Spring 2020

IT_Zoom Security Updates

University of Maine System Information Technology

Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

Matthew Revitt <matthew.revitt@maine.edu>

IMPORTANT - ZOOM Security Update & Information

1 message

IT at UMaine <it.at.umaine@maine.edu> Thu, Apr 2, 2020 at 4:56 PM
Reply-To: IT at UMaine <it.at.umaine@maine.edu>
To: UM-EMPLOYEES@lists.maine.edu

Dear UMS Students, Faculty, and Staff,

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 within the UMS, but worldwide. This increased attention has brought with it increased scrutiny and concern around the security and privacy practices of Zoom. To their credit, 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 identified flaws earlier this week 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 that has presented itself 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, please feel free to consult our US:IT Zoom Support Resources page or to 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.

Sincerely,
The US:IT Zoom Support Team