INNOVATION AT THE CROSSROADS OF EDUCATION AND TECHNOLOGY

EDITOR
R. Nia Marotina

INNOVATION AT THE CROSSROADS OF EDUCATION AND TECHNOLOGY- 2025

ISBN: 978-625-6080-49-2

DOI: 10.5281/zenodo.17407165

Edited By

R. Nia MAROTINA

October / 2025

Ankara, Türkiye

Date: 21.10.2025

Farabi Publishing House
Ankara, Türkiye
www.farabiyayinevi.org

adopted by Esma AKSAKAL
ISBN: 978-625-6080-49-2

INNOVATION AT THE CROSSROADS OF EDUCATION AND TECHNOLOGY

EDITOR
R. Nia MAROTINA

AUTHORS
Dr. Chukwunonye N. ANYAKOHA
R. Nia MAROTINA
Fajar SEPTIAN
Agustyar NURFAISAL
Linus TANKO
Afiniki BAHAGO
Victor Yunana BOWMAN

TABLE OF CONTENTS

PREFACE

This book explores how innovation is reshaping education and enterprise in emerging economies. From financial systems to digital platforms, the chapters highlight the urgent need for adaptive strategies that prepare individuals and institutions for a rapidly evolving world.

The first chapter focuses on financial innovation and its impact on business education, while the second addresses cyber risk management for MSMEs navigating digital threats. The third investigates how social media influences academic success among future caregivers in Nigeria.

Together, these studies offer insights into the challenges and possibilities of modern education and entrepreneurship. They invite readers to rethink traditional models and embrace forward-looking solutions for sustainable growth.

Editoral Team
October 21, 2025
Türkiye

CHAPTER 1
FINANCIAL INNOVATION AND THE FUTURE OF BUSINESS EDUCATION IN EMERGING ECONOMIES

[1]Dr. Chukwunonye N. ANYAKOHA

[1]Department of Business Education, Faculty of Vocational and Technical Education, University of Nigeria, Nsukka, Enugu State, Nigeria, chukwunonye.anyakoha@unn.edu.ng,
ORCID ID: 0000-0002-1907-9295

INTRODUCTION

Financial innovation refers to the introduction and adoption of new financial instruments, services, processes, or technologies that improve the efficiency, accessibility, security, and inclusivity of financial systems. In today's digital economy, financial innovation is largely technology-driven, encompassing tools such as mobile money, digital payment systems, blockchain, cryptocurrencies, peer-to-peer lending, robo-advisors, digital banking, and fintech solutions. These innovations leverage big data, artificial intelligence, cloud computing, and mobile technologies to reshape how financial services are delivered and consumed, making them faster, cheaper, more user-friendly, and accessible across geographic and socioeconomic divides. Emerging economies such as Nigeria, Ghana, Kenya, and India have become leading hubs for financial innovation due to several interlinked factors.

1. LITERATURE REVIEW

Financial innovation generally refers to the creation, development, and adoption of new financial products, services, processes, or institutions that alter the way financial intermediation, risk management, payment, or capital raising happens. Khraisha & Arthur (2018) define financial innovation as a process, carried out by any institution, that involves the creation, promotion and adoption of new (incremental or radical) products, platforms, and processes or enabling technologies that introduce new ways or changes in how financial activity is carried out. The evolution of financial innovation has been shaped by several forces: regulatory change, technological advances, globalization, competition, and evolving consumer demand. After the 2008 financial crisis, there has been a re-evaluation of financial innovation and its risks, along with interest in how complexity has increased. Khraisha & Arthur (2018) discussed how financial innovation is increasingly seen as combinatorial (i.e. new products/processes are built by combining existing ones), adaptive, incremental or radical, and how innovations diffuse over time. Technological drivers (fintech, digital platforms, mobile/digital payments) are increasingly central.

The recent bibliometric work (Kou & Lu, 2025) shows that FinTech, AI/ML, blockchain, etc., are among emerging technologies in financial innovation.

Also, the evolution involves not just innovation in products but in governance, regulation, and institutions. For example, "financial innovation and its governance" explores how innovations are managed and regulated once they are underway.

1.1 Theoretical Review

This chapter is anchored on two theories namely; Scumpeter's Theory of Innovation (Creative Destruction) and Financial Intermediation theory. The Schumpeter's Theory of Innovation (creative destruction) was promulgated by Jospeh Schumpeter and it posits that innovation is the engine of economic growth by way of "creative destruction," in which old technologies, processes, firms, or institutions are destroyed and replaced by new ones. Innovation is endogenous; entrepreneurs or firms introduce new goods/services/processes, which disrupt existing structures, giving rise to new ones. While Schumpeter focused originally on industrial technology, economists have extended his theory to financial innovation. Empirical and theoretical work in recent years has tried to see whether financial innovation works similarly: does it displace older financial institutions or processes? Does it generate dynamic inefficiency or risk? For example, the IMF working paper "Is Schumpeter Right? Fintech and Economic Growth" (2024) finds evidence that financial innovation (especially fintech) promotes growth—particularly in developing countries. It supports the Schumpeterian view that financial innovation can drive growth via increased financial intermediation and providing financial resources for fixed capital formation.

Furthermore, the recent work "Investment and Innovation in Emerging Versus Advanced Market Economies: a Schumpeterian Approach" (Lianos & Sloev, 2023) examines how emerging markets often lag in innovation despite higher investment, due to financial and economic cost constraints. This reflects that creative destruction in emerging markets may be more constrained. Schumpeter's framework helps explain how financial innovation disrupts incumbents, though critics warn it may cause instability, regulatory arbitrage, or harmful excess destruction if unmanaged.Some studies take an institutional or governance perspective to address such risks.

The financial intermediation theory concerns how financial institutions (banks, etc.) act as intermediaries: taking deposits, giving loans, reducing information asymmetries, pooling risks, monitoring borrowers, reducing transaction costs etc. Traditional theories include those around transaction cost economics, agency theory, asymmetric information (Akerlof, Stiglitz), delegated monitoring (Diamond).

In the context of financial innovation, financial intermediation theory helps to explain how innovation alters or enhances these intermediary functions, or in some cases disintermediates them (e.g. via fintech, peer-to-peer lending, blockchain). Innovation may change how intermediation occurs (e.g. more efficiently, more transparently), or the role of intermediaries may evolve. Empirical studies support that financial innovation can improve financial intermediation. For example, a study in Nigeria on the "Nexus Between Financial Innovation and Financial Intermediation in Nigeria's Banking Sector" (Ejinkonye & Okonkwo, 2021) examines how innovations such as ATMs, mobile banking, POS, and internet banking relate to banks' deposit mobilization, which is a core intermediation function. They found that some innovations (e.g. ATMs) were significantly positively related to deposit mobilization; others less so. "Impact of Financial Innovation and Institutional Quality on Financial Development in Emerging Markets" finds that financial innovation, along with high institutional quality, positively influences financial development (which includes effective intermediation). Thus, financial intermediation theory provides both a way to understand the mechanisms (how innovations help to reduce cost, improve reach, reduce information asymmetry) and a benchmark for what successful innovation should do.

1.2 Empirical Review

Olanuga and Asogho (2024) in their study titled "Financial Innovation, Economic Growth and Sustainable Development " presented recent studies on the effects of financial innovation on economic growth and sustainable development in Nigeria. The financial sectors worldwide are becoming increasingly important and competitive. Therefore, in order to compete successfully, it is necessary to possess flexibility and adaptability to change, as well as a willingness to embrace innovation.

Financial markets are becoming more advanced and complex due to financial innovation, which helps direct capital towards productive sectors that are necessary for economic growth and development. The study employed time series data. Statistical data analysis techniques were employed to evaluate the secondary data on financial innovation. Research indicates that financial innovation has a significant impact on both economic growth and sustainable development in Nigeria. The study found that financial innovation variables have a positive effect. Therefore, financial institutions should prioritize easy and secure access to financial services when developing their financial innovation strategies. Regulatory bodies, on the other hand, should establish a regulatory environment that promotes innovative solutions capable of influencing economic growth and sustainable development.

Ejinkonye and Okonkwo (2021) in their study titled "Nexus Between Financial Innovation and Financial Intermediation in Nigeria's Banking Sector" evaluated the relationship between financial innovation and financial intermediation in Nigeria. It seems that banks in Nigeria may have a problem of deposit-loan mismatch and losing customers to start-ups given increasing cost of deposits attributable to disruptive practice arising from financial innovations. The specific objectives of this study were to examine the relationship between financial innovation (value of the automated teller machine, internet banking, mobile banking, point of sale transactions) and financial intermediation (commercial banks deposit mobilization) in Nigeria for the period 2009–2018. This study was anchored on the financial innovation theory of Joseph Schumpeter, which states that technology creates opportunities for new profits and super profits as a result of increased investment by banks or financial institutions on products of innovation.

The ordinary least square was used to estimate the parameters. The data used were extracted from the Central Bank of Nigeria statistical bulletinThe results show a positive and significant relationship between financial innovation (ATM usage) and financial intermediation in Nigeria, while internet banking and mobile banking show positive but insignificant relationships. Point of sale (POS) transactions show no positive or significant relationship.The f-test result showed that financial innovations proxies jointly related significantly to commercial banks' deposits.

The work concludes that financial innovations contributed to commercial banks' deposits in Nigeria. The researchers recommended among others that banks should improve on the security of transactions done on their platforms, continue to improve and partner with start-ups in technological infrastructure, improve on power and network stability, deploy more innovative products, and improve on the efficiency of bank staff by regular training.

Sanga and Aziakpono (2025) in their study titled "FinTech developments and their heterogeneous effect on digital finance for SMEs and entrepreneurship: evidence from 47 African countries" examined whether FinTech developments heterogeneously contribute to the growth of digital finance for SMEs and entrepreneurship in 47 African countries from 2013 to 2020.The paper uses a novel method of moments quantile regression, which deals with heterogeneity and endogeneity in diverse conditions for asymmetric and nonlinear models. The empirical results reveal that the rise of FinTech companies offering services in Africa heterogeneously increases digital finance for SMEs and entrepreneurship in their different stages of growth. FinTech developments have a strong and positive impact in countries with higher levels of digital finance than those with lower levels.

FinTech developments and digital finance positively and significantly influence entrepreneurship in Africa, particularly in the nascent and transitional development stages of entrepreneurship. Institutional quality has a considerable positive moderating effect when used as a control rather than an interaction variable. The results suggest the need to promote FinTech developments in Africa: to provide a wide range of alternative digital finance schemes to SMEs and to promote entrepreneurship, especially in countries where entrepreneurship is in the nascent and transitional development stages. The results also underscore the need to promote FinTech development through supportive regulations and institutional quality to reduce risks related to FinTech and digital financing schemes.

Okoli and Tewari (2021) in their study titled "Does the Adoption Process of Financial Technology in Africa Follow an Inverted U-Shaped Hypothesis? (Okoli & Tewari, 2021)" investigates non-linear/inverted U-shaped Fintech adoption process among a panel of 32 African countries spanning from 2002–2018.

The study argues that Fintech adoption in Africa will continue to rise and not follow the inverted U-shaped process if sustained through greater trade openness. The dynamic system GMM techniques found a strong evidence for an inverted U- shaped adoption process for the 32 African markets and 24 frontier African markets but violated among the emerging (N = 3) and fragile (N = 5) groups. The first lag of Fintech compatibility and the contemporaneous levels of relative- advantage, complexity, trial-ability and observe-ability were its main determinants. The study concludes that Fintech will be replaced with new innovations in future irrespective of possible sustainability strategy. The need to strengthen African financial markets' innovativeness to have a competitive edge on Fintech's replacement is stressed.

Alabi and Okoye (2022) in their study titled "The Effect of Technology Adoption on Financial Inclusion: A Cross-country Panel Analysis between China and Nigeria" examined the effects of Technology Adoption on Financial Inclusion with focus on Automated Teller Machines, Internet usage and Mobile Cellular subscriptions as the major drivers in a cross-country analysis between China and Nigeria. The study employed Pooled OLS and Feasible Generalized Least Squares estimators. Financial Inclusion is represented by number of depositors with Commercial Banks per 1,000 adults' population. The results reveal that Automated Teller Machines, Internet usage and Mobile Cellular Subscriptions exert insignificant positive effects on Financial Inclusion both in China and Nigeria. The technology variables however exert significant positive impact on Financial Inclusion as represented by other dummy countries in the Panel. The study also found that GDP growth rate has significant negative relationship with Financial Inclusion in China and Nigeria as well as the rest of the world as represented.

David-West, Oni and Ashiru (2022), in their study on mobile money and financial inclusion in Nigeria, used a mixed-method approach incorporating both supplier and consumer perspectives through documentary analysis, focus groups, interviews, and surveys.

Relying on the diffusion of innovations theoretical framework, the study explores the utility of mobile money not only to assess its role in enhancing financial inclusion, but also to better tailor current applications for low-income users.

The study identifies four key factors hindering the diffusion of mobile money: lack of customer demand and experimenters, lack of integration in the ecosystem, lack of trust and preference for effective local savings schemes, and policy short-termism leading to operational unsustainability.Our paper reveals interest dynamics that can advance a more long-term mobile money regulatory policy which takes care of the concerns of the unbanked poor.

1.3 Gaps in the Literature and Emerging Issues

Financial innovation has attracted growing academic attention; however, several key gaps continue to exist. One such gap is the limited integration of Business Education (curriculum, pedagogy) in studies of financial innovation. Firstly, there is little empirical work on how business education (in universities, tertiary institutions) embeds financial innovation topics (fintech, blockchain, digital finance) into curricula; how well students are prepared for financial innovation environments; how pedagogies (e.g. experiential learning, case-based learning, projects) contribute. Secondly, there is significant skills and competencies gap as many studies report that innovation in financial systems demands new skills digital literacy, regulatory understanding, risk management in digital context but few studies focus on whether business education is responding to these demands. In addition, there is a deficit in empirical studies linking Business Education to financial innovation outcomes.

While studies exist in financial literacy linked to education, or financial intermediation, fewer exist that connect business education interventions (courses, modules, pedagogical methods) to actual adoption or performance of financial innovation in firms or in financial institutions. Furthermore, many empirical studies come from Africa broadly, some from Nigeria, but less from many other emerging economies; also less work on intra-country differences (urban vs rural, institutions vs informal sector) especially in Business Education. In addition, there is a need for more longitudinal work on how financial innovation evolves over time in relation to educational trends, regulation, technology; how schools adapt, which innovations are sustained, which fail.

From theory and empirical work, some propositions emerge. Firstly, financial innovation can be both a driver of growth (through improving intermediation, lowering costs, increasing access) but also a source of risk/disruption requiring governance. The Schumpeterian and financial intermediation theories help explain mechanisms. Furthermore, in emerging economies, including Africa and Nigeria, fintech, mobile money, digital banking etc., have shown positive effects on inclusion, SME finance, entrepreneurship—but with heterogeneity, i.e. not all innovations or contexts yield the same outcomes. Also, strong institution quality, regulatory frameworks, infrastructure (ICT, internet, mobile access), trust, and human capacity (skills, education) seem to be consistent enablers. In addition, Business Education is under-explored as a lever for shaping how well financial innovation is adopted, diffused, governed, and leveraged. There is potential for business schools, training institutions, and tertiary institutions to play significant roles by equipping students and practitioners.

Financial innovation is a dynamic and evolving field, combining theories from economics (Schumpeter, financial intermediation), innovation studies (diffusion, adoption), and technology adoption. In emerging economies, there is solid empirical evidence that financial innovation (fintech, mobile money, etc.) contributes positively to growth, financial inclusion, and SME development—but with heterogeneity arising from institutional quality, infrastructure, skills, regulation, trust, etc. However, there remains a substantial gap in linking this with Business Education: how tertiary / business schools prepare students and practitioners for financial innovation; what curriculum, pedagogy, competencies are in place; and whether such educational interventions affect innovation outcomes. Addressing these gaps is important for both academic understanding and policy, especially in emerging economies where financial innovation may be a key route to development, inclusion, and economic growth. Bridging this divide requires a multidisciplinary approach that integrates financial, technological, and educational reforms. Strengthening the role of business education could significantly enhance the effectiveness, sustainability, and governance of financial innovation efforts.

2. NATURE AND DRIVERS OF FINANCIAL INNOVATION

Financial innovation takes many forms: new payment rails and instruments (mobile money, e-wallets), process innovations (algorithmic credit scoring, robo-advisors), structural innovations (marketplaces and platform finance), and regulatory- or policy-driven changes (sandboxes, open banking frameworks). Conceptually, innovations can be incremental (cost and efficiency improvements to existing services) or radical (new value propositions that reconfigure markets). Recent reviews emphasise that modern financial innovation is highly technology-mediated, data-driven, and platform-centric — blending technological capability with regulatory adaptation and business model design. AI and machine learning have transformed risk assessment, customer engagement, fraud detection, and personalization. Banks and fintechs apply supervised and unsupervised learning to alternative data (mobile phone usage, transaction histories, social signals) to build credit-scoring models that serve customers previously excluded from formal credit markets. AI also powers chatbots, virtual assistants, and dynamic pricing models, reducing transaction costs and enabling 24/7 services. Recent empirical and review studies show that AI adoption in banking improves operational efficiency and can enable new product types, but also raises challenges around explainability, bias, and regulatory oversight (Gyau et. al, 2024).

Blockchain's promise lies in decentralised record-keeping, cryptographically secure transfers, and potential reductions in reconciliation costs for interbank settlement and trade finance. Use cases include tokenization of assets, programmable smart contracts, and cross-border payment corridors. However, researchers and practitioners caution that blockchain is not a panacea; its comparative advantage depends on trust models, throughput/cost trade-offs, and regulatory clarity. For low-cost retail payments and inclusion efforts, simpler mobile-money architectures have often been more effective than public blockchains (Kou, 2025). Mobile phones and mobile network infrastructure have arguably been the most consequential technological enabler for inclusion and payments in many emerging economies. Mobile money platforms convert basic handsets into financial access points, enabling deposits, transfers, and merchant payments without traditional bank branches.

The ubiquity of smartphones (and cheaper data) further enables app-based wallets, USSD services, and integrated value-added services (insurance, micro-credit). The OECD and World Bank document strong links between digitalization and broader access to financial services (OECD, 2024). APIs and cloud platforms have lowered the cost of building interoperable services, encouraging modular ecosystems (payment processors, lending platforms, accounting integrations). Open banking initiatives push incumbents to share customer-permissioned data with third parties, unlocking competition and product innovation while requiring robust privacy and security frameworks. The result is an environment where fintech startups can rapidly compose services on top of legacy infrastructure (OECD, 2024). Financial inclusion access to useful and affordable financial products and services is both a development objective and a market opportunity. In many low- and middle-income countries, large unbanked populations and informal-sector dynamics create strong demand for low-cost, accessible payment and savings mechanisms. Mobile money has demonstrably increased account ownership and transaction activity in Sub-Saharan Africa, catalyzing small business activity, formalization, and household resilience. The World Bank's Global Findex and related reports emphasize mobile account adoption as a central pathway to inclusion, attributing rapid gains to mobile-enabled payments rather than traditional branch expansions. Thus, inclusion goals have directly stimulated product design (USSD, cash-in/cash-out agent networks, micro-savings) targeted at low-income, rural, and previously excluded users (World Bank, 2024).

3. IMPLICATIONS FOR BUSINESS EDUCATION

Business education is at a crossroads. The accelerating pace of digital transformation—driven by FinTech, blockchain, artificial intelligence, and data analytics—means that graduates must be prepared not only in traditional managerial theory but also in the tools, methods, and mindset of the digital economy. For business schools to remain relevant and impactful, they must rethink curricula, pedagogy, and partnerships. One key area of implication pertains to curriculum reform and embedding fintech, digital finance, blockchain and analytics.

Historically, business curricula have emphasized accounting, finance, marketing, operations, strategy, and management. While these remain foundational, they must now be complemented by modules that reflect the realities of a digital financial ecosystem. As Chen et al. (2020) note, FinTech education is inherently interdisciplinary encompassing finance, technology, regulation, and strategy requiring collaboration across departments (Anilkumar and Laxmana, 2024). The urgency of updating curricula is also underscored by institutional analyses such as those from AACSB, which argue that business schools must revisit priorities in the face of shifting learner demographics, digital disruption, and stakeholder expectations.

Some core themes that can be incorporated include, but are not limited to; fintech and digital finance, blockchain and distributed ledger technologies, financial analytics and data science, interdisciplinary integration as well as ethics, governance and regulations. Fintech and digital finance includes topics such as peer-to-peer lending, digital payments, robo-advisors, mobile money, crowdfunding, and embedded finance. On the other hand, Blockchain and Distributed Ledger Technologies include the fact that the curriculum should cover blockchain fundamentals (consensus protocols, smart contracts, tokenomics) and their business applications (supply chain, digital identity, DeFi).

Instructors may use “sandbox” environments or private blockchain deployments to let students experiment. Zalan and Toufaily (2017, mentioned by Chen et al.) point out that fintech labs and sandbox environments enhance experiential understanding (Anilkumar and Laxmana, 2024). Financial analytics and data science includes courses in data analytics, machine learning for finance, predictive modeling, natural language processing for sentiment analysis, and algorithmic trading are essential. Also, students should become comfortable with programming tools (e.g. Python, R), data visualization, and large-scale datasets. Interdisciplinary integration entails the fact that curricula should intentionally integrate technology (e.g. computer science or information systems) with business domains. Osabute et al. (2023) argue that FinTech advances require transdisciplinary approaches.

Ethics, governance and regulation are also another important factor due to the fact that because these digital tools involve issues of privacy, security, systemic risk, and regulation, courses must include modules on ethics, regulatory frameworks, and governance in digital finance.

Once curricula are revised, the next challenge is how to teach complex, evolving content effectively. Traditional lectures are unlikely to suffice; instead, blended and adaptive instructional strategies are needed. Blended learning combining face-to-face and online modalities allows flexibility, personalization, and scalability. Students may view lectures or modules asynchronously, freeing class time for discussion, problem-solving, or project work. The shift toward Education 5.0 envisions learner-centric environments supported by AI, virtual reality, and adaptive systems; business education must align with this paradigm (Ahmad et al., 2023). For example, educators can embed micro-lectures, quizzes, and interactive content in an online platform, reserving class time for deeper engagement. Blended models also allow for inviting remote guest lecturers from industry or regulators, regardless of location.

4. CASE STUDIES & PROBLEM-BASED LEARNING

Business education has long used case studies; but to handle FinTech, blockchain, and analytics, cases must be up to date and sometimes even in progress. Real-time or near-real-time case studies—drawing on current events in digital finance—help students engage with uncertainty and evolving contexts. For example, integrating news-based financial cases into courses has been shown to improve engagement and link classroom theory to ongoing market developments. Problem-based learning or challenge-based learning (CBL) frameworks further enhance student agency by asking learners to address real-world challenges (e.g. designing a digital payments solution for underserved markets). The principle of CBL is to anchor learning in authentic challenges that demand interdisciplinary thinking.

4.1 Simulations, Sandboxes, and Role Play

Financial simulations and fintech sandboxes give students hands-on exposure in a safe environment. For instance, simulated trading platforms allow learners to test algorithmic strategies without real financial risk. In addition, blockchain sandboxes allow students to deploy smart contracts, test consensus protocols, or build small decentralized applications. Also, regulatory role-play exercises can simulate interactions between fintech firms, banking regulators, and consumers. Such experiential approaches help students internalize complex dynamics rather than simply memorizing theory.

4.2 Agile and Scrum-Inspired Pedagogies

Agile approaches to teaching—breaking a semester into sprints, allowing iterative feedback, embracing change—can align well with fast-evolving content. Neumann and Baumann (2021) describe adopting an "eduScrum" approach in higher education, combining real-world projects from partner organizations with agile pedagogy. Students organized into cross-functional teams worked in sprints, iteratively delivering value and adapting as new information emerged. The method improved student engagement and relevance. arXiv Given the rapid shifting of fintech tools, adopting agile pedagogy helps classes remain responsive; instructors can pivot modules, include new tools or cases midstream, and allow student-led exploration.

4.3 Capstone & Integrative Projects

Capstone projects that require students to propose and execute a fintech or digital finance initiative—often in alliance with real partner organizations are a powerful integrative tool. Students may, for example, design a mobile money extension or a micro-lending algorithm and pitch to real investors or institutions. Project management methods, threaded across the curriculum, help students develop structure and discipline in working on real problems. Fullick-Jagiela et al. (2023) discuss embedding project management practices to foster problem-solving, critical thinking, and teamwork across business curricula.

5. OPPORTUNITIES AND CHALLENGES

The rapid expansion of digital technologies, fintech innovations, and blockchain applications has reshaped not only the global financial ecosystem but also the landscape of business education. Business schools are no longer preparing graduates solely for traditional careers in banking, management, or accounting. Instead, they are tasked with equipping students to navigate a dynamic environment defined by digital finance, entrepreneurship, cybersecurity, and global interconnectedness. The intersection of fintech and education presents significant opportunities for enhancing entrepreneurship, driving financial inclusion, and creating new job markets. However, it also brings formidable challenges in the form of cybersecurity threats, infrastructural limitations, a widening skills gap, and regulatory uncertainties. Pertaining to opportunities, digital transformation has created fertile ground for entrepreneurship. Fintech innovations, mobile payments, and digital marketplaces enable students and graduates to explore entrepreneurial ventures with relatively low entry barriers.

According to Li et al. (2021), fintech has democratized access to capital and resources, reducing dependence on traditional financial intermediaries. Platforms such as crowdfunding, peer-to-peer lending, and digital wallets allow small businesses and startups to access financing more efficiently. For business education, this entrepreneurial environment provides a unique opportunity to integrate innovation and startup culture into curricula. Students can learn not only the principles of entrepreneurship but also apply them in fintech contexts, developing prototypes of mobile apps, blockchain solutions, or payment gateways. Hackathons and startup incubators hosted by universities have become effective methods of fostering entrepreneurial skills (Mhlanga, 2020). These activities not only train students in creativity and problem-solving but also encourage real-time collaboration with investors and industry players. Furthermore, fintech entrepreneurship supports small and medium enterprises (SMEs) by providing easier access to alternative finance. Business schools that emphasize digital entrepreneurship can produce graduates who contribute to the development of inclusive economies and sustainable innovation ecosystems. This approach strengthens the link between education and real-world impact.

Another opportunities is the promotion of financial inclusion. One of the most transformative opportunities presented by fintech is its potential to drive financial inclusion, particularly in emerging markets. According to Demirgüç-Kunt et al. (2018), access to digital financial services has significantly increased participation in the global economy, enabling millions of unbanked individuals to engage in transactions, savings, and credit activities. Mobile money services such as M-Pesa in Kenya and Paga in Nigeria illustrate how fintech can bridge gaps in financial access. For business education, this presents both a teaching and research opportunity. Students can explore real-world case studies of how digital finance impacts marginalized communities, and they can develop projects aimed at extending inclusion through innovative digital solutions.

Educational institutions also have the chance to promote social entrepreneurship, training students to design fintech applications that prioritize the underserved. Business schools can partner with fintech firms and microfinance institutions to give students experiential learning opportunities that combine commercial viability with social impact. The promotion of financial inclusion also reshapes the ethical and social responsibilities of business education. Training future managers and entrepreneurs to view inclusion as both a business opportunity and a societal imperative enhances the value of education in producing socially responsible graduates.

Creation of new job markets in fintech is also another veritable opportunity stream. Fintech is one of the fastest-growing job markets globally. The demand for professionals in areas such as data analytics, cybersecurity, blockchain development, and digital product management has skyrocketed. The World Economic Forum (2020) identified fintech and digital finance as top sectors contributing to the "jobs of tomorrow," requiring interdisciplinary skillsets that combine business acumen with technical proficiency. This creates an opportunity for business schools to realign their offerings to meet labor market needs. Integrating modules on artificial intelligence in finance, blockchain applications, and regulatory technology (RegTech) can help students secure positions in this rapidly expanding sector. This shift also calls for updated curricula that reflect the latest industry trends.

Additionally, fintech job markets encourage collaboration between business schools and industry stakeholders. Partnerships with fintech startups, banks, and consulting firms allow universities to design curricula that reflect industry demands. According to Gomber et al. (2018), industry–academia collaborations are vital in closing the employability gap in digital finance. New job markets also extend beyond traditional employment. Graduates may pursue freelance roles in fintech consultancy, app development, or financial analytics, promoting more flexible and decentralized career paths. For business education, preparing students to thrive in both structured corporate environments and entrepreneurial ecosystems enhances adaptability and resilience.

5.1 Challenges Limiting Effective Integration of Fintech

Fintech is expanding rapidly and creating immense opportunities; however, it also presents significant challenges. Firstly, the increasing reliance on digital systems in finance introduces significant cybersecurity concerns. Fintech platforms often manage sensitive customer data, making them prime targets for cybercriminals. According to the International Monetary Fund (IMF, 2020), cybersecurity risks in fintech are a growing systemic threat, with potential consequences for financial stability. For business education, this presents a dual challenge. First, curricula must incorporate cybersecurity literacy, ensuring students understand the risks and prevention mechanisms associated with digital finance. Second, institutions themselves must safeguard their digital learning platforms and fintech labs against attacks. As Jagtiani and John (2018) note, the success of fintech depends not only on technological innovation but also on the trust and security embedded within financial systems. Cybersecurity also has ethical and legal dimensions. Business graduates must be trained to consider data privacy, compliance with international regulations such as GDPR, and the reputational risks associated with breaches. However, not all institutions have the resources or expertise to adequately train students in cybersecurity, widening the knowledge gap.

5.2 Structural and Regulatory Barriers to Fintech Education

A significant challenge in some regions is the lack of infrastructure. While fintech is revolutionizing finance in many parts of the world, infrastructural challenges remain, especially in developing economies. Limited internet penetration, unreliable electricity supply, and insufficient digital infrastructure hinder the adoption of fintech and, by extension, the integration of fintech into business education. In sub-Saharan Africa, for example, mobile money has achieved remarkable success, but disparities in infrastructure mean rural areas often lag behind urban centers (Asongu & Odhiambo, 2019). Business schools in regions with infrastructural deficits face difficulties in offering hands-on fintech education. Without reliable internet and modern computing facilities, students may be confined to theoretical knowledge without practical exposure. Furthermore, disparities in infrastructure contribute to inequality among institutions. Elite universities with advanced facilities can offer fintech labs, blockchain simulations, and data analytics training, while underfunded schools may struggle to provide even basic digital access. Skill gap among educators and students is also another significant challenge to rapid fintech expansion. The skills gap is one of the most persistent challenges in integrating fintech into business education. Many educators were trained in traditional business models and lack expertise in emerging areas such as blockchain, data science, or digital finance. As a result, they may struggle to deliver relevant content or rely heavily on outdated materials (Nweke & Chinedu-Eze, 2022).

On the student side, digital literacy levels vary significantly. While some students are highly tech-savvy, others struggle with basic computational skills. This creates uneven learning experiences and limits the effectiveness of innovative teaching strategies such as simulations or fintech labs. Addressing the skills gap requires substantial investment in faculty development, industry collaboration, and curriculum redesign. Initiatives such as faculty training programs, co-teaching with industry practitioners, and continuous professional development are necessary. However, these require resources that may not be available to all institutions, particularly in resource-constrained regions.

Regulatory Uncertainties is also another significant challenge. The regulatory landscape for fintech is complex and often inconsistent across jurisdictions. Innovations such as cryptocurrencies, peer-to-peer lending, and digital assets frequently outpace regulatory frameworks, creating uncertainty for entrepreneurs, investors, and educators.

Arner et al. (2017) describe this as a "regulatory trilemma," where regulators must balance financial stability, consumer protection, and innovation. For business education, regulatory uncertainty poses multiple challenges. First, it complicates the design of curricula, as educators must teach evolving rules that vary globally. Second, it creates difficulties in preparing students for real-world practice, since strategies that are permissible in one jurisdiction may be illegal in another. Third, it can deter partnerships between business schools and fintech firms, as regulatory risks may discourage experimentation. At the same time, regulatory uncertainty offers an opportunity for business education to lead in policy research and advocacy. Business schools can serve as platforms for dialogue between regulators, fintech firms, and the public, producing research that informs balanced and adaptive policies. Nevertheless, without stable regulatory environments, the ability of business education to fully embrace fintech remains constrained.

6. BALANCING OPPORTUNITIES AND CHALLENGES

The opportunities and challenges of fintech in business education are closely intertwined. Entrepreneurship, financial inclusion, and new job creation are often limited by infrastructural deficits, skills gaps, and regulatory uncertainties. Similarly, while fintech opens avenues for experiential learning and industry collaboration, cybersecurity risks demand careful management. To maximize opportunities and mitigate challenges, business schools must adopt holistic strategies:

1. Curriculum Innovation Embedding fintech, blockchain, and cybersecurity modules.
2. Faculty Development Continuous training and collaboration with industry experts.
3. Infrastructure Investment Securing funding for digital labs and reliable networks.

4. Policy Engagement Encouraging research and dialogue to shape fintech regulation.
5. Inclusive Pedagogy Ensuring all students, regardless of digital literacy, gain exposure to fintech concepts.

The digital revolution has redefined the purpose and content of business education. Fintech presents remarkable opportunities for enhancing entrepreneurship, promoting financial inclusion, and creating new career pathways. However, the sector also faces pressing challenges, including cybersecurity risks, infrastructural deficits, skills shortages, and regulatory uncertainties. The ability of business education to seize opportunities while navigating challenges will determine its relevance in preparing future business leaders. By embracing innovation, fostering collaboration, and addressing systemic gaps, business schools can position themselves as critical drivers of digital transformation. Ultimately, the goal is to ensure that graduates are not merely consumers of technology but leaders who harness fintech for sustainable economic and social impact.

7. CASE STUDIES AND PRACTICAL INSIGHTS

Nigeria: The Rise Of Mobile Payments (Paga, Opay)

Nigeria's fintech scene expanded rapidly during the 2010s and exploded after 2015, driven by smartphone penetration, improving internet access, and large unbanked segments seeking convenient payment options. Paga and OPay exemplify two different but complementary models. Paga began as a payments and remittance platform targeting both banked and unbanked customers through an agent network and simple mobile interfaces that enabled transfers, bill payments, and merchant acceptance.

OPay, initially launched as part of broader app ecosystems, combined digital wallets with an extensive agent network and on-the-ground services (cash-in/cash-out), aggressively pursuing scale and retail presence (JM S eleyon, 2024). Empirical work on Nigeria shows mobile payment platforms have contributed to expanding financial access, especially when combined with agency banking and USSD options that do not require smartphones (IIARD study, 2025). However, challenges remain: intermittent infrastructure, regulatory friction, fraud risk, and consumer trust issues.

Fintechs like Paga and OPay mitigate some barriers by blending digital onboarding with human agents and partnerships with banks and merchants; this hybrid model has proven resilient in contexts where pure digital adoption is slower (BDO Africa, 2024). This approach not only increases accessibility but also fosters greater user confidence in digital financial services. Continued investment in infrastructure and regulatory support will be crucial for sustaining growth and inclusion in Nigeria's fintech sector.

Kenya: M-Pesa As A Model Of Financial Inclusion

M-Pesa's rollout in Kenya provides one of the clearest global examples of mobile money achieving mass adoption and measurable impacts on poverty and inclusion. Since its commercial launch in 2007, M-Pesa's agent networks and simple SMS/USSD interface allowed millions to send, receive and store value without traditional bank accounts. Case studies and empirical analyses through the 2010s and into the 2020s indicate M-Pesa boosted financial access, improved household risk-sharing, and contributed to small business activity and welfare improvements (Ndung'u, 2021; Fabregas et al., 2022).

Some research attributes modest reductions in extreme poverty to the platform's liquidity and transfer capabilities (Fabregas et al., 2022; Reach Alliance, 2021). But M-Pesa's story also points to limits. While account ownership rose sharply, usage intensity and savings behavior varied by income and gender; service quality, fees, and agent liquidity occasionally constrained use. Regulators and providers learned that ubiquity of simple access (feature phones + agents) plus a regulatory environment that allowed innovation were key to success (Osabutey, 2024). M-Pesa's lesson for other markets is that context-appropriate technology (not necessarily smartphones or apps), coupled with distribution and trust, drives inclusion.

India: UPI, Digital Payments and Financial Literacy Initiatives

India's Unified Payments Interface (UPI), launched in 2016 and scaled rapidly through interoperable real-time payments, represents a different pathway: high-tech, interoperable infrastructure that removed frictions in merchant and person-to-person payments.

UPI's architecture—open APIs, bank interoperability, and instant settlement—made it easy for diverse apps to offer payment rails, fueling explosive growth in transaction volumes and financial access (Cornelli et al., 2024). By 2020–2024, UPI became central to India's digital payments ecosystem, facilitating not only urban e-commerce but also rural merchant payments via QR and offline modes. Research and policy reviews note UPI's contribution to inclusion, though complementary measures (financial literacy, device access, and merchant onboarding) determined impact depth (BIS, 2024). Importantly, India paired infrastructure expansion with digital literacy initiatives and regulatory nudges that encouraged safe usage and consumer protection. The combined approach—world-class payment rails plus literacy and oversight—offers a template for scaling digital payments while mitigating fraud and exclusion.

7.1 How Business Education is Adapting (or lagging)

Business Education programs face a classic challenge: curricula and pedagogy change more slowly than industry. In Nigeria and many African countries, universities have begun to introduce fintech modules, short courses, and industry partnerships, but uptake is uneven. Recent surveys and reports emphasize a growing push to embed fintech topics (digital payments, regulatory tech, analytics) into entrepreneurship and finance courses, and to use applied methods (case studies, hackathons, industry placements) (Stouraitis & Tsanis, 2025; Shino, 2022). Yet many programs still offer only "awareness" modules rather than deep, hands-on training in payments infrastructure, regulatory frameworks, or product design. In Kenya, the M-Pesa example has stimulated research and case teaching, but formal curricula sometimes lag practical innovation: graduates may understand theory of financial inclusion but lack practical skills for agent management, risk controls, or designing low-touch UX for feature-phone users (Osabutey, 2024). India's rapid UPI adoption has prompted top institutions and professional programs to create fintech specializations and short courses (Cornelli et al., 2024), but scale and access remain challenges: many regional colleges have limited capacity to teach the technical and regulatory intricacies.

CONCLUSION

Financial innovation has emerged as a powerful driver of economic transformation, reshaping how individuals, businesses, and governments access, manage, and utilize financial resources. From mobile banking platforms to blockchain applications, innovation continues to break down barriers to financial inclusion, enhance efficiency, and stimulate entrepreneurial activity across both developed and emerging economies.

This progress highlights the critical importance of financial innovation in not only improving competitiveness but also creating pathways for sustainable development. However, the benefits of financial innovation cannot be fully realized without a deliberate effort to align Business Education with these rapid changes. Business Education must evolve beyond traditional approaches, integrating digital competencies, financial technologies, and experiential learning into curricula to adequately prepare students for dynamic market realities. If educational institutions lag, a widening skills gap may emerge, leaving graduates underprepared for the demands of a fintech-driven economy. The opportunities that financial innovation presents such as enhancing entrepreneurship, deepening financial inclusion, and generating new job markets are substantial. Yet, these opportunities are tempered by challenges including cybersecurity threats, inadequate infrastructure in some regions, regulatory uncertainties, and the pressing need to upskill educators and learners. Balancing these dynamics requires thoughtful strategies at both institutional and policy levels.

Going forward, future research should focus on curriculum innovation that embeds financial technology and digital literacy into Business Education programs. Equally vital is the exploration of models for industry-education collaboration, ensuring that universities and training institutions work closely with fintech firms, policymakers, and businesses to develop relevant, future-ready skills. By bridging this gap, Business Education can serve as a catalyst for equipping graduates who not only adapt to financial innovation but also drive it, thereby contributing meaningfully to sustainable economic growth and inclusive development.

REFERENCES

Ahmad, S., Umirzakova, S., Mujtaba, G., Amin, M. S., & Whangbo, T. (2023). Education 5.0:

Alabi, A. W., & Olaoye, F. O. (2022). Effect of Technology Adoption on Financial Inclusion: A among students in Nigerian universities. Journal of African Business, 23(3), 400–420.

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). Fintech and regtech: Impact on regulators and banks. Journal of Banking Regulation, 19(4), 1–14

Asongu, S. A., & Odhiambo, N. M. (2019). Mobile money innovation and inclusive banking: Examining the role of AI technology innovation in boosting banks financial

BDO Africa. (2024). Fintech in Africa report (June 2024). BDO.

Bontadini, F; Filippucci, F; Jona-Lasinio, C; Nicoletti, G & Alessandro Saia, N (2024). Digitalization. Business Digital Journal, 21(1).

Chen, X., Gomber, P., Koch, J.-A., & Siering, M. (2020). The emergence of fintech in higher

Cornelli, G., et al. (2024). Faster digital payments: Global and regional perspectives (BIS Cross-country Panel Analysis between China and Nigeria. European Journal of Business Database 2017: Measuring financial inclusion and the fintech revolution. World Bank.

David-West, O., Oni, O., & Ashiru, F. (2022). Diffusion of Innovations: Mobile Money Utility

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). The Global Findex development in Africa: Evidence from panel data. World Development, 123, 104629.

Ejinkonye, R. C., & Okonkwo, I. V. (2021). Nexus Between Financial Innovation and Financial evidence. Technological Forecasting & Social Change. ScienceDirect

Fabregas, R., et al. (2022). Mobile Money and Economic Activity: Evidence from Kenya. PLoS financial inclusion. International Journal of Financial Studies, 8(3), 45.

Flutterwave. (2024). Flutterwave 2024 report & year-in-review. Flutterwave. (Company report Follow an Inverted U-Shaped Hypothesis A Evaluation

of Rogers Diffusion of Innovation from China. Small Business Economics, 56(4), 1517–1538.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution:

IIARD. (2025). Impact of mobile payments on financial inclusion in Nigeria. Journal of IMF. (2024). Financial Access Survey: 2024 highlights (International Monetary Fund).

International Monetary Fund (IMF). (2020). Cybersecurity risk supervision. IMF. Interpreting the forces of innovation, disruption, and transformation in financial services.

Jackson, D., et al. (2023). Advancing Fintech through a transdisciplinary approach. PMC / NCBI.

Jagtiani, J., & John, K. (2018). Fintech: The impact on consumers and regulatory responses.

Khraisha, T., & Arthur, K. (2018). Can we have a general theory of financial innovation

Kou, G., et al. (2025). FinTech: a literature review of emerging financial technologies and their learning in business education utilizing project management practice and skills.

Li, Y., Spigt, R., & Swinkels, L. (2021). The impact of fintech on entrepreneurship: Evidence making that worse. Time. (Discussion of blockchain and financial inclusion challenges.) Management & Social Studies, 14(1), 34-51.

Mulili, Benjamin. (2022). Digital Financial Inclusion: M-PESA in Kenya. 10.1007/978-3-030-

Ndung'u, N. S. (2021). A Digital Financial Services Revolution in Kenya: The M-Pesa Case

Neumann, M., & Baumann, L. (2021). Agile methods in higher education: Adapting and using

Nweke, G. E., & Chinedu-Eze, V. C. (2022). Digital literacy and the adoption of fintech services

OECD. (2024). Digitalisation of financial services, access to finance and aggregate economic of financial services, access to finance and aggregate economic performance.

Okoli, T. T., & Tewari, D. (2021). Does the Adoption Process of Financial Technology in Africa

Olunuga, O. A., & Ashoghon, M. B. A. (2024). Financial Innovation, Economic Growth and One / PMC.

Osabutey, E. L. C. (2024). Mobile money and financial inclusion in Africa: Emerging literature. International Review of Financial Analysis 96 (2), 30 – 39.

Portuguez-Castro, M. (2024). Reimagining the future of business education through educational processes? A conceptual review. Financial Innovation, 4, Article 4.

Raelin, J. A. (2025). Bridging the gap: Work-based learning in business. Requirements, enabling technologies, and future directions. Research, 4(3), 162-179.

Roy, K., & Swargiary, K. (2024). Bridging the theory-practice gap in business education:

Seleyon. J.M (2024). An outlook from Opay microfinance bank Nigeria limited. Journal of Economics and Business, 100, 1–6. 5

Stouraitis, V., & Tsanis, K. (2025). Fintech as syllabus and support tool in entrepreneurship Study. African Economic Research Consortium. Emerging Markets Journal 21 (3) 9-15

TechCrunch. (2020). Stripe acquires Nigeria's Paystack for $200M+ to expand into African The Palgrave Handbook of FinTech in Africa and Middle East.

Time. (2019). Women worldwide struggle to access banking services—Blockchain is only

World Bank. (2024). Financial inclusion overview and Global Findex briefs. World Bank.

World Economic Forum. (2020). The future of jobs report 2020. World Economic Forum.

CHAPTER 2
EDUCATION CYBER RISK MANAGEMENT FOR MSMEs

[1]R. Nia MAROTINA
[2]Fajar SEPTIAN
[3]Agustyar NURFAISAL

[1]STAI Ki Ageng Pekalongan, niamarotina@gmail.com, ORCID ID: 0000-0002-7362-9761
[2]STAI Ki Ageng Pekalongan, ORCID ID: 0009-0003-0451-4455
[3]STAI Ki Ageng Pekalongan, ORCID ID: 0009-0009-7044-6079

INTRODUCTION

The development of information and communication technology (ICT) has had a revolutionary impact on the dynamics of the modern business world, including the Micro, Small, and Medium Enterprises (MSME) sector. Digital transformation, marked by the adoption of online services such as e-commerce, social media, and electronic payment systems, has opened up wider market access for MSME players, even enabling them to operate across regions without geographical barriers. This phenomenon provides significant opportunities to increase competitiveness, operational efficiency, and sustainable business growth.(Sulistyowati et al., 2025)

However, behind these conveniences, cases of information technology (IT) system hacking and data breaches affecting a number of businesses and government agencies are rampant. Most recently, 34 million passport holder data and 337 million population data in Indonesia were breached. According to the latest report from the National Cyber Security Index (NCSI) dated April 28, 2023, Indonesia's cybersecurity level is ranked 48th with a score of 63.64. There are 12 indicators used by the NCSI in the report, ranging from the development of cybersecurity policies and personal data protection to the fight against cybercrime (National Cyber Security Index, 2023). The Kaspersky report (2021) notes that MSMEs are one of the main targets of cyber attacks, mainly due to weak security systems and low awareness of the importance of digital data protection. (Anantadjaya, 2023). Low cybersecurity literacy among MSME players has resulted in a lack of effective risk mitigation strategies, making this sector vulnerable to data theft, system hacking, and disruption to business integrity and continuity.

Essentially, MSMEs are only users of Software as a Service (SaaS) companies such as marketplaces and other online-based services. The problem, according to an Accenture survey, is that nearly 80% of organizations introduce innovations faster than their ability to protect them. Government support in building cybersecurity and national cyber defense organically through a special agency with full authority to manage and handle cybersecurity, namely the National Cyber and Crypto Agency, does need improvement. Organically means that national security and defense are built by Electronic System Operators in a universal and sustainable manner.

This is because the implementation of strategies designed to build ideal cyber security for Indonesia has been hampered due to "(1) Institutional aspects that still need to be evaluated in achieving strategic objectives; (2) Aspects of the implementation of guidelines and operational standards; (3) procedures that have not been fully implemented; (4) human resources whose quality needs to be improved; (5) limited facilities and infrastructure as well as information systems that are not yet fully integrated (Ginanjar, 2022). he role of the government will be greatly needed in relation to providing cyber resilience, particularly in the industrial sector, especially small and medium-sized enterprises such as MSMEs, because at the global level, SMEs contribute to more than 90 percent of the business economy worldwide (World Bank Group, 2023). However, even though special institutions have been established by the government, the government cannot stand alone.

MSME entrepreneurs should still be able to assign one of the structures or institutions within their organization to be at the forefront of their digital transformation security, because ideal cyber resilience can only be built with the support of adequate cyber security awareness. This shows us that the implementation of cybersecurity must be integrated and not solely rely on the government's role in cybersecurity defense, which is very limited in terms of technical action on all aspects of business operators' operations. Cybersecurity resilience is necessary to ensure that operations can continue to run continuously and sustainably, even under attack or after an attack. Cybersecurity itself is a proactive action to mitigate risks in order to minimize the potential impact.(Balafif, 2023)

In this context, there is an urgent need to strengthen the capacity of MSMEs in facing digital risks. This can be achieved by improving understanding of security protocols, providing cyber literacy training, and implementing data protection policies that are in line with the principle of prudence. In addition, the development of adaptive and inclusive security systems is also an important part of supporting the digital resilience of MSMEs, especially in the midst of an increasingly digitized business ecosystem. Additionally, effective collaboration between the public and private sectors should be fostered to strengthen the digital security infrastructure of MSMEs.

This introduction serves as a basis for further examining the dynamics of cyber threats to MSMEs in the digital era, as well as formulating strategic steps that can be implemented practically and policy-based to build sustainable and responsive digital protection.

1. DEFINITION OF CYBER CRIME

The terms cyber and technology are rooted in the word technique, which comes from the Greek word Technikos, meaning skill or art. Meanwhile, the word logos conveys the meaning of principle or fundamental principle. These two terms were then adapted and used in the cyber realm, particularly in relation to software (Lestari, 2013)

Along with the era of globalization, the use of cyberspace has increased in almost all aspects of society. Cyberspace can be understood as a virtual environment where individuals and communities interact and connect through networks, especially the internet, to carry out various daily activities. This use is usually directed at specific objects or sectors in accordance with the objectives of its development (Indonesia, 2014)

Terminologically, cyber is often used as a synonym for cyberspace. This word originates from the concept of cybernetics. Initially, the term cyberspace was not intended to describe interactions carried out through computer networks. However, in 1990 John Perry Barlow began to expand its meaning by directly associating the term cyber with the internet.

The development of cyberspace has had mixed consequences. On the one hand, it has had a positive impact in terms of ease of access to information, communication, and efficiency of human activities. On the other hand, it has negative impacts in the form of potential misuse of technology, which is known as cyber crime. This crime includes various forms of legal violations and modus operandi that arise from the misuse of internet applications and networks. Therefore, it is crucial to implement robust cybersecurity measures and raise awareness to mitigate the risks associated with cybercrime.According to McDonnell and Sayers, cyber threats can be categorized into three main types, namely (Indonesia, 2014).

Hardware Threat

This threat arises when certain devices are installed or used in a system that can interfere with network performance and other hardware. The objectives can vary, ranging from damaging the system to weakening the existing technology infrastructure.

Software Threat

This threat occurs through the entry of malicious software (malware) that steals data, damages systems, or manipulates important information. This type of threat is often one of the most common cyber attacks encountered.

Data/İnformation Threat

This type of threat involves the dissemination or use of certain data and information for purposes that are detrimental to other parties. The misuse of this information can have serious consequences for individuals, organizations, and countries.

2. CYBER RISK MANAGEMENT CONCEPTS

Cyber crime risks can pose serious threats, including loss of data and information systems, disruption of activities, and various other forms of disruption that exploit computer networks and the internet. Meanwhile, risk management can be understood as a process of identifying and managing risks that organizations will inevitably face in their efforts to achieve their strategic objectives. Another definition explains that the essence of risk management is to increase control over areas that can influence results, while minimizing uncertainty in aspects that are beyond control, where the relationship between cause and effect is not fully visible.

Based on these two definitions, risk management is a continuous process that must be carried out throughout defense management activities, especially in dealing with cyber crime threats. Risk management serves to plan anticipatory measures in dealing with risks and uncertainties, so that the objectives that have been set can still be achieved optimally.

According to the Institute of Risk Management, there are several important elements in risk management, namely: (Bernstein, 1998)

1. Risk Assessment → the process of identifying, describing, and estimating potential risks.
2. Risk Evaluation → the stage of making decisions about significant risks that must be followed up, adjusted to the organization's risk appetite.
3. Risk Treatment → implementation of responses to risks through the selection of appropriate handling strategies.

The stages of risk management that can be applied to anticipate cybercrime include: (Bernstein, 1998)

Identify (Identification)

At this stage, cybercrime risks are identified periodically by examining the factors that trigger attacks. All potential threats that could cause losses are carefully mapped, then risk measurement is carried out based on two main aspects, namely the probability of occurrence and the impact it causes.

Assess (Assessment)

Risk assessment is carried out to measure the level of cybercrime threats to various aspects, especially national defense. Although difficult to measure directly, this level of risk can be analyzed using a risk matrix to illustrate the potential losses that may occur.

Treat (Treatment/Response)

The results of risk identification and assessment form the basis for determining treatment strategies. The actions chosen can be to accept, transfer, reduce, or avoid the risk. In the context of cybercrime, the steps generally taken are to minimize the potential for information and data theft, both at the individual and institutional levels.

Control

The final stage is to conduct continuous monitoring to assess the effectiveness of risk management implementation. At this stage, an early warning mechanism that can be accessed by security control authorities, such as the Ministry of Defense of the Republic of Indonesia, is required.

With an appropriate monitoring and adjustment system in place, efforts to anticipate cybercrime can be carried out quickly and measurably. Cyber risk management can be understood as a systematic process that aims to identify, assess, and control risks related to digital information systems and data owned by an entity. In the context of MSMEs, this risk management not only covers the security of hardware and software, but also customer information, transaction systems, and internal digital communications that are carried out every day. According (Mukhlis et al., 2024), good risk management practices involve assessing threats, identifying vulnerabilities, and implementing security controls that are appropriate to the capacity and needs of the organization.

For MSMEs with limited resources and technical knowledge, cyber risk management must be carried out efficiently and without complexity. Therefore, an approach that is easy to understand and implement without requiring high costs or advanced technical expertise is needed. Strengthening simple but effective cyber risk management can be the first step for MSMEs to build digital resilience in facing the challenges of a business world that is increasingly integrated with information technology.i.(Utami et al., 2024).

3. MSME DIGITALIZATION AND CYBER CHALLENGES

The ongoing digital transformation has encouraged thousands of MSMEs in Indonesia to start utilizing digital platforms such as marketplaces, social media, and app-based payment systems. The use of this technology does bring convenience and efficiency, but it also increases the risk of cyber attacks. Many MSME players are not yet aware that the customer information and transaction data they manage are valuable digital assets that are vulnerable to exploitation by irresponsible parties.. (Tayibnapis, 2021). This ignorance and negligence often leave MSMEs unprepared to face the ever-evolving digital threats.

Most MSME players in Indonesia do not yet have basic digital protection systems such as antivirus and data backup. Many also do not understand the importance of regular system updates and digital security training for their staff. In addition, budget constraints are a major obstacle that leads to low investment in cyber protection (Samsumar et al., 2025).

In fact, risks such as information leaks or identity theft can cause losses that are far greater than the costs required for preventive measures. Therefore, an educational approach is needed to encourage collective awareness so that MSMEs begin to make digital security an integral part of their daily business operations.

4. SWOT ANALYSIS OF MSME DIGITAL TRANSFORMATION STRATEGIES

Analysis of internal and external factors in SWOT Analysis from the business side as well as the adoption and utilization side of MSME digital transformation strategies. The cyber resilience framework strategy that is aligned with the business strategy of MSMEs in Indonesia is as follows: (Balafif, 2023)

Strength Factors of Digital Transformation for Indonesian MSMEs:

- Focus on customer satisfaction and trust
- Effective supply chain (lead time < 3 days)
- The marketplace in Indonesia is incremental (continuously growing);
- The prices of gadgets such as laptops and mobile phones are becoming more affordable;
- Free utilization of e-commerce through marketplaces
- Online platforms make business capital investment more affordable;
- Additional benefits from advertising, sponsorships, and promotions
- Reaching a wider consumer base;

Weaknesses of Digital Transformation of Indonesian MSMEs:

- Self-awareness of cyber security;
- The paradigm of cyber security as an expense rather than an investment;
- Lack of literacy and utilization of company valuation based on intangible assets, such as goodwill.

Opportunities for Indonesia's MSME Digital Transformation:

- Having a professional governance structure;
- Reducing the risk of human error and internal fraud
- Balancing profitability, efficiency, and solvency with a disruptive approach;
- Availability of telecommunications infrastructure in the form of wired and wireless networks as well as satellites that cover all SME areas;
- Existence of IT entrepreneur communities/human resources and free online training facilities
- Shift in the behavior of Indonesians from offline to online transactions.

Threats to the Digital Transformation of Indonesian SMEs:

- Hacker attacks can occur at any time
- Individual factors become dominant
- Increased time shifting process;
- Increased number of competitors
- Dynamic changes in youth market trends

5. CYBER RISK MANAGEMENT STRATEGIES FOR MSMES

Understanding risk is based on two main elements, namely probability and consequence. This is because risk is something that cannot be completely avoided, so a proper understanding of risk management is very important in formulating strategies. One of the tools used to assess risk is the Risk Matrix, which in the context of cyber crime assesses risk based on a combination of the probability of occurrence and the consequences it causes.

The risk matrix states that the higher the level of cyber crime risk, the greater the need to improve defense strategies. In other words, risk management is a fundamental component in strategy design, because through risk management, budget requirements for risk mitigation can be calculated. In efforts to ward off cyber crime, the expenses required to maintain the confidentiality of national information and data are not insignificant.

Therefore, the application of risk management enables the formulation of more effective and efficient strategies in dealing with these threats. In addition, risk also serves as an integrative metric for evaluating various alternative actions and prioritizing resource allocation. In the decision-making process, risks with the highest priority should receive funding and attention before risks with lower priorities.

Various literature suggests that there are a number of cyber risk management strategies that can be applied by MSMEs, even with limited resources. Some of these include using trusted free versions of firewalls and antivirus software, routinely backing up data to external storage or the cloud, and educating employees about types of digital threats such as phishing, spam, and malware. In addition, MSMEs are also advised to use transaction platforms that have integrated security systems such as encryption and two-factor authentication (Sulianta, 2025a).

Cyber resilience is an organization's preparedness to deal with business disruptions caused by such attacks, its ability to recover from chaos, and its systemic ability to adapt and evolve from each attack. This requires organizations to understand their internal operating environment and digital ecosystem. The summarized cybersecurity resilience approach and model constitute a managerial cybersecurity resilience framework due to its focus on managerial practices. In addition, this framework takes into account concepts such as reviewing digitalization capabilities based on the influence of digital technology on the acceleration of business processes, such as the use of heterogeneous resources (Mishra et al., 2007); Improvisational skills (Pavlou & Sawy, 2010); Access to information (El Sawy et al., 2010) and online knowledge (Rai et al., 2006); Continuously improving learning skills to evaluate progress in the digital environment and efficiently readjust resources through planning and preparation using competence, adaptation to context, and learning from experience, which are characteristics of digitalization skills (Gebremeskel et al., 2023).

5.1 Guiding Principles

The Indonesian MSME cyber resilience framework will be developed with reference to the current cyber security legal framework in Indonesia, which is based on the following principles: (Balafif, 2023)

1. Electronic Information and Transactions Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions. With several adjustments in accordance with PRESS RELEASE No. 17/HM/KOMINFO/02/2023 concerning the Second Amendment to the ITE Law for Harmonization with the Criminal Code [12]. Where the Minister of Communication and Information Technology stated that the ITE Law refers to the Budapest Convention on Cybercrime and updates criminal law provisions by providing a cyber context to criminal law provisions, and the Minister of Communication and Information Technology also stated that in accordance with Article 622 paragraph 1 letter r of the Criminal Code, there are provisions in the ITE Law that are revoked and declared invalid, including:

- The provisions of Article 27 paragraph 1 concerning decency and paragraph 3 concerning defamation and libel;
- The provisions of Article 28 paragraph 2 concerning hate speech based on SARA;
- The provisions of Article 30 concerning illegal access;
- The provisions of Article 31 concerning interception or wiretapping;
- The provisions of Article 36 concerning aggravated punishment for causing harm to others;
- The provisions of Article 45 paragraph 1 concerning criminal penalties for violations of Article 27 paragraph 1 concerning decency and paragraph 3 concerning criminal penalties for violations of Article 27 paragraph 3 concerning defamation and libel;
- Provisions of Article 45 paragraph 2 concerning criminal penalties for violations of Article 28 paragraph 2 concerning hate speech based on SARA;
- Provisions of Article 46 concerning criminal penalties for violations of Article 30 concerning illegal access;

- Provisions of Article 47 regarding criminal penalties for violations of Article 31 related to interception or wiretapping, and;
- Provisions of Article 51 paragraph 2 regarding criminal penalties for violations of Article 36 related to aggravated penalties for causing harm to others.

2. Ministry of Defense Regulation No. 82 of 2014 concerning Cyber Defense Guidelines.
3. Indonesian National Standard (SNI) IEC/ISO 27001:2013 requirements for the establishment, implementation, maintenance, and continuous improvement of an Information Security Management System (ISMS);
4. SNI ISO/IEC 27018:2016, Information technology – Security techniques Code of practice for the protection of personal information (PII) in public cloud services acting as PII processors;
5. Information Security Index (KAMI Index). An evaluation tool to analyze the readiness of information security in government agencies based on ISO/IEC 27001:2009 (Directorate General of Telematics Applications, 2013).

To achieve Cyber Resilience, companies must also develop the ability to mitigate and recover from attacks quickly while ensuring that essential business operations continue to run, even in degraded conditions or using alternative means, also known as Resilience. In general, it can be concluded that both resistance and resilience are two interrelated steps. The eight tasks involved in this work adjustment are based on the relationship between attack resistance and cyber resilience: (Balafif, 2023)

1. Identify the reasons for conducting an assessment. Clearly state the objectives and reasons for the assessment to all employees and clarify the scope of the assessment. It must cover areas where protected data is created, transmitted, and stored.
2. Identify the types of threats. Determine the types of threats faced, or events such as power outages or phishing;
3. Identify vulnerabilities. Find vulnerabilities in systems, networks, or applications that could compromise data;

4. Determine the likelihood of a breach occurring. Using the different stages of the risk assessment guide, determine the likelihood of a data breach occurring;
5. Determine the impact of the breach. Once you know the likelihood of a breach, you can determine the negative impact it will have on the company;
6. Determine the risk. Combining the likelihood and impact of threats will give you an idea of the business risk determination;
7. Evaluation results. Employees and management must be aware of the risk assessment results so they can begin to implement the recommended practices and policies;
8. Maintain assessment recommendations. Once the recommendations have been implemented, SMEs must take the appropriate steps to ensure that the risks have been mitigated.

However, the implementation of these strategies still faces various obstacles. The main obstacles come from limited funds, low priority given to security issues, and a lack of technical knowledge on the part of business owners and their employees. In many cases, SMEs only focus on increasing sales and operational efficiency, without realizing that digital security is also an important part of business continuity. Therefore, cyber risk management strategies must be designed in such a way that they do not burden SMEs, both in terms of cost and implementation, but are still able to provide adequate protection against digital risks (Sulianta, 2025b).

6. LITERATURE GAP ANALYSIS

A literature review shows that although there are many studies on cyber threats to MSMEs (Napu et al., 2024), There is still little in-depth discussion of risk management approaches that are truly applicable and suited to the characteristics of MSMEs in Indonesia. Most literature only provides general solutions or refers to practices implemented in developed countries, without considering local limitations such as low digital literacy, budget constraints, and uneven infrastructure. This has led to a gap between theory and actual implementation in the field.

There is still a void in studies evaluating the effectiveness of government policies in encouraging the implementation of digital security practices in the MSME environment. In fact, support in the form of strategic policies and incentives plays a crucial role in shaping business behavior while encouraging increased resource allocation for investment in cybersecurity. To address these challenges, it is necessary to develop new approaches that are more relevant and contextual, particularly those that take into account local characteristics and the limitations faced by MSMEs. Alternative approaches could include community-based models, region-specific training programs, or collective security systems that can be used jointly by groups of MSMEs in a single region (Hartatik et al., 2023).

CONCLUSION

The rapid progress of information and communication technology has become a major driver of change in the global economy, reshaping how businesses, including Micro, Small, and Medium Enterprises (MSMEs), operate and compete. In Indonesia, the digital transformation of MSMEs has brought about significant opportunities through the use of online marketplaces, social media platforms, and electronic payment systems. These tools have enabled business actors to transcend geographical boundaries, reach broader markets, and improve efficiency in ways that were previously unimaginable. The potential for growth and innovation within this sector is therefore immense, positioning MSMEs as crucial contributors to Indonesia's digital economy and sustainable development.

However, the same transformation that brings convenience and growth also introduces unprecedented risks. The rise of cyber threats such as hacking, phishing, data breaches, and ransomware highlights the vulnerability of MSMEs in the digital space. The increasing number of cyberattacks targeting both private and public sectors in Indonesia demonstrates the urgent need for a stronger and more integrated approach to cybersecurity. Indonesia's cybersecurity is fragile, evident from data leaks of millions and its moderate National Cyber Security Index ranking. MSMEs, lacking strong protection and cybersecurity knowledge, are especially vulnerable.

With cases involving the leakage of millions of population and passport data, Indonesia's cybersecurity infrastructure is shown to be fragile, as reflected in its moderate ranking on the National Cyber Security Index. MSMEs, which often lack robust protective systems and cybersecurity literacy, stand at the frontline of these risks. Their limited resources, combined with the perception of cybersecurity as a cost rather than an investment, further aggravate the situation and expose them to severe financial and reputational losses.

The government has recognized these challenges by establishing the National Cyber and Crypto Agency (BSSN) and issuing various regulatory frameworks such as the ITE Law, the Ministry of Defense Cyber Defense Guidelines, and ISO-based standards on information security. These measures represent important steps toward building a national framework for cyber resilience. Yet, despite these initiatives, institutional weaknesses, fragmented implementation, insufficient infrastructure, and a shortage of skilled human resources hinder the effectiveness of government-led cybersecurity policies. This indicates that while the role of the government remains vital, it cannot serve as the sole defender of the nation's digital ecosystem. MSMEs themselves must play a proactive role in securing their digital assets and building internal resilience.

The urgency of strengthening cybersecurity for MSMEs lies in the need to integrate risk management directly into their business strategies. Cyber risk management is not simply a technical matter but a strategic process that involves identifying potential threats, assessing their likelihood and impact, developing appropriate responses, and continuously monitoring and improving defenses. By employing tools such as the risk matrix, MSMEs can prioritize their limited resources to address the most pressing vulnerabilities. In practice, even simple measures such as using trusted antivirus software, implementing multi-factor authentication, conducting regular data backups, and training employees in cybersecurity awareness can significantly reduce exposure to cyber risks. These actions may appear basic, but for MSMEs with limited budgets and technical knowledge, they represent practical and effective steps toward building resilience.

Cyber resilience is more than just protection against attacks; it is the capacity of an organization to maintain operations during a disruption and to recover swiftly afterward. For MSMEs, this means developing both resistance and adaptability. Preventive measures must be combined with responsive mechanisms, such as incident response plans and data recovery systems, while lessons from past experiences must be used to strengthen future preparedness. By adopting this mindset, MSMEs can transform cybersecurity from being a reactive measure into an integral part of their long-term growth strategy.

The literature on MSME cybersecurity reveals significant gaps that must be addressed to develop a more contextualized approach for Indonesia. Many existing studies rely on models from developed countries, where infrastructure, literacy, and resources differ significantly from local realities. As a result, proposed solutions are often difficult to implement in the Indonesian context, where MSMEs struggle with budgetary constraints, low awareness, and unequal access to technology. Furthermore, there has been insufficient analysis of the effectiveness of government policies in promoting cybersecurity practices among MSMEs. Without such evaluation, interventions risk being more symbolic than practical. Thus, future research and policymaking must focus on tailored approaches that align with the unique characteristics of Indonesian MSMEs.

The way forward lies in a collaborative effort that bridges the gap between policy, practice, and local conditions. Government support must be complemented by initiatives from the private sector, academic institutions, and local communities. Public–private partnerships can provide MSMEs with access to affordable cybersecurity tools, while community-based training programs and regional collective security systems can overcome resource limitations by pooling efforts and sharing knowledge. Encouraging a cultural shift in how MSMEs perceive cybersecurity is equally essential, transforming it from a burdensome cost into a strategic investment for customer trust, competitiveness, and long-term continuity. In reflection, the sustainability of MSMEs in Indonesia's digital transformation depends on their ability to embrace cybersecurity as a fundamental pillar of their business.

Neglecting this dimension not only threatens individual enterprises but also undermines the broader national agenda of building a resilient digital economy. Conversely, by cultivating awareness, adopting affordable protection strategies, and embedding cyber resilience into their operations, MSMEs can ensure that digital transformation becomes a driver of inclusive and sustainable growth rather than a source of vulnerability.

In conclusion, the challenge facing Indonesian MSMEs in the digital era is not merely how to innovate but how to innovate securely. Cybersecurity and digital resilience are inseparable from the vision of a competitive and sustainable business sector. The path forward demands a balanced approach where innovation and protection advance in harmony. Only through such integration can MSMEs secure their future, safeguard the trust of their customers, and strengthen their role as vital contributors to Indonesia's digital economy in an increasingly interconnected and vulnerable world.

REFERENCES

Anantadjaya, S. P. D. (2023). Strategı Pengelolaan Sdm Era Iot. Pengelolaan Sumber Daya Manusıa, 67.

Balafif, S. (2023). Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework. Jurnal Informatika: Jurnal Pengembangan IT, 8(3). https://doi.org/10.30591/jpit.v8i3.5662

Bernstein, P. L. (1998). Aganst the Gods - The Remarkable True Story of Risk. In USA: John Wiley & Sons Inc.

El Sawy, O. A., Malhotra, A., Park, Y. K., & Pavlou, P. A. (2010). Seeking the configurations of digital ecodynamics: It takes three to tango. Information Systems Research, 21(4).

Gebremeskel, B. K., Jonathan, G. M., & Yalew, S. D. (2023). Information security challenges during digital transformation. Procedia Computer Science, 219. https://doi.org/10.1016/j.procs.2023.01.262

Ginanjar, Y. (2022). Strategı Indonesıa Membentuk Cyber Securıty Dalam Menghadapı Ancaman Cyber Crıme Melaluı Badan Sıber Dan Sandı Negara. Jurnal Dinamika Global, 7(02).

Hartatik, H., Rukmana, A. Y., Efitra, E., Mukhlis, I. R., Aksenta, A., Ratnaningrum, L. P. R. A., & Efdison, Z. (2023). Tren Technopreneurshıp: Strategi & Inovasi Pengembangan Bisnis Kekinian dengan Teknologi Digital. PT. Sonpedia Publishing Indonesia.

Indonesia, K. P. (2014). Pedoman Pertahanan Siber. Kemhan RI.

Lestari, R. (2013). Pengaruh Manajemen Risiko Terhadap Kinerja Organisasi. Riset Akuntansi Dan Bisnis, 13(2).

Mishra, A. N., Konana, P., & Barua, A. (2007). Antecedents and consequences of Internet use in procurement: An empirical investigation of U.S. manufacturing firms. Information Systems Research, 18(1). https://doi.org/10.1287/isre.1070.0115

Mukhlis, E. N. A., Judijanto, L., Sukma, F. H., Sari, H. P. R., Munizu, M., & Sinulingga, G. (2024). Enterprise Risk Management: Teori dan Implementasi Manajemen Risiko. PT. Sonpedia Publishing Indonesia.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha

Kecil Menengah di Era Ekonomi Digital di Indonesia. Sanskara Ekonomi Dan Kewirausahaan, 2(03), 156–167.

Pavlou, P. A., & Sawy, O. A. E. (2010). The "third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities. Information Systems Research, 21(3).

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. MIS Quarterly: Management Information Systems, 30(2). https://doi.org/10.2307/25148729

Samsumar, L. D., Nasiroh, S., Farizy, S., Anwar, C., Mursyidin, I. H., Rosdiyanto, R., Widiyanto, W. W., Mutiarawan, R. A., Mukin, R., & Yusnanto, T. (2025). Keamanan Sistem Informasi: Perlindungan Data dan Privasi di Era Digital. Hadla Media Informasi.

Sulianta, F. (2025a). Literasi Digital Tingkat Lanjut-Computer Security. Feri Sulianta.

Sulianta, F. (2025b). Literasi Digital Tingkat Lanjut-Computer Security. Feri Sulianta.

Sulistyowati, R., Listiadi, A., Subroto, W. T., Ramadhani, S. N., Sarfita, D., Damayanti, F., Wulandari, L., Reffandi, K. S., Syafitrih, Z. E., & Silfina, I. (2025). Pembelajaran Ekonomı Dıgıtal: Konsep, Transforması Pasar Dan Kesıapan Teknologı. Penerbit Tahta Media.

Tayibnapis, A. Z. (2021). Kebangkitan UMKM di Indonesia. Jakad Media Publishing.

Utami, T., Purnomo, B., Estiana, R., Padilah, H., Harto, B., Judijanto, L., Munizu, M., Adrian, A., Ratnaningrum, L. P. R. A., & Nurrohman, R. (2024). UMKM DIGITAL: Teori dan Implementasi UMKM pada Era Society 5.0. PT. Sonpedia Publishing Indonesia.National Cyber Security Index. (2023). Skor Indeks Keamanan Siber.

World Bank Group. (2023). Improving SMEs' access to finance and finding innovative solutions to unlock sources of capital. worldbank.org/en/topic/smefinance.

CHAPTER 3
THE DOUBLE-EDGED SWORD OF SOCIAL MEDIA: INVESTIGATING ITS EFFECTS ON PRE-SERVICE CAREGIVERS' ACADEMIC SUCCESS IN KADUNA STATE COLLEGE OF EDUCATION, GIADAN WAYA, NIGERIA

[1]Linus TANKO
[2]Afiniki BAHAGO
[3]Victor Yunana BOWMAN

[1]Department of Early Childhood Education, Kaduna State College of Education, Gidan Waya tankolinus7@gmail.com, ORCID ID: 0009-0009-3207-1093
[2]Department of Primary Education, Kaduna State College of Education, Gidan Waya
[3]Department of Primary Education, Kaduna State College of Education, Gidan Waya

INTRODUCTION

The introduction of communication networks over the last few years on a global scale, along with their accompanying impact on social networking website interactions, has affected every segment of society. Many people cannot do without the internet, smartphones and other gadgets. The most affected group in society by the introduction of the internet and smart

Phones are the students. Bell, Bishop and Prybylski (2015) explained that about two-thirds of the students reported using social networking website while in class, studying, or doing homework. As such, social media websites, such as LinkedIn, Facebook, YouTube, Twitter, WhatsApp, and Instagram, if not well-managed, can pose safety risks, as they create opportunities for students to procrastinate while trying to complete their homework (Ibenegbu, 2019). Hence, in a survey of 102 students, 57% stated that social networking websites have made them less productive (Karpinski, 2009). These are the results of the level at which students use these gadgets to access materials from the internet, chat with friends and family, and for other purposes.

Similarly, preservice teachers in college download pictures and images that distract them from their studies. Internet access is readily available and reliable to everyone, especially students with data plans. Due to these, it becomes difficult for teachers to control the students' use of the internet, desktop computers and smartphones. This has not gone without significant consequences on the learning behaviour of the Pre-service caregivers. The irresistible attraction of social networking sites, which makes information solicited or unsolicited readily available, has encroached on the learning time and habits of students (Adaja & Ayodele, 2013). In fact, the globalisation and propagation of internet facilities are among the key factors that have defined and shaped the current generation of young people in Nigeria (Ndaku, 2013).

In connection with the use of social networking sites, Bell, Bishop, and Przybylski (2015) found a continuing decline in grades among students who use these sites. This was supported by Kirschner and Karpinski (2010), who found a significant negative relationship between Facebook use and academic performance. They concluded that students who use Facebook spend fewer hours per week studying, on average, than non-users of Facebook, resulting in lower mean grade point averages (GPAs).

The study aligns with Adaja and Ayodele (2013), who confirmed that students who most frequently access Facebook and Twitter to connect and share information with others do not have sufficient time to complete their school assignments. Similarly, Oberst (2010) reported that social media sites encourage negative behaviours for students, such as procrastination, and they are more likely to drink and use drugs. However, every day, many students spend countless hours immersed in social networking sites, such as Facebook, WhatsApp, Instagram and Twitter, which, if not checked, is not healthy for their learning behaviour and academic progress in college.

Research carried out by Ibenegbu (2019) revealed that among youths aged 15-25 in Nigeria, they are interested in aspects concerning the accessibility and use of the internet for communication and entertainment. Findings of the study revealed 35% of the targeted group in the entire country had access to the internet, with Lagos leading the pack at 49% with internet access, Kano at 30% and Ibadan at 26%. This information seems to have implications because the youth between 15 and 25 years form the college group age. Social networking sites appear to be providing the music students enjoy, as well as computer games, videos, online banking, text messaging, online chatting, and information (Adaugo, Ovute, & Obochi, 2015). They therefore end up spending most of their time listening to music and surfing the Internet from their ever-available mobile phones.

A study by Karpinski (2009) was on the use of social media among adolescents in Tanzania. The design employed was a mixed-methods study to investigate young people's web and mobile phone user behaviour. The methodology employed consisted of administering a questionnaire to 60 adolescents and conducting in-depth interviews with eight students. Findings revealed that youth in Ntwara and Dar es Salem access the internet mainly through electronic devices. The implications for the students using social media technologies led them to become addicted, which resulted in indiscipline in schools, poor academic performance, lack of morals, neglect of studies, violence, identity crises, and dress code, among many. According to Ndaku (2013), cheating in examinations has been observed in various forms, including the use of smartphones and websites, which poses a significant challenge.

Similarly, Adaja and Ayodele (2013) argued that there is evidence that while social media is used as a means of communication, it can also be used to propagate negative learning behaviour among students in Nigeria. This, by itself, is significant for understanding the common development of learners' attitudes towards social networking websites and the associated implications for learning activities. This is because learning behaviours have a direct significance to the academic performance and attitude progression of the students in the college. This research was therefore intended to investigate how the learning behaviour of students in college is influenced by the infiltration of social networking websites in society, especially among Nigeria Certificate in Education (NCE) students at Kaduna State College of Education (KSCOE), Gidan-Waya, Kaduna State, Nigeria.

Preservice caregivers welcomed the introduction of social media with great excitement. These preservice caregivers were always seen everywhere, having fun and developing habits of using social media, which has become a standard part of both their academic and recreational lives. The number of people using social networking websites (SNW) continues to grow every year. Statistics indicate that more than 90 million active internet users come from Nigeria (Ibenegbu, 2019). Social networking websites in Nigeria provide preservice caregivers with positive experimental cognition, which, when absorbed and enthusiastically applied, directly enhances their future perceptions of interactions and system satisfaction. Consequently, this increases their goal to continue using the behaviour, and it can act as a partial mediator of perceived enjoyment and continuance intentions. It also speeds up the formation of a usage habit, which can raise the intention to engage in the delightful behaviour (Bell, Bishop, & Przybylski, 2015).

Preservice caregivers are students in the department of Early Childhood Care and Education (ECCE) who are receiving training at the Nigerian Certificate in Education (NCE) to provide care and optimise development for children aged 0 – 5 years in Public Primary Schools of Kaduna State (Educational Research and Development Council [NERDC], 2007). They are not exempt from SNW use in their unique area of specialisation, the ECCE.

In all, the Preservice caregivers stand to benefit from SNW, but it can be dangerous when abused. This paper aims to investigate the benefits and risks of gratification with SNW among Preservice caregivers at the College. Social media is a "collection of technologies" that allows people to create virtual networks of contacts, share text, video, and images with these contacts, and view and respond to contacts' posts (Boyd & Ellison, in Turel, 2018). A study conducted by Ohno (2018) involving 3,288 students in Japan found that 26.1% of high school students use the internet negatively, averaging approximately 5 hours per day. In a similar study (n = 15,191), 4.6% of high school students and 5.7% of Junior High School Students in Tokyo exhibited a high tendency towards Internet addiction (Ministry of Internal Affairs and Communications, Japan, 2016). This trend signals some dangers associated with excessive Internet use.

Social Networking Websites (SNW) are web-based services that allow individuals to create profiles, a list of users with whom to share connections and views across the connections linking the system (Ellison, 2013). Social media provides platforms for networking for youths in Nigeria. Preservice caregivers benefit from engaging with SNW, which helps them reach their full potential in school and social work. The top ten most popular Social Networking Websites in Nigeria are LinkedIn, Skype, Snapchat, Twitter, Google+, Facebook Messenger, YouTube, Instagram, Facebook, and WhatsApp (Ibenegbu, 2019). Among students in Nigeria, Adaja and Ayodele (2013) identified the most popular SNW mainly used as Facebook (54%), MySpace (15%), Twitter (13%), Facebook Messenger (11%), and YouTube (10%). The major devices used for SNW among Preservice caregivers are desktops, mobile devices, and tablets. Scholars from different fields have examined various SNW in order to understand their benefits and dangers to users (Turel, 2018; Limayen & Cheung, 2011; Ohno, 2018; Turel, Serenko, and Boutis, 2010; Young, 2010; Adaja & Ayodele, 2013).

In every College setting, the academic achievement of students in the NCE programmes is their ultimate goal and objective.

Apart from high intellectual outcome differences in academic achievement, especially among caregivers of children with special needs, these differences could be attributed to variations in gratification with SNW, which affects their study habits (Pitan, 2013). Some benefits of SNW to preservice caregivers in the College of Education, Gidan Waya, among others, as identified by this study, include meeting new people, staying in touch with friends and relatives, posting messages and photos, watching online videos, playing games, chatting, and helping to improve written language communication skills. Similarly, some dangers of gratification with SNW identified include neglecting important things to do because of absorption in SNW, interference with other activities or academic work, added financial burden, cyberbullying, reduced school performance, and increased work-family conflict (Turel, 2018). Therefore, the primary learning objective for preservice caregivers in the NCE program at the College of Education, Gidan-Waya, will be enhanced by any effort to identify the advantages and risks associated with gratification using SNW.

1. THEORETICAL FRAMEWORK OF THE STUDY

The study is grounded in the uses and gratification theory developed by Elihu Katz, Jay Blumler, and Michael Gurevitch in 1974. The theory considers that the audience actively seeks out specific media and content to achieve certain results or gratification that satisfy their personal needs. The central issue becomes "who uses which content from which media under which conditions and reasons." The theory aims to explain the use of media in terms of the motives and self-perceived needs of audience members. It emphasises the fact that the audience is not a passive receiver of media content, but that "they actively influence the message" in that they "selectively choose, attend to, perceive and retain the media message based on their needs, benefits and so on (Adaja & Ayodele, 2013).

The assumptions from this theory are that the audience is conceived as active; in this sense, Preservice caregivers actively enjoy SNW use and can benefit from it under control or else become addicted. Again, the choice and gratification of media depend on the audience size; that is, people use the media to their advantage more than the media use them.

In such situations, Preservice caregivers tend to achieve maximally from SNW to improve their academic achievement at the NCE level. Another assumption is that the media compete with other sources of need satisfaction, especially face-to-face communication.

Therefore, students must be informed that they enjoy SNW; care is needed to focus on media sources that will help support their schoolwork and achievement. Furthermore, the following assumption is that the goals of media use can be derived from data supplied by the individual audience members themselves. The implications are that, to benefit from and enjoy SNW, preservice caregivers will need to purchase data for accessibility to websites, thus incurring competing costs of data and other educational expenses. The final assumption of the theory is that it is the individual audience member who decides to view the media based on the value they place on it. Thus, educational values should be the main reason for their enjoyment of SNW. The underlying presumption is that media users, in this case, the preservice caregivers, selectively engage with media that possess the features or characteristics that can meet or satisfy their needs in the college. Thus, this study is limited to preservice caregivers in the College of Education at Gidan-Waya. It is expected that the findings obtained and recommendations proffered could be helpful to all stakeholders in early childhood education.

2. STATEMENT OF THE PROBLEM

It is common to see preservice caregivers and other students enjoying SNW on their phones in sensitive and highly organised places, such as in class, rest areas, churches, mosques, and even as they walk along the highway. This behaviour has become a source of concern to many who believe in the acquisition of knowledge and skills. Students tend to benefit from the enjoyment of SNW by using slang and shortened forms of words on these sites, and they rely mainly on the computer's grammar and spelling check features. The dangers associated with this reduce their language usage and creative writing skills.

The preservice caregivers who are overly involved in activities on SNW most often find it hard to concentrate on their studies as a result of divided attention between their books, time spent surfing the Internet, watching movies, especially naked pictures or pornography, and online games. They rely heavily on information that is easily accessible on these Social Networking Websites, which in turn could reduce their learning and research capabilities. As such, there is a need to identify the benefits and dangers of enjoyment with SNW among youths. This study aims to address the gap by examining the benefits and risks of enjoyment with SNW on the achievement of preservice caregivers in the College of Education, Gidan-Waya, Kaduna State, Nigeria.

2.1 Aim And Objectives

This study aims to determine the benefits and dangers of SNW on the achievement of Preservice caregivers in the College of Education, Gidan–Waya. Specifically, the objectives of the study are to:

- Determine the prevalence of devices used for enjoyment with SNW by preservice caregivers in the College of Education, Gidan-Waya.
- Examine the most prevalent SNW used by preservice caregivers in the College.
- Determine the mean differences in the academic achievement of Preservice caregivers in the College of Education, Gidan–Waya.
- Find out the mean differences in the benefits of enjoyment with SNW on male and female preservice caregivers in the College of Education, Gidan–Waya; and
- Determine the mean differences in the risks of enjoyment with SNW on male and female Preservice caregivers in the College of Education, Gidan–Waya.

2.2 Research Questions

1. What is the most prevalent SNW used by preservice caregivers in the College?
2. What is the prevalence of devices used by Preservice caregivers for enjoyment with SNW in the College of Education, Gidan-Waya?

3. What are the differences in the academic achievement mean scores of male and female Preservice caregivers' enjoyment with SNW in the College of Education, Gidan–Waya?
4. What are the differences in the mean scores of benefits and enjoyments of male and female Preservice caregivers on their academic achievement in the College of Education, Gidan–Waya?
5. What are the differences in the danger mean scores of enjoyments with SNW of male and female Preservice caregivers on their academic achievement in the College of Education, Gidan–Waya?

2.3 Hypotheses

1. There is no significant mean difference in the Academic Achievement of Male and Female Preservice caregivers in the College of Education, Gidan–Waya.
2. There is no significant mean difference between the benefits of enjoyment with SNW on Male and Female Preservice caregivers' achievement in the College of Education, Gidan–Waya.
3. There is no significant mean difference between the dangers of enjoyment with SNW on male and female Preservice caregivers' achievement in the College of Education, Gidan–Waya.

2.4 Method

The study employed a descriptive survey research design to investigate the benefits and dangers of enjoyment with social media on the achievement of preservice caregivers in the College of Education, Gidan–Waya. The study population consisted of 558 Preservice caregivers in the 2018/2019 academic session at the College, while the target population was 158 students in the NCE 300 level of the College. The sample consisted of 50 respondents, comprising 25 males and 25 females, who were selected using a stratified random sampling technique. A researcher made an instrument titled "Benefits, Dangers of Enjoyment with Social Networking Websites Preservice Caregivers Questionnaire" (BDSNWPCQ) on a 5-point scale, which was adopted from a "multi-item duality of enjoyment" scale measured on 7 7-point Likert–type scales (Limayem & Cheung, 2010) and used for this study.

The research instrument was subjected to face and content validity, and its reliability was established at 0.80. One hundred fifty copies of the questionnaires were administered, retrieved, and used for analysis. The frequency counts and percentage were used to answer the research questions, while the t-test was used to test the hypotheses generated for the study at a 0.05 (two–tailed) significance level.

3. RESULTS

Data for the study were collected and collated, and are presented in Table 1–5. Research Question 1: What is the prevalence of Social Networking Websites used by Preservice caregivers for enjoyment with Social Networking Websites in the College of Education, Gidan-Waya?

Table 1. Showing the prevalence of Social Networking Websites used by Preservice Caregivers in the College of Education, Gidan-Waya

Social Networking Websites	**Male**		**Female**		**Total**	
	Freq.	%	Freq.	%	Freq.	%
You Tube	4	8	3	6	7	14
Instagram	1	2	0	0	1	2
Facebook	6	12	5	10	11	22
Twitter	2	4	1	2	3	6
WhatsApp	12	24	16	32	28	56
LinkedIn	0	0	0	0	0	0
Total	**25**	**50%**	**30**	**50%**	**50**	**100%**

Table 1 shows the analysis of the most prevalent Social Networking Websites used by Preservice Caregivers in KSCOE, Gidan-Waya. Thus, of the 25 male preservice caregivers' respondents, 12 (24%), preferred use of WhatsApp platform; 6 (12%), Facebook; 4 (8%), YouTube; 2 (4%), Twitter; 1 (2%), Instagram; and 0 (0%), LinkedIn; while of the 25 females' preservice caregivers' respondents, 16 (32%), preferred WhatsApp platform; 5 (10%), Facebook; 3 (6%), You Tube; 0 (0%) Instagram; 1 (2%) Twitter and 0 (0%) LinkedIn.

Generally, the most prevalence of Social Networking Websites used as indicated by the 50 preservice caregivers' respondents is WhatsApp 28 (56%); followed by Facebook, 11 (22%); and You Tube, 7 (14%) while the least preferred platform as indicated by the respondents was LinkedIn, with 0 (0%); This finding indicates that prevalence of Social Networking Websites used by Preservice Caregivers in the College of Education is WhatsApp platform. Research Question Two: What is the most prevalent device used in accessing SNW by Preservice caregivers in the college?

Table 2. Showing the most prevalent device used by Preservice caregivers of enjoyment with social networking websites in the College of Education, Gidan-Waya

SN	Device			
	Computer	**Handset**	**Tablet**	**Total**
Male	2	22	1	**25**
Female	3	20	2	**25**
Total	**5**	**42**	**3**	**50**

Table 2 shows the analysis of the most prevalent device used by preservice caregivers of gratification with Social Networking Websites in KSCOE, Gidan-Waya. Thus, of the 25 male preservice caregivers, 22 (88%) used a handset, 2 (8%) used a computer, and 1 (4%) used a tablet, while the 25 female preservice caregivers, 20 (80%) used a handset, 3 (12%) used a computer and 2 (8%) used tablet. This finding indicates that the most prevalent device used by preservice caregivers of gratification with Social Networking Websites in the College of Education, Gidan-Waya is a handset.

Hypothesis 1: There is no significant mean difference in the Academic Achievement of Male and Female Preservice caregivers in their enjoyment of SNW in the College of Education, Gidan–Waya.

Table 3. Showing the summary of the t-test for the Academic Achievement of Male and Female Preservice caregivers ' enjoyment with Social Networking Websites in College of Education, Gidan–Waya

Gender	N	Mean	SD	df	t-cal	t-crit	Decision
Male	25	54.28	9.1037	48	0.130	2.011	Accepted
Female	25	53.96	8.3191				

Table 3 Shows that at 48 degrees of freedom, t-cal. (0.130) is smaller than t-crit. (2.011). So, the means are not significantly different. It suggests that the null hypothesis is accepted, implying that there is no significant mean difference in the academic achievement of males (M = 54.28, SD = 9.104) and females (M = 53.96, SD = 8.320).

This indicates that the null hypothesis cannot be rejected, meaning there is no statistically significant difference in the average academic performance between males (M = 54.28, SD = 9.104) and females (M = 53.96, SD = 8.320).It implies that there is no significant difference in the enjoyment of Preservice caregivers with SNW in the College of Education, Gidan-Waya. This indicates that gender does not play a significant role in how preservice caregivers enjoy social networking websites. Therefore, interventions aimed at enhancing academic achievement or enjoyment of SNW can be designed without gender bias.

Hypothesis 2: There is no significant mean difference between the benefits of enjoyment with SNW on Male and Female Preservice caregivers' achievement in the College of Education Gidan–Waya.

Table 4. Showing Summary of t–test for benefits of enjoyment with SNW in relation to male and female Preservice Caregivers in the College of Education, Gidan–Waya

Gender	N	$\bar{X}$	SD	df	t.cal	t-crit	Decision
Male	25	75.84	13.966	48	1.12	2.01	Accepted
Female	25	80.36	11.745				

N = 50, level of significance = 0.05

Table 4 shows that at a 0.05 level of significance, the absolute value of t–cal (1.12) is smaller than the t–crit value (1.12 < 2.011), so the means are not significantly different. All these indicate that the null hypothesis should be accepted. Therefore, the benefits of enjoyment with SNW for both male and female preservice caregivers do not differ significantly.

This suggests that both genders derive similar levels of enjoyment from social networking websites. Consequently, strategies to enhance the benefits of SNW can be applied equally to male and female preservice caregivers.

Hypothesis 3: There is no significant mean difference between the dangers of enjoyment with SNW on male and female Preservice caregivers' achievement in the College of Education Gidan–Waya.

Table 5. Showing Summary of t–test for dangers of enjoyment with SNW in relation to male and female Preservice Caregivers in the College of Education, Gidan – Waya

Gender	N	$\bar{X}$	SD	df	t.cal	t-crit	Decision
Male	25	73.16	13.735	48	1.06	2.01	Accepted
Female	25	68.20	18.956				

N = 50, level of significance = 0.05

Table 5 Indicates that at a 0.05 level of significance, the calculated t-value is smaller than the critical t-value (1.06 < 2.01), so the means are not significantly different.

4. DISCUSSION

Analyses of the preservice caregivers' responses indicated that their enjoyment of their most preferred social networking websites is neither beneficial nor poses a risk in relation to their achievement. Thus, WhatsApp, Facebook, and YouTube, which ranked first, second, and third among the social networking websites they enjoy most, were identified. These are personal and leisure websites, rather than educational resources like E-Libraries, online playbooks, and Microsoft Word, which will support their academic work. Another finding of the study is that the achievement of male and female Preservice caregivers is not significantly related to their enjoyment of social networking websites. This could be attributed to the negative habits developed towards enjoying social networking websites due to a lack of good orientation, which Pitan (2013) observed as a significant factor affecting the academic achievement of students.

Again, the study's findings indicate that the means of benefits and dangers associated with social networking websites for preservice caregivers are not significantly different in relation to their achievement.

This implies that, given the proper orientation and support, they will benefit more from social networking websites to achieve better results.

Blumler and Katz (1974) supported these findings in their postulation that users of social networking websites actively seek out specific media and content to meet their personal needs. Thus, the Preservice caregivers' personal needs are more focused on non-educational than educational use of networking sites, which occupy their time, money (data), energy, and attention. This suggests that with targeted guidance, preservice caregivers can shift their focus towards more educational uses of social networking websites. Encouraging purposeful engagement may enhance their learning outcomes and overall professional development.

CONCLUSION

The benefits of Social Networking Websites are important to preservice caregivers, as they support their learning and widen their scope in the current knowledge and skills required for handling children. Also, they could benefit from online courses from around the globe that they would not have access to in the state. When their Social Networking Websites are not controlled, they become addicted and pose a danger to their learning at college. Recommendations on how to benefit from and avoid dangers of enjoyment with Social Networking Websites have been made. It is believed that if the College authorities, students, and governments play their part as expected in the College, a favourable networking environment will be provided and accessible under control for Preservice Caregivers, who will benefit and enjoy with Social Networking Websites for their academic achievement and enhance their caregiving skills in Kaduna State and Nigeria in general.

Recommendations

Based on the above findings, regarding the positive and negative effects of social media gratification on the achievement of preservice caregivers in the College of Education, Gidan-Waya, Kaduna State, it is recommended that:

- There should be a proper orientation programme by the Students Affairs Unit in collaboration with the Computer Science department for students, especially the Preservice Caregivers, on when and how to operate and benefit from Social Networking Websites such as the e-library, LinkedIn, playbooks, Microsoft, and so on, to support their academic work.

- Social media, being an effective tool of transformation, should be used to intensify campaign enlightenment on issues of the students' future. They should be able to manage their time and spend an average amount of time on educational Social Networking Websites.
- Parents and other stakeholders in education need to play a role in helping preservice caregivers balance school life and Social Networking by putting checks and balances with respect to usage.
- School administrators and lecturers should help Preservice Caregivers be aware of the dangers of engagement with Social Networking Websites and explain what they are losing in the real world by sticking to these websites.
- The college authorities and Kaduna State government should help provide a free internet system in the College environment and a management Information System, which will enable students to benefit from Social Networking in their educational pursuits.

REFERENCES

Adaja, T. A. & Ayodele, F. A. (2013). Nigerian Youths and Social Media: Harassing the Potential for Academic Excellence. Kuwait Chapter of Arabia Journal of Business Management Review, 2, 5, Pg 65 - 75

Adaugo, C. Q., Ovute, A. O., & Obochi, C. I. (2015). The Influence of Social Media on Nigerian Youths: The Experience of Aba Residents. Journal of Research in Humanities and Social Science, 3(30, 12–20.

Bell, V. Bishop, D. V. M; & Przybylski, A. (2015). The Debate over Digital Technology and Young People. British Medical Journal, doi: https:/10:1136/bmj.h3064

Blumber, J. G. & Katz, E. (1974). The Uses of Mass Communications. Beverly Hills: C. A. Sage.

Brydolf, C. (2009). Minding my Space: Balancing the Benefits and Risks of Students in Line Social Networking. Education Digest, 73, 2, 4 – 6.

Chaudhari, B., Menon, P., Saldhannha, D., Tewari, A., & Bhattacharya, L. (2015). Internet Addiction and Its Determinants among Medical Students. Industrial Psychiatry Journal, 24, 2, DOI: 10.4103/097 – 6748

Elison, D. A. (2013). Social Networking Site: Definition, History, and Scholarship. Journal of Computer Mediated Communication, 1 – 11.

Ibenegbu, G. (2019). Statistics of Social Media Users in Nigeria. Retrieved from www.legit.ng/1169202-statistics-social-media...

Karpinski, A. C. (2009, April). A description of Facebook use and academic performance among undergraduate and graduate students. Paper presented at the Annual Meeting of the American Educational Research Association, San Diego, CA.

Kirschner, P. A. & Karpinski, A. C. (2010). Facebook and academic performance. Computers in Human Behaviour, 1(26), 1237 – 1245.

Limayen, M. & Cheung, C. M. K (2011). Predicting the Continued use of Internet-based Learning Technologies: The role of habit. Behaviour & Information Technology, 30, 1, 91, 99.

Ministry of Internal Affairs and Communications, Japan (2016), Chugakusei no Internetto noriyo jokyo to izon keiko ni kansuru chosa (Survey on Internet use and Internet addiction tendency of junior high school students).

Nigeria Education Research and Development Council (NERDC), (2007). National Policy for Integrated Early Childhood Development in Nigeria. Yaba: Lagos: NERDC Printing Press.

Ndaku, A. J. (2013). Impact of social media on students' academic performance (A study of students of the University of Abuja). Unpublished Research Project.

Oberst, P. A. (2010). The Social Network: Psychological Educative. Retrieved from: http://sixtentences.ning.com/profile/LindsaOberst

Ohno, S. (2018). Positioning of Escapism Internet Addiction Problems. International Society for the Study of Behavioural Development Bulletin 2, 74, 14 – 16

Turel, O. (2018). Understanding Excessive Use of Social Media. International Society of the Study of Behavioural Development, Bulletin, 2, 74, 9 – 11.

Turel, O., Serenko, A. & Bontis, N. (2010). User Acceptance of Hedonic Digital Artefacts: A Theory of Consumption Values Perspective. Information & Management, 47, 1, 88 – 95.

Young, K., Bradford, P. A. (2010). Understanding Gaming Addiction. Bradford, P.A.: Centre for Internet Addiction Recovery. Pp 1 – 30.

ISBN: 978-625-6080-49-2