International Journal of Business and Economics Research
2026, Vol. 15, No. 4, pp. 89–95
https://doi.org/10.11648/j.ijber.20261504.12

Review Article

The Cost of Visibility: Facebook Engagement Behaviours, Data Breaches, and Student Influencer Livelihoods in Kenya

Yussuf Motari Okari[1, *], Robert Nyamao Nyabwanga[2], Eliza Buyeke Ogucha[3]

[1]Department of Business Administration, Kisii University, Nairobi, Kenya
[2]Department of Mathematics and Actuarial Science, Kisii University, Nairobi, Kenya
[3]Department of Tourism and Hospitality, Kisii University, Nairobi, Kenya

Abstract

University students are becoming active participants in the gig economy. They frequently utilize social media networks such as Facebook to obtain advertising revenue or brand sponsorships, thereby monetizing their accounts to generate additional income for survival on campus. The intensive engagement on these digital platforms exposes them to data breaches that can potentially collapse their online businesses. However, the relationship between online visibility and digital vulnerability remains ambiguous. To address this critical knowledge gap, this study examined the nexus of Facebook engagement behaviors, data breaches, and student influencer livelihoods in Kenya. Specifically, the investigation explored engagement intensity and breach frequency, the predictive power of behavioral risk factors, gender-based disparities in digital reach and risk, student risk-engagement profiles, and the ultimate livelihood impact of security breaches among student influencers. Anchored on Resource Dependence Theory (RDT), the study adopted a mixed-methods design, collecting data from 440 observations across 100 Facebook influencer pages alongside testimonials from five student influencers. Data was analyzed using quantitative and qualitative techniques. Findings revealed that Facebook engagement behaviors directly influence data breaches, averaging 1.57 breaches per week, with individuals in the high-engagement stratum experiencing seven times the breach frequency of their low-engagement counterparts. T-test analysis found no statistically significant gender differences in risk ($p = .5313$), suggesting that the economic necessity to scale reach overrides demographic disparities in risk-taking. Furthermore, logistic regression identified suspicious link clicks (x_{10}) as the dominant predictor, where each interaction increases breach odds by 11.7 times, explaining 56% of the variance in digital security outcomes ($R^2 = .5595$). Qualitative evidence suggests association between data breaches and the survival of online businesses, which severely disrupts student livelihoods. The study recommends policies that support Business Account Recovery, digital livelihood insurance, and tiered security for high-reach creators. Theoretically, it suggests extending RDT by incorporating demographic parity.

Keywords

Student Livelihood, Resource Dependence Theory, Cost of Visibility, Cybersecurity, Digital Livelihood

*Correspondence: Yussuf Motari Okari (ymotari@kisiiuniversity.ac.ke)

Received: 17 May 2026; **Accepted:** 28 May 2026; **Published:** 27 July 2026

1. Background to the Study

The transition from personal social networking to a commercialized influencer economy has fundamentally redefined digital engagement, moving from the community-focused Social 2.0 to an algorithm-driven Social 3.0 era [2]. Rather than using platforms solely for interaction, student influencers now utilize them as commercial spaces where visibility translates directly into digital livelihoods [5, 6, 14]. In the Kenyan context, this shift is pronounced: top-tier influencers earn millions of shillings annually, with the national creator economy estimated to exceed Ksh 1.07 billion as of 2025. This growth is supported by strategic frameworks like the National Information Communications and Technology (ICT) Policy of 2020, which positions the digital economy as a primary driver for youth employment.

However, this heightened participation exposes student influencers to a "paradox of connectivity." To sustain income, they depend on high performance metrics—engagement rate, click-through rate, and follower growth—which necessitate prolonged online presence and frequent interactions with unknown users. These same strategies amplify their digital vulnerability. Empirical evidence suggests that users with high levels of interaction are significantly more susceptible to social engineering, phishing, and malicious links [1, 9, 15]. The scale of this threat is evident in recent data from the National KE-CIRT/CC, which detected 2.5 billion cyber threat events in Q1 2025 alone—a 201% increase from the previous quarter.

Adopting a cross-sectional research design, this study examines the relationship between Facebook engagement behavior, data breaches and student's livelihoods in Kenya. Grounded in Resource Dependence Theory [10], the analysis explores how financial reliance on digital platforms incentivizes students to maximize reach at the expense of privacy. This trade-off creates a critical tension: the pursuit of visibility often leads to security breaches that ultimately disrupt the very digital income streams the students seek to protect.

2. Research Objectives

This study investigates Facebook engagement behavior, data breaches and student's livelihoods in Kenya. Specifically, the study seeks:

1) To evaluate the relationship between engagement intensity and breach frequency among student Facebook influencers.
2) To analyze the predictive power of behavioral risk factors among student Facebook influencers.
3) To investigate gender-based disparities in digital reach and risk among student Facebook influencers.
4) To classify student influencers based on risk-engagement profiles.
5) To analyze the livelihood impact of security breaches among student Facebook influencers.

3. Conceptual and Theoretical Foundation

3.1. The Resource Dependence Theory

This study is theoretically grounded in Resource Dependence Theory (RDT). The theory posits that the survival of any entity is contingent upon its ability to acquire and maintain critical external resources [8]. In the digital economy, student influencers are defined by an asymmetric interdependence: they rely entirely on Facebook's proprietary algorithms and audience reach for economic survival, yet they lack any control over these "vital resources.

This systemic dependence directly shapes online behavior, forcing influencers into a power imbalance where visibility takes precedence over security to sustain "resource flow." Driven to satisfy algorithmic demands for engagement, student creators face strategic compulsion to interact with unfamiliar accounts and public interfaces—an operational necessity that drastically expands their digital attack surface. This behavioral pattern mirrors documented evidence regarding digital entrepreneurs who frequently compromise security protocols to maintain uninterrupted market presence [1]. Within the Kenyan ecosystem, chronic resource scarcity systematically pushes students toward these high-risk, high-reward digital ventures [10]. Ultimately, Resource Dependence Theory (RDT) contextualizes these actions, demonstrating that student influencers accept heightened cybersecurity risks as a rational economic trade-off to secure vital resources required for self-support.

3.2. Facebook Engagement behavior, Data Breaches and Student Influencer Livelihood

Facebook engagement—comprising reach, audience growth, and click-through rates—functions as the fundamental currency of the influencer economy [5, 12]. For student influencers, these metrics are not merely social indicators but critical drivers of their digital livelihoods. In the Kenyan context, this income often serves as a vital financial pillar, supplementing or replacing traditional funding like parental support or HELB loans [4]. As digital platforms evolve into economic ecosystems, the ability to convert "likes" and "shares" into tangible support for educational and living expenses has turned social media into a primary workplace for youth [9, 11].

However, this economic opportunity is tethered to significant digital risk [7]. Data breaches—defined as the unauthorized compromise of an account's integrity—become more probable as engagement intensity increases. High interaction frequency enhances "target attractiveness," making influencers lucrative marks for phishing and social engineering [3, 13]. This is particularly acute in Kenya, where cyber threats have surged due to systemic vulnerabilities [7, 17]. The pressure to

remain "always on" to maintain visibility creates a state of structured invisibility [6], where the drive for engagement forces students to lower their defensive guards, such as clicking suspicious links in the pursuit of brand collaborations.

Ultimately, Facebook engagement operates as a double-edged sword. While essential for financial survival, an expanding digital footprint increases the "attack surface" for cybercriminals. The loss of an account for a student influencer is not a mere technical glitch but a "business closure" that triggers immediate financial instability [12, 16]. Therefore, safeguarding digital integrity is no longer just a technical necessity—it is a fundamental requirement for the economic security and long-term well-being of the modern student entrepreneur.

4. Methodology

4.1. Research Design

This study adopts a mixed-methods research design, combining a longitudinal quantitative case study with a qualitative component. By monitoring 440 observations from Facebook influencer pages, the research utilizes a descriptive and predictive analytical framework to map the "security-utility trade-off" inherent in the influencer economy. To complement this numerical data, the study incorporated qualitative research through semi-structured interviews and first-hand statements from influencers who have experienced total or partial loss of livelihood due to security breaches. These qualitative statements are essential for contextualizing financial shocks, uncovering the "Security-Utility" conflict and validation of Predictive Metrics.

4.2. Population and Sampling

A convenience sample of 100 Facebook pages, each with over 5,000 followers, was selected for the study. From these pages, a total of 440 observations were collected. Furthermore, five Facebook influencers who had lost their pages due to security breaches were conveniently selected as key respondents. Convenience sampling was chosen because it provided easy access to active pages with large audiences, ensuring the availability of sufficient and relevant data within the study's time frame.

4.3. Data Collection

The investigators engaged ten trained research assistants to monitor the identified Facebook pages daily for 4 weeks. They collected data on age, gender, and data breach incidents, alongside various Facebook activity metrics. An interview guide was also utilized to collect qualitative data regarding the loss of livelihood resulting from breaches experienced by influencers. The metrics examined included Time (Week), Data Breach Incidents (Y), Clicks on Suspicious Links, Fake News or Misinformation Reports, Engagement Rate, Click-Through Rate (CTR), and New Followers per Week, as presented in Table 1.

Table 1. *Description of Variables.*

Variable	Description
T	Time (Week)
Y	Data Breach Incidents (count or binary)
x10	Clicks on suspicious links
x11	Fake news or misinformation reports
x14	Engagement rate
x15	Click-through rate (CTR)
x13	New followers per week

4.4. Data Analysis Techniques

The study employed a multi-tiered analytical approach to investigate the relationship between Facebook engagement behavior, data breaches and student's livelihoods in Kenya. The approach used is as follows:

1) Descriptive Analysis, utilizing means and standard deviations to establish usage baselines and identify variances between casual users and high-reach accounts. To explore demographic influences, Independent-samples T-tests were conducted to evaluate potential gender-based disparities in reach and behavioral risk. To address the skewed nature of influencer data, the study utilized Classification and Distributional Analysis. This involved applying Median-based thresholding and Kernel Density Estimates (KDE) to categorize participants into "High" and "Low" engagement groups.
2) Binary Logistic Regression was used for Predictive Risk Modeling, allowing the researchers to quantify how specific behavioral risks influence the probability of a security breach. The model's diagnostic accuracy was then validated using Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) metrics.
3) The study utilized Methodological Triangulation by integrating qualitative data through NVivo software. This allowed for the thematic coding of influencer testimonials regarding livelihood loss, which was then cross-referenced with the quantitative findings. By merging statistical patterns with narrative depth, this approach ensured a comprehensive validation of the "security-utility trade-off" within the student influencer economy.

5. Results

5.1. Descriptive Statistics

Descriptive statistics, including the number of observations, mean, standard deviation, minimum, and maximum values, are presented in Table 2.

Table 2. Descriptive Statistics.

Variable	Obs	Mean	Std. Dev.	Min	Max
Y	440	1.568182	2.663323	0	17
x14 (High)	95	0.9960	0.8684	0.3298	5.8951
x14 (Low)	94	0.1428	0.0865	0.0032	0.3153
x15 (High)	5	162.3732	76.3518	90.6571	245.75
x15 (Low)	5	50.9322	23.9787	18.0931	74.0911

The descriptive statistics in Table 2 reveal a clear contrast in security and engagement metrics across the sample. Data security breaches (Y) averaged 1.57 incidents per week, with a significant range from zero to a maximum of 17 incidents. When categorizing engagement and reach levels, the following patterns emerge:

1) High-engagement users (n=95) maintained an average rate of 0.996, nearly seven times higher than the low-engagement group (n=94), which averaged 0.143. The high-engagement group also showed much greater volatility, with a maximum rate of 5.895 compared to just 0.315 in the low group.
2) On reach intensity (x15), there was a disparity which was more pronounced in reach metrics. The high-reach group (n=5) averaged 162.37, peaking at 245.75. In contrast, the low-reach group (n=5) averaged 50.93, with a minimum value of 18.09.

These results highlight a steep hierarchy within the influencer economy, where a small segment of "high-reach" and "high-engagement" accounts operate at scales significantly larger than the average student user.

5.2. Gender Differences in Facebook Usage Frequency: T-Test Analysis

T-test statistics for the difference in Mean between Males and Females for the various indicators of Frequency of Use of Facebook is presented in Table 3.

Table 3. Gender Differences in Facebook Usage Frequency.

Variable	Mean (Male)	Mean (Female)	Diff (M–F)	t-value	p-value	Sig.
x10	1.941	2.122	-0.181	-0.627	0.5313	
x13	4102.94	11789.21	-7686.28	-1.151	0.2502	

The independent-samples t-test results indicate that gender does not significantly influence these specific indicators of Facebook usage. Regarding suspicious link clicks (x10), females exhibited a slightly higher mean (2.122) than males (1.941); however, the mean difference of -0.181 is statistically insignificant ($p = 0.5313$), suggesting that both genders engage with risky digital content at comparable rates.

Similarly, while the reach and audience metric (x13) showed a substantial numerical disparity between the female mean (11,789.21) and the male mean (4,102.94), the resulting difference of -7,686.28 proved non-significant ($t = -1.151$, $p = 0.2502$). Gender-neutral profile suggests that the "need for livelihood" drives both males and females toward similar risk-taking behaviors. An interview with a female lifestyle creator echoed this: *"In this game, you can't afford to be picky. Whether you are a guy or a girl, you click on links for potential 'collaborations' because that's where the money is. We are all equally desperate to scale."* This narrative supports the T-test finding that vulnerabilities are driven by economic necessity rather than gender. The findings show gender-neutral risk profile which contradicts the assertions of the RDT theory which assumes that power varies by demographic access.

5.3. Engagement Rate Distribution and Classification Analysis

The histogram was used to present the engagement profiles of the student Facebook influencer pages, as shown in Figure 1.

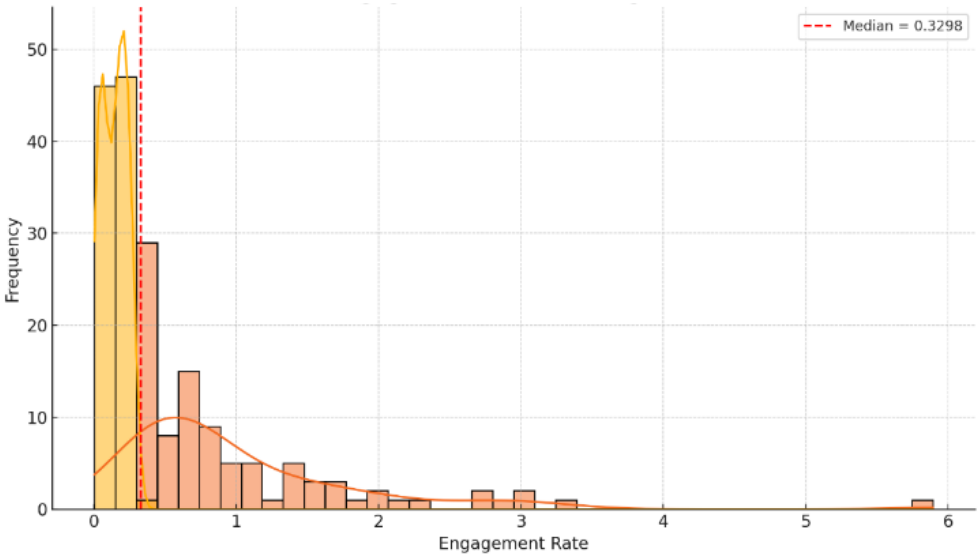

Figure 1. Distribution of Engagement Rates with High /low Classification.

Table 4. Profiles of Engagement.

Engagement Level	Count	Mean	Std Dev	Min	25%	Median	75%	Max
High	95	0.9960	0.8684	0.3298	0.4222	0.7275	1.2311	5.8951
Low	94	0.1428	0.0865	0.0032	0.0586	0.1559	0.2102	0.3153

The highly right-skewed distribution of engagement rates isolates a small "engagement elite." While the median threshold (~0.33) provides a robust classification, the outliers (exceeding 5.0) represent the most vulnerable "suitable targets" for attackers. A tech-reviewer influencer described this Paradox of Reach: "The more viral I went, the more 'fishing' emails I got. It's like my success was a beacon for hackers. You spend all your time building a livelihood, but that same reach makes you the biggest target on the platform." The findings confirm the RDT proposition that actors must adapt their behavior to capture critical resources, even if doing so creates a 'Paradox of Reach' that increases vulnerability.

5.4. Effect of Suspicious Clicks on Data Breach Likelihood

The logistic regression was used to test the relationship between *Suspicious Clicks on Data Breach Likelihood as presented in Table 5:*

Table 5. Logistic Regression Results for Data Breach Prediction (x10).

Variable	Coefficient	Std. Error	z-value	p-value	95% CI
x10 (Suspicious clicks)	2.461	0.263	9.38	<0.001	[1.949, 2.979]
Constant	-1.741	0.202	-8.62	<0.001	[-2.137, -1.345]

Model Statistics:

1) Observations = 440
2) LR $\chi^2(1) = 333.12$ ($p < 0.001$)
3) Pseudo $R^2 = 0.5595$

The logistic regression identifies suspicious clicks (x10) as a dominant predictor, with a Pseudo (R^2) of 0.5595. The extreme 11.7x increase in breach odds per click underscores the fragility of the digital marketplace. This statistical risk is validated by a student influencer's account of an "offer"

click: "I clicked a link for a supposed 'Facebook Monetization' reward. Within minutes, my login was changed and my page was used to post crypto scams. My followers felt betrayed, and my reputation—my only way to make money—was destroyed." These voices confirm that the 56% variation explained by the model represents a catastrophic livelihood shock for students who rely on these accounts for self-support.

6. Conclusion

The study establishes that university students are securing their livelihoods in the digital marketplace, where platforms such as Facebook serve as primary commercial engines. However, this economic independence is built on a precarious "Security-Utility Trade-off." The data confirms a "Paradox of Reach": as students scale their engagement to capture vital resources, they become "suitable targets" for cyber-attacks, experiencing an average of 1.57 breaches weekly. The most critical driver of this vulnerability is behavioral; a single interaction with a suspicious link increases breach odds by 11.7 times. Ultimately, because digital vulnerability is driven by the universal economic "need to scale," it transcends demographic boundaries, creating a gender-neutral risk profile where the drive for financial survival consistently overrides security protocols.

7. Recommendation

7.1. Recommendations for Practice

1) *Digital Livelihood Insurance and Recovery*: The study recommends the implementation of digital livelihood insurance, where institutions can support "Account Recovery Units." Since a breach represents a "business closure," students need rapid-response mechanisms and insurance frameworks to salvage their reputation and income streams.
2) *Behavioral-Based "Red-Flag" Training:* Institutions should provide targeted training focused on identifying behavioral triggers, such as malicious links, that lead to account compromise.
3) *Tiered Security for the "Engagement Elite":* High-reach influencers should adopt advanced security measures, including Hardware Security Keys (YubiKeys) and Facebook Business Manager verification, to protect their commercial assets.

7.2. Recommendations for Theory

1) *Updating Resource Dependence Theory (RDT):* This study suggests that RDT should be updated for the digital age to account for demographic parity in risk, acknowledging that digital resource scarcity creates universal vulnerabilities.
2) *Integration of Micro-Behavioral Variables*: Future applications of RDT should integrate micro-behavioral variables to explain how individual actions impact institutional or economic stability.
3) *Formalizing the "Paradox of Reach"*: Theoretical frameworks should formally adopt the "Paradox of Reach" as a construct to demonstrate that the search for resources can simultaneously create new threats and vulnerabilities.

Abbreviations

AI	Artificial Intelligence
RTD	Resource Dependency Theory
ICT	Information Communication and Technology
CTR	Click Through Rate
AUC	Area Under Curve
ROC	Receiver Operating Characteristics
KDE	Kernel Density Estimates

Author Contributions

Yussuf Motari Okari: Conceptualization
Robert Nyamao Nyabwanga: Formal Analysis
Eliza Buyeke Ogucha: Writing – review & editing

Conflicts of Interest

There is no conflict of interest.

References

[1] Abubakar, A. (2020). The digital dilemma: Algorithmic engagement and the expansion of students' cyber threat surfaces. Academic Press.

[2] Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 3(1), 7.

[3] Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. European Management Journal, 36(4), 431–438.

[4] Bhatt, M. D., Vyas, C., & Vohra, A. (2025). Exploring The Role of Influencer Marketing in Shaping Consumer Behaviour in the Age of Social Media Among Generation Z. International Journal of Environmental Sciences, 11(19s), 2025.

[5] Bian, B., & Wang, H. (2025). Content Value Dynamics in Digital Platforms: Strategic Monetization and Operational Design. Mathematics, 13(23), 3815.

[6] Duffy, B. E., & Hund, E. (2015). "Having it all" on social media: Entrepreneurial femininity and self-branding among fashion bloggers. Social Media + Society, 1(2), 1–11.

[7] Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F.,... & Telang, R. (2016). Do or do not, there is no try: user engagement may not improve security outcomes. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (pp. 97-111).

[8] Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource dependence theory: A review. Journal of management, 35(6), 1404-1427.

[9] Isler, A. (2025). The Impact of Social Media and Influencers on Generation Z's Purchasing Behaviour: Influencer Marketing (Doctoral dissertation, Dublin, National College of Ireland).

[10] Kivunja, C. (2015). Teaching students to learn and to work well with 21st century skills: Unpacking the career and life skills domain of the new learning paradigm. International Journal of Higher Education, 4(1), 1–11.

[11] Mbego, S. O. (2025). The rise of influencer marketing and its implications on Kenyan legacy media houses' revenues.

[12] Mishra, M. S., Sachan, M. P., Rathi, M. J., Adarsh, M., Singh, K., & Sethi, R. (2024, September). Monetization Strategies on YouTube vs. Instagram: A Study of Content Creator Revenue Models in the Digital Age. In Proceedings of the 2nd ICSSR Conference on "India Towards Viksit Bharat (Vol. 2047, pp. 13th-14th).

[13] Ndung'u, N. S., & Waema, T. M. (2019). The digital economy in Kenya: Legal, regulatory and policy frameworks. Africa Digital Rights Hub.

[14] Ondiek, M. A. (2021). The digital hustle: Gig work, micro-influencing, and the financial landscapes of Kenyan university students. East African Journal of Humanities and Social Sciences, 4(2), 112–125.

[15] Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, R. (2021). Predicting individual differences to cyber-attacks: Knowledge, arousal, emotional and trust responses. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15(4).

[16] Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective.

[17] Velázquez, H. L. C. (2025). Strengthening Global Cooperation: International Legal Frameworks for Combatting Emerging Cyber Threats and Cybercrime.