KKIK - FSRD

Jurnal Sosioteknologi

Website: https://journals.itb.ac.id/index.php/sostek/index

Showcasing Luxury on Social Media: What Are The Effects? An Anomaly among Lecturers

Menampilkan Kemewahan di Media Sosial: Bagaimana Pengaruhnya? Sebuah Anomali di antara Dosen

Erwin Kurniawan A[1], Dian Wahyuningsih[2], Dio Caisar Darma[3]

Faculty of Economics and Business, Mulawarman University, East Kalimantan, Indonesia[1]
Faculty of Economics and Business, Langlangbuana University, West Java, Indonesia[2]
Department of Management, Sekolah Tinggi Ilmu Ekonomi Samarinda, East Kalimantan, Indonesia[3]

diocaisar@stiesam.ac.id

ARTICLE INFO

Keywords:
social climbing, Facebook, WhatsApp, account theft, material and non–material losses

ABSTRACT

In almost every job, technological advancement plays a vital role in making it easier for humans, including social media. Today, there is a diminution of solidarity, which is contradictory to the "concept of caring". Users are increasingly indifferent, sometimes selfish, and exaggerate when they come into contact with posts on social media, thus triggering hacking by irresponsible individuals to achieve certain advantages. This paper is dedicated to investigating discriminatory actions against lecturers in the Faculty of ABC–University of XYZ who use Facebook and WhatsApp to show off all the luxuries of life. Through the experimental–qualitative design, the sample invited "social climbing" lecturers who experienced material and non-material losses. This study describes that respondents who experienced material impacts due to hacking were more dominant than those who suffered non-material losses. Most judged that the hacking addressed to respondents was triggered by a dominant intensity on social media rather than going about their daily routines. However, in the long term, lecturers express their attitude toward improving integrity as an academic community. Recognizing this reality, the practical implications of regulation and lawlessness in cyberspace need to be enforced. In addition, these findings also set the agenda for future studies.

INFO ARTIKEL

Kata kunci:
panjat sosial, Facebook, WhatsApp, pencurian akun, kerugian materi dan nonmateri

ABSTRAK

Hampir pada setiap pekerjaan, determinasi teknologi memegang peranan vital untuk memudahkan manusia, termasuk media sosial. Dewasa ini timbul penipisan terhadap solidaritas yang kontradiktif terhadap "konsep kepedulian". Para pengguna semakin berperilaku acuh, berperilaku tidak normal, dan berlebihan ketika bersinggungan dengan postingan di media sosial, sehingga memicu peretasan oleh oknum yang tidak bertanggung jawab untuk keuntungan tertentu. Artikel ini didedikasikan untuk menyelidiki aksi diskriminatif terhadap dosen di lingkungan Fakultas ABC–Universitas XYZ yang menggunakan Facebook dan WhatsApp dalam memamerkan segala kemewahan hidup. Penelitian ini menggunakan metode eksperimen kualitatitif, sampel penelitian adalah dosen-dosen "panjat sosial" yang mengalami kerugian materi dan nonmateri. Hasil penelitian menunjukkan para responden yang mengalami dampak materi akibat peretasan lebih dominan dibandingkan dosen yang mengalami kerugian

secara nonmateri. Sebagian besar menilai jika peretasan yang dialamatkan kepada responden dipicu oleh itensitas yang dominan di media sosial daripada menjalani rutinitas sehari-hari. Akan tetapi, dalam jangka panjang, para dosen mengekspresikan sikap untuk memperbaiki integritas sebagai civitas akademika. Berdasarkan realita tersebut, implikasi praktis terhadap regulasi dan pelanggaran hukum di dunia maya perlu ditegakkan. Selain itu, temuan ini juga menjembatani agenda studi masa depan.

https://doi.org/10.5614/sostek.itbj.2023.22.1.2

Introduction

The digital transition across the nation brings concrete changes. The shift from the conventional era to the modernization of technology has helped and accommodated human work in a more effective direction that saves energy, costs, and time (Ramadania et al., 2021). Without draining a lot of energy, each individual and community can communicate from different distances and locations without physically meeting face-to-face. The massive progress of a technology unwittingly kills morality, social civilization, and human culture (Arogyaswamy, 2020; Defleur, 1982; Walsh, 2020). According to Holmes (2005), social media, which is seen as fragile and erodes humanity, includes deceiving the anti-climax reality of netizens. There are symptoms that appear when people start to neglect empathy in public spaces, campuses, entertainment venues, reunions, and even family routines because they are too busy playing smartphones without caring about the surrounding environment or the erosion of tolerance. "Social climbing" tends to build a reputation, so friends and other users on social media have the perception that "likes", and "comments" are part of success (Bardoscia et al., 2013; Holland-Smith, 2017).

Social media such as Facebook (FB) and WhatsApp (WA), which are popularly installed and loved by generations, are vulnerable to racism, verbal acts that hurt other people's feelings, sexual harassment, crime through data leakage, and other disgraceful actions (Endeley, 2018; Fatehkia, O'Brien & Weber, 2019; Wijnberg & Le-Khac, 2021; van Steden & Mehlbaum, 2021). On the other hand, in the terminology of "happiness", the status features provided by these two types of platforms do take over from individual fatigue but are only "pseudo." A series of actions that cannot be accounted for by certain individuals are to be traded for certain purposes. FB and WA are interconnected, and these two devices complement each other with the motive of making it easier for users (Jang-Jaccard & Nepal, 2014). Then, the authentication option is also verified from the email. It is conceivable if one of them is breached and misused to weaken the user in the temporary to permanent period. In fact, an easy way for social climbing predators to see and track individual performance is through the activity level of social media users or individual desires that promote their interests through photos uploaded, status updates, and videos sharing about everyday life. Like a "game", netizens' behavior is a "slice of a circle" that shows emotional expression (Çelik, 2016; Fu et al., 2021; Fu et al., 2022).

For example, in emerging markets that adhere to a "democratic system", Indonesia provides autonomy for its citizens, who use social media openly and freely. This does not happen in China, where social media applications are controlled by a government that implements "socialism", closing and restricting access to widespread news from outside influences that might destroy the harmony of national unity through mass panic, avoiding outside public opinion, and political propaganda. Creemers (2017), Bamman, O'Connor & Smith (2012), Gallagher & Miller (2021), Ruan, Knockel & Crete-Nishihata (2021), Qin, Strömberg & Wu (2012), and Zheng (2013) see the tendency of "foreign doctrine" being inseparable from the "trade war", including technology exchanges with other countries, which triggers China to empower and appreciate domestic creativity more than foreign works whose confidentiality is still in doubt.

The level of cybersecurity in Indonesia is weak (Rizal & Yani, 2016). Recently, in August–September 2022, the emergence of a hacker named "Bjorka", who claimed to be from Poland, deliberately hacked the security system of the Indonesian government (Hanafi, 2022; Sutikno & Stiawan, 2022). His actions

are classified as "black hacking", where he tries to trick the government into asking for a copy of the money. Government data that was breached, then distributed and traded on the "Dark Web" includes: Indihome customers; registration data for smartphone owners; General Election Commission (KPU) data; state officials' data; correspondence documents belonging to President Joko Widodo; and other government websites, including letters sent by the State Intelligence Agency (BIN).

Problem Statement

The series of problems experienced by social climbing also tarnish the intellectuals in Indonesia (Astuti, 2021; Lim, 2013). Also, the practice of using social media on the grounds of being able to boost and support academic productivity is a dilemma (Hays, 2012). Although this is a natural thing, sometimes it violates the norms and goes against institutional principles. Achievements that we are always proud of on social media actually take turns stimulating tensions between lecturers, students, and other educators at the university. There are jobs that are hampered or even just have reduced lecture hours to continue to exist on social media (Shimizu, 2015). Holistic sensitivity decreases, along with habitats that group together in equalizing points of view (Massey et al., 2014). Worse yet, the mindset of social media activists who are not academics actually thinks that they are intellectuals who have a lot of busyness and money and often ignore safety and details, the hallmarks of an academic who works in an exclusive zone without strict supervision and a flexible schedule. In this way, contradictory posts on social media, such as ideas and innovations as symbols of knowledge, visual fantasy, individual perspectives, ideals, privacy activities, and the distribution of philanthropy, have the opportunity to attract attention from "cyber-crime".

Crime on social media is not a new issue. Most of the hacked accounts include: email, FB, and WA. The difficulty in dismantling the syndicate that addressed the academic community that launched the attack was because they first knew the potential victims were intensely displaying their residence address, bank accounts, houses, telephone numbers, and some were also showing email and social media accounts. This is certainly an irony that arouses the instincts of criminal behavior. The various fraud patterns identified include identity fraud, site hacking, spoofing, phishing, ransomware, and carding. Surprisingly, it is also often carried out by predatory journals in the name of "Scopus" through scientific conferences and the lure of publication through the "fast-track review" route with high costs and unreasonable procedures (e.g., Oviedo-García, 2021; Richtig et al., 2018; Torres, 2022).

Main Purpose

On the Asian scale in general, social media activists are growing rapidly compared to Europe, Africa, and other continents. Social media community networks in Asia are growing along with internet use and competitive "lifestyles" (Ardi & Putri, 2020; Dao et al., 2014; Martin, Lewis & Sinclair, 2013; Tapsell, 2020). This is true for both synthesis and criticism. Pang et al. (2021) argues that a social media product that is marketed through a certain "branding" has surrounded Asia, which drags its activists into the truth of "self–esteem". This implies social jealousy due to excessive showing off on social media (Altuwairiqi, Jiang & Ali, 2019; Jiang & Ngien, 2020; Lin & Utz, 2019; Lin, van de Ven & Utz, 2018; Maharani, 2021; Tandon, Dhir & Mäntymäki, 2021). Opinions that develop against the ideal perception can understand literacy and logical implications.

Interestingly, there are few publications that censor issues related to chaos and transactional incidents within the scope of the university, especially intimidation of lecturers who actually spend time on social media. Only information is limited to the exploration and evaluation of intimidation in social networks against the lower middle and upper middle income groups, but it does not lead to a landscape that is rich in people like lecturers. Observed from a distance, at first it seemed that there was no risk in using social media, but the maturity of how one behaved on social media was tested. To respond to the complexity of the fears of lecturers who are fond of social media, the focus of this study is to analyze the

material losses and non-material losses of the lecturer forum case. In science, the relevance of studies is multidimensionally focused today by the chaos of social media, the urgency of anxiety that lecturers must be aware of, and comprehensive experiences to improve lecturer ethics in social media.

The organization of the paper is divided into 5 parts. Section 1 (Introduction) focuses on the background, problem statements, and objectives of the study. Section 2 (Method): constructing the population and sample, data collection, and analysis approach Section 3 (Results) outlines the investigation's findings. Section 4 (Discussion and Conclusions) describes the study outputs with different related publications and displays the results. Section 5 (Theoretical Contributions and Managerial Implications): recommends policy parameters and provides suggestions for reflecting on the weaknesses of the study to consider future research directions.

Method

Population and Sampling

The population criteria in this study are 128 lecturers in the initialized campus "Faculty of ABC–University of XYZ. This campus was founded in 1990 and is located in Samarinda City (East Kalimantan Province, Indonesia). The sample was set up to observe lecturers who often exhibited luxury on social media and who argued that they had experienced criminal acts on WhatsApp, Facebook, or both. Only 84 samples (N = 84) were willing to be invited. These lecturers also had a history of material and non-material losses.

Data Collecting

The data collection procedure begins with permission from the head of the institution to get participants from related professions. The respondents represented the chronology and the series of reactions through the video service "Zoom Meeting". The stages of determining the respondent unit, restructuring the sample, and collecting data are conducted from December 2021 to August 2022.

Analytical Approach

The technique of filtering the data is operated through an experimental-qualitative model. Instruments for tabulating data were selected using a questionnaire format (e.g., Curiel et al., 2020; Drury et al., 2022). Then, the question items were given to the respondents based on their agreed-upon personal perceptions and were constructed without any intervention from their superiors. We also provide structured parallel clusters for respondents who have bad experiences with, or problems related to social media at the same time. The process of data articulation was modified into a descriptive form.

Result and Discussion

Respondent's Attention

Table I describes the characteristics of informants who used Facebook (FB) and WhatsApp (WA). Of the 84 questionnaires that were distributed and filled out openly by lecturers at the Faculty of ABC, we found that 47.62% did not use the two applications simultaneously but 34.52% actually used them together, and only 17.86% used them together sometimes. Sadly, respondents answered that 57.14% of these two applications were connected, and 42.86% ensured that they were not integrated between WA and FB. The lecturers were relatively enthusiastic about FB (61.39%) than WA (38.1%). Referring to this survey, 71.42% of respondents also empower other applications (Instagram and YouTube). A total of 20.24% use microblogs to fill vacancies in certain courses for students via links that are linked and look for lecture materials or references, and 8.33% just use Twitter to satisfy their hearts.

Table I Intensity of social media (N = 84)

No.	Questions	Answer	F	%
1.	Consuming FB and WA applications at the same time?	Yes	29	34.52
		Sometimes	15	17.86
		No	40	47.62
2.	Between the two, are they in sync?	Yes	36	42.86
		No	48	57.14
3.	Which one is more popular between FB and WA?	FB	52	61.9
		WA	32	38.1
4.	Other social media alternatives? *Mention…*	Twitter	7	8.33
		Instagram	29	34.52
		Microblog	17	20.24
		YouTube	31	36.9
5.	Tempo (per week) using FB and WA?	<3	14	16.67
		3–6	20	23.81
		7–10	33	39.29
		11–14	11	13.1
		>15	6	7.14
6.	The time (hours per day) spent on social media?	<1	15	17.86
		1.5–2	28	33.33
		2–2.5	26	30.95
		2.5–3	8	9.52
		3–3.5	3	3.57
		>3.5	4	4.76
7.	When was the last time you made a "status" on FB and WA?	A while ago	5	5.95
		Yesterday	31	36.9
		Last week	37	44.05
		Last month	11	13.1
8.	What posts are uploaded?	Photo	27	32.14
		Videos	19	22.62
		Writing status	38	45.24
9.	What forms are often posted on social media?	Routine on campus	6	7.14
		Learning module	13	15.48
		Food	22	26.19
		Vehicles	15	17.86
		Home	1	1.19
		Vacation	7	8.33
		Others	20	23.81
10.	Consider uploading status?	Social chat	4	4.76
		Academic branding	34	40.48
		Eliminate boredom.	16	19.05
		Educate	7	8.33
		Just curious	11	13.1
		Looking for a partner	2	2.38
		Explore conference ads	10	11.9
11.	Hope to get a response from fellow social media activists?	Yes	45	53.57
		No	39	46.43

(Source: interview output)

Respondents also responded that the duration spent on social media had taken up 7–10 times per week (32.29%), and when viewed by hours, what was surprising was that they had lost time, spending almost 1.5–2.5 hours per day (64.28%). On average, 80.95 percent of the lecturers at the Faculty of ABC admit that they have shared their status on Facebook and WhatsApp for one week. At its peak, part-time employees are actually needed to upload status updates (45.24%), photos (32.14%), and videos (22.62%).

From the "ninth question", personal inspiration for playing social media is posting food at a restaurant (26.19%), new types of cars (17.86%), and other varied posts as much as 23.81%, consisting of words or motivational sentences, songs, religious lectures, satire against certain individuals, motivational advertisements, live-streaming, and hobbies. These are "normal" things. Initiatives from other propositions also prove that uploads on social media are intended for "academic branding" to gain fame, while 19.05% of respondents think that social media is effective in getting rid of stress, 13.1% want to peek at other people's activities, and 11.9% claim that service advertisements on social media are a trusted source to get information, such as publishers who provide journal and book publication opportunities to follow. Elaboration of the study confirms that 53.57% of lecturers are imperative in the form of "likes" or "comments" from colleagues, students, and family. In essence, 46.43% of lecturers actually reacted "don't care" to get any interest in the "11th question".

Hacking Pattern

Table II below shows an unpleasant social climbing experience. In the corridor throughout 2021–2022, 60.71% of lecturers answered that social media accounts had been stolen, and 39.29% said they had. Weak systems on Facebook (78.57%) and WhatsApp (21.43%) have been predicted by respondents who point out that security protection is not intensive. There were 78.57% of respondents who said that Facebook aggressively was the most frequently hacked, and 21.43% of their WA applications experienced the tragedy of burglary. This is relatively extreme by a kind of "scraping time", considering that 71.43% of respondents had their social media hacked four times, while what was more fundamental was hacking five to seven times (17.86%). Then, 29.76% of respondents suspected that hacking was due to hackers displaying luxury that seemed to be rich, 28.57% due to "human error" where the cellular card suddenly died and the password deliberately repeatedly asked for a new password, and 21.43% assumed that due to a well-known position where there is ambition that is closer to a conflict of interest whose actors already know the identity of the victim and a broad relationship factor that touches 20.24% stated that they are famous, so this dimension triggers hacking.

Table II Hacking Capacity (N = 84)

No.	Questions	Answer	F	%
12.	Have social media accounts ever been stolen?	Yes	51	60.71
		No	33	39.29
13.	What apps were hacked?	FB	66	78.57
		WA	18	21.43
14.	How often is social media hacked?	4	60	71.43
		5–7	15	17.86
		>8	9	10.71
15.	What is the reason for the key being hacked?	Human error	24	28.57
		Have extensive relationships.	17	20.24
		Famous positions	18	21.43
		Showing wealth	25	29.76
16.	What are the common forms of hacking?	Lame account	13	15.48
		Duplicate profile	30	35.71
		Virus attack	9	10.71
		Post screenshots, videos, and photos	10	11.9
		Mastering to be obeyed emotionally	22	26.19
17.	What is the orientation towards hacking? (*Go to Tables 3 and 4*)	Material	59	70.24
		Non–material	25	29.76
18.	Are there any preventive measures?	Yes (*go to Table 6*)	62	73.81
		No (*stop, go to Table 5*)	22	26.19

(Source: interview output)

The most common forms of hacking exposed are duplication of profiles (35.71%) with fake identities and real accounts crashing due to guessed passwords. As many as 26.19% of respondents believed that they were emotionally manipulated by certain perpetrators and were subsequently hypnotized to immediately take emergency measures as the result of a scenario of fake colleagues and family members who experienced misfortunes such as accidents and were in pain. Accounts that were totally hi-jacked reached 15.48%, and another 11.9% is those that went viral through illegal screenshots, videos, and photos. It was confirmed that there were efforts of resistance and criticism that had an impact on career decline. Interestingly, 10.71% were exposed to virus attacks which hackers used to blackmail the owners through threats of pornographic videos, fake links and advertisements, and other fraudulent schemes.

Table III Material Loss (N = 59)

No.	Components	Answer	Frequency	Percentage
19.	Intellectual property sabotage	○ Yes ○ No	18 41	30.51 69.49
20.	Direct threats and violence	○ Yes ○ No	4 55	6.78 93.22
21.	Damage to credibility	○ Yes ○ No	33 26	55.93 44.07
22.	Transfer credit, data packages, or some money	○ Yes ○ No	59 0	100 0

(Source: interview output)

Material losses and non–material losses that are the result of crimes related to social media in question 17 in Table II conclude that, out of 84 respondents, 59% admitted to material losses and 25% experienced non–material losses. Technically, this explanation is framed in Tables III and IV. Table III examines the frequent occurrence of violations of intellectual property for 41% of lecturers. They claim that the hackers took pictures and videos illegally. In addition, 93.22% stated that they had also been directly threatened using instructions that must be obeyed, for example, the theft of money and property. Separately, 55.93% of them were unable to stop fraud in the form of defamation, and all respondents also did not stem the financial draining fraud, including transferring credit, data packages, and money.

Table IV Non–Material Loss (N = 25)

No.	Components	Answer	Frequency	Percentage
23.	DDoS injection	○ Yes ○ No	17 8	68 32
24.	Phishing e-mails	○ Yes ○ No	25 0	100 0
25.	Privacy breach	○ Yes ○ No	16 9	64 36
26.	Abuse	○ Yes ○ No	11 14	44 56
27.	Access without permission	○ Yes ○ No	20 5	80 20
28.	Illegal content	○ Yes ○ No	23 2	92 8

(Source: interview output)

The points from Table IV confirm that, tragically, 68% of respondents were injected with a distributed denial of service (DDoS) attack, where the perpetrator tried to combine network resources on a machine that was not available to the respondent through a service interruption of a host located on the

internet. The level of privacy violations on social media is the starting point for low awareness of filling out a form on the internet that includes personal data (phone number, access to log in via email, password, home address, and code on an ATM, as shown by 64% of respondents). Forms of harassment such as gender harassment, seductive behavior, sexual bribery, sexual terror, sex texting, and body-shaming have cornered 56% of respondents, thus tarnishing their reputation. There is also unauthorized access by hackers who infiltrate and check social media using geolocation or spyware. This risky condition is also a disaster for 92% of respondents whose social media accounts are infiltrated by illegal content that is unethical, tarnishes the law, and is vulnerable to public order.

Table V Reaction to "Question 18, Option: No" (N = 22)

No.	Questions	Answer	Frequency	Percentage
29.	Are you stressed?	o Yes	10	45.45
		o Sometimes	3	13.64
		o No	8	36.36
30.	Are you frustrated?	o Yes	15	68.18
		o Sometimes	6	27.27
		o No	1	4.55
31.	Are you desperate?	o Yes	12	54.55
		o Sometimes	10	45.45
		o No	0	0
32.	Do you feel panic?	o Yes	9	40.91
		o Sometimes	8	36.36
		o No	5	22.73

(Source: interview output)

The reaction of respondents who do not take alternatives and delay the search in maintaining when social media is hacked has an impact on feelings of stress (45.45%), frustration (68.18%), dropouts (54.55%), and panic (40.91%). Although this was relatively difficult, over time they chose to create new FB and WA accounts.

Short-Term Solution

Recently, respondents have been optimistic about reprioritizing hacked accounts through three strategies: 77.42% self-repair, arguing that these tips can save expenses; 95.16% share their experiences of exchanging income, not closing themselves, and partnering with colleagues who have hacked; and 59.68% contact professional services through expert advice or experts hired according to their field. Good skills and control to adapt and minimize hacking attacks on social media indicate that respondents have the insight to survive even though the situation is always increasing.

Table VI Mechanisms and Initiatives (N = 62)

No.	Components	Answer	Frequency	Percentage
33.	Fix it yourself	o Yes	48	77.42
		o Sometimes	14	22.58
34.	Sharing experience	o Yes	59	95.16
		o Sometimes	3	4.84
35.	Contracting professional services	o Yes	37	59.68
		o Sometimes	25	40.32

(Source: interview output)

Discussion and Conclusions

The phenomenon of social climbing, shows off all luxuries on FB and WA, indicates that users need "recognition" from others (Dewi et al., 2019; Wang, 2015). The depletion of the tradition of politeness is a "dark side" perspective that reflects the individual degree or level of economic welfare of the rich class to fall into a trap that not only creates social inequality and material controversy but is also a target for intimidation by organized crime mafia nests.

Velandia-Morales, Rodríguez-Bailón & Martínez (2022) assume that the abundance of wealth does not guarantee a peaceful life, but instead stimulates suspicion and unfairness from others about how one gains wealth in a short time without knowing for sure the individual hard work to achieve it. Compared with other countries, the FB users in Indonesia as of January 2022 were among the highest globally, ranking third after India and the USA (Katadata, 2022). This increasing trend is a big wave that excites the psychological aspect of social climbing. Uniquely, in the 2021 period for internet users aged 16–64 years, Rollason (2021) released the number of users reaching around 2 billion as of July 2021. The most dominant nation that uses WA is Kenya (97%), then South Africa is in second place at 96%, and Nigeria is third (95%). Furthermore, Indonesia is in the last position in the "10 largest", where around 87% of the population uses WA.

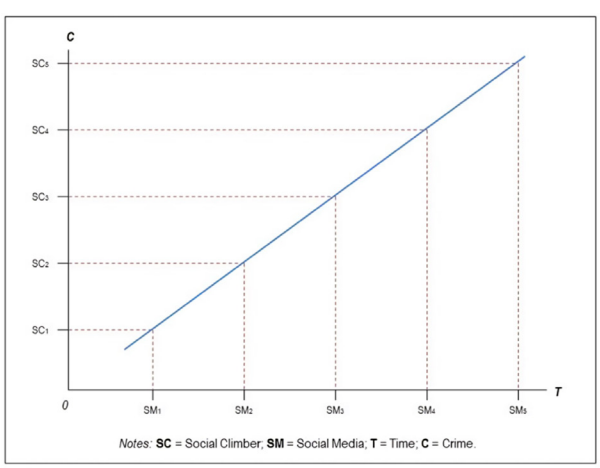

Figure 1 The "social climber" analogy and its consequences
(Source: Own)

The findings in this study found that the more active one is on social media, especially for "social climbers", the more likely one is to be cheated. Social media does not show the authenticity of individual characters and traits. This term is illustrated by the fact that the taller the "tree", the stronger the wind blows, which triggers the tree roots to wobble because it carries a heavy load of leaves and twigs. Accordingly, Figure 1 above demonstrates the "social climber" analogy. As the direction of the ladder is getting higher and higher, Figure 1 speculates that, with increasing social media users, it is also symmetrical with criminal threats. There is a positive interaction between the "dotted line" which represents the volume of social media use, and the parallel "linear line". Thus, the more climbers spend time in cyberspace, the more their "respect is depleted", and they actually get closer to being deceived by criminals. Moreover, the break time is also intended to show off wealth, resulting in the cointegration of the "bottom left to top right" graph.

In this case, the purpose of using social media was positive, such as for refreshing, but instead it came across as arrogant because of the users' immaturity in thinking. This became the "root problem" of social unrest, commercialization of industry in academic circles, degradation of the sense of togetherness, isolation of disrespectful attitudes, such as not respecting other people's opinions, barriers to healthy competition, provocation, personal ego, exploitation of luxury, and dependence on irrational presence.

Many of the respondents did not know the latest features from FB and WA that can be connected, although the bad news of inferential "big data" has been experienced by some netizens (Majid & Kouser, 2019; Pallivalappil, Jagadeesha & Prasad, 2021; Pybus, Coté & Blanke, 2015; Rader & Wash, 2015; van der Schyff, Flowerday & Lowry, 2020; Vishwanath, 2019). According to what is stated, social climbing does not care that it alters and reduces comfort (Rak, 2007), thus offending other netizens due to social media relations that have relatively pioneered social rifts (Meikle, 2016), misleading exposure (Browning, 2017), mistakes that break friendships (Romero-Iribes & Smith, 2019), and chaos among families. (Rickly-Boyd, 2012).

Theoretical Contributions and Managerial Implications

The anomaly that "boasts itself" is the wrong element. Insincere intentions based on continuous "social recognition" urge individuals to control other people's views of themselves or otherwise strengthen authority by putting aside the opinions of others. Every human being has different characteristics. If not realized, social climbers tend to be depressed, as in this finding. The theoretical contribution emphasizes the horizon of knowledge related to the commitment of social media users to be wiser and open up as a way to learn from mistakes so that they do not repeat themselves in the future. In other words, there is introspection that refrains from showing off wealth. Despite the doubts, the unification of conducive communication through agreement among users is seen as preferable.

The managerial implications are focused on the integrated supervision of the help desks on Facebook and WhatsApp, especially the reporting of data theft, restoring and cleaning reputation, and temporarily disabling applications. Stakeholders, especially leaders on campus, i.e., the Chancellor and Dean, have the authority to give disciplinary sanctions to lecturers who are still doing social climbing, including: administrative punishment, prohibition on social media, removal of compensation, and dismissal. Respondents who are involved in the academic field should create a sustainable generation. Therefore, the topic of this study is to ensure that there are variables that are missed so that future research directions consider implementing competent improvements.

Acknowledgment

The authors appreciate the professional comments by an anonymous reviewer in the Jurnal Sosioteknologi from ITB. There is no specific funding for this study. Survey data during the interview process is a narrative told by informants transparently and is the responsibility of the author.

References

Altuwairiqi, M., Jiang, N., & Ali, R. (2019). Problematic attachment to social media: Five Behavioural archetypes. *International Journal of Environmental Research and Public Health, 16*(12), 2136. https://doi.org/10.3390/ijerph16122136

Ardi, Z., & Putri, S. A. (2020). The analysis of the social media impact on the millennial generation behavior and social interactions. *Southeast Asian Journal of technology and Science, 1*(2), 70–77. https://doi.org/10.29210/81065100

Arogyaswamy B. (2020). Big tech and societal sustainability: An ethical framework. *AI & Society, 35*(4), 829–840. https://doi.org/10.1007/s00146-020-00956-6

Astuti, Y. D. (2021). Digital literacy competence of Indonesian lecturers on analysis hoax in social media. *Library Philosophy and Practice, 5234*, 1–13.

Bardoscia, M., De Luca, G., Livan, G., Marsili, M., & Tessone, C. J. (2013). The social climbing games. *Journal of Statistical Physics, 151*(3-4), 440–457. https://doi.org/10.1007/s10955-013-0693-0

Bamman, D., O'Connor, B., & Smith, N. (2012). Censorship and deletion practices in Chinese social media. *First Monday, 17*(3), 5. https://doi.org/10.5210/fm.v17i3.3943

Browning, G. (2017). Being a social climber: The effects of a rock-climbing intervention on the social interactions and motor skills of individuals with autism spectrum disorder. *Thesis*. Master of Arts in Psychology in the College of Science and Mathematics, California State University, Fresno.

Çelik, M. (2016). The impact of social media on luxury consumption. *The Turkish Online Journal of Design, Art and Communication, 6*(4), 437–445. https://doi.org/10.7456/10604100/007

Creemers, R. (2017) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China, 26*(103), 85–100. https://doi.org/10.1080/10670564.2016.1206281

Curiel, R. P., Cresci, S., Muntean, C. I., & Bishop, S. R. (2020). Crime and its fear in social media. *Palgrave Communications, 6*(1), 57. https://doi.org/10.1057/s41599-020-0430-7

Dao, W. V-T., Le, A. N-H., Cheng, J. M-S., & Chen, D. C. (2014). Social media advertising value: The case of transitional economies in Southeast Asia. *International Journal of Advertising, 33*(2), 271–294. https://doi.org/10.2501/IJA-33-2-271-294

Defleur, L. B. (1982). Technology, social change, and the future of sociology. *The Pacific Sociological RevieW, 25*(4), 403–417. https://doi.org/10.2307/1388922

Dewi, P. K., Qowim, M. R. F., Aristantia, S., Maulidia, M., & Fibrianto, A. S. (2019). Phenomenon of social climbing in the younger generation in Malang City hotels. *Advances in Social Science, Education and Humanities Research, 404*, 265–270. https://doi.org/10.2991/assehr.k.200214.046

Drury, B., Drury, S. M., Rahman, M. A., & Ullah, I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media, 30*, 100211. https://doi.org/10.1016/j.osnem.2022.100211

Endeley, R. E. (2018) End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security, 9*(1), 95–99. https://doi.org/10.4236/jis.2018.91008

Fatehkia, M., O'Brien, D., & Weber, I. (2019). Correlated impulses: Using Facebook interests to improve predictions of crime rates in urban areas. *PloS ONE, 14*(2), e0211350. https://doi.org/10.1371/journal.pone.0211350

Fu, P., Jing, B., Chen, T., Xu, C., Yang, J., & Cong, G. (2021). Propagation model of panic buying under the sudden epidemic. *Frontiers in Public Health, 9*, 675687. https://doi.org/10.3389/fpubh.2021.675687

Fu, P., Jing, B., Chen, T., Yang, J., & Cong, G. (2022). Identifying a new social intervention model of panic buying under sudden epidemic. *Frontiers in Public Health, 10*, 842904. https://doi.org/10.3389/fpubh.2022.842904

Gallagher, M., & Miller, B. (2021). Who not what: The logic of China's information control strategy. *The China Quarterly, 248*(1), 1011-1036. https://doi.org/10.1017/S0305741021000345

Hanafi, D. (2022). Terungkap, hacker Bjorka ternyata membeli data pejabat dari situs Dark Web [It was revealed that Bjorka hackers actually bought official data from the Dark Web site]. Retrieved from https://www.volkpop.co/nasional/pr-2104735265/terungkap-hacker-bjorka-ternyata-membeli-data-pejabat-dari-situs-dark-web

Hays, N. A. (2012). Social climbing: A contextual approach to understanding the effects of social hierarchy on individual cognition and behavior. *UCLA Electronic Theses and Dissertations*. Retrieved from https://escholarship.org/uc/item/7zf5k4rs

Holland-Smith, D. (2016). Social capital, social media, and the changing patterns of participation in climbing. *Sport in Society, 20*(9), 1101–1117. https://doi.org/10.1080/17430437.2016.1269078

Holmes, D. (2005). *Communication theory: Media, technology and society, 1st Ed*. California: SAGE Publications Ltd. https://dx.doi.org/10.4135/9781446220733

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jiang, S., & Ngien, A. (2020). The effects of instagram use, social comparison, and self-esteem on social anxiety: A survey study in Singapore. *Social Media + Society, 6*(2), 1–10. https://doi.org/10.1177/2056305120912488

Katadata (2022). Indonesia masuk daftar pengguna Facebook terbanyak, urutan berapa? [Indonesia is included in the list of the most Facebook users, in what order?]. Retrieved from https://databoks.katadata.co.id/datapublish/2022/03/23/indonesia-masuk-daftar-pengguna-facebook-terbanyak-urutan-berapa

Li, H. (2013). Many clicks but little sticks: Social media activism in Indonesia. *Journal of Contemporary Asia, 43*(4), 636–657. https://doi.org/10.1080/00472336.2013.769386

Lin, R., van de Ven, N., & Utz, S. (2018). What triggers envy on social network sites? A comparison between shared experiential and material purchases. *Computers in Human Behavior, 85*, 271–281. https://doi.org/10.1016/j.chb.2018.03.049

Lin, R., & Utz, S. (2015). The emotional responses of browsing Facebook: Happiness, envy, and the role of tie strength. *Computers in Human Behavior, 52*, 29–38. https://doi.org/10.1016/j.chb.2015.04.064

Maharani, A. C. (2021). The influence of excessive use of social media. *Indonesian Journal of Social Sciences, 13*(1), 11–20. https://doi.org/10.20473/ijss.v13i1.26351

Majid, I., & Kouser, S. (2019). Social media and security: How to ensure safe social networking. *International Journal of Humanities and Education Research, 1*(1), 36-38.

Martin, F., Lewis, T., & Sinclair, J. (2013). Lifestyle media and social transformation in Asia. *Media International Australia, 147*(1), 51–61. https://doi.org/10.1177/1329878X1314700107

Massey, A. R., Byrd-Craven, J., Auer, B. J., & Swearingen, C. L. (2014). Climbing the social ladder: Physiological response to social status in adolescents. *Adaptive Human Behavior and Physiology, 1*(1), 72–92. https://doi.org/10.1007/s40750-014-0009-x

Meikle, G. (2016). *Social Media: Communication, sharing and visibility*. New York, NY: Routledge.

Oviedo-García, M. Á. (2021). Journal citation reports and the definition of a predatory journal: The case of the Multidisciplinary Digital Publishing Institute (MDPI). *Research Evaluation, 30*(3), 405–419. https://doi.org/10.1093/reseval/rvab020

Qin, B., Strömberg, D., & Wu, Y. (2017). Why does China allow freer social media? Protests versus surveillance and propaganda. *Journal of Economic Perspectives, 31*(1), 117–140. https://doi.org/10.1257/jep.31.1.117

Pallivalappil, A. S., Jagadeesha, S. N., & Prasad, K. (2021). Social engineering attacks on Facebook –A case study. *International Journal of Case Studies in Business, IT, and Education, 5*(2), 299–313. https://doi.org/10.47992/ijcsbe.2581.6942.0135

Pang, B., Deshpande, S. A., Nguyen, T.-M., Kim, J., Almosa, Y. A., Arif, A., Arli, D., Bakpayev, M., Erdogan, B. Z., Fujihira, H., Gallage, H. P. S., Kadir, M. A., Ong Lai Teik, D., Satawedin, P., Weinreich, N. K., & Yousef, M. (2021). A critical overview of social marketing in Asia. *Social Marketing Quarterly, 27*(4), 302–323. https://doi.org/10.1177/15245004211053847

Pybus, J., Coté, M., & Blanke, T. (2015). Hacking the social life of big data. *Big Data & Society, 2*(2), 1–10. https://doi.org/10.1177/2053951715616649

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity, 1*(1), 121–144. https://doi.org/10.1093/cybsec/tyv008

Rickly-Boyd, J. M. (2012). Lifestyle climbing: Toward existential authenticity. Journal of *Sport & Tourism, 17*(2), 85–104. https://doi.org/10.1080/14775085.2012.729898

Rollason, H. (2021). What countries are the biggest WhatsApp users? Retrieved from https://www.verint.com/blog/what-countries-are-the-biggest-whatsapp-users/

Rak, J. (2007). Social climbing on Annapurna: Gender in high-altitude mountaineering narratives. *ESC: English Studies in Canada, 33*(1-2), 109–146. https://doi.org/10.1353/esc.0.0030

Ramadania, R., Rosnani, T., Fauzan, R., & Darma, D. C. (2021). The study of perceived risk and e-service convenience towards satisfaction and trust of online academic users in Indonesia. *International Journal of Media and Information Literacy, 6*(2), 387–395. http://dx.doi.org/10.13187/ijmil.2021.2.387

Richtig, G., Berger, M., Lange-Asschenfeldt, B., Aberer, W., & Richtig, E. (2018). Problems and challenges of predatory journals. *Journal of the European Academy of Dermatology and Venereology, 32*(9), 1441–1449. https://doi.org/10.1111/jdv.15039

Rizal, M., & Yani, Y. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies, 4*(1), 61–78. https://doi.org/10.21512/jas.v4i1.967

Romero-Iribas, A., & Smith, G. M. (2019). Friendship without Reciprocation? Aristotle, Nietzsche, and Blanchot. *Good Society, 27*(1-2), 1–28. https://doi.org/10.5325/goodsociety.27.1-2.0001

Ruan, L., Knockel, J., & Crete-Nishihata, M. (2021). Information control by public punishment: The logic of signalling repression in China. *China Information, 35*(2), 133–157. https://doi.org/10.1177/0920203X20963010

Shimizu, M. T. (2015). Lofty domains: Social climbing and visual dominance in elevated urban views. *Photography and Culture, 7*(2), 141–168. https://doi.org/10.2752/175145214X13999922103129

Sutikno, T., & Stiawan, D. (2022). Cyberattacks and data breaches in Indonesia by Bjorka: Hacker or data collector? *Bulletin of Electrical Engineering and Informatics, 11*(6), 2989– 2994. https://doi.org/10.11591/eei.v11i6.4854

Tandon, A., Dhir, A., & Mäntymäki, M. (2021). Jealousy due to social media? A systematic literature review and framework of social media-induced jealousy. *Internet Research, 31*(5), 1541–1582. https://doi.org/10.1108/INTR-02-2020-0103

Tapsell, R. (2020). Social media and elections in Southeast Asia: The emergence of subversive, underground campaigning. *Asian Studies Review, 45*(1), 117–134. https://doi.org/10.1080/10357823.2020.1841093

Torres, C. G. (2022). Editorial misconduct: The case of online predatory journals. *Heliyon, 8*(3), e08999. https://doi.org/10.1016/j.heliyon.2022.e08999

van der Schyff, K., Flowerday, S., & Lowry, P. B. (2020). Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment. *Heliyon, 6*(8), e04714. https://doi.org/10.1016/j.heliyon.2020.e04714

van Steden, R., & Mehlbaum, S. (2021). Do-it-yourself surveillance: The practices and effects of WhatsApp neighbourhood crime prevention groups. *Crime, Media, Culture, 1*, 1–18. https://doi.org/10.1177/17416590211041017

Velandia-Morales, A., Rodríguez-Bailón, R., & Martínez, R. (2022). Economic inequality increases the preference for status consumption. *Frontiers in Psychology, 12*, 809101. https://doi.org/10.3389/fpsyg.2021.809101

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

Wang, J. (2015). The dark side of luxury consumption: Psychological and social consequences of using luxury goods. *Dissertation*. Partial fulfillment of the requirements for the degree of Doctor of Philosophy in University of Minnesota.

Walsh, J. P. (2020). Social media and moral panics: Assessing the effects of technological change on societal reaction. *International Journal of Cultural Studies, 23*(6), 840–859. https://doi.org/10.1177/1367877920912257

Wijnberg, D., & Le-Khac, N-A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation, 38*, 301132. https://doi.org/10.1016/j.fsidi.2021.301132

Zheng, H. (2013). Regulating the internet: China's law and practice. *Beijing Law Review 4*(1), 37–41. http://dx.doi.org/10.4236/blr.2013.41005