Preface

Cybersecurity measures must be improved. This should be done by encouraging current students to work with the community around them, improving their skills and understanding of people, and by better understanding users and their weaknesses.

Currently, computer science students at the University of Virginia have limited experience working with projects that emulate the work they will be expected to do in their careers. The class that is most like the expected work is CS 3240—Advanced Software Development, in which students engage in a semester-long project. However, the scope of the project is limited to a university environment, so students only gain a limited understanding of future projects in the real world. To improve students' skills, I propose enhancing their experience with projects that last for the duration of their time at UVA. The benefits of this project would be two-fold: students would gain real world experience with clients and their projects could help the Charlottesville community.

The relative simplicity of social engineering attacks makes the among the most common of all cyberattacks. Such attacks evade cybersecurity measures by exploiting vulnerabilities in user psychology to bypass technology barriers. Attackers, targets and law enforcement influence a social engineering attack's degree of success. Assessing these groups and how they behave can give further insight into their goals. When social engineering attacks are successful, it is usually due to the attacker's success at exploiting users' habitual cognitive heuristics and their hopes. Study of their interaction can reveal opportunities to improve cybersecurity.