Automatic detection of misinformation - assignment 3

Do not actually attack or potentially compromise anyone's security or privacy without first obtaining appropriate approval. (Check with the instructor if you're unsure.)

You are free to select any project related to the course focus of technology-enabled misinformation. Possible project types include:

- *Attacks*: Investigate, evaluate, extend, or develop a technique for creating or spreading digital misinformation (e.g., using the DeepFakes code available here).
- *Measurements*: Conduct a measurement, quantitative or qualitative, to assess the nature or prevalence of a misinformation-related problem (e.g., analyzing the advertisement data released by Facebook available here, or the Twitter data available here).
- *User Studies*: Conduct a user study, either formative (e.g., studying people's attitudes about technology-enabled misinformation) or evaluating a particular defense.
- *Defenses*: Design and prototype a new defense, or technically evaluate an existing defense that has been proposed (e.g., the defenses mentioned here or here).

The analysis

Here, you should reflect and write about the message. Who is likely to be fooled by this? What special knowledge is required to detect it? How much effort does it take to check the claim? Who is likely to make that effort? How professional is the result? How important is that? Include all these points in your report.

Assignment hand-in

Essay
Description of what you did and why. It should be written as an essay, and be around 1000 words. This should show how well you understand the target, and how information behaves in it. Rely on the material in the lectures and make sure that you cite relevant papers.

Deadline: December 6