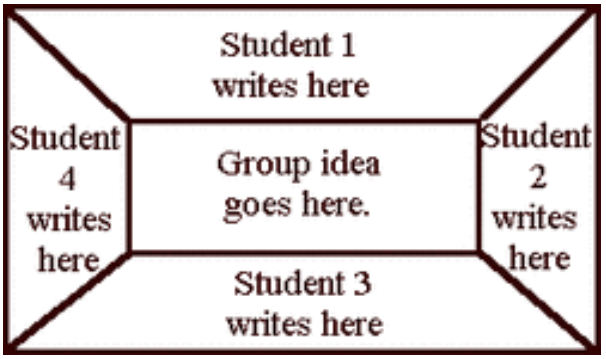
Lesson 1:
Class discussion of cyber crimes/ cyber events they have heard of and form groups around particular themes or events they are interested in.

Placement Activity: What I know/think already
Group discusses a particular cyber event/crime and pool their information. At this stage students may have conflicting views - this can be a rich source of questions they can investigate.
Prompt questions?

- ☐ What happened?
- ☐ Who was involved?
- ☐ What was the purpose of this event?
- ☐ Did anyone benefit from this event? If so, how? If not, why?
- ☐ Was anyone disadvantaged as a result of this event? If so, how? If not, why?
- ☐ What questions do I have about this event?



Lesson 2/3 Case study research

Groups decide how they will go about investigating a particular cyber event/cyber crime.
What do they want to find out? What headings will they use?
The guiding questions from week one can be used here but equally the questions or views/assumptions students have can be explored.
Group decides on the format of the case study and how they can present their findings. This is an opportunity for students to be creative, use the resources available to them, and present their findings comfortably. Consider wall displays, posters, digital storytelling (sways etc), video presentations, podcasts, dramatic retelling.

Lesson 4 Case Studies presented/viewed

Lesson 5: Reflection: What have I learned?
Students review their initial beliefs and opinions from week 1 and identify what they would change and what they would keep the same. They could repeat the placement activity to help them in this.
What advice would they give to people to avoid being a victim of this particular cyber event/ cyber crime?
Are there common themes arising from the different case studies?
What do they want to find out next about cyber security?