

From: Mark Silis and Krishna Rajagopal teachremote@mit.edu
Subject: Securing Zoom meetings and classes to prevent disruption
Date: March 29, 2020 at 12:01 PM
To: fisherp@mit.edu



Mark Silis, Vice President for Information Systems and Technology
Krishna Rajagopal, Dean for Digital Learning

To the MIT community:

As MIT gears up for remote classes starting Monday, we know that many of you are using or planning to use Zoom to facilitate your teaching, learning, and day-to-day work. We have heard your concerns about recent reports of people abusing features of the Zoom platform to disrupt online meetings, and are taking steps to prevent such disruption to MIT's online learning environment and broader community.

MIT has worked with Zoom to provide greater security options for all MIT meetings and webinars using mit.zoom.us, including those for online classes as well as other individual or group purposes.

Choose security to prevent disruption

Effective Sunday, March 29, new meetings and webinars now have the option of requiring participants to authenticate using MIT Touchstone to join. Note that **individual hosts MUST choose [these settings](#)** on a per-meeting (or per-account) basis.

Guidelines for all MIT Zoom meeting hosts:

- For sessions that are part of our **remote teaching effort**, we **strongly urge** allowing only **Touchstone-authenticated** participants.
- For uses other than remote teaching, if non-MIT attendees are invited, we strongly recommend requiring a meeting password.

MIT does not recommend allowing attendees to join any Zoom session without requiring either a password or Touchstone authentication.

Preserve safety and choice

Requiring user authentication will prevent the most common “ZoomBombing” scenarios that have been reported, while allowing MIT to continue to leave other features unchanged and available for virtual interactions. Choosing this approach allows us to try to safely preserve the same dynamic and flexible environment MIT is known for in this new remote teaching, learning, and working paradigm.

Update your existing meetings

We strongly urge you to consider updating any meeting you have already created to require Touchstone authentication for all class sessions and any MIT-only meetings, or to require a password if non-MIT attendees are invited, as this new option will not be automatically applied retroactively.

Use best practices

If you are using Zoom for meetings, classes, or events with people from outside of MIT, please be mindful of the risks and use appropriate settings to minimize disruption and support your needs.

For more information and tips on providing a positive online teaching, learning, and working experience for you, your students, and your colleagues, visit this [Knowledge Base article](#), and this [blog post](#) from Zoom.

Data privacy

We have also been asked recently about data privacy. MIT’s contractual agreement with Zoom was developed by a consortium of US higher-education institutions and provides protections for the security and privacy of our data. In addition, all videos that any of us produce on Zoom and store in the Zoom Cloud can only be accessed by those who authenticate using MIT Touchstone.

Contact support

For 24x7 support from Information Systems and Technology (IS&T) for students, as well as for non-teaching IT needs, contact:

- servicedesk@mit.edu
- or call 617-253-1101

For resources, tools, and support for those teaching remotely, visit [MIT’s Teach Remote website](#) and the [Teach Remote community](#).

For specialized 24x7 support for remote teaching/class facilitation for instructors, contact:

- teachremote@mit.edu
- or call 617-324-3578 (617-32-HELP-U)

Thank you,

Mark Silis

Krishna Rajagopal

Massachusetts Institute of Technology
77 Massachusetts Ave | Cambridge, MA 02139
This e-mail has been sent to fisherp@mit.edu.
[Unsubscribe](#) or [report a technical issue](#).