Tridium X Hacker Notes (4/1/2022)

First Game Feedback:

-Establish a presence in kids’ heads

-Hearthstone type of game, fighting covid but in a card game. It works and a viable way to communicate these things.

-Concern: Age range – too simplified for high school, more for middle school. Can you abstract this for most of the threats?

-Randomly select actions or give hints? Give context clues. There is something that sets it up, this guy lures you in, and you pick one out of the four options given to you. Cybersecurity is a lot of trial and error.

-In middle school student idea, fire- burn things up, wall-separate guy from me. What happens if I investigate? You get kicked out and have to try again. If it’s a wrong decision, how do I know it’s the wrong decision? What’s the consequence?

Find a way to abstract these concepts. If you’re not careful, it’s not just a fun game. What will they be getting from the game. What are the objectives we want to deliver from this game.

Second Game Feedback:

-Where do you figure out where the problem is. Which one of these is throwing a flag.

-Easier to teach, harder to execute

-Articulate how you want to show the cybersecurity into puzzle games, how does it translate into these puzzles?

Third Game Feedback:

-You have a botnet, those are the bad guys.

-How are you implementing the loop within the images.

-City – self contained breach scenarios.

-More linear level based type concept

-Does it pop up a question on every breach?

-Mini gamed based, there’s a minigame on each scenario.

-What age group?-younger 6-8th.

-Are you able to fix with other countermeasures? Work with a timer. Good choice, bad choice, how to fix it. Keep punishing the player more would be awesome. It causes another breach in somewhere else.

-Choose your adventure kind of approach. Lessons learned, are you helping them to learn why they made the right decisions.

-Bad decision -> zombie computers swarming you.

-Think through how you would teach the issues.