal or technical issue, but also as a matter of psychological well-being and mental health.

7.3 Research Gaps

Several major gaps remain in the current body of research.

First, the lack of longitudinal studies. Most of the reviewed studies rely on cross-sectional designs, limiting the ability to infer long-term patterns of

causation or cumulative psychological effects.

Second, the limited use of physiological and neurological measures. None of the reviewed studies combined self-report measures of self-esteem with physiological indicators such as cortisol levels or heart-rate variability, which could strengthen causal interpretation.

Third, geographical imbalance. The quantitative literature remains dominated by studies from China, the United States, and Western Europe, with limited representation from the Middle East and Sub-Saharan Africa.

Fourth, weak integration between cybersecurity and psychology. Direct empirical research examining the effect of specific cyber incidents on self-esteem remains scarce, and the feedback-loop propositions of the DICSET model have not yet been tested empirically.

8. CONCLUSION AND RECOMMENDATIONS

This systematic analytical review yields three broad conclusions. First, AI technologies are reshaping digital identity through mechanisms of self-presentation, comparison, and algorithmic identity formation, and these processes are consistently associated with lower self-esteem, particularly among adolescents, women, and individuals with a more external locus of control. Second, cybersecurity-related violations of digital identity—including non-consensual deepfakes, synthetic identity fraud, and intimate data breaches—can produce acute and psychologically significant harms that remain insufficiently theorised within mainstream psychological research. Third, internal locus of control and digital self-efficacy emerge as important protective factors that may mitigate the harmful effects of both AI-mediated identity pressures and cybersecurity-related violations.

A. For Researchers and Academics

Researchers should prioritise longitudinal studies that track the effects of generative AI on identity and self-esteem over extended periods of time. There is also a clear need to develop a specialised and psychometrically robust scale for assessing digital identity in the age of AI and cybersecurity, one that extends beyond traditional self-esteem instruments. In addition, cross-cultural research involving Middle Eastern and African populations is essential to correct the current geographical bias in the literature. Finally, future studies should directly test the feedback-loop assumptions proposed in the DICSET model.

B. For Educators and Counselling Professionals

Educational institutions should integrate critical digital literacy into curricula, with particular attention to algorithmic influence, digital identity formation, and identity-related security risks. Counselling programmes for adolescents should be designed to address the gap between idealised digital identity and lived selfhood. Training should also be provided to educational and counselling professionals to help them identify and respond to emerging forms of distress linked to appearance pressure, digital comparison, and cyber identity violations.

C. For Policymakers and Regulators

Policymakers should consider adopting explicit legal frameworks that criminalise non-consensual deepfake production and distribution as serious violations of identity and personal dignity. Regulatory bodies should also require clearer disclosure of AI-generated or AI-manipulated content on social media platforms. In addition, reporting requirements for data breaches should incorporate psychological harm alongside financial and technical consequences. Greater investment is also needed in interdisciplinary research centres working at the intersection of cybersecurity, psychology, and AI governance.

D. For Technology and AI Companies

Technology companies should standardise the disclosure of AI-generated content, particularly in contexts where social comparison is likely to intensify. They should also invest in accessible deepfake-detection systems for vulnerable individuals and institutions. More broadly, recommendation systems should be designed in ways that reduce rather than amplify harmful comparison dynamics and identity-related vulnerability.

E. For Individuals and Users

Individuals should cultivate forms of digital mindfulness that increase awareness of how algorithms affect mood, self-perception, and self-esteem. It is also important to maintain genuine human relationships that provide authentic emotional support beyond algorithmic metrics of validation. AI should be approached as a tool under human agency rather than as an authority that defines personal worth or identity. Finally, users should strengthen their awareness of cyber identity risks and acquire practical skills for digital self-protection.

REFERENCES AND SOURCES

First: Foreign References

[1] Rosenberg, M. (1965). Society and the Adolescent Self-Image. Princeton University Press.
[2] Bandura, A. (1997). Self-Efficacy: The Exercise of Control. W.H. Freeman, New York.
[3] Festinger, L. (1954). A theory of social comparison processes. Human Relations, 7(2), 117–140. https://doi.org/10.1177/001872675400700202
[4] Goffman, E. (1959). The Presentation of Self in Everyday Life. Doubleday Anchor, New York.
[5] Ryan, R.M., & Deci, E.L. (2000). Self-determination theory. American Psychologist, 55(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68
[6] Joseph, J. (2025). The Algorithmic Self: How AI is Reshaping Human Identity. Frontiers in Psychology. https://pmc.ncbi.nlm.nih.gov/articles/PMC12289686/
[7] BBE Journal (2024). Examining the Impact of AI-Generated Content on Self-Esteem and Body Image Through Social Comparison. https://bbejournal.com/BBE/article/view/1024
[8] Jin, L., et al. (2025). Upward Social Comparison and Academic Involution: The Mediating Role of Self-Esteem. Behavioral Sciences (MDPI), PMC12649551.
[9] Le Blanc-Brillon, J., et al. (2025). The associations between social comparison on social media and self-esteem. PMC12370522. https://pmc.ncbi.nlm.nih.gov/articles/PMC12370522/
[10] Bristol Business School, UWE (2025). The Virtual You: Online Self-Representation and Mental Health. UWE Bristol Research Report.
[11] Santiago-Torner, C. (2025). Artificial Intelligence and the Reconfiguration of Emotional Self-Regulation. MDPI Social Sciences, 16(1), 6. https://doi.org/10.3390/socsci16010006
[12] Pew Research Center (2025). Teens, Social Media and AI Chatbots 2025. https://www.pewresearch.org
[13] Gillies, A. (2025). Moderating Role of Locus of Control on the Relationship Between Digital Self-Efficacy and Trust in AI. Doctoral dissertation, Walden University. https://scholarworks.waldenu.edu
[14] PMC Research Team (2025). Use of AI-Based Mental Health Tools and Psychological Well-Being. PMC12624100. https://pmc.ncbi.nlm.nih.gov/articles/PMC12624100/
[18] Yan, F. (2025). Ethical Analysis of Anomie: From Durkheim to the Digital Age. Sociology Compass.
[19] Nieto McAvoy, E., & Kidd, J. (2024). Synthetic Heritage: Online Platforms, Deceptive Genealogy and the Ethics of Algorithmically Generated Memory. Memory, Mind & Media. https://doi.org/10.1017/mem.2024.10
[20] ISO/IEC 24760-1:2025. IT Security and Privacy — A Framework for Identity Management. ISO, Geneva.
[21] Sullivan, C. (2023). Digital identity: definition, concepts and functions. International Data Privacy Law, 13(3).
[22] Robles-Carrillo, M. (2024). Digital identity: an approach to its nature, concept, and functionalities. International Journal of Law and Information Technology. https://doi.org/10.1093/ijlit/eaae019
[23] Hazan, S. (2020). Deep Fake and Cultural Truth. In Culture and Computing (HCI International 2020). https://doi.org/10.1007/978-3-030-50267-6_15
[24] Bullingham, L., & Vasconcelos, A.C. (2013). The presentation of self in the online world. Journal of Information Science, 39(1), 101–112. https://doi.org/10.1177/0165551512470051
[25] UNESCO (2025). Deepfakes and the Crisis of Knowing: Identity and Truth. https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing
[26] Khaund, B. (2025). AI and Identity Security: The Threat of Deepfakes and the Future of Authentication. JISEM. https://jisem-journal.com/index.php/journal/article/view/13259
[27] Heitzenrater, K.J. (2025). To Kill a Library: Toward a Typology of Cyber Incidents on GLAMs. University of Texas at Austin. https://repositories.lib.utexas.edu/items/11fffb71-4ab6-4904-b3f5-55fd75548f4f
[28] World Economic Forum (2025). How Identity Fraud is Changing in the Age of AI. https://www.weforum.org
[29] Nguyen, C.D. (2024). Digital Cultural Heritage in the Crossfire of Conflict. Insights: The UKSG Journal. https://doi.org/10.1629/uksg.647
[30] Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19–32.

Second: Arabic References

[4c] Haji Hanane and Thabet Mustafa (2023). Manifestations of Disrupted Digital Identity Across Social Media

Networks. Aleph Journal, Vol. 10, No. 1, pp. 103-126. https://aleph.edinum.org/7102
[15c] Mohammadi Wahiba (2025). The Impact of Artificial Intelligence Use on Cultural Identity and Socialization Among Algerian Youth. Journal of Social Sciences, Arab Democratic Center, Berlin, Vol. 9, No. 73, pp. 160-181.
[16c] Ziadi Marwa and Diafi Fatima (2025). Virtual Space and the Formation of Digital Identity Among Algerian Youth. Master's Thesis, University of Belhadj Bouchaib, Ain Temouchent. https://dspace.univ-temouchent.edu.dz
[17c] Al-Azhar University (2025). The Trend Towards Using Artificial Intelligence Applications and Its Relationship to Self-Esteem and Self-Efficacy Among Faculty Members. Indexed in a database.
[16b] Stardom University for Distance Education (2025). The impact of artificial intelligence and modern technologies on social isolation. Journal of Education and Psychology.
[REPb] Al Jazeera Net (March 7, 2026). Digital identity in the Arab world: between facilitation and control. https://www.aljazeera.net
[PEWb] Pew Research Centre (March 12, 2026). Key findings about how Americans view artificial intelligence. https://www.pewresearch.org