New Zoom password requirement notice

What is happening?

When you log into maine.zoom.us with your @maine.edu account tomorrow, the following two settings will be enabled:

1. Require a password when scheduling new meetings
   A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

2. Embed password in meeting link for one-click join
   Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

When is this happening?

Thursday, April 9th

What is happening?

When you log into maine.zoom.us with your @maine.edu account tomorrow, the following two settings will be enabled:

1. Require a password when scheduling new meetings
   A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

2. Embed password in meeting link for one-click join
   Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

Why is this happening?

This is to help improve the experience and security of hosting meetings and classrooms with Zoom. While you may change these settings on your own, IT strongly recommends leaving it in place in order to protect your meetings or classes from unwanted guests, otherwise known as Zoombombing.

What else can you do to reduce the risk of Zoombombing?

Make sure you have the latest version of Zoom with all of the security and feature updates. More information about Zoom and how to update your application is available on our Zoom Support Resources page.

Minimize the use of Personal Meeting IDs (PMI). IT suggests that you use these sparingly as these meeting IDs never change which makes them an easier target for Zoombombers and others who may unintentionally join your meetings/classes.

You can also visit our page for more ways to prevent Zoombombing.

Have questions or need assistance?

You may contact IT through our new LiveChat tool, email and/or by leaving a voicemail message. Please visit itsupport.maine.edu for more information.

This is to help improve the experience and security of hosting meetings and classrooms with Zoom. While you may change these settings on your own, IT strongly recommends leaving it in place in order to protect your meetings or classes from unwanted guests, otherwise known as Zoombombing.

What else can you do to reduce the risk of Zoombombing?

Make sure you have the latest version of Zoom with all of the security and feature updates. More information about Zoom and how to update your application is available on our Zoom Support Resources page.

Minimize the use of Personal Meeting IDs (PMI). IT suggests that you use these sparingly as these meeting IDs never change which makes them an easier target for Zoombombers and others who may unintentionally join your meetings/classes.

You can also visit our page for more ways to prevent Zoombombing.

Have questions or need assistance?

You may contact IT through our new LiveChat tool, email and/or by leaving a voicemail message. Please visit itsupport.maine.edu for more information.