4-3-2020

Coronavirus Community Updates_UMS-IT Zoom Security Update, April 2

University of Maine

Novel Coronavirus Community Updates

Frequently Asked Questions

VIEW ALL FAQS

Resources and updates

- Remote teaching resources from CITL
- Remote learning resources from UMaine Online
- Tools for remote work, teaching and learning from UMS Information Technology
- U.S. Centers for Disease Control and Prevention Coronavirus Disease information
- Maine Centers for Disease Control and Prevention Coronavirus Response
- Maine Emergency Management Agency
- Latest announcements from Maine Governor's Office
- University of Maine System Information and updates regarding Coronavirus
- Innovation partnership for COVID-19 response

UMS-IT Zoom security update, April 2

April 3, 2020 | Coronavirus, UMaine and UMM updates, UMS

With the increased need for remote instruction and telecommuting over the past weeks, Zoom has become an essential and indispensable tool for many of us — not just here in the University of Maine System, but worldwide. This increased attention has brought with it increased scrutiny and concern around the security and privacy practices of Zoom. Zoom has responded quickly to these challenges, and we wanted to provide the UMS community with an update on a couple of key items on this front:

Zoom Application Security

Security experts have identified flaws with both the Mac and Windows versions of Zoom, including an exploit that could allow malicious actors to steal your Windows credentials or more. Zoom has patched these items and released updates to their Mac and Windows applications. US:IT is strongly advising all users to update their Zoom applications as soon as possible. This can most easily be done by opening the app, clicking on your profile picture in the top right, and selecting Check for Updates. For more information on updating, please see this Zoom Support article. Please note that we also strongly advise individuals to never click on a link provided in chat, email, or elsewhere by someone that you do not know or trust.

Zoom Bombing

Another risk is "Zoom Bombing," which involves malicious actors joining a meeting and using hate speech, sharing inappropriate images, and more. There are a number of steps that you can take to protect your meetings to help prevent this from happening. This includes: not sharing Zoom meeting links publicly; using a waiting room in the meeting; requiring a password to connect to a meeting; limiting who can share their screen in a meeting; and restricting who can chat with each other in a meeting. For more information on how to better secure your meetings or classes, please visit our Zoom Bombing Support Page.

If you have any additional questions or concerns, consult the US:IT Zoom Support Resources page or contact US:IT Support. For more information on all of the steps that Zoom is taking to ensure the safety and privacy of their customers, please review this letter from Zoom's founder and CEO.

At UMaine, the Center for Innovation in Teaching and Learning offers additional information on Zoom.