



Secure Communications on Online Learning Platforms

PROF. SHARAD SINHA,
HEAD, DEPARTMENT OF TEACHER EDUCATION, NCERT

Need for secure communications

Recent years have witnessed a sudden shift and increased use of technology by the teachers

- With the sudden shift to remote and hybrid learning models, teachers had to quickly adapt to digital tools and online platforms to continue delivering education
- These platforms offered a wide range of features and functionalities to support teaching and learning, communication, assessment, professional development, and collaboration among educators
- It's important for teachers to explore these platforms, consider their specific needs and preferences, and choose the ones that align with their teaching goals and objectives
- It is crucial for teachers and users to be aware of the potential threats associated with the use of online platforms.



Initiatives by the MoE

- DIKSHA (Digital Infrastructure for Knowledge Sharing)
- E-Pathshala
- National Repository of Open Educational Resources (NROER)
- SWAYAM (Study Webs of Active-Learning for Young Aspiring Mind)
- VIDWAN



Online Platforms

- There are several online platforms specifically designed for teachers to support various aspects of their work. Some popular online platforms used by teachers are:
- Learning Management Systems (LMS):
 - Google Classroom
 - Canvas
 - Schoology
 - Blackboard
 - Moodle



Communication & Collaboration Tools:

- Microsoft Teams
- Zoom
- Slack
- Remind
- Edmodo



Content Creation and Sharing Platforms

- Nearpod
- Pear Deck
- Flipgrid
- Padlet
- Seesaw



Assessment and Grading Platforms:

- Kahoot!
- Quizlet
- Socrative
- Edpuzzle
- GradeCam



Professional Development and Networking:

- EdWeb
- TeachBoost
- Edutopia
- Twitter (educator communities and chats)
- LinkedIn Groups (education-focused groups)



Virtual Classroom Platforms

- Microsoft Teams
- Google Meet
- Zoom
- Cisco Webex
- Big Blue Button



Curriculum Resources and Lesson Planning:

- Teachers Pay Teachers
- Share My Lesson
- CommonLit
- BetterLesson
- PBS LearningMedia



Online Student Engagement and Gamification

- Classcraft
- Breakout EDU
- ClassDojo
- Gimkit
- Quizizz



Internet Safety

- Internet is a public space
- It's intertwined closely with our online lives
- Effects are far reaching
- Understanding importance of Netiquettes
- Importance of clean digital footprints is important
- Identifying online predators
- Awareness of IT Act, including clauses that deal with hacking, stealing of data
- Knowledge of modifying privacy settings on FB, WhatsApp, Insta, LinkedIn etc.



Major security issues in online communications

- Phishing
- Data breaches
- Malware and viruses
- Weak authentication and access control
- Lack of encryption
- Insider threats
- Social engineering
- Insecure file sharing
- Privacy concerns



What should the Teachers do?

To mitigate these security issues:-

- **teachers should practice strong password hygiene,**
- **enable two-factor authentication (2FA),**
- **use secure and encrypted communication channels,**
- **stay vigilant for phishing attempts,**
- **keep software and devices updated,**
- **follow best practices for online security and privacy.**
- **stay informed about emerging security threats**
- **regularly review and adhere to their institution's security policies and guidelines.**



Contd.

- **Choose reputable and secure platforms:**
- **Use secure and unique login credentials:.**
- **Encrypt communications**
- **Be cautious with file sharing:**
- **Verify recipient identities**



Contd.

- **Be vigilant and sceptical**
- **Learn to identify phishing attempts**
- **Never share sensitive information**
- **Enable two-factor authentication (2FA)**
- **Use strong, unique passwords**



Contd.

- **Be cautious with links and attachments:**
- **Keep software and devices updated:**
- **Educate students and colleagues:**
- **Report suspicious activity:**
- **Stay informed**
- **Following reputable sources**



Thanks!

