Novel Teaching Learning and Evaluation activities for imbibing the concepts of cyber security as perennial thought-process in the learners' digital life

Deepti Patole[1], Purnima Ahirao[1], Yogita Borse[1]

[1]Department of Information Technology, K J Somaiya College of Engineering,Mumbai
[1] deeptipatole@somaiya.edu
[2] purnimaahirao@somaiya.edu
[3] yogitaborse@somaiya.edu

Abstract: The use of Internet by students is growing exponentially every year. This younger generation learns technology quickly, but is ignorant about ensuring the safety by reading disclaimers or licenses before agreeing to them. Also they are more social online than in real world, hence they do not hesitate in sharing their life online which they probably won't share in person. These all things can result in some irreversible loss, if misused by cyber criminals. Thus it has become very necessary to make this young generation aware about security aspects of the digital world i.e cyber security. The objective was not just to make them aware of all the dangers present out there, but also to inculcate the safety habits in their day to day digital life. This could be only done by having complete interactive classes, rather than conventional teaching. Hence planning and execution of different teaching as well as evaluation methods were done, wherein the student's active participation was encouraged. The tasks included preparation of unique cyber- crime diary, Dramatization/Presentation, Video Creation, poster presentation. The Paper focuses on all Teaching- Learning techniques as well as evaluation methodologies used for creating awareness among the current generation about safe journey into their digital life. The paper also discusses the feedback received from students regarding the techniques and efforts used for enriching their knowledge about cyber security.

Keywords: Cyber Security, Threats, Cyber laws, Interactive Classroom Teaching. Evaluation methodologies

1. Introduction

Security is a vast domain and it plays a vital role when it comes to digital world. Internet is a two edged sword as it serves the humanity it can also be used against humanity. Now a days each and every individual is linked to internet for reasons such as banking, shopping, E-commerce and surely social networking. A common man using internet is usually aware of its uses and functionalities but unaware about the risks involved. This makes him/her the soft target of cyber-attacks. Eventually, these soft targets can work as gateways for the cyber criminals to malign any secure system. Human beings are social and have a natural tendency to trust, which makes them the weakest link of the security chain. Even though the highest possible security techniques are employed to safeguard the system, the system is still vulnerable to a simplest attack which is through a trusted user who is unaware of safety measures. This is possible because any system or application based in cyber space, needs to satisfy the requirements of end user as well as protect the system or application against any cyber-attack. There exists a thin line between safe and unsafe use of internet facilities. The internet is infinite and the threats are piggybacked to the numerous facilities it provides. Hence Cyber Security Awareness becomes a very crucial part of the world dominated by Internet. But this can only be effective, if the internet users get trained about the safety measures. Application of knowledge regarding the online safety in day to day online activities can prevent frauds and crimes from happening at the large scale.

Purnima Ahirao
[1]Department of Information Technology, K J Somaiya College of Engineering,Mumbai

email: purnimaahirao@somaiya.edu

2. Related Work

As suggested in article [1] the classroom teaching has evolved over the period from teacher centric to learner centric. The author has presented a model where the fundamental concepts can be learnt by learners outside the classroom as self-paced lectures, and the classroom teaching can be devoted to discuss the concepts with students in interactive manner, This also enables the teacher to redesign the course to achieve clearer understanding of the learners than that of a teacher centric classroom teaching [1][2][8]. The Micro-lecture is a critical component in keeping the class attentive on the important concept in discussion [1][3]. In flip-classroom, the pairing and sharing phase may result into loss of focus on the topic to be discussed in class as planned by instructor. Here these micro-lectures play a vital role of bringing the class on

right note, redirecting the discussion towards right direction and reinforcing the students discussion to make it fruitful. These micro-lectures are typically one to three minutes in length and are incorporated when needed on the basis of classroom dynamics. Micro-lectures are usually used for distance learning [4] where the students are learning on their own devices via video lectures and assignments. The conventional 45 minutes lecture does not serve good as the attention span, which is pretty less when studying in distance mode. Also in actual class where the instructor and students are co-located, the best attention span of students is not more than 10 minutes [5]. Hence micro-lecture within a flip-classroom plays a vital role of keeping the lecture on right track. According to the study[9][10], involving students in the form of a group or team and then giving them a case study makes their learning perceptions more clear as compared to Textbook Reading. The paper suggests that use of case study method of content delivery is significantly more effective than any other method. Presenting content in the form of stories and narrations increase the Bloom's taxonomy level of cognitive learning as suggested in the study[6].Case studies further facilitates interdisciplinary learning and understanding[11] and thereby roots the connections between the academic topic and the real world scenario which forms the crux of the topics in Cyber Security. The concepts of cyber security need to be learnt voluntarily by learners rather than taught by any instructor [9][10]. Thus from the research done on pedagogical techniques it can be observed that emphasis on effective learning is the vital objective of many researchers and practitioners.

3. Teaching and Evaluation Methodologies

The presented work in this paper is based on conduction of an interdisciplinary course "The Cyber Security Awareness" which is offered to Third year undergraduate Engineering students. The students are from different disciplines such as Computer, IT, Mechanical, Electronics and Electronics & Telecommunication. The course is conducted over one semester with a series of 3 lectures per week.

The course is designed in such a way that the learner will initially get essence of what cyber security is and will evolve to understand how to tackle different real life situations and stay safe online. Also the students are exposed to various Indian IT acts which provide introduction to legal aspect of cyber security. This course enables the learner to understand the risks present in cyber space. This knowledge cannot be imbibed in learner's life, if taught in conventional manner of one way teaching. It has to be an interaction session wherein the students actively participate in understanding the concepts. The knowledge gained should be guiding them in their real life to keep themselves safe. The active involvement of learner throughout the course is necessary to achieve this. To retain interest of students till the end of course and to get new students based on feedback of the ex-students is one of the purpose of many training course. Even here, the purpose was similar but with added responsibility of making more and more Engineering students aware and alert when dealing and working in digital world. The execution of the lectures was planned in such a way that the students would feel that they are involved in discussion. Hence the lectures would usually start with discussion on a real life case recently happened by referring some newspaper article or some other online resource. Students were encouraged to take part in discussion by giving their inputs about the case, like how and why that crime might have happened and how it could have been prevented, Whether they have had any similar kind of experience in past they would like to share. This approach made students part of discussion, rather than just listeners thereby imbibing the related theory concept in their day to day life. This also made them think about the way they should behave if similar situation arise in their own life in future. Also the Internal assignments were designed in such a way that, even if the student is doing average quality of work, he/she would need to explore the happenings around the globe for topic assigned. The aim of these assignments was to make the students peep outside their safe zone and understand the severity of the cyber-crime. Students gave quite a good feedback about the different ways of learning proposed for them, whereas the evaluation procedure based on rubrics was made easy. In order to make these lectures interactive but still stay on track of the concept to be discussed about, various teaching methodologies were used. To conduct these activities in the class a google classroom was created, where the students could access shared study material as well as students could be intimated regarding next class activities.

3.1 Teaching-Learning Methods

While conducting lecture sessions on Cyber Security and awareness, it was required to keep the content of the discussion contemporary as well as covering the fundamentals of cyber security. This is the reason the lectures were planned with the blend of Case studies around the globe and subsequent discussion about them in the classroom. Also classroom discussion about fundamental rules to be followed whenever dealing with netizens in this digital world was carried out. The overall structure of lecture session is as stated in figure1.

The Students were encouraged to go through the content shared with them via content sharing platform of Google classroom. This content was of following categories

a. Newspaper feeds related to cyber fraud or cyber security.

b. News Articles published related to recent happening in area of cyber frauds or crimes anywhere in the world.

c. The Reports published by government or government supported agencies, which contained the details and statistics related to cyber-frauds or crimes in past 1 year or so.

d. Videos on cyber-crime.

Content related to Cyber-crime cases shared 1 or 2days prior to lecture via Google classroom such as:

1. Newspaper Feeds
2. Case Studies published by International or national Agencies like Interpol, ENISA (ENISA 2019). Indian government
3. Videos

Class-room session: **55 minutes**

15 minutes: Discussion on contemporary case from newspaper related to concept planned for the lecture or Discussion on cyber- crime cases shared prior to lecture.
10 minutes: micro-lecture [4] emphasizing concept at length
10 minutes: Think-Pair-Share activity where students are made to think in a direction to come up with dos and don'ts when in similar situation narrated by instructor. Sometimes followed by poll to figure out inclination of students' thought process
10 minutes: micro-lecture [4] to clarify the misconceptions and provide further details depending on questions raised by students.
10 minutes: Interactive recap.

Fig 1: Outline of Teaching Learning method using case studies.

There were three ways of Teaching-Learning planned and executed, they are as follows:

- Case study
  - •Through Newspaper Feed
  - • Reports published by various international Government supported organizations in Cyber Security field
  - •Through Videos
- Think Pair Share Activity
- Flipped Classroom
- Micro Lecture

The brief details of the model used to conduct the classes are as follows.

3.1.1 Case Study:

First the type of attack was explained and then the real life case was discussed which makes the concept more clear. Also the precautionary measures as well as the IT act applicable were informed to the Students. The Students were also encouraged to share articles which they might have encountered in their day to day life. Some students used to share their own experience. They also did talk about any other articles which they encountered on internet or newspaper. Below mentioned are the sample news articles which were shared with Students during the lecture.

Case Example: Explanation of Cyber Stalking Case

Ff fig 2: Newspaper feed used in lecture for initialization of discussion.

As shown in the figure 2 the case of cyber stalking was shared with the students. important points about the case reflecting the cyberstalking crime was discussed by the teacher and students were also informed about how to avoid being victim of cyberstalking.

3.1.2 Think Pair Share Activity:

The students were asked some kind of analytical question based on a real life case. The students were given time of two to three minutes to think on that problem or case quietly. The students were made to sit as two to three students per bench. Every group were asked to share their thoughts about the problem for next 2 to 3 minutes. Later teachers helped in channelling the discussion and student's perspective about the problem was shared with whole class. Teachers then took part in discussion to appreciate the students analysis, discussed the matter with deeper concepts as well as to correct the misconceptions if any. This activity created a healthy environment amongst the classmates as well as teacher, wherein the doubts got cleared very easily and the concepts were absorbed by students much more effectively.

Example of Think Pair Share Activity: In this Students were asked to think about the overall security measures to be used while living in the digital world. Then they paired with their partners and shared their points. The Teacher then summarized and concluded the concept with steps required for precautionary measured of digital security.

3.1.3 Flipped Classroom:

Google Classroom was used for this activity. Students were given online resources. Students were asked to comment on the content shared online on the google classroom platform. This commenting was not mandatory and did not carry any evaluation, But was a source of looking at the direction the students were thinking about the concept for the teacher. And then the concept was discussed in the lecture session

in detail.

Example of Flipped Classroom Activity: Students had visited the link and discussion and clarification was carried out in the lecture session.

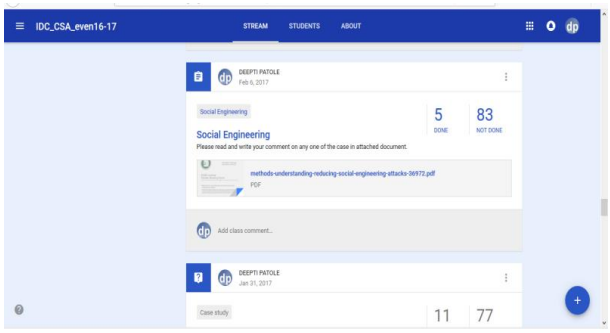
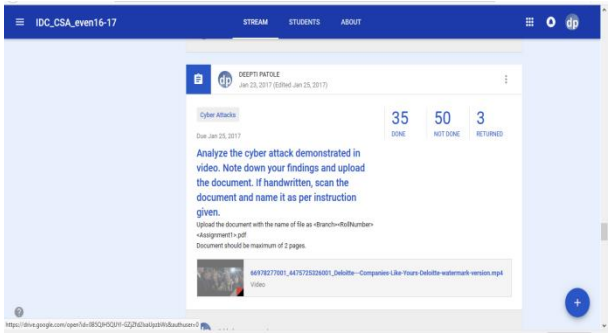


Fig3: Screenshot 1 of resource sharing for Flip classroom Activity over google classroom.

Fig4: Screenshot 2 of resource sharing for Flip classroom Activity over google classroom.



3.1.4 Micro Lecture: This was more of clearing the concepts, misconceptions and Summarization of overall content discussed. This was helpful in keeping the session in the purview of topics being discussed.

3.2 Evaluation Methods

The evaluation Methods used were designed in such a way that the student were asked to explore the online resources related to Cyber Security so as to complete the Task assigned. The assignments were unique for each student and hence students were needed to put genuine efforts in fulfilling the requirements of tasks. The tasks assigned as internal assessment were as follows:

3.2.1 Case Study Diary: Each Student was assigned a country and cyber-crime category namely Crime against Individual, Crime against Property, Crime against Government. For each of the case the student had to find at least 2 cases happened in history and write their comments as per following points.

1) How the crime might have taken place
2) How it could be prevented.
3) IT Laws applicable to the crime in those cases.

Example : A case study diary on crimes happened in Italy from the category crime against property was prepared by a student. In this diary the following details were included, such as

- The case article from the source
- Abstract in students own words,
- Analysis about how that crime might have happened ,
- Comment on how it could be prevented
- Which cyber laws can be applicable to such type of crime?


CYBER SECURITY AWARENESS

IA 2 - CASE STUDY 1

Topic: Cyber attack on property in Italy

Case article: Abusive computer system access, revealing industrial secrets by Six ex-Hacking Team Staffers

Case Article:

Six probed in Italian cyber crime investigation

Six former employees at the Milan-based HackingTeam, a controversial Italian firm which sells surveillance ware to governments and agencies with dodgy rights records, are being questioned over alleged cyber crime.

Fig5: Example of Case study Diary of Country Italy and Category Attack against Property.

Rubrics for Case Study Diary: Following Rubrics table was followed for evaluation of the Internal Assessment of Case Study Diary

Table 1: Rubrics of Evaluation Tool: Case Study Diary

	If any student scores 0 marks in case article selection criteria, all further marking scheme will be null. The complete scheme is applicable only on proper case selection as per assignment		
	Criteria	Considerations for evaluation	
1	Case Article (2 marks)	Proper Selection of Case (2-1marks)	Improper Selection of Case (0 marks)

2	Abstract (5 marks)	Proper Understanding of the article in own language (5-3 marks)	Improper Understanding of the article (2-0 marks)
3	View on how the crime might have happened (5 marks)	To the point interpretation and analysis of the crime (5-3 marks)	Vague interpretation and analysis (2-0 marks)
4	Precautionary and defensive measures (5 marks)	Plausible Identification of Defensive and preventive measures (5-3 marks)	Implausible Identification of Defensive and preventive measures (2-0 marks)
5	IT act applicable and reason (3 marks)	Reasonable Identification and justification(3 marks)	Irrational identification and no or incorrect justification (2-0 marks)
6	Total (20)		

3.2.2 Presentation or Dramatization:

Students were asked to explore any cyber-crime topic of their interest and Present it in the class either using PowerPoint Presentation or in the form of Drama. Many students presented the concept in the form of drama.

Rubrics for Presentation / dramatization / demonstration

Table 2. Rubrics of Evaluation Tool: Presentation/dramatization /demonstration

	Criteria	Considerations for Evaluation	
1	Content (5 marks)	Quality Content with deep study of the case (5-4 marks)	generic Content with vague study of the case (3-0 marks)
2	Question Answers (5 marks)	Answered >= 70 % of the audience and faculty questions (5-4 marks)	Answered <70 % of the audience and faculty questions (3-0 marks)
3	Presentation and Punctuality (10 marks)	Proper way of Presentation in form of slides/dramatization /demonstration with good group co-ordination and more than or equal to 75 % attendance for others presentations. (10-7 marks)	Improper way of Presentation in form of Slides/dramatization /demonstration with poor group co-ordination and less than 75 % attendance for others presentations. (6-0 marks)
4	Total (20 marks)		

3.2.3 Poster Designing:

The Students were asked to create Posters showing the different types of Cyber Crime cases, ways in which they are usually committed and also their preventive measures. Students had chosen wide range of cases/topics and prepared self-explanatory Posters for the same. Students were encouraged to use material with Creative commons license. And were evaluated with rubrics where weightage was given to inclusion of creative commons license in the poster they created to understand the concept of copyright.

Fig6. Example of Poster Submitted with Creative Common's License

Rubrics for Poster Designing

Table 3. Rubrics of Evaluation Tool: Poster Designing.

	Criteria	Considerations for Evaluation		
1	Content	**(6-5)** Self-Explanatory Poster with Excellent Coverage of content with appropriate diagrammatic representation.	**(4-2)** Good coverage of Content without diagrams	**(1-0)** Poor coverage of content and inappropriate positioning of content on poster.
2	Presentation And Question Answers	**(3-2)** Well-presented and well-answered with explanation and elaboration	**(1)** Presented but answers with no explanation and elaboration	**(0)** Poor Presentation And no answers
3	Openness of the resource	**(1)** Poster contains image of the creative commons license along with permissible operations on the resource		**(0)** No License has been provided.
4	Total	**10**		

3.2.4 Video Making:

Students also prepared Videos for different Cyber Crime categories and their causes as well as prevention. With this Students also explored different Video creating tools. Here the Students were also asked to do peer review of other' videos based on some criteria.

Following is the sample of video created by students to express their views and findings from the content they explored on their selected area in Cyber security. The Students shared video using YouTube services. This repository of all the YouTube videos' links was shared with all the students .

Case: 1. Sample Video screenshot of IA task submission

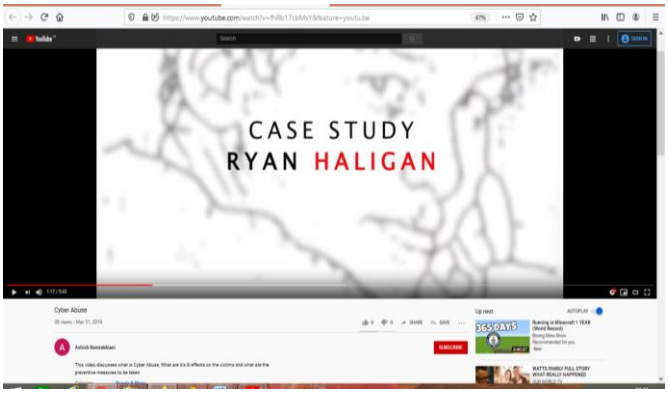


Fig7. Example of Video Created by Students based on Selected topic. Video Link[12]

Rubrics for Video Making:

Table 4. Rubrics of Evaluation Tool: Video Making.

Criteria	Considerations for Evaluation		
Content	**(6-5)** Self-Explanatory video with Excellent Coverage of content with appropriate diagrammatic representation .	**(4-2)** Good coverage of Content without diagrams	**(1-0)** Poor coverage of content and inappropriate planning of content in video.
Conclusion	**(2)** Well-summarized conclusion	**(1)** Inappropriate Conclusion	**(0)** Poor Presentation And no answers
References	**(1) Due credit given to resources used**		**(0) No references**
Open'ness of the resource	**(1)** Video contains image of the creative commons license along with permissible operations on the resource		**(0)** No License has been provided.
Total	**10**		

4. Results and Discussion

The interdisciplinary course was conducted for Third Year Engineering Students of disciplines namely Computer, Information Technology, Electronics, Mechanical and Electronics and Telecommunications. Number of students participating as Learners on an average is around 60. The overall conduction of lectures and evaluation was duly validated by timely feedback from learners during course conduction.

4.1 Overall Impact*:* Figure 8 shows the overall feedback given by the students for the techniques used for learning as well as for evaluation

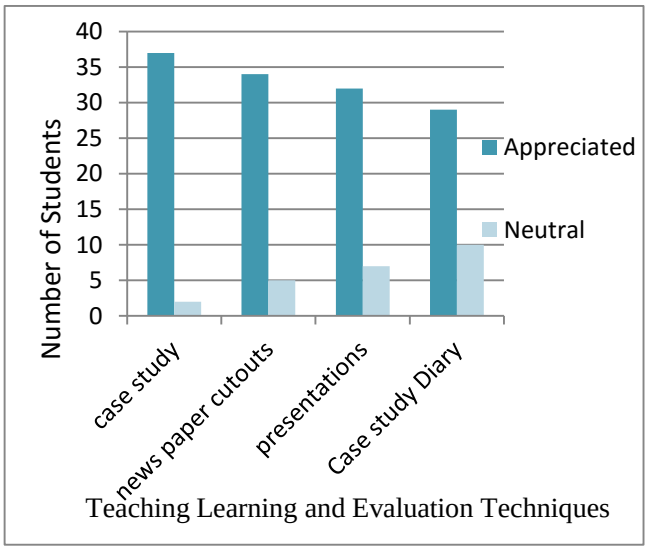


Fig 8. Feedback Summary of Teaching Learning and Evaluation methods used

4.2 Think Pair Share Activity Feedback

Feedback for Think Pair Share Activity: Students appreciated this method of learning by giving Feedback as shown in the figure 9. The feedback was collected from 14 students, who participated in activity.

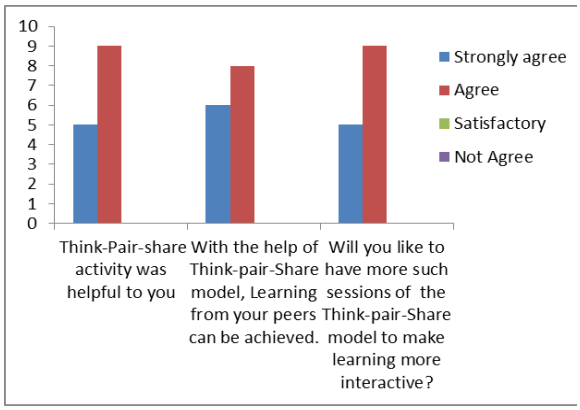


Fig 9 Feedback Summary of Think Pair Share activity

.4.3 Constructive feedback:

Different constructs were formulated and the feedback received was mapped to the constructs.

The formula used is

% of students response appreciating respective constructs =

(Number of students comments depicting fulfilment of concerned construct as well as Appreciation of the Technique /Total Number Responses Appreciating the Technique) * 100

Figure 10 shows the constructive feedback received from the students.

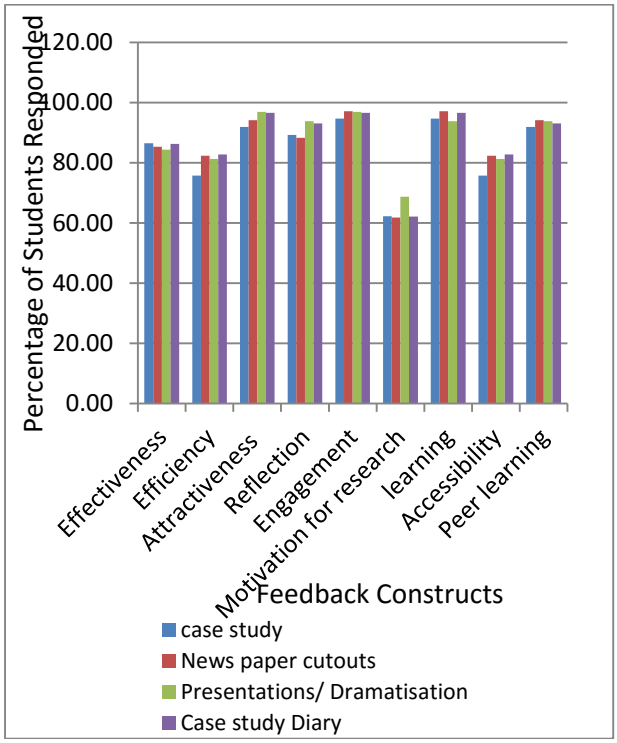


Fig 10 . Percentage of Students Appreciated the tools "Case Study, NewsPaper cutouts, Presentation/ Dramatization, Case Diary" and achievement of corresponding construct.

Figure 11 shows the constructive feedback received from the students for other evaluation tools.

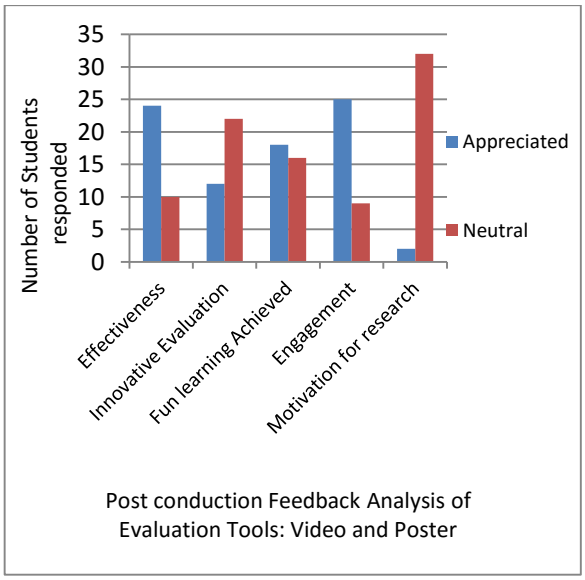


Fig 11: Feedback Analysis of Evaluation Tools: Video and Poster

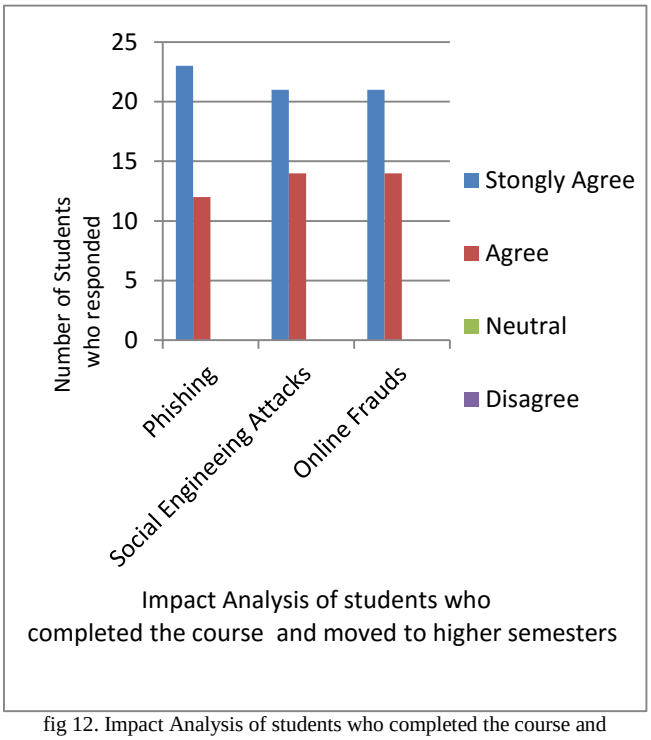


fig 12. Impact Analysis of students who completed the course and moved to higher semesters

Figure 12 shows the overall impact of the course understanding amongst the students after they moved on to the higher semester. From the feedback of students it could be concluded that the approach followed for the conduction of lectures was helpful for them in their day to day life. As they could feel the difference in their perspective of looking at Emails, phone calls as well as mobile messages they received. They could effectively analyse and identify cyber attacking scenarios as compared to genuine scenarios and accordingly keep themselves as well as their near and dear one's safe online

5. Conclusion

Using these various Methods and Techniques of Teaching Learning as well as Evaluation have played a vital role in imparting in-depth knowledge of the concepts of cyber security. It demanded learning technique which can be mapped to real life cases. Accordingly methods were chosen to cater to the way of understanding the concept which was interactive and one step ahead of awareness. As students are from engineering background, they were given the zest of the technicality of the attacks along with the alertness of the matter in concern. Feedback and positive comments from students emphasized that the methods used helped them to grasp the concepts in a very lucid manner.

These methods and techniques prove that changing the teacher centric approach to learner centric approach is useful for the better understanding of concepts which are important according to current generation perspective. The approaches mentioned in the paper also contribute for the lifelong learning of the students so that they continue to be safe in the digital world and also share the same in their social circle. The current generation are in the trap of Hyper-adoption where technological advancements are attractive and increasing significantly but there is no authority to control the hazards or disadvantages of this adoption. So the only way is, to make them aware and alert them about the ill effects.

Acknowledgement

We acknowledge that the work done in this paper was possible with immense support of our college, K J Somaiya college of Engineering.

We would also like to acknowledge one of our Senior colleague Mrs Shailaja Gogate Madam, for her immense support and guidance during the course conduction.

References

[1] Jacqueline E. McLaughlin, PhD, MS, Mary T. Roth, PharmD, MHS, Dylan M. Glatt, Nastaran Gharkholonarehe, PharmD, Christopher A. Davidson, ME, LaToya M. Griffin, PhD, Denise A. Esserman, PhD, and Russell J. Mumper, PhD , The Flipped Classroom: A Course Redesign to Foster Learning and Engagement in a Health Professions School , Academic Medicine, Vol. 89, No. 2 / February 2014

[2] Sarah J. DeLozier1 & Matthew G. Rhodes1Flipped Classrooms: a Review of Key Ideas and Recommendations for Practice, Published online: 6 January 2016 Springer Science+Business Media New York 2016, Educ Psychol Rev (2017) 29:141–151, DOI 10.1007/s10648-015-9356-9

[3] Kee TP. The one minute lecture. Educ Chem. 1995;32:100–101.

[4] Yang, Ying & Zhang, Xiaohui & Tian, Dan. (2017). Micro-Lecture Design and Practice In The Internet Plus Era. 10.2991/iccia-17.2017.120.

[5] Attention span during lectures: 8 seconds, 10 minutes, or more? Neil A. Bradbury, Advances in Physiology Education 2016 40:4, 509-513, doi:10.1152/advan.00109.2016.

[6] Anderson LW, Krathwohl D. A taxonomy for learning, teaching, and assessing: a revision of bloom's taxonomy of educational objectives, complete edition. Longman Publishing Group; White Plains, New York: 2000

[7] An argument and plan for promoting the teaching and learning of neglected tropical diseases

[8] Nadezhda O. Yakovleva, Evgeny V. Yakovlev, Interactive teaching methods in contemporary higher education, Pacific Science Review, Volume 16, Issue 2, 2014, Pages 75-80, ISSN 1229-5450, https://doi.org/10.1016/j.pscr.2014.08.016.

[9] Ian Cullinane, Catherine Huang, Thomas Sharkey, and Shamsi Moussavi. 2015. Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging. J. Comput. Sci. Coll. 30, 6 (June 2015), 75-81.

[10] Herreid, Clyde Freeman, and Nancy A. Schiller. "Case Studies and the Flipped Classroom." Journal of College Science Teaching, vol. 42, no. 5, 2013, pp. 62–66. JSTOR, JSTOR, www.jstor.org/stable/43631584

[11] Robert W. Scapens, Researching management accounting practice: The role of case study methods, The British Accounting Review, Volume 22, Issue 3, 1990, Pages 259-281, ISSN 0890-8389, https://doi.org/10.1016/0890-8389(90)90008-6. (http://www.sciencedirect.com/science/article/pii/0890838990900086)

[12] Sample Video link of IA task submission: https://www.youtube.com/watch?v=fhRb17LbMsY&feature=youtu.be accessed on 20th November 2019