A Case Study on Teaching Social Engineering to Swiss and Cameroonian University Students in a Virtual and Cross-Cultural Setting

Hermann Grieder[1] [0000-0001-9984-8615], Bettina Schneider[1][0000-0001-8460-3658], Franka Ebai[1] [0009-0007-5921-4862], Eyongabi Carlson Ngwa[2]

[1] University of Applied Sciences and Arts Northwestern Switzerland, Basel, Switzerland
[2] SwissLink Higher Institute of Business & Technology, Kumba, Cameroon

hermann.grieder@fhnw.ch, bettina.schneider@fhnw.ch, franka.ebai@fhnw.ch, carlson@ swisslinkedu.ch

Abstract. This paper presents a descriptive case study on integrating social engineering education into a business school curriculum, utilizing a cross-cultural approach. The case study was conducted at the School of Business, University of Applied Sciences and Arts Northwestern Switzerland (FHNW) in collaboration with SwissLink Higher Institute of Business and Technology in Cameroon supported by the Swiss-Cameroonian non-governmental organization (NGO) Turacos in the context of an elective module. During the six-week course, Swiss students were instructed in weekly sessions on social engineering topics and tasked with transforming their knowledge into learning materials for Cameroonian students. Subsequently, groups of Swiss students conducted virtual mentoring sessions, delivering lessons to their Cameroonian counterparts. Despite facing cultural, technological, and didactical challenges, both Swiss and Cameroonian students provided positive feedback. The study sheds light on the effectiveness of cross-cultural teaching methodologies in a virtual setting and underscores the importance of the cultural dimension of social engineering.

Keywords: Social Engineering, Cross-Cultural Education, Student Collaboration, Active Learning, Business School, Mentoring.

1 Introduction

Social engineering is a prevalent and evolving cybersecurity threat that relies on manipulating human psychology to gain unauthorized access or extract sensitive information [1]. To increase protection, social engineering should be an essential part of cybersecurity education at universities.

This paper presents a case study on teaching social engineering via a cross-cultural approach in Swiss and Cameroonian business schools, following the structure proposed by [2]: Introduction, Findings, Discussion, Conclusions, and Recommendations. This

Smuts, Hanlie & Hinkelmann, Knut (2024). Proceedings of the 4th Conference Society 5.0 - Innovation for Sustainable and Inclusive Social Good, Volume 2,
Mauritius, 26-28 June 2024, DOI: 10.5281/zenodo.11612759
DOI: 10.5281/zenodo.11619371

first section elaborates on the cultural dimension of social engineering and its relevance for students as future business managers.

1.1 Background on Social Engineering

Social engineering constitutes a multifaceted domain within cybersecurity, exploiting human psychology to compromise security. The National Institute of Standards and Technology (NIST) defines social engineering as an *"attempt to trick someone into revealing information that can be used to attack systems or networks"* [2]. Several types of social engineering, including phishing, pretexting, and impersonation target individuals' trust and manipulate them into divulging sensitive information. [3] identified for 2020 to 2022 social engineering, specifically phishing, as top crime type. The impacts of successful social engineering attacks range from data breaches to financial losses and compromised reputation, with the European Union Agency for Cybersecurity (ENISA) highlighting that targeted users stand as primary recipients of these malicious attacks [4]; moreover, the impacts can extend to physical and psychological harm [5].

Tactics, techniques, and procedures (TTPs) employed in social engineering schemes are diverse, adapting to technological advancements and evolving communication channels. Social engineering methods are commonly employed not only for initial access but also at later stages in incidents or breaches, with prominent instances including business email compromise (BEC), fraud, impersonation, counterfeiting, and, in more recent times, extortion [4]. Furthermore, the rise of phishing-as-a-service (PhaaS) due to its accessibility and affordability significantly contributes to the widespread occurrence of social engineering attacks. [6] has identified PhaaS offerings priced as low as $15 per day or a flat rate of $40 for a phishing kit (including email templates, templates of spoofed websites, potential target contact lists, guides to execute an attack, and customer support), enabling individuals with limited technical knowledge to execute sophisticated phishing attacks. Consequently, threat actors encompass a spectrum, from organized cybercriminal groups to malicious individuals, each leveraging social engineering to exploit vulnerabilities in human behavior.

1.2 Relevance of Social Engineering for Business Managers

Social engineering holds notable relevance for businesses and their managers. In the annual "Risk Barometer" study conducted by [7], the topics *cybersecurity* and *business interruption* ranked as the biggest concerns for organizations. The study unveiled that both in Europe and Africa & Middle East cyber incidents rank as the number one and two most important business risk respectively. Business managers responsible for safeguarding sensitive data face heightened risks such as phishing attacks and impersonation. The impact extends beyond financial losses to reputational damage. While accurate numbers on cybercrimes, including phishing, are not accurately measurable, due to factors such as voluntary and under reporting [8], the global financial damages for businesses and individuals are estimated to be in the trillions [3], [9]. As businesses embrace digital communication, the importance of educating students as future business managers on social engineering tactics becomes paramount. Understanding these

manipulative strategies can guide decision-makers to implement proactive measures, fortifying organizational defenses and fostering a resilient cybersecurity posture.

1.3 Relevance of Cybersecurity and Social Engineering for Cameroon

The surge in digitalization across African nations has led to a rapid increase in internet accessibility, presenting both opportunities and challenges for organizations. During the second quarter of 2023, Africa witnessed a significant 23% year-over-year surge in weekly cyber-attacks per organization [11]. Particularly, Cameroon (ranked 81st on the Cyber-Safety Index) emerges as a high-risk area for cyber threats [12]. This underscores the urgent need for cybersecurity experts and innovative solutions to bolster organizational resilience. However, many African countries lack comprehensive cybersecurity education [10] with limited programs available in both public and private universities.

In Switzerland, cybersecurity curricula often emphasize technological and organizational aspects [13], yet they often neglect the human element, particularly the cultural dimension [14]. Research findings highlight however, that culture plays an important role in shaping attitudes towards privacy and security [15], emphasizing the need for cross-cultural research, especially in social engineering. In this context, [16] argue that a cost-effective approach to enhancing cybersecurity capabilities in low-income countries involves focusing on the social and cultural dimensions.

1.4 Context of the Case Study

This case study is situated at the FHNW School of Business, which aims to develop innovative specialists and managers for the evolving global landscape [17]. The school offers a bachelor program in business information technology (BIT), with students able to choose electives valued at 3 ECTS each, spanning six weeks with weekly four-hour lectures. Although there is a mandatory IT Security course, a dedicated social engineering elective has been newly introduced by the Competence Center Digital Trust[1]. This course is supported by SwissLink Higher Institute of Business and Technology[2] (short: SwissLink) and Turacos[3], a non-governmental organization promoting cross-cultural exchanges and cybersecurity education in Cameroon. While SwissLink provides business and engineering courses, the university curriculum offers no dedicated course on cybersecurity. Hence, the collaboration with FHNW and the aim to bridge this gap by equipping students with relevant cybersecurity knowledge.

1 https://digitaltrust-competence.ch
2 https://swisslinkedu.com
3 https://www.turacos.ch

2 Findings

This section provides deeper insights into the learning objectives, the design and implementation of the social engineering course.

2.1 Course Objectives

Our course stands out from traditional social engineering courses by integrating it into cultural contexts and fostering cross-cultural skills in a virtual setting. We aimed to make the cultural aspects of social engineering tangible through direct exchanges with students from Switzerland and Cameroon. The course draws inspiration from the concept of Collaborative Online International Learning (COIL), emphasizing the creation of an environment conducive to cultivating cross-cultural skills through IT-enabled connections between classrooms situated in different geographic locations [11]. The detailed course objectives are outlined in **Table 1**.

Table 1. Learning objectives of the social engineering course (Swiss perspective)

Learning Objective	Description
Knowledge and understanding	Students demonstrate profound knowledge and understanding of social engineering concepts, tactics, and countermeasures encompassing techniques like phishing, pretexting, and impersonation. They also cultivate awareness of the cultural aspects of social engineering and its implications on individuals, organizations, and society.
Application of knowledge and understanding	Students can craft culturally and contextually relevant learning materials by understanding the social and cultural dynamics in Cameroon. This enables them to customize educational content to align with local perspectives, norms, and communication styles effectively. Students display proficiency in leading mentoring sessions for Cameroonian students, emphasizing the identification and application of suitable methods. They acquire skills to evaluate the educational needs, cultural intricacies, and technological resources of the Cameroonian student body. This enables them to adjust mentoring approaches to promote engagement, comprehension, and knowledge retention effectively.
Ability to reflect	Students exhibit the capability to reflect on their mentoring sessions, conducting thorough analyses to recognize successes, challenges, and areas for enhancement. They cultivate the ability to objectively evaluate the effectiveness of their strategies, considering participant engagement, comprehension, and learning outcomes. This fosters a mindset of continuous improvement, empowering students to enact constructive changes in subsequent mentoring sessions.

2.2 Course Design

To design the course content the ACM Curricula Recommendations on Cybersecurity [13] shed light on the essential components of a well-rounded education in this field. The topics *"types of social engineering attacks," "psychology of social engineering attacks," "misleading users,"* and *"detection and mitigation of social engineering attacks"* form its cornerstone. In alignment with these recommendations, our course incorporates each of these topics. However, we go a step further by integrating additional subjects tailored to the Cameroonian environment. Recognizing the evolving landscape of cyber threats and societal challenges unique to our context, we include in our curriculum the exploration of "mobile money" (*"a recent innovation that provides financial transaction services via mobile phone, including to the unbanked global poor"* [14], with most users being in Sub-Saharan Africa (22%) and of those 27% being in West Africa [15]) and "fake news".

The design of the course is outlined in **Table 2**. It is structured into six weekly lectures, each covering one specific topic in the field of social engineering.

Table 2. Design of the social engineering course

Topic	Description
1. Introduction	Joint one-hour online session with Swiss and Cameroonian lecturers and students, aimed at conveying the course context, conditions, and a first introduction of both student parties. Swiss students also received an introduction into the Cameroonian culture followed by a first input lecture of the topic *social engineering kill chain*.
2. Phishing	The focus is set on *phishing* as a key threat in the field along with its various forms, including, Smishing, Vishing, and QRishing, the motivation and impacts to individuals and businesses, and the TTPs employed by threat actors.
3. Mobile Money	*Mobile money*, a financial service facilitated through mobile devices, is crucial in Africa for its role in bridging banking gaps and facilitating financial inclusion. Mobile money services expose users to social engineering risks, as fraudsters exploit human vulnerabilities through manipulative tactics, posing a threat to their financial security.
4. Fake News	*Fake news* involves disseminating misleading or false information to deceive and manipulate public opinion. In Africa, fake news holds significance due to its potential to influence political dynamics, exacerbate social tensions, and impact public trust. Social engineering exploits human psychology, often through misinformation, to manipulate individuals into divulging sensitive information or taking certain actions.
5. Internet Hygiene	*Internet hygiene* involves adopting safe online practices. In Africa, where digital connectivity is rising, promoting internet hygiene is crucial for safeguarding personal data and privacy. Social engineering exploits human

	psychology online, emphasizing the need for heightened awareness and education to counteract cyber threats in this evolving digital landscape.
6. Closing	Joint one-hour online session with Swiss and Cameroonian lecturers and students, aimed at summarizing the learning content and reflecting upon the learning journey. The Cameroonian students that successfully finished the course were awarded with a certificate. After feedback from the Cameroonian students, an interactive feedback session with Swiss students followed.

The course structure was comprised of one-hour input sessions by the lecturer, where Swiss students received topic-relevant content. Subsequently, the Swiss students were allocated dedicated time to craft their learning materials, allowing for the application of theoretical concepts. The culmination of each session involved a feedback mechanism, where lecturers provided feedback and evaluations on the created learning material. This cyclic process of input, creation, and feedback aimed at fostering a dynamic learning environment, ensuring students not only absorbed theoretical knowledge but also actively applied it, receiving constructive guidance to refine their educational materials.

The Swiss students were instructed to self-organize with their peers in Cameroon about the time and modality of the mentoring session. After each mentoring session, Swiss students were required to deliver a reflection report on the mentoring sessions, including their successes and challenges, and improvements to the learning material and mentoring session.

2.3 Course Implementation

The course took place from the 13th of November 2023 to the 18th of December 2023, with 27 Swiss and 23 active Cameroonian participants. Turacos facilitated the formation of groups and the collection of reflection papers from Cameroonian students. Swiss students were organized into groups (two to three students), with each group assuming the role of mentors for Cameroonian students. Simultaneously, Cameroonian students were assigned to specific Swiss groups, fostering a collaborative learning environment. Communication was facilitated through a dedicated WhatsApp or Telegram group, enabling students to coordinate mentoring sessions, discuss weekly content, and plan meeting schedules. This approach not only enhanced the sense of community but also provided a platform for effective cross-cultural exchange.

The students demonstrated a high degree of adaptability to the various challenges they faced preparing and conducting the mentoring sessions. Exemplarily, they chose modalities that best suited their respective groups, especially to circumvent challenges with the poor internet connectivity in Cameroon, ranging from sharing slides and assignments in the WhatsApp channel to conducting Google Meet sessions if possible. Email correspondence was also used to communicate between the groups. The learning materials were not only created based on the weekly input but were also tailored to suit the cultural nuances of the Cameroonian audience. Additionally, Swiss students

designed assignments, such as weekly quizzes and topic-specific homework, to reinforce the learning experience.

Evaluation of the students' learning materials was conducted by lecturers using a comprehensive set of criteria. The criteria included assessing how well the materials were adapted to the target group, evaluating the planning of interaction with the target group, verifying the correctness and currency of the content, assessing the persistence and flexibility in mentoring, and examining the reflection and lessons learned from the process. Notably, the Cameroonian students, as one essential stakeholder, were not subject to formal evaluation, as the course was offered free of charge and did not result in ECTS credits. However, the Cameroonian students had to partake in their mentoring sessions and submit weekly reflection papers to receive a certificate of attendance at the end of the course. Overall, this innovative approach to cross-cultural education reflects the commitment to inclusivity and mutual learning.

3 Discussion

This section is dedicated to learning and feedback from the lecturers and students. Positive aspects are elaborated and fields for improvement are identified and discussed.

3.1 Lecturers' Learning and Feedback

The positive feedback from lecturers supports the continuation of the course, led by three FHNW teachers collaborating to enable mutual learning and improvement. This team approach brought together subject matter experts on social engineering and cross-cultural exchange, benefiting students by leveraging the diverse skill set of the lecturers. Teaching as a group enhanced efficiency, enabling parallel feedback for the student groups, and offering a range of perspectives on learning material. Additionally, the course provided lecturers with opportunities to expand their cultural competence through interaction with students from different countries. While this collaborative teaching model is not common in universities and poses cost-effectiveness challenges, personal commitment made it feasible for three lecturers to participate initially. Future offerings may require additional resources and could potentially involve fewer lecturers as experience grows. However, effective management of stakeholders and interactive settings will always demand significant involvement from the lecturers. Coordinating the course for the first-time posed challenges in group management and coordination.

Moreover, educators and coordinators from SwissLink and Turacos underscored the importance of this course, especially for Cameroonian students. It provides them with the opportunity to engage in an international program from their home countries. This alleviates the financial burden of travel expenses that often deter some from pursuing such opportunities.

3.2 Swiss Students' Learning and Feedback

Swiss students submitted weekly reflective papers about their mentoring sessions with their Cameroonian peers. These papers were submitted via the FHNW's study portal – Moodle. Based on the collected reflective papers, the Swiss students' learning journey aligns with the classical four-phase model of cultural learning: Honeymoon, Crisis, Adjustment, and Adaptation [16].

Honeymoon Phase: Most students were very enthusiastic about the meaningful cultural exchange, as highlighted by the quote: *"The [Cameroonian] students' keen interest in more information was encouraging, signifying the session's success and the need for ongoing education in cybersecurity. This mentoring experience was a chance for knowledge exchange and a meaningful opportunity for cultural interaction, emphasizing the importance of cross-cultural communication in education, particularly in dynamic fields like cybersecurity."*

Crisis Phase: Swiss students experienced heightened insecurity and overwhelming responsibility in organizing mentoring sessions independently. This pressure led to frustration and the need for lecturer support, necessitating solutions tailored to individual needs, such as reorganizing group assignments, reaching out to lecturers in Cameroon, and lecturer participation in mentoring sessions. Further challenges arose due to e.g., technical issues, leading to frustrations among Swiss students. Support from lecturers was crucial in finding solutions.

Adjustment Phase: Students made significant efforts to adjust. This involved rescheduling, recording, or transitioning mentoring groups to asynchronous mode. During this phase, Swiss students gained valuable experience in cross-cultural collaboration. For instance, they found success in improving the interaction by individually reaching out during mentoring sessions to gather feedback, despite the cultural norm in Switzerland, where singling out individuals from a group may be seen as impolite.

Adaption Phase: Most groups adapted well to the collaboration process, recognizing that it operated differently from their accustomed methods in Switzerland. A high level of reciprocal learning between Swiss students and their Cameroonian peers took place. Notable was the exchange of insights on mobile money fraud, a prevalent topic in Cameroon.

Overall, as evidenced by the following quote, the mentoring approach combined with a virtual setting proved highly effective for learning both the subject matter of social engineering and soft skills, as well as fostering cultural understanding: *"Stepping into the shoes of a mentor was both challenging and rewarding. This role reversal also highlighted the importance of empathy, patience, and adaptability in guiding others through their learning journey. Organizing the mentoring sessions demanded a new set of skills."*

3.3 Cameroonian Students' Learning and Feeback

As aforementioned, Cameroonian students submitted reflection papers via email to Turacos. Despite the technical challenges of partaking in a virtual course, the

Cameroonian students nonetheless could benefit. The key lessons that the students highlighted in their reflection papers include:

Ability in handling sensitive information: Some students mentioned that not only have they learned how to interact with sensitive information on social networks, but they have also learned how to securely store such information. *"This exercise will help me on how to use and interact with sensitive information on social networks and the importance of discretion when storing data."*

Improved cyber threats awareness: Despite ongoing frauds in Cameroon, cybersecurity is not a topic commonly discussed among students. Following their participation in the course, the students pointed out that they have become more conscious of cyber threats and have developed a proactive mindset in guarding against cyber threats and unsolicited emails. *"With this exercise I have gotten to understand how cyber attackers do get information about their target using platforms like Facebook, Google, and Instagram. I have also learned about what open-source intelligence is and how both the cyber attackers and cyber security professionals use this in their daily routine."*

"This topic is relevant to my personal life as an individual and my career. This is because with this knowledge so far, I now know what social engineering is and what the impacts are, and the motivations of social engineering threat actors. Talking about phishing and learned that I need to keep my accounts safe by using additional authentication methods to avoid such attacks."

Guarding against fake news: It is common for people in Cameroon to get their news from Facebook and WhatsApp. Hence, the dangers of fake news were also a valuable lesson for the Cameroonian students.

Some wrote that they have learned how to carefully vet new sources before sharing the news. *"My key takeaways include the importance of scrutinizing sources, promoting responsible sharing of information, and the need for regulatory measures and cooperation between tech companies and policymakers to proactively address fake news."*

In the final session, a few Cameroonian students also expressed positive feedback towards their Swiss mentors. They appreciated especially the ability of the Swiss students to pass the content in a clear manner.

4 Conclusion

4.1 Concluding Summary

Examining the Social Engineering course critically revealed certain limitations in its
In response to the escalating global challenges posed by social engineering and cybersecurity threats, there is an increasing emphasis on continuous education and awareness training. Organizations worldwide recognize the imperative of equipping individuals with the knowledge and skills necessary to navigate the evolving landscape of digital risks. Ongoing education and awareness training in social engineering and cybersecurity play a pivotal role in addressing global challenges in the digital landscape. These

initiatives, crucial for both individuals and organizations, serve as proactive measures against evolving cyber threats. Notably, international collaboration, as exemplified in the case with Cameroon, underscores the potential for cross-cultural exchanges to enhance understanding and fortify collective defenses. This collaborative approach is particularly beneficial for students not directly enrolled in cybersecurity courses, providing them with essential knowledge and skills to navigate the increasingly interconnected digital world.

By fostering a culture of cybersecurity awareness and education, we contribute to a more resilient global community better equipped to confront the multifaceted challenges posed by social engineering and cyber threats. The collaboration between the FHNW, the SwissLink University and Turacos proved to be successful, resulting in reported increased awareness and understanding of social engineering threats and countermeasures, delivered through modern technological communication channels in the form of online classrooms.

By achieving the learning objectives as outlined in section 2.1 the course allowed Swiss students to solidify their knowledge and understanding of Social Engineering by adopting the role of a mentor and to gain cultural experience of Cameroon and Cameroonians.

4.2 Limitations

Examining the course critically revealed certain limitations in its design, execution, and educational context.

Course design: In this first iteration, a lot of unknown and limiting factors had to be covered in the course design. As an example, it was not possible that the Cameroonian students were granted with ECTS. Hence, their commitment to stick to a six-week course was hard to predict in advance. This led to a setup that would allow the Swiss students to complete the course despite a potential drop-out of the Cameroonian peers. This design was useful for the start. However, it placed FHNW into the teacher and SwissLink into the learner role; this did not reflect reality. As for example, for the topic of mobile money fraud, the Cameroonians were the experts and provided background and practical cases. In future, the course design should be adapted to foresee both institutions and their participants as learners and teachers simultaneously.

Course execution: One limitation in executing the course was the infrastructure. A particular constraint was the inadequate internet accessibility in Cameroon for participating in mentoring sessions beyond school hours. This constraint might have impeded the engagement of students, particularly those who faced challenges accessing online resources outside of the educational institution.

Educational context: It was a challenge to handle the various familiarity levels among participants. While some students found the course content entirely new, others expressed prior knowledge. To address this, there is a future need for a more nuanced approach, allowing more advanced students to delve deeper and ensuring a balance that caters to the diverse backgrounds of both sets of participants.

These limitations highlight the importance of considering contextual factors, such as internet accessibility and tailoring content to accommodate varying levels of familiarity, to enhance the overall effectiveness and inclusivity of the social engineering course.

5 Recommendations and Future Research

In reflecting on our course and considering avenues for improvement and future research, several key recommendations emerge.

Firstly, building upon the foundational knowledge that some students bring as preknowledge, our focus should be on adapting the course content to facilitate deeper learning. This adaptation could involve incorporating advanced concepts, case studies, and real-world examples that resonate with Swiss students, thereby enhancing their engagement and understanding.

Secondly, to enhance motivation, we propose granting all students ECTS and linking the certificate of attendance to specific requirements, e.g. completing assignments, or achieving a mandatory attendance rate. This approach not only incentivizes active involvement but also ensures that participants are fully immersed in the learning process, thereby maximizing the benefits derived from the course.

Furthermore, recognizing the limitations concerning internet connectivity, we propose the establishment of dedicated time slots for the mentoring sessions. By aligning these sessions with Cameroonian school hours, we aim to provide students with optimal conditions for participation, including access to a stable internet connection and reduced scheduling conflicts.

In addition to these practical considerations, our ongoing research includes the measurement of Information Security Awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) [17]. By employing this tool, we seek to assess the effectiveness of our course in enhancing participants' awareness of information security practices and principles. Importantly, we intend to analyze the results from both a *a priori* and *posteriori* perspective, allowing us to gauge the impact of the course over time and identify areas for refinement and improvement, ensuring that the course remains relevant, engaging, and impactful.

References

[1] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[2] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology,” National Institute of Standards and Technology, NIST SP 800-61r2, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[3] FBI, “Internet Crime Report 2022,” 2022. Accessed: Jan. 04, 2024. [Online]. Available: https://www.ic3.gov/

[4] ENISA, “ENISA Threat Landscape 2023,” ENISA. Accessed: Jan. 04, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[5] WEF, “Global Risks Report 2022,” World Economic Forum. Accessed: Jan. 04, 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/

[6] TrendMicro, “Phishing as a Service Stimulates Cybercrime,” Trend Micro. Accessed: Jan. 04, 2024. [Online]. Available: https://www.trendmicro.com/en_us/ciso/23/c/phishing-as-a-service-phaas.html

[7] Allianz, “Allianz Risk Barometer 2023,” 2023. Accessed: Jan. 03, 2024. [Online]. Available: https://www.allianz.com/en/press/news/studies/230117_Allianz-Risk-Barometer-2023.html

[8] J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli, and P. Kijewski, “2020 Cybercrime Economic Costs: No Measure No Solution,” in *2015 10th International Conference on Availability, Reliability and Security*, Aug. 2015, pp. 701–710. doi: 10.1109/ARES.2015.56.

[9] Cybersecurity Ventures, “Top 10 Cybersecurity Predictions and Statistics For 2023,” Cybercrime Magazine. Accessed: Jan. 04, 2024. [Online]. Available: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

[10] U. Orji, “Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa,” *International Journal of Criminal Justice*, vol. 3, pp. 60–98, Jun. 2021, doi: 10.36889/IJCJ.2021.002.

[11] P. Appiah-Kubi and E. Annan, “A Review of a Collaborative Online International Learning,” *International Journal of Engineering Pedagogy (iJEP)*, vol. 10, no. 1, Art. no. 1, Jan. 2020, doi: 10.3991/ijep.v10i1.11678.

[12] NICCS, “Social Engineering from Cybrary | NICCS.” Accessed: May 12, 2024. [Online]. Available: https://niccs.cisa.gov/education-training/catalog/cybrary/social-engineering

[13] ACM, “Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.” Accessed: May 12, 2024. [Online]. Available: https://www.acm.org/education/curricula-recommendations

[14] J. Aron, “Mobile Money and the Economy: A Review of the Evidence,” *The World Bank Research Observer*, vol. 33, no. 2, pp. 135–188, Aug. 2018, doi: 10.1093/wbro/lky001.

[15] GSMA, “State of the Industry Report on Mobile Money,” 2023. Accessed: Jan. 04, 2024. [Online]. Available: https://www.gsma.com/sotir/

[16] K. Oberg, “Cultural Shock: Adjustment to New Cultural Environments,” *Practical Anthropology*, vol. os-7, no. 4, pp. 177–182, Jul. 1960, doi: 10.1177/009182966000700405.

[17] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” *Computers & Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.