**BUSINESS NEEDS**

1. **Enhancing User Experience and Privacy**: In the evolving landscape of social media platforms like Instagram, prioritizing a secure and positive user experience emerges as a critical factor for retaining users and bolstering platform credibility. The capability to discern and eliminate phishing links and hate speech from comments significantly contributes to cultivating a safer and more enjoyable user environment. Phishing links not only jeopardize user privacy but also pose substantial security threats. The project's core objective of identifying and flagging phishing comments aims at safeguarding users against scams, identity theft, and other fraudulent schemes orchestrated through social engineering tactics.
2. **Upholding Platform Integrity**: Instagram, akin to its counterparts, heavily relies on user-generated content to sustain user engagement and platform appeal. However, the proliferation of hate speech and offensive content poses a direct threat to the platform's reputation and user engagement metrics. By deploying a robust system capable of identifying and eliminating such content, the project ensures the preservation of platform integrity, thereby nurturing a healthier online community.
3. **Regulatory Compliance**: Numerous jurisdictions have enacted stringent regulations governing online content, especially concerning hate speech and privacy protection. Through the active detection and mitigation of hate speech dissemination and phishing links, the project aids Instagram in adhering to relevant legal mandates. This proactive stance reduces the risk of regulatory fines or legal repercussions due to non-compliance, thereby bolstering Instagram's legal standing and reputation.
4. **Informed Decision Making through Data Analysis:** Harnessing the power of a machine learning-based detection system empowers Instagram to harness data analytics for comprehensive insights into the prevalence and attributes of harmful content across the platform. These insights serve as a cornerstone for data-driven decision-making processes pertaining to content moderation strategies, platform optimizations, and user education initiatives, thereby ensuring continual improvement and enhancement of user experience and platform integrity.

**REFERENCES:**

1. S. Aiyar and N. P. Shetty, “N-Gram Assisted Youtube Spam Comment Detection,” Procedia Computer Science., vol. 132, pp. 174–182, 2018, doi: 10.1016/j.procs.2018.05.181.
2. R. Chrismanto, A. K. Sari, and Y. Suyanto, “CRITICAL EVALUATION ON SPAM CONTENT DETECTION IN SOCIAL MEDIA,” Journal of Theoretical and Applied Information Technology (JATIT), vol. 100, no. 8, pp. 2642–2667, 2022, [Online]. Available: <http://www.jatit.org/volumes/Vol100No8/29Vol100No8.pdf>
3. Chrismanto and Y. Lukito, “Klasifikasi Komentar Spam Pada Instagram Berbahasa Indonesia Menggunakan K-NN,” in Seminar Nasional Teknologi Informasi Kesehatan SNATIK), 2017, pp. 298–306.
4. F. Prabowo and A. Purwarianti, “Instagram online shop’s comment classification using statistical approach,” in Proceedings - 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2017, 2018, pp. 282–287. doi: 10.1109/ICITISEE.2017.8285512.
5. W. Zhang and H.-M. Sun, “Instagram Spam Detection,” in 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), Jan. 2017, pp. 227–228. doi: 10.1109/PRDC.2017.43.
6. Priyoko and A. Yaqin, “Implementation of naive bayes algorithm for spam comments classification on Instagram,” in 2019 International Conference on Information and Communications Technology, ICOIACT 2019, 2019, pp. 508–513. doi: 10.1109/ICOIACT46704.2019.8938575.
7. N. A. Haqimi, N. Rokhman, and S. Priyanta, “Detection Of Spam Comments On Instagram Using Complementary Naïve Bayes,” IJCCS (Indonesian Journal of Computing and Cybernetics Systems, vol. 13, no. 3, p. 263, Jul. 2019, doi: 10.22146/ijccs.47046.
8. T. Wu, S. Wen, Y. Xiang, and W. Zhou, “Twitter spam detection: Survey of new approaches and comparative study,” Computers & Security, vol. 76, pp. 265–284, Jul. 2018, doi: 10.1016/j.cose.2017.11.013.
9. A. Mandadi, S. Boppana, V. Ravella and R. Kavitha, “Phishing website detection using machine learning,” in 2022 IEEE 7th Int. Conf. for Convergence in Technology (I2CT), Mumbai, India, pp. 1–4, 2022. <https://doi.org/10.1109/i2ct54292022.9824801>
10. A. Kulkarni and L. L. Brown, “Phishing websites detection using machine learning,” International Journal of Advanced Computer Science and Applications, vol. 10, 2019. <https://doi.org/10.14569/ijacsa.2019.0100702>