**What is the project about**

Hi everyone, our project is “Shall we play a game: human and ransomware interaction”. The group consists of myself, Kevin Zhang, and my partner Charlie Thomas.

**Research Question:**

**Our main research question is: What, if any, are the overlooked human-dependent features of a ransomware attack? How do we examine rational action with a game theoretic framework?**

When conducting our literature review, we found the difficulty in studying ransomware is the inherent "knowledge" of an attack on the part of the subject. We designed an interactive game that has the user take the guise of a decision maker. In this case, users are a Pizza Tycoon chief financial and operations officer.

We realized deception is important in the deployment of the study to fully examine rational decision making in a less-than-perfect situation. The term “Perfect” here refers to the concept of perfect information within a game.

**Basic Methods:**

We utilized Li and Liao’s 2020 paper on "Ransomware2.0 - to sell or not to sell" as a basis for our research. They provide a theoretic game theory model on rational action from the perspective of both ransomware Victim and the attacker. Our experiment takes this concept further, by creating a proof of concept implementation

Example of the Game

User Interface - We use an applet caled twilio, which allows surveys and interactive prompt to be interacted with via text on a phone.

~~3 phases~~

~~"Distraction" Phase - simple prompts that have the user make a rational economic decision (invest in a fleet of new delivery cars, plus 1 point, dont invest, 0 points).~~

~~"Ransomware Event" - The user is given a ransomware prompt where it is implied that the work they had done is now held hostage.~~

~~"Decision making" Phase - deciding what to do to manage risk and retrieve their held hostage data. Information, as opposed to the distraction phase, is not necessarily rational or with perfect information.~~

~~Human Protections and IRB concerns:~~

~~Only PII obtained are netIds and phone numbers, which are removed from final data analysis~~

~~Data is de-anonymized and separated by scrubbing PII and assigning each grouped person/information a random digit participant ID.~~

~~The subjects examined are all NYU affiliated individuals (whether current undergrads, graduates, or alumni), which may affect the final result (education level). We would like to see the results of the study deployed externally for different populations. There is a potential that individuals working may have more training and expertise than students~~

~~Twilio Backend.~~

~~Backend - showed in this slide, is a decision tree that guides the user to a certain point. Twilio creates a unique situation where variables can be passed between different nodes and saved after texts are received. The purpose of his is to make the study accessible to those who do not have technical knowledge. However, it does require the user to have a phone and an unlimited text plan, which may skew the population slightly.~~

**Summary of Key Results:**

~~The metrics we wished to examine are the ultimate choices made (paying, negotiating, or denying the ransomer), as well as user rationality (making economic decisions) and user sentiments.~~

~~Although we are still at gathering results at the moment, we see a positive trend of results towards paying or negotiating. This may be because we offered the user information on the attacker's reputation, which is itself a risk heuristic. (The attacker 60% likely to return data without selling, the risk is worth it).~~

~~We hope to have a thorough analysis and larger sample size by the final paper. In terms of future research, it may be worth it to expand the project in population size and scope - it may be worthwhile to conduct a separate session and take observation notes on the subject in order to construct a “stress” metric.~~