View the PDF version of this newsletter

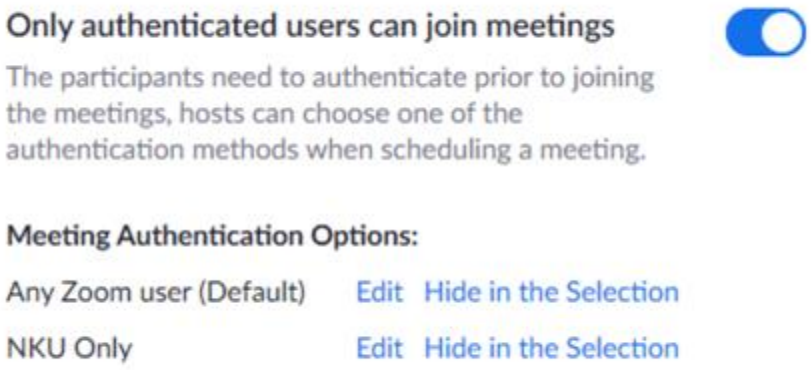
April 2020

Zoom Authenticated User Option

Effective immediately, you are able to restrict Zoom meetings to users with an NKU email. Now when scheduling or creating your meeting, you will have the additional option to choose from either "Any Zoom User" or "NKU Only".

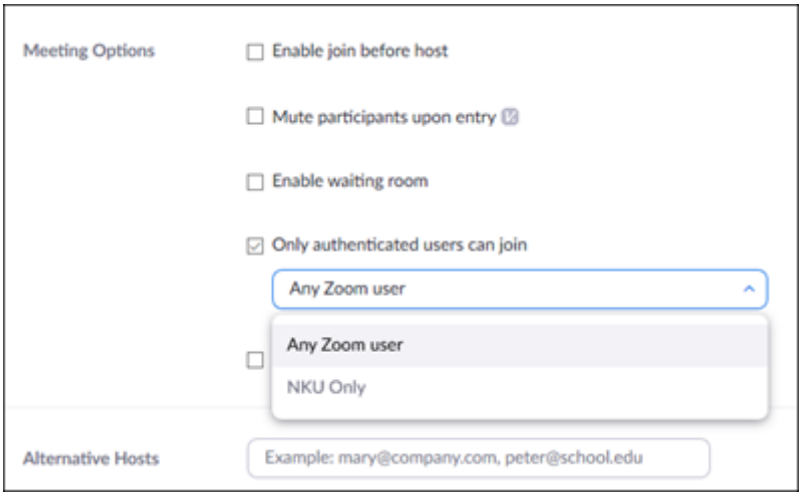
To enable this feature, log into Zoom, (https://nku.zoom.us)

- Sign in to configure your account
- Go to settings on the left side
- Enable "Only authenticated users can join"
- There is nothing else you need do on this page

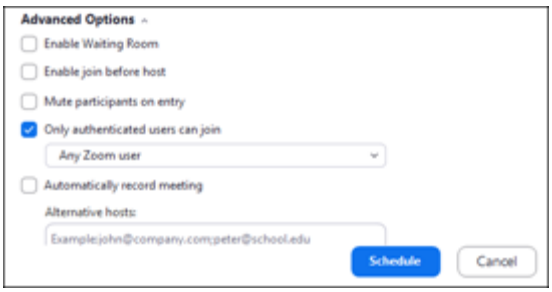


Now when scheduling or creating your meeting, you will have the additional option to choose from either "Any Zoom User" or "NKU Only".

Web:



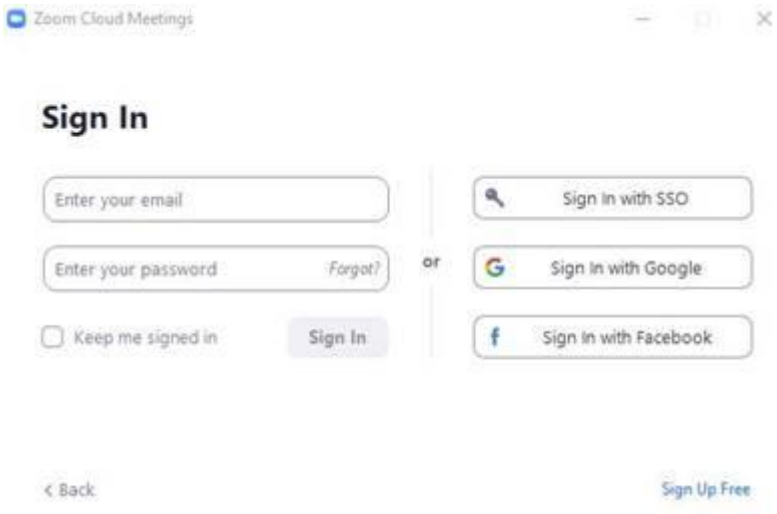
Canvas Client:



Any Zoom User means your participants are required to sign into zoom before joining the meeting. They do not need to use an NKU email account to sign in to attend the meeting.

NKU Only means only those with an **@nku.edu** or **@mymail.nku.edu** email address will be able to join the meeting. This may be a new step for students and participants logging in. So please alert them in advance that they will need to sign in with their NKU email credentials.

Important Note: If the meeting uses the "NKU only" profile, participants will need to use "Sign in with SSO" and input the NKU domain. Only “nku” is needed (.zoom.us is in the selection by default)



Please contact the IT Help Desk (859-572-6911) with any questions.

Zoom Security – Credentials on Dark Web!

If you have ever had a Zoom account signing in via https://Zoom.us (without NKU prefix to the web address) please login and change your password. About 500,000 account credentials have been placed for sale on the dark web. It is important to change your password immediately, even if you do not currently use that account. Follow the account security recommendations from Zoom, especially if you discuss sensitive or protected information.

Your single sign on account, https://**NKU**.Zoom.us (with **NKU**) is protected.

Remember to NEVER use your NKU password anywhere outside NKU resources. Your NKU password should be unique to your NKU account.

How to Hold Zoom Virtual Office Hours

To hold virtual office hours for your classes, you can use the Waiting Room feature in Zoom to set this up. This feature allows you to select the students one by one.

1. In your Canvas course, from the left menu, click **Zoom**.
2. Click **Schedule a New Meeting**.

    a. In the **Topic** header, name your Zoom meeting "Office Hours."
    b. Under **Time Zone**, check the "Recurring meeting" checkbox, then from the "Recurrence" drop-down menu, **select No Fixed Time**. (This will generate a meeting link that can be used at any time and will expire after 365 days.)

c. Under **Meeting Options** - deselect **Enable join before host**. (Students who join the meeting before you will see a notice to wait.)
d. Select **Enable waiting room**.
e. Click **Save.**

Once your meeting has been created, you may share it in one of the following ways, making sure to also state when you will hold your office hours:

(a) Copy the **Invite Attendees Join URL** and share it with your students via an Announcement or email.

(b) Click **Copy the invitation link** to copy and send the meeting information listed to your students via an Announcement or email.

(c) Tell students to access the meeting by clicking Zoom from the Canvas menu.

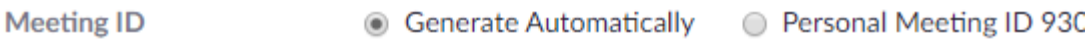
In your message, make sure to state when you will hold your office hours.

Zoom Bombing

There is a default setting on Zoom that permits any meeting participant to share their screen. Meeting hosts should be aware that anyone who has the link to a public meeting can jump in (bomb). These links are often shared on social media and are easy to find on public event pages.

Here are some reminders for using Zoom to host public events:

- When you share your meeting link on social media or other public forums, your event becomes **extremely** public. ANYONE with the link can join your meeting.
- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting and you don't want random people crashing your personal virtual space after your meeting is over. Select *Generate Automatically* meeting ID:



- Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.

Familiarize yourself with Zoom's settings and features so you understand how to protect your virtual space. For example, the Waiting Room is an exceedingly helpful feature, allowing hosts to control who comes and goes. For additional Zoom information visit IT's Virtual Campus

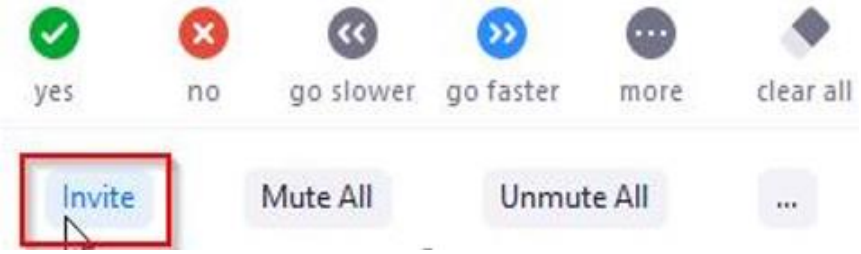
---

Zoom Update

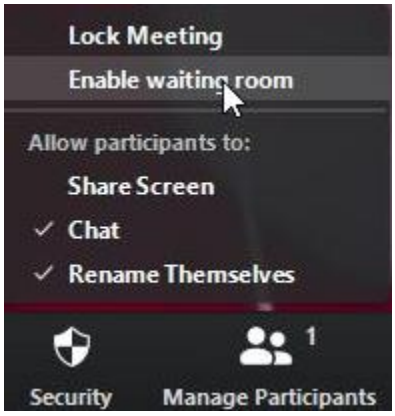
Zoom recently pushed out a security update that resolves many of the reported security issues. When prompted by the Zoom client, be sure to install these security patches.

Recent updates include:

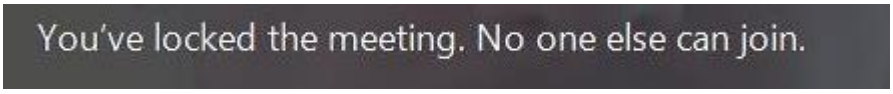
- The Invite button has now been moved to the “Participants” tab



- There is now a “Security” tab where the “Invite” button was previously located. You can “Enable Waiting Room” as well as “Lock Meeting”. You can also change participant permissions.



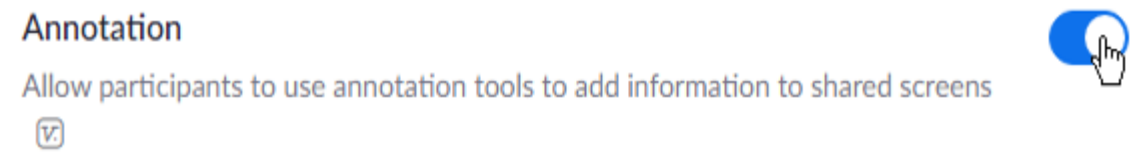
- When a meeting is locked, no one else can join the meeting.



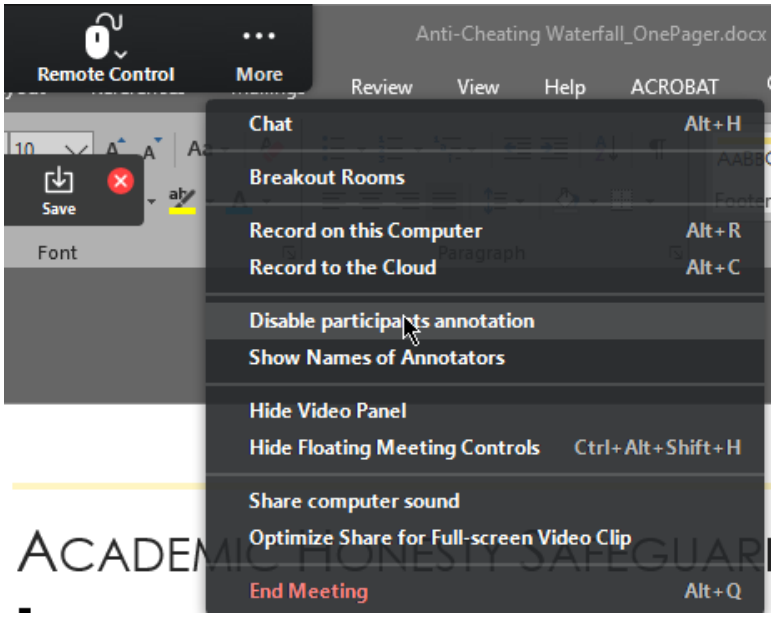
Additional Zoom Security

If a Zoom participant clicks on the "more" option while the host is sharing their screen, they can annotate. This can result in people writing inappropriate things while the host is sharing their meeting. To prevent unwanted annotations the recommendation is for hosts to disable participant’s annotation ability for public meetings.

You can deactivate annotation during a screen share *for* ***all of your Zoom meetings*** by going to nku.zoom.us, select settings, and then disabling the "Annotation" feature:



To turn annotations off in individual meetings you can click the "More" button then "Disable participants annotation" after a meeting has started and you are sharing your screen. In addition, meeting hosts can also check the "Show Names of Annotators" to see who is annotating.



Zoom Recording Password

Recent security changes within Zoom have resulted in new password protection for all Zoom cloud recordings between Friday, April 10th and the morning of Tuesday, April 14th, when IT rescinded the password requirement.

For Zoom recordings between 4/10 and 4/14, the password is in the email informing the instructor that the recording has been processed to the cloud; unless they know to look for it, they may miss it.

For added security, the only way the student gets the password is if the instructor shares it with them. However, instructor shouldn't forward that particular email to students because it also contains "host only" information.

Recording passwords may be turned off via the Zoom website. This feature cannot be changed within Canvas, it must be done in the web portal. To see if your recordings have a password, and to turn it on or off, go to http://nku.zoom.us :

- Sign in to Configure your Account
- Go to Recordings (left side)
- Click on the title of recording
- Click Share (this is where you can access the password to copy or remove)

How to Add a Password to Previously Scheduled Zoom Meetings

Zoom has recently added passwords to scheduled Zoom meetings.

If you have a previously scheduled Zoom meeting without a password, that you would like password protected, go to http://nku.zoom.us :

- Sign in to Configure your Account
- Go to Meetings (left side)
- Click on the title of meeting
- click edit this meeting,

- Click require meeting password.

Sending Secure Documents through Email

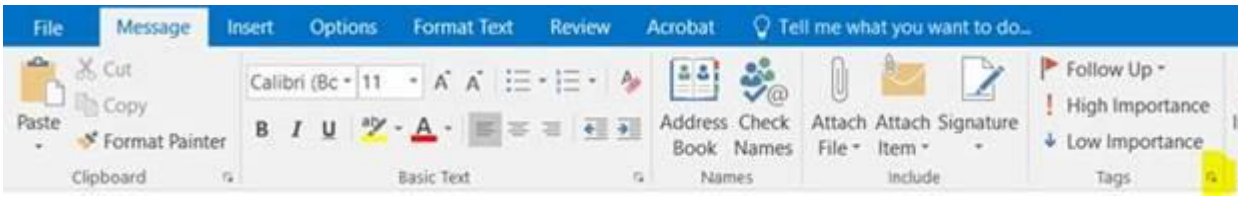
Standard email is **not** a secure method to share sensitive data or personally identifiable information. Email messages can be compromised if they are intercepted in-transit. To prevent data compromise, you can easily add encryption to emails, protecting the message and its attachments

Remember to encrypt all email messages with sensitive information. For example, vendor forms may contain sensitive information like SSN's, TIN's, etc.

When emailing any personally identifiable information (PII), remember to encrypt the email message.
To encrypt an email message in Outlook, you do just 2 THINGS:

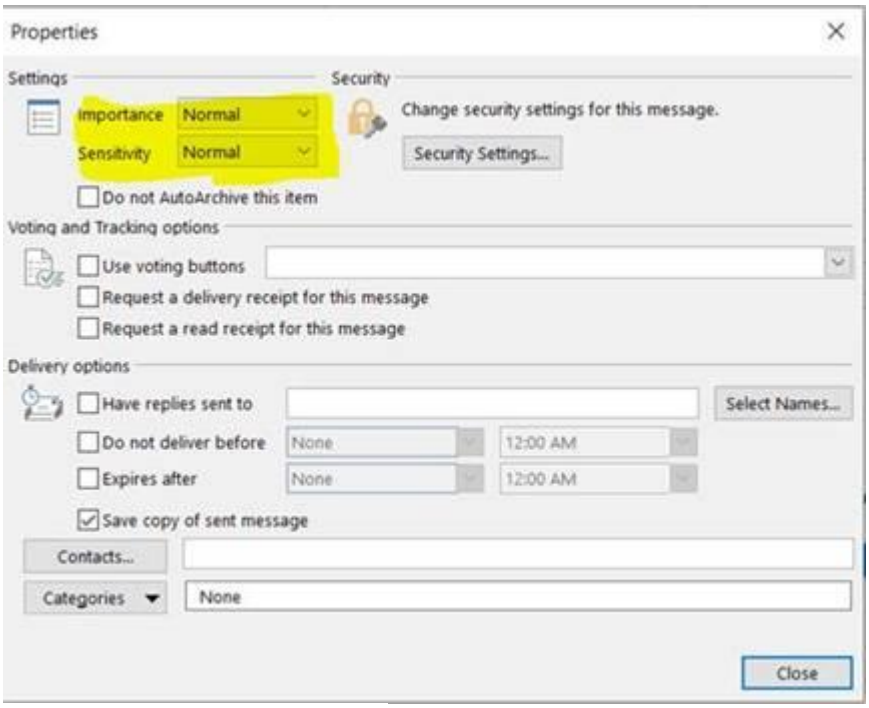
1. Set the Importance to "High"
2. Set the Sensitivity to "Confidential"

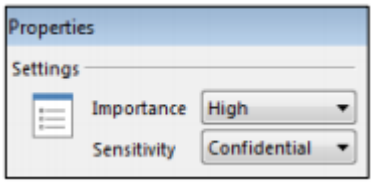
The only slightly-tricky part is that the sensitivity option is hidden in the Outlook window. To reveal it, click the expansion arrow next to **Tags**:



This dialog box appears after clicking the arrow next to Tags:

1 Set the Importance to “High”
2 Set the Sensitivity to “Confidential”





Security Tips for Working at Home

NKU IT has created twelve security tips for staying protected while working from home. Contact the IT Help Desk if you need assistance with any of these tips.

Use OneDrive to Securely Share Documents

Saving your work in OneDrive makes it accessible from any internet connected device. It is saved to secure cloud storage and automatically backed up. All files that you store in OneDrive are initially set to private, and available only to you. You may choose to share specific files with specified colleagues to enable easy collaboration. Check out

the Working in OneDrive tutorial. You will learn how easy it is to store, retrieve and work with your data from any location.
