ESSAY TITLE

E-tales of digitally (in)secure education

E-tales of digitally (in)secure education

> "*At first, there were scribbling all over the presentation like drawing hearts, stars around the margins and so on and then suddenly, the miscreant typed out* F*CK YOU *in bold red letters; all across her presentation. Honestly, we all went blank. Some students had their videos on; after this, many of them switched off their cameras… Ma'am's voice cracked midway and, she immediately closed the meeting.*"
>
> – Anisha (name changed),

a post-graduate student of a Central University of India, recalls witnessing her traumatic and utterly shocked (read shaken) senior professor's lecture on a zoom call.

Such is the present-day scenario! Morbid? Definitely, yes.

With pandemic infesting upon every nook and cranny of our lives, every aspect of our life and living has come to a standstill for the past couple of years (years or ages; I still ponder). The digitalisation of our tangible happiness has extended an extra inch of the problematic scenario. Was a threat to security and invasion of privacy any less in the 21st century, that at this juncture, we have to welcome an additional member, 'Cyber insecurity' too?

It is true with work from home schedules, 'schooling vis-à-vis teaching' from home has also begun in total swing (initially, with great enthusiasm and now crawling reluctantly). Focussing primarily on the online education sector, every hierarchical position has been affected by the pandemic's twisted whims. In this essay, I intend to argue that online education is a brewing ground of contestations with regard to security and relevance; thereby, stating the need for constant alertness while being online!

Why is online education gaining the centre position?

To begin with, the basic tenet of education is and forever will be to 'democratise' knowledge. For instance, if we consider the traditional model of teaching-learning mechanism, how far has this method achieved the earlier motto of education? Painstakingly, not much.

Statistically, a survey was undertaken in the United States of America that witnesses better learning spaces in the graduate online lectures than offline or the classroom lectures. Fifty-two per cent of the graduate candidates based in the USA nod in affirmation (Duffin).

The pedagogical shift from the physical to the virtual classroom has grown more inclusive. Students of any age, any background (in context to financial stability) and from any location can access material from anywhere in the world; thus, knowledge is just a click away. With better effectiveness, the online classrooms with a plethora of visual slides and fascinating audio-video presentations bring better retentivity factors amongst pupils.

Thus, quite evidently, online education has become very relevant and equally handy for students and teachers. The shift to the online mode is not an old phenomenon. It is this newness that has brought about a string of problematic episodes. The pandemic has forcibly shifted the classes from the offline to the online mode without any time to learn or process the steps to 'properly' use the online method for teaching and learning.

Online education and its various delivery platforms are being hindered every day with 'deliberate' errors. With students, the teachers are also facing trouble conducting the classes. This consequential cyber insecurity has pulled out a series of cyberbullying cases ranging from verbal insults to shameful pictorial depictions on-screen.

What are the major junctures of cyber insecurities?

> *"13-year daughter, who is a student at Asian World School, received sexually explicit content on her chat box in a private message in the midst of a web class on Zoom"*
> ("Abuse, bullying during online classes worry parents, teachers | Jaipur News").

Virtual sexual abuse Vs 13-year-old girl, an innocent mistake or a pathetic situation?

It is indeed a pathetic situation, and labelling such an act as an innocent mistake, simply 'neglects' the mental trauma the girl must have undergone. Contextually, it is imperative to understand that body politics remain an essential point of discussion even in the virtual world of abuse. Exoticising a gender and triggering psychosexual hate comments reveal not only the present looming problematic online mesh but also at large projects the degenerative tapestry of humanity.

Here, undoubtedly, this example explicitly showcases that the first attempt at cyberbullying in online classrooms is the 'sharing' of classroom links to students outside the respective institutions or miscreants hacking into classrooms. To some extent, restricting and locking up the online classroom may hinder the earlier proposition of democratising education but can create safer spaces. Additionally, the lecture(s) can be recorded, and the online materials distributed during the online sessions can, later on, be shared or uploaded online for better reach.

More often than not, the miscreants are registered students rather than an outsider. With students, many teachers and professors have and are continuing to face harrowing cyberbullying cases; on a daily basis. According to an article published by The New Indian Express (KK), many teachers had to take up part-time jobs (like delivering pizzas, or tailoring or working at local boutiques) during the pandemic induced financial issues to cater to their family needs in addition to their jobs at school. However, once the information of the part-time jobs was mischievously made public, many students started to bully their teachers in the disguise of changed or fake IDs. The online harassment went to an unimaginable extent to force a English teacher of Bengaluru to commit suicide as well. Many teachers have already quit their jobs to distance themselves from the mental trauma, and a close colleague of the deceased teacher further remarked regarding the pathetic scenario- "At least 14 teachers in our institute have quit, citing they were not ready to face these kinds of harassment from students" (KK). What is worse in this situation is not only being harassed but also being left alone without (legal or institutional) support to curb the menace.

In addition to the online classroom lectures, both the students and the teachers are exposed to online materials in terms of pdf, zip files and word documents for reference. Importantly, how safe are these websites that initiate 'hustle free' downloading?
Warning: freebies will always cost you more! Threatening? Meant it.

While downloading materials online, students (from both schools and universities) quite naturally tend to provide details like phone number, email id, name (and sometimes residential address too) and so on to the portals. One might ask, what is wrong with it? Well, when one provides the respective personal details online, he can easily get exposed to cyber hacking. The phone numbers linked to Aadhar cards (or any other identification cards) and bank accounts can soon position the person as a cyber victim with exposed identity, perhaps also looting money and the continuing thread of mental trauma.

In addition to the casual downloading of online materials, students and teachers also have to download various online applications like Google Meet, Zoom and Moodle (herein referring to the most used online platforms only) to access the regular online classes. Most of the time, downloading an unknown version, a pirated version, or a fake application with the same name as the earlier online applications can unknowingly cause major issues, thereby beginning the vicious cycle of cyberbullying, hacking, and depression. The first year of the pandemic witnessed significant reports of cybercrimes; accurately, "270,171 cases" were detected in the second half of 2020 ("Cyber threats in online education sector increased by 60% in H2 2020"). Amongst earlier mentioned online platforms, Zoom happened to be more prone to hacking than the rest.

Moreover, while teaching vis-à-vis submitting assignments, either party needs to share their screens to make the data available. At these hours, usually, "AnyDesk and Teamviewer Quick support" (Shinde) like applications come to the easy rescue. However, sadly, the easier the help arrives, the cybercrimes tiptoes around the same time. Scared? Better scared than an oops! These applications use a third-party connection which is highly prone to the insecurity that can let out credentials via a simple click. At present, rather than using these applications, the Universities and schools are using the 'share the screen' option available in Google Meet and Zoom Meeting. Yes, it is easy to use and more secure than the earlier mentioned online applications.

Having analysed the cyber threats and insecurities, how to layout a secure and encrypted online platform?

What is the way out?

The solutions to the present web of cybercrimes and cyber insecurity are many. The most important portal to start with is the warning! All the participants (from the highest authority to the students) of online education need to internalise the online platform(s) to be problematic. Hence, the caution to usher the constant need to be safe and tread on carefully. Simply internalising is not enough. There are certain red flags to look out for and consequentially raise the alarm for the respective issue and as a note of caution for the future victims (if any).

Prioritise Quality

At first, it is crucial to undertake a qualitative analysis of the cyber safety measures through the signposts of DOs and DON'Ts on the online platform. Remarkably, the Ministry of Home Affairs has introduced a segment on cyber education in the school curriculum for class VI and above students. With a mission to expand the cyber awareness program, 'Cyber Jagrookta Diwas' will be marked on the first Wednesday of every month of the year (Wadhawan). Also, the Department of School Education & Literacy, Ministry of Human Resource Development, Government of India, under its pilot scheme, 'Pragyata' has enlisted the potential ways by which the digital education needs to be conducted; involving the students (and the parents of pre-primary to primary students) and teachers. The most notable element in this scheme is ethical training. Yes! Online ethics are real! Mind your netiquettes, please! Likewise, students need to be appropriately taught with practical lessons to infuse in them the need to be respectful in all circumstances. For instance, being physically absent (like on an online call) or being anonymously present virtually ought not to be seen as an advantage to bully either the peers or the tutors. Through these practical lessons, the students will be capable of imbibing (online) integrity and will essentially build a good moral character.

Most importantly, the online safety-related curriculum needs to curate and prioritise material for all students (providing exceptional care for the differently-abled children). Along with these safety measures, the scheme offers additional filtered content by collaborating with Universities and schools to provide them with internet connections. Notably, these internet connections will sieve to block out obscene and malicious content (which can lead to cases of sextortion and sexting).

Being mindful of all the possible qualitative measures, have we forgotten an utmost important safety measure? Sadly, yes! Mental peace, health and sanity. The online lectures need to be appropriately distributed during the day. The assignments, rather than being strenuous, can be creative. All these little gestures in the large academic world will help in boosting the mental capacity of the students vis-à-vis the teachers. Resonating with NCERT's "Safe to learn _ English.", the online education which has magically erased the line differentiating the comforting home and the scheduled classroom has to provide space for the mental blossoming. Better the spirit, better will be the retentivity!

How about quantity now?

In addition to the qualitative cyber safety measures, quantitative or case specific cyber security measures should also be undertaken. To begin with, the potential threats to online education sadly comes from both ends (the students and their teachers or professors). One might sadly recall the shocking incident which took place during an online lecture conducted by Seema Singh (an Associate Professor of IIT Kharagpur) wherein she allegedly lashed out Casteist slurs at the marginalised students. The professor, after her alleged 'obnoxious' comments, arrogantly stamped an upper hand on the case, "The professor at IIT KGP is all-powerful…What I have to do, I will do. You can go to the Ministry of Women and Child. Go to Ministry of SC, ST, and Minorities (sic). Nothing can prevent me from doing what I have to do to you" (Murti). Surprisingly, could the professor have this 'supposed' upper hand or liberty during the offline classes; I hope not. So, the online education platforms also posit a space for unimaginable indecency under the garb of 'virtual flexibility'. During these instances of cyberbullying (particularly on the grounds of caste and class), the victims can lodge complaints first at the institutional level and then right up to the respective Ministry. Likewise, in this case, the Professor was suspended by IIT Kharagpur, and the National Commission of Scheduled Castes are yet to take further 'concrete' action (Sahoo).

Daily, all the participants in the online education system need to adhere to a list of protocols in order to look out for the red flags. While attending an online lecture, the students should name their systems with their official names and roll numbers (as registered with the academic institutions). They should join the links from verified sources only. For instance, the professors can send across email id specific invites; these invites will be encrypted and hence, will not be hindered by outsiders or miscreants. These invitation links can be enabled in both Google Meet and Zoom. Additionally, receiving inappropriate messages or remarks during the scheduled online lectures or afterwards needs to be registered with the higher authority.

The deal, as mentioned above, is possible when the audience is a known one. What if the audience is an unknown one? The host can generate public links for the latter, and the targeted audience needs to register for the lecture at their own ease. Most importantly, when a shared link is generated, the host should record the entire lecture with continuous monitoring of the chat box. The host and the users can take up this precaution religiously and save themselves from lewd comments that may sail through phishing attacks. The phishing attacks usually hack personal meetings and draw out personal credentials that can further dismantle

the workings of the computer (through the inflow of uncontrollable downloading of various malware applications).

Most often than not, for accessible communication, the teachers tend to create WhatsApp or Telegram groups for distributing the study materials and the assignments. Consequentially, the participants' phone numbers in these online groups soon become visible to all. Usually, the girls become easy targets in these situations wherein they constantly receive remarks drenched in sexual innuendoes, nasty comments and inappropriate images. To restrict the flow of these messages, the students can move to the settings of these applications and enable the privacy options, which will help them hide their phone number from the gaze of the other fellow group members.

Furthermore, while downloading online materials, be it in the form of PDF or word files, the users need to be extra careful. Notably, the users tend to download PDFs more as compared to the latter because of their reliability and readability factors. Unfortunately, the cybercriminals are targeting these documents to infuse various malicious programs in them, which can reveal personal credentials and bank details at a single click ("Safety and security on the Internet"). The PDFs are mostly filled with spyware and malware to disfunction the personal computers and make them a hub of cyber oriented viruses. Various spam messages can also get generated in the respective email ids by downloading fake applications and malicious PDFs. If opened, the spam or the unsolicited messages can soon gain access to passwords of all the accounts linked to the email ids (and yes! Also, to your bank accounts). Beware!

Therefore, it is vital to ensure strong passwords for all online websites ranging from email to online research paper downloading websites. A quick hammering! Passwords need to be complex, different for all the websites, and should not be disclosed to anybody else. Always sharing is not caring! Sometimes sharing can invite risks as well. Honestly, why transform sharing into daring?

Online education: Fragile. Handle with Care.

With everything shifting online, from pharmacy to job cubicles, the online platform indeed needs to be secured and 'dignified'. In the same line of events, witnessing the ongoing pandemic surge, the continuation of online education also seems to be a long term investment. Since online education is still on the pitch, online safety precautions and preventions are

equally necessary. In addition to the doable external help and arrangements, users need to internalise the netiquettes. To recapitulate in a nutshell, one needs to necessarily go with the flow; but tactfully derail from falling prey to insecurities. And yes! While keeping safe from the cyber virus, remember to distance out from the Coronavirus too.

Too much work! Indeed!

Works Cited

"Abuse, bullying during online classes worry parents, teachers | Jaipur News." *Times of India*, 21 January 2021, https://timesofindia.indiatimes.com/city/jaipur/abuse-bullying-during-online-classes-worry-parents-teachers/articleshow/80373538.cms. Accessed 11 December 2021.

"Cyber threats in online education sector increased by 60% in H2 2020." *HT TECH*, 14 February 2021, https://tech.hindustantimes.com/amp/laptops-pc/news/cyber-threats-in-online-education-sector-increased-by-60-in-h2-2020-71613304733584.html. Accessed 12 December 2021.

Duffin, Erin. "• Why administrators at higher education institutions chose to create an online program US 2019." *Statista*, 17 May 2021, https://www.statista.com/statistics/731103/reasons-why-administrators-of-higher-education-institutions-chose-to-create-an-online-program-us/. Accessed 11 December 2021.

KK, Karthik. "Lewd texts, bullying during e-classes leave teachers helpless." *The New Indian Express*, 15 October 2020, https://www.newindianexpress.com/states/karnataka/2020/oct/15/lewd-texts-bullying-during-e-classes-leave-teachers-helpless-2210363.amp. Accessed 11 December 2021.

Murti, Aditi, et al. "IIT Kharagpur Professor Filmed Using Casteist Slurs Once Published a Study on Social Inclusion." *The Swaddle*, 27 April 2021, https://theswaddle.com/iit-kharagpur-professor-filmed-using-casteist-slurs-once-published-a-study-on-social-inclusion/. Accessed 15 December 2021.

"Safe to learn _ English." *NCERT*, https://ncert.nic.in/pdf/announcement/Safetolearn_English.pdf. Accessed 15 December 2021.

"Safety and security on the Internet." *WHO | World Health Organization*, https://www.who.int/goe/publications/goe_security_web.pdf. Accessed 15 December 2021.

Sahoo, Priyanka. "IIT suspends professor for remarks on SC, ST students." *Hindustan Times*, 13 May 2021, https://www.hindustantimes.com/india-news/iit-suspends-professor-for-remarks-on-sc-st-students-101620866328960.html. Accessed 15 December 2021.

Sarkar, Brinda. "How life has been for our children in this pandemic." *Telegraph India*, 12 November 2021, https://www.telegraphindia.com/my-kolkata/lifestyle/how-life-has-been-for-our-children-in-this-pandemic/cid/1838538. Accessed 12 December 2021.

Shinde, Shalaka. "Online theft cases using remote access apps on the rise." *Hindustan Times*, 5 August 2021, https://www.hindustantimes.com/cities/others/online-theft-cases-using-remote-access-apps-on-the-rise-101628102445878-amp.html. Accessed 12 December 2021.

Wadhawan, Aditya. "Cyber security courses: Cyber security courses in schools for increased safety." *Times of India*, 15 November 2021, https://timesofindia.indiatimes.com/home/education/news/cyber-security-courses-in-schools-for-increased-safety/articleshow/87719896.cms. Accessed 12 December 2021.

DETAILS OF THE PARTICIPANT

NAME: SHARBARI GHOSH
UNIVERSITY REGISTRATION NUMBER: 393648
COURSE NAME AND YEAR: MA ENGLISH LITERATURE;
FINAL YEAR (2020-2022)
NAME OF THE DEPARTMENT: DEPARTMENT OF ENGLISH
NAME OF THE UNIVERSITY: BANARAS HINDU UNIVERSITY

DETAILS OF THE HEAD OF THE DEPARTMENT

NAME: PROF. KRISHNAMOHAN PANDEY
CONTACT DETAILS: 9450871426