Full name and semester: Srichandana Chakilam, Spring 2023

Title: Identifying spam accounts by analyzing 50 comments under a popular meme page's (9gag) post on Instagram.

Word Count: Identifying Spam Accounts on Instagram (440 words)

Research Question: The paper aims to answer the following research questions:

1. How are spammers trying to successfully trap the Instagram users?

Background: The social media is a fast-growing network that allows people all over the world to connect, collaborate and communicate effortlessly. Leaving comments on the pages we follow is a great way to increase the engagement with that page as per Instagram's algorithm. But a wrong approach in commenting on a post would be troublesome. There is a downside to everything. In recent times, there has been several cases of cyber-crime where innocent audience are targeted through comments. The spam accounts lure the users into their trap by posting explicit comments under popular pages. The comments could sometimes be hyperlinks leading to unsafe websites, asking for financial or personal information, or just ask us to check out their page to increase their follower count. The comments from spam accounts contains comments that are not relevant to the post or caption.

Data: A post from a popular meme page on Instagram – 9gag that has many comments is selected and first 50 comments are extracted manually and recorded in excel file. As Instagram is the most used application and is easily accessible to everyone, the presence of spam accounts is more, which will give us a better scope of analyzing the issue and makes a perfect dataset to answer our question. For this, we will be looking at the comments that has no relevance with the post or the caption, the comments which are explicit, the comments which has suspicious links.

Method: To perform this research, I shall collect first 50 comments from 9gag's latest post and prepare a codebook. The codebook consists of 2 categories – *Spam* and *Legit* based on below patterns in the comments:

1. Hyperlinks leading to insecure websites.
2. Luring comments.
3. Irrelevant comments.

The total and average frequency of the spam comments can then be estimated. This can help us in understanding how the hackers are trying to trick users.

References:

[1] Detection of Spam Comments on Instagram Using Complementary Naïve Bayes - Nur Azizul Haqimi*1, Nur Rokhman2, Sigit Priyanta31Master Program of Computer Science and Electronics, FMIPA UGM, Yogyakarta, Indonesia2,3Department of Computer Science and Electronics, FMIPA UGM, Yogyakarta, Indonesia

[2] Detecting spam comments on Indonesia's Instagram posts - Ali Akbar Septiandri1 and Okiriza Wibisono2 School of Informatics, The University of Edinburgh, 11 Crichton St, Edinburgh EH8 9LE, UK

[3] https://www.icpsr.umich.edu/web/ICPSR/cms/1983
[4] https://www.cloudflare.com/learning/bots/what-is-a-spambot/
[5] https://www.pepperit.com.au/instagram-spam-bots/
[6] https://www.quirks.com/articles/analyzing-the-content-of-social-media-data