FAQs on Zoom, Privacy, and Security at UC Davis

1. What are the top 10 things that I can do to ensure security and privacy of my Zoom sessions?
2. What is Zoombombing?
3. How do I protect against Zoombombing and what are the top features I need to be aware of?
4. What do I do if I have been Zoombombed?
5. Can instructors be liable for privacy violations on Zoom?
6. Are the privacy concerns with Zoom and Facebook relevant to the campus?
7. Should Zoom be used on the encrypted setting only?
8. Are there privacy concerns with the release of recorded lectures?
9. How long may I retain my course's recordings?
10. How do I protect my faculty Intellectual Property (IP) rights with Zoom lectures? What if lectures have been made available to students then shared with others?
11. Zoom generates attendee reports for the instructor. Reports list a student's mobile telephone number as well as their email address. Is this allowed under FERPA laws?
12. Are there privacy concerns with the Zoom Attention Tracker feature?
13. Are student privacy or FERPA guidelines relaxed during the pandemic?
14. What information does Zoom collect? How do Zoom's privacy protections compare to similar platforms?
15. Has the campus assessed Zoom's security?
16. Who do I contact for answers to general questions about Zoom, outside of security and privacy concerns?
17. These FAQs didn't address my concern. Who should I contact for help or request an update to these FAQs?

Answers to FAQs

1. **What are the top 10 things that I can do to ensure security and privacy of my Zoom sessions?**

    1) Use the most current version of Zoom;
    2) Do not post Zoom links or invites on social media including public websites;
    3) Use a unique ID for each meeting;
    4) Utilize meeting passwords;
    5) Turn off embed password in meeting link (if applicable, this will force users to type in a password rather than have one click access);
    6) Enable Waiting Rooms and have the host allow users in one by one, or all at the same time, once all attendees have been verified;
    7) Authenticate users: Accept connections only from a specific domain (if applicable to your domain only, account settings only);

8) Lock meetings once all participants have joined (if applicable);
9) Disable file transfer settings (during zoom meetings; not necessary in basic chat);
10) Contact your local IT resource if you need help/support

How-to guidance on the above can be found here.

2. **What is Zoombombing?**

   Zoom sessions that are not password protected can be hijacked or joined by uninvited individual(s). This flaw gave rise to Zoombombing, a type of cyberattack, where an individual(s) would enter a Zoom meeting and broadcast obscenities or take control of the screen.

3. **How do I protect against Zoombombing?**

   To reduce the risk of Zoombombing, follow these tips recommended by the FBI:

   - Do not make meetings or classrooms public.
     In Zoom, there are two options to make a meeting private: require a meeting password and/or use the waiting room feature and control the admittance of guests.
   - Restrict meeting participants to those who are logged into Zoom or even to those with a UC Davis computing account.
   - Do not share a Zoom link on a social media post or other public website. Provide the link directly to specific people.
   - Manage Zoom screen-sharing options by disabling participant screen-sharing or changing screen-sharing to "Host Only."
   - Update your Zoom app to ensure you have access to the latest fixes

   Zoom has additional recommendations on its privacy and security page and best practices for securing your virtual classroom.

4. **What do I do if I have been Zoombombed?**

   Call the IT Express Desk at 530-754-HELP.

   Use the Zoom toolbar security options:

   - Disable Video
   - Mute participants
   - Turn off file transfer
   - Turn off annotation
   - Control recording
   - Or end the meeting

- Remove participants

You should also report the incident to the UC Davis Information Security Office at cybersecurity@ucdavis.edu and the Privacy Office at privacy@ucdavis.edu.

5. **Can instructors be liable for privacy violations on Zoom?**

   Instructors are not liable for Zoom flaws. As long as you are using Zoom as recommended by the campus, not posting your lectures on a publicly accessible website, and students are adequately advised of privacy-protective alternatives, we do not see any reasonable basis for instructor liability.

6. **Are the privacy concerns with Zoom and Facebook relevant to the campus?**

   The recent privacy concerns were limited to the Zoom iOS app. Therefore, the issue impacted only individuals who use Zoom on an iOS/Apple device. Zoom has since stated that that code was fixed and that there is no longer sharing with Facebook. If you use Zoom on an Apple device, please make sure your Zoom version is updated. The most recent version of Zoom is available at https://support.zoom.us/hc/en-us/articles/201362233-Where-Do-I-Download-The-Latest-Version-.

7. **Should Zoom be used on the encrypted setting only?**

   Yes, Zoom meetings are encrypted by default.

8. **Are there any privacy concerns with the release of recorded lectures?**

   Yes, we encourage faculty to avoid the "publish" link on Zoom. This link is shareable and could be re-posted on a public website. Instead, faculty are encouraged to use Aggie Video to share lectures with students, which allows sharing to be limited to UC Davis. Also, ensure that you have programmed the customized, pop-up notice to students telling them what they can and cannot do with the recordings or screen shots; this will further limit inappropriate sharing or use. An example pop-up notice that can be used for all meeting recordings:

   "This session and any personal information you share during the session will be recorded for the purpose of facilitating the course and/or test environment. Participants are prohibited from redisclosing, posting, or transmitting session information. Students who wish to opt-out of being personally identified while recorded must contact the instructor immediately and may use an instructor-authorized alternative."

9. **How long may I retain my course's recordings?**

   Recordings should be deleted once they are no longer needed for their educational purpose. Your Zoom administrator can set "automatic deletion" settings for all

recordings after a certain number of days. Some units have established 100 days as the automatic deletion period, with a reminder of 7 days before the automatic deletion and a 30-day safety valve for instructors who forget after the 100 days and want to retrieve their lectures.

10. **How do I protect my faculty Intellectual Property (IP) rights with Zoom lectures? What if lectures have been made available to students then shared with others?**

    Students should be advised that lectures must not be shared with anyone outside the classroom. Inappropriate sharing may be subject to discipline pursuant to the university's student misconduct policies. Please see the following guidance on protecting an instructor's IP rights: https://www.library.ucdavis.edu/service/scholarly-communications/instructor-copyright/.

11. **Zoom generates attendee reports for the instructor. Reports list a student's mobile telephone number as well as their email address. Is this allowed under the Family Educational Rights and Privacy Act (FERPA)?**

    FERPA allows a student's mobile phone number and email address to be communicated to an instructor, provided the instructor does not further disclose that information and limits the use of that information for the student's legitimate educational interest.

12. **Are there privacy concerns with the Zoom Attention Tracker feature**?

    Due to privacy concerns, this feature was permanently removed by Zoom on April 2, 2020. See https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking

13. **Are student privacy or FERPA guidelines relaxed during the pandemic?**

    The Department of Education issued COVID-specific FERPA guidance, advising that the FERPA Health & Safety Emergency Exception may be used to respond to COVID-19 pandemic safety needs: See https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf.

    The Department of Education also reissued Remote Learning Guidance at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20%20Virtual%20Learning%20032020_FINAL.pdf.

14. **What information does Zoom collect? How does Zoom's privacy protections compare to other similar platforms?**

Zoom's current Privacy Policy (revised March 29, 2020) commits to never selling customer information and to not using customer data stored on the Zoom app for advertising.

Although Zoom's privacy policy (https://zoom.us/privacy) describes how and the extent to which data is used and collected, that privacy policy has recently been criticized as needing to be more specific. Zoom has acknowledged these criticisms and committed to changes and a more detailed policy in the coming months. The UC Davis Privacy Office and Information Security Office will continue to monitor Zoom's privacy policy changes and practices.

15. Has the campus assessed Zoom's security?

The UC Davis Information Security Office Vendor Risk Assessment team has reviewed Zoom, including its third-party attestations regarding security. The team completed a formal risk assessment report for the campus Chief Information Security Officer and Chief Information Officer. If you have questions about Zoom and the results of this assessment, please contact cybersecurity@ucdavis.edu.

16. I have other more general, non-security and non-privacy questions on how to use Zoom. Who can help or where can I find additional resources?

The Zoom section of the Keep Teaching website should be your first stop: https://keepteaching.ucdavis.edu/zoom-web-conferencing.

The IT Knowledge Base websites also have resources and helpful articles:

- Zoom guide for faculty, http://kb.ucdavis.edu/?id=5640
- Zoom guide for staff, http://kb.ucdavis.edu/?id=5704
- Zoom guide for students, http://kb.ucdavis.edu/?id=5642

17. **These FAQs didn't address my concern. Who should I contact for help or request an update to these FAQs?**

If you are aware of other Zoom security and privacy issues, please contact the UC Davis Privacy Office at privacy@ucdavis.edu, and the Information Security Office at cybersecurity@ucdavis.edu.

Help us improve this campus resource as we are continually updating these FAQs and working on solutions to emerging issues.