Virus & Security

Last Modified on 03/27/2024 1:28 pm EDT

Security Guidelines

Security is a responsibility shared with you, Wharton Computing, and the Wharton Information Security Office. Working together, we can ensure that your data and the School remain secure. This article provides guidelines and best practices that you can use in your day-to-day activities to enhance and maintain the security of your University-related accounts and information.

> If you have any questions or concerns about anything in this article, please reach out to the Wharton Information Security Office at security@wharton.upenn.edu.

The Wharton Computing Accounts & System Policies article contains more information about specific account and system policies.

Security Best Practices

The following best practices apply to all Wharton faculty, staff, and students. We are all part of keeping our data and colleagues protected.

Share Safely

Information containing private or sensitive data ("High" and "Moderate" data according to the Penn Data Risk Classification) may only be shared or accessed in accordance with the University's Information Security Policy.

Secure sharing options include:

- Wharton-approved cloud storage accounts (PennBox, Dropbox)
- SecureShare

> Always take a moment before you share any data to think about what data is included and if it is considered private by the University or your department.

Protect Information & Systems

Protecting data is important; to do that, the data must be stored in a secure and appropriate place. Protect all information on all systems. University data's confidentiality must be safeguarded, no matter where it resides.

As you think about the safeguards you have in place, remember:

- You have to know the risk to prevent it. Know the level of classification that your data falls into so you can make appropriate decisions regarding its protection.
- Your Wharton Computing Representative is always willing to talk with you about measures you can take to enhance protections.

- The Wharton Information Security Office is available to assess your data and make recommendations around storage and necessary protections.

Report Possible Problems

Security incidents happen; the sooner we know, the sooner we can help.

Report any unauthorized access or suspicious behavior related to Wharton's confidential data or system as soon as possible. If you suspect Wharton's information has been exposed, please contact Wharton’s Information Security Office.

Ways You Can Help

The best way you can help the Penn community is to be familiar with University Information Security and Privacy policies. In addition, practicing the following will help keep everyone secure:

Manage your Password

A strong and unique password is essential to account security, as your password is the front line and often the only defense against someone with malicious intent. The strongest password is unique, random, and at least 15 characters.

At a minimum, we recommend a password containing letters, numbers, and symbols and using unique passwords for all your websites/services. Our article about password guidelines and tips is written to cover PennKey and Wharton account passwords specifically but can be applied to any other account.

The elements of a good password also, by nature, make those passwords difficult to remember. Add in the fact that you should be using different passwords for each service you encounter, and suddenly, you have a large number of difficult-to-remember passwords you need to remember!

To help with this, **Wharton offers premium access** to a service called LastPass. This is an *encrypted password manager* that stores your account credentials for you. You will only need to remember the Master Password for your LastPass account, which then stores all your other passwords. This will allow you to create & set very strong passwords while not having to remember all of them.

To learn how to access this service, see our LastPass: Managing Passwords (and more) at Penn article.

Antivirus

Wharton Computing offers free virus protection software for both Windows and Mac users to help keep your devices safe from viruses and spyware. To learn more about this service, see our Antivirus article.

> For staff & faculty, your Wharton-owned and managed computers should already have antivirus installed on them.

Two-Step Authentication

Two-step authentication provides an additional layer of protection when accessing your account(s), and we recommend you enable it for any accounts that support it. For more information about two-step at Penn, see our

Two-Step Verification starter article.

Phishing

Phishing messages are crafted to appear legitimate, but they are designed to trick you into sharing data or access with hackers.

If there is the least hint that a message may not be what it seems, take the time to verify it or contact yourWharton Computing representative to confirm. We would much rather help you determine a message is not a threat than have you (and us) subjected to the consequences of a phished account.

To learn more about phishing, see our Phishing article.

If you think your account has been compromised, see our Compromised Account article to find out what to do.

Copyright/Student Conduct

Materials subject to copyright or license restrictions should not be openly shared on the PennNet network, nor should any related activities take place. Doing so may result in disciplinary sanctions and/or fines.

To learn more about the policies, see the Office of Student Conduct (OSC) website and File Sharing and the Penn Acceptable Use Policy on Electronic Resources.

Useful Resources

- Wharton Information Security Office
    - Email: security@wharton.upenn.edu
- University Information Security Policies
- University Data Risk Classification
- University Privacy Policy
- Partner with Wharton's Information Security Office : they can provide security & privacy guidance, security risk reviews/assessments, support, and more.

Questions?

Faculty & PhD Students: Academic Computing Services

Staff: Administrative Support

Students: Wharton Computing Student Support

Threat Protection/Antivirus Software at Wharton

The University of Pennsylvania offers threat protection and antivirus software solutions for faculty, staff, and students. For computers managed by Wharton Computing (typically faculty, staff, and the public computers in labs, classrooms, and hallways), the Crowdstrike software must be installed and running. For unmanaged computers (typically student computers, and those not managed by Wharton Computing), the University provides Sophos Home free of charge.

For more information such as recommendations and helpful tips, please see our full Virus Protection article.

Before You Start

Managed v. Unmanaged: Wharton Computing manages many computers on campus -- these are called "managed computers". Wharton Computing also supports people who are using computers that aren't managed by Wharton Computing -- these are called "unmanaged computers".

- Managed computers: purchased by Wharton/Penn; built, configured, and maintained by Wharton Computing staff.
- Unmanaged computers: purchased by individuals or by Wharton/Penn using personal funds.

Are You Already Protected?

The first step is to determine whether you are already protected. Recommendations at Wharton differ depending on whether you are faculty, staff, or student and whether Wharton Computing is managing your computer.

Unmanaged Computers (Students, Faculty & Staff with Unmanaged or Personal Computers)

Student computers and some personal computers owned by faculty and staff are "unmanaged" -- they are not part of the Wharton Computing-managed computing environment. These computers should have antivirus protection installed -- we recommend Sophos Home (for Macs) or Windows Defender (for Windows 10).

Read More →

Managed Computers (Staff, Faculty)

Wharton Computing uses the Crowdstrike software to protect staff and faculty machines that are managed by Wharton Computing. (Student computers are not managed by Wharton Computing.)

Read More →

Choosing Your Antivirus Software

There are several conditions that will determine which steps you take to install the appropriate antivirus software: who you are, and what kind of computers you are using.

	Student	**Faculty**	**Staff**
Unmanaged Mac	Sophos Home	Sophos Home	Sophos Home
Managed Mac	N/A	Crowdstrike	Crowdstrike

Unmanaged Windows	Windows Defender	Sophos Home	Sophos Home
Managed Windows	N/A	Crowdstrike	Crowdstrike

Antivirus Download Links

For unmanaged computers, Wharton Computing recommends using Sophos Home software on MacOS devices. Windows 8 & 10 devices are already protected by the built-in antivirus software, Windows Defender.

MacOS	Windows 10	Windows 10 (if Defender is not an option)
Sophos Home	Windows Defender	Sophos Home

Sophos Home FAQs

Here are a few questions we hear from users about Sophos Home:

Read More →

Questions?

Students - email support@wharton.upenn.edu.

Faculty - contact your Academic Distributed Representative (login required).

Staff - email admin-support@wharton.upenn.edu.

For more information regarding security threats and antivirus software, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.

Antivirus Software: How To Protect Yourself Against Viruses

This article provides information on protecting yourself from viruses, malware, and other malicious software. It lists recommended protection software, helpful tips, and what to do next if you think you've been infected.

Faculty and Staff: Computers purchased by the University will automatically have Crowdstrike (a centrally-managed antivirus program) installed on them. These computers will not need the software listed below.

For personal computers, Penn offers the site-licensed Sophos Home, free of charge, to members of the Penn community using the links below.

If you have questions or concerns please reach out to Wharton Computing using the links inQuestions, below.

Antivirus Software

Most Antivirus software now requires a subscription. If you prefer not to maintain a subscription, we recommend using Sophos (free to members of the Penn Community) or Windows Defender (for Windows machines).

Faculty and Staff who are using a computer managed by Wharton Computing already have antivirus installed automatically and can skip this section.

Active Defenders

- **Windows** → Sophos Homeis offered by the University for free. Best for Staff and Faculty use.
- **Windows 10/11** → Windows Defender is the default antivirus software on Windows 10 & above. Best for Student use.
- **MacOS** → Sophos Homeis also offered for MacOS by the University.

Scanners

- MalwareBytes scans your computer for any potential malicious or suspicious software & processes.

Helpful Tips

Be Aware of Sites & Attachments

As computers become more networked and standardized, it gets easier and easier to catch computer viruses. You can get viruses from downloads over the internet, from opening e-mail attachments, or from another infected system or device.

Many self-propagating viruses will mail themselves to you before the original sender has discovered that his/her machine is infected. Be suspicious of any attachments, but be extra vigilant about inappropriate subject lines and attachment titles (for example, if someone you barely know sends you an e-mail called **ILOVEYOU**).

Back Up Data Frequently

Some viruses are so damaging that they will render your files useless or unrecoverable. In that case, your only hope of recovery is with back-ups made prior to infection.

Update, update, update!

Microsoft & software developers frequently release patches to fix known issues for their services. These fixes include known security issues that may leave your computer or program vulnerable to viruses and other attacks. To manually update, press the Windows key + S (⊞ + s), type **check for updates**, and then click the **Check for Updates** setting.

Sophos Home

The University of Pennsylvania offers free antivirus software to faculty and staff in the form of Sophos Home. Below are the links to download this software, along with some Frequently Asked Questions.

> Faculty and Staff who are using a computer managed by Wharton Computing already have antivirus installed automatically and can skip this section. However, Sophos is available for personal use as well, so can be installed on non-managed machines.

Download Links

Wharton Computing recommends using this software on MacOS devices. Windows 10 & 11 devices are already protected by the built-in antivirus software, Windows Defender.

> **Note:** If you're still running Windows 8/8.1, Wharton Computing recommends updating to Windows 10 for optimal performance if supported by your device.

Windows 8.1, 10, or 11	Windows 8.1, 10, or 11	MacOS
Sophos Home for Windows Staff and Faculty	Windows Defender Students	Sophos Home for Mac Students

Sophos Home FAQs

What if I already have antivirus software?

If you are satisfied with your current antivirus software and are able to update the virus definition files on a regular basis then you can continue the use of your current antivirus software, but you might need an additional anti-spyware program. If you are not able to update the virus definition files or your antivirus subscription is expired, you will need to switch to Sophos Home.

Why should I switch to Sophos Home?

The university pays for a Sophos Home subscription that includes virus definition updates and spyware scans in addition to virus scans. It is also supported by Wharton Computing, so you can get assistance with the program should you encounter any problems.

Will I get technical support if I switch toSophos Home?

Yes, Wharton Computing offers support for Sophos Home and will be able to help you install and configure the antivirus software.

If your computer has a virus...

Students: If you think you have a virus, please stay calm and follow the directions in our Virus Removal article. We also encourage you to call, email, or drop by our Support Office (SHDH 114) in person so we can help with the situation.

Faculty & Staff: Please contact your Wharton Computing Representative or the Wharton Information Security Office at security@wharton.upenn.edu.

Questions?

Students: visit the Student Computing Website.

Faculty: contact your Academic Distributed Representative (login required).

Staff: email admin-support@wharton.upenn.edu.

For more information regarding security threats and antivirus software, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.

Firewalls: What They Are & Why Use Them

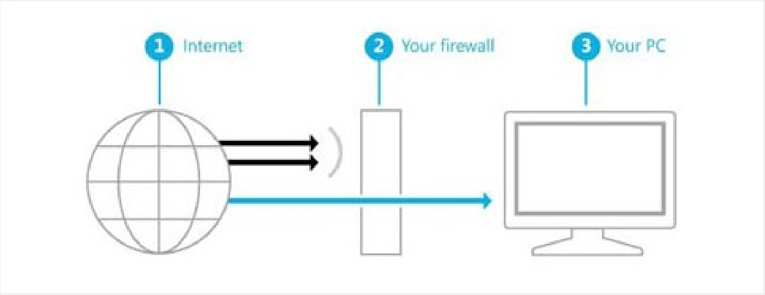
This article will give you an overview of what a firewall is, how it works, and will provide instructions on how to ensure your personal computer's firewall(s) are enabled.

> **Faculty & Staff:** Faculty and Staff using Wharton-imaged or Wharton-provided devices may not be able to change Firewall (Crowdstrike) settings. This article applies only to personally managed computers.
>
> For additional questions or requests, please reach out to your IT support representative or the Wharton Information Security Office at security@wharton.upenn.edu.

What is a firewall?

1. A firewall is a network security system that establishes a barrier between a trusted, secure internal network and another network that may not be secure.

2. Additionally, a firewall can help prevent hackers or malicious software from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.



Enable/Disable Firewall

Warning: Only turn off your Firewall if you are installing a separate antivirus software that includes a firewall *and* active defender.

Windows

Follow Microsoft's directions on how to turn your Firewall on or off.

MacOS

Follow Apple's directions on how to turn your Firewall on or off.

Allow Trusted Applications

You can allow applications you trust. **Only choose this option for applications you know are safe.**

Questions?

Students - Wharton Computing Student Support

Faculty - Academic Distributed Representatives

Staff - Administrative Support

For more information regarding security threats and antivirus software, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.

Web Browser Security

This article covers the update process for Web Browsers.

Faculty and Staff on Wharton-Managed Machines:

Your browsers should update automatically but it's still a good idea to follow the steps listed below.

Web Browsers

Healthy Computing requires regularly updating your computer, but we often forget to update our web browser(s). Since so much of computing now takes place in a web browser, it is considered one of the largest attack vectors for malware.

Most major browsers (e.g. Chrome, Edge, Safari, Firefox, and DuckDuckGo) are quick to fix vulnerabilities and auto-update, and all you need to do is restart your browser regularly! The Wharton Information Security Office **recommends restarting your browser each day to allow any applicable updates to apply.**

Your open tabs should reappear or if not, you can restore the previous session from the “History” menu in your browser to pick up from where you left off while being up-to-date!

Updating your Browser

There are several ways to update your browsers.

Restart (Updates Automatically)

A restart of your browser usually updates it immediately -- all you need to do is close all open instances of the browser, and restart. Your open tabs should reappear or, if not, you can restore the previous session from the “History” menu in your browser to pick up from where you left off.

Manual Update

You can also manually check your browsers for updates, although how you do it varies by Operating System:

- **macOS:** click the application title in the top menu bar just to the right of the Apple logo, and select “About [Browser Name]” from the menu that appears
    - For Safari, macOS delivers updates via software updates in Settings; seeUpdate to the latest version of Safari - Apple Support
- **Windows:** click “Help” in the top menu bar of the application, and select either “About [Browser Name]” or “Check for Updates” from the menu that appears.

Browser Resources and Recommendations

For more information on security options for major browsers, here are places to start:

- **Chrome**: https://support.google.com/chrome/answer/114836?hl=en&co=GENIE.Platform%3DDesktop
- **Microsoft Edge**: https://support.microsoft.com/en-us/microsoft-edge/enhance-your-security-on-the-web-with-microsoft-edge-b8199f13-b21b-4a08-a806-daed31a1929d
- **Safari**: https://support.apple.com/guide/safari/welcome/mac (choose Table of Contents and then Security for

your version)
- **Firefox**: https://support.mozilla.org/en-US/products/firefox/protect-your-privacy

These practices and recommendations also apply to other web browsers that may not be listed here.

Questions?

Contact your Wharton Computing Representative or the Wharton Information Security Office for more information.

Google Security & Privacy Checkups

The Google Security & Privacy checkups provide a quick and effective way to ensure that your Google account is secure and private. These checklists can be used on any Google account, whether it is personal or school-provided.

Google Security Checkup	Google Privacy Checkup

Access requirements: Must have an active Google account.

Google Security Checkup

Google's Security Checkup is a great way to ensure that your account is secure and isn't being accessed by anyone but you. It can also help highlight security flaws on your account that may be easily missed.

- Manage apps with access to your account
- Review signed-in devices
- Review recent security events
  - i.e. New Sign-ins, App Password creation & deletion, etc.
- Enable Two-Step Verification

Google Privacy Checkup

Google's Privacy Checkup allows you to personalize which types of data Google collects as well as allowing you to manage the visibility of your account.

- Review activity controls
    - Web & App activity
    - Device Information
    - Voice & Audio activity
- Edit publicly-available information about your account
- Manage Tailored Ads

Questions?

Faculty & PhD Students: Academic Distributed Representatives

Staff: Administrative Support

Students: Wharton Computing Student Support

For more information regarding Google Security and Privacy, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.

Frequently Asked Questions

Q: I no longer use an app (i.e. G Suite Sync for Outlook) and want to remove its access to my Google Account. How can I do this?

A: The first step of the Google Security Checkup allows you to review and manage any apps that have been granted access to your account.

Q: Are security & privacy checks available for my devices as well?

A: If you are a student, yes! Simply drop by the Tech Center at SHDH-114 and ask to participate in a Device Tune-up & Security Session. If you are faculty or staff, please contact your Academic Distributed Representative or Administrative support, respectively.

Q: What if I notice a device or location that isn't mine has accessed my account?

A: Reset your Google account password as soon as possible, as well as any other passwords that may be the same or similar. Contact your IT support team if you have additional questions (see *Questions?* above).

Google Login Challenge: How, When, and Why

This article provides guidance regarding Google's Login Challenges. More specifically, it is designed to describe when they appear, why they appear, and what you can do about it.

> **Note:** This article only applies to students whose Google accounts were created **before December 2023**.

Account security is of utmost concern for both Google and Wharton Computing. When Google determines that a user is logging in from either:

1. **An unknown device** (*new phone, tablet, laptop, or desktop*)
2. **An unusual or new location** (*different state or country*)

They may prompt the user with a login challenge. The login challenge you receive depends on the information you have associated with your account.

Faculty, Staff, and PhD Students

Contact your IT Support Representative or the Wharton Information Security Office at security@wharton.upenn.edu for the best option to use for recovery.

Adding Recovery Information

1. Navigate to myaccount.google.com.
2. Log in with your **Google Account.**
3. Click the **Security** tab.
4. Scroll down to **Ways we can verify it's you.**
5. Choose a **recovery option** (phone or email) and follow the instructions to verify your information.

Various Login Challenges

Scenario 1: No recovery information

You will be prompted with the following Login Challenge if you do not have a recovery phone number or a recovery email address associated with your account.

Read More →

Scenario 2: Only recovery phone number

You will be prompted with the following Login Challenge if you only have a recovery phone number associated with your account.

Read More →

Scenario 3: Only recovery email address

You will be prompted with the following Login Challenge if you only have a recovery email address associated with your account.

Read More →

Scenario 4: Both recovery phone number & recovery email address

You will be prompted with the following Login Challenge if you have both a recovery phone number and a recovery email address associated with your account.

Read More →

Additional Note: Other Help

Read More →

Questions?

Students - Wharton Computing Student Support

Faculty - Academic Distributed Representatives (login required)

Staff - Administrative Support (login required)

For more information regarding Google login information, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.

Virus Removal Procedure

If your personal computer has a virus, use the steps below to try removing it on your own.

Faculty and Staff should NOT attempt to remove viruses on any machine provided to them by Penn.

If you suspect you have a virus, disconnect your computer from the network, power it off, and contact your Wharton Computing Representative or the Information Security and Privacy Team at security@wharton.upenn.edu right away for assistance.

Virus Removal Procedure

We've compiled a set of simplified steps for PC and Mac to make it easy for you to try and fix your own computer. Students can make an appointment (before 2 pm) with Student Support to have their machines scanned and cleaned if more help is needed.

Before You Start:

- Back up your computer's data to an external hard drive or other source not attached to your computer to prevent any loss of important data.
- Make sure you're comfortable downloading and installing software on your computer.

Windows/PC

The procedure below is simplified for your convenience and remedies most situations.

Read More →

Virus Removal Procedure (Mac)

The steps for removing viruses from Macs are fairly straightforward.

Read More →

Questions?

Contact your Wharton Computing Representative or the Wharton Information Security Office at security@wharton.upenn.edu for more information.

Spam: Why You are Receiving Spam from a University Email

Spam from a university email address can be caused by a few situations:

- Your account, or another university account, has been compromised
- Your email, or another university email, is being spoofed
- An account user has sent inappropriate emails before

Compromised Account

Students

If you believe someone's account has been compromised in any way, follow the instructions provided below immediately:

1. Reset your Wharton and PennKey passwords
   - If you believe your device has been compromised, use another computer or call Student Support to help you change your passwords.
2. Change passwords that are similar or the same as your compromised password
   - Unique, complex passwords are one of the best ways to secure your account(s). Password managers, such as LastPass, autofill your credentials for you, allowing for easy and convenient account management while using long, complex, and secure passwords.
3. Notify the Wharton Computing Support Team of the problem (support@wharton.upenn.edu)
4. Complete the Gmail Security checklist
5. Determine if your password has been exposed in a data breech athttps://haveibeenpwned.com/ and/or https://monitor.firefox.com/

Faculty, Staff, and PhD Students

Please contact your IT Representative immediately.

Email Spoofing

Some spammers **spoof** email addresses that make it appear as if the mail they send is coming from a university email address. Unfortunately, there is not much Wharton Computing can do except suggest that you report the website/sender for spamming to sites like and or http://www.spamhaus.org/.

You might need to look up the site's IP address at a site like this:
http://get-site-ip.com/

Questions?

Students: Email support@wharton.upenn.edu

Faculty: Contact your Academic Distributed Representative (login required)

Staff: Email admin-support@wharton.upenn.edu

PhD Students: Contact your Academic Distributed Representative (login required)

LastPass: Managing Passwords (and more) at Penn

To help you keep track of your passwords, the University of Pennsylvania has partnered with LastPass to make this password management software available to all members of the Penn community.

Before You Start

You'll need the following to use the University's version of LastPass:

- A standard Internet Browser
- An active PennKey account
- Your current login credentials to any site you want to add to LastPass

NOTE: Choose a strong but memorable Master Password! If you forget your password, **account recovery can be very difficult**. If you are unable to go through account recovery, your account will need to be reset (and you may lose all your data)! See LastPass' help site for more details.

Sign up for LastPass

Instructions for signing up for LastPass Premium:

- https://www.isc.upenn.edu/how-to/lastpass.

LastPass Tips

- **Strong Password:** When setting up the account, make sure to choose a strong, unique password that isn't used for anything else.
- **Add Secure Notes:** LastPass is a useful website that can be utilized to keep track of many things, not just passwords. The "Add Secure Note" feature allows you to keep track of information that you need secure and accessible, whether it's a WiFi network login, social security number, or a PIN code.
- **Password Recovery:** Add a recovery phone # by going to **Account Settings -> General -> SMS Account Recovery**. This is recommended in case you need to recover the account.

- **Extra Security:** Add an extra layer of security: Go to **Settings** and choose **Multi-Factor** options to add an extra layer of security.
- **Chrome Tip**: If you use Chrome, we recommend that you **do not use Chrome's autofill** password option for the LastPass website. If anyone has access to the computer, then they'll automatically have access to LastPass, which will then give access to everything on your LastPass account.

- Take a look at our Google Security & Privacy Checkups article for more information regarding Google Chrome's password security and privacy settings.

For more information, consult the Last Pass FAQ.

Student Note: Students will not lose any data stored in their LastPass Premium account when the subscription expires, but Multi-Factor options will no longer be available.

LastPass Security Breach Recommendation

Although the University's Information Security team has determined the risk of hackers accessing secure information is low for most LastPass users, it is critical to stay prepared in case a security breach does occur.

We recommend taking the following steps **as soon as you are made aware of a breach:**

- Change your LastPass **master password** as soon as possible. Make it a complex password, as recommended in the PennKey Password Rules.
- Change any passwords stored in LastPass that have **access to potentially sensitive data**, including:
  - Your PennKey password
  - Your Wharton Account password
  - Banking and other financial account passwords (e.g. Ben Financials)
- Enable Two-factor authentication for LastPass and any other accounts that support it.
- Change credentials that are stored with links to login pages.
- Change or remove additional sensitive information stored in LastPass, such as addresses or other identifying information.

Recommendations

In addition to the Action Items listed above, we recommend that you:

- Change all passwords stored in your vault, starting with your most important ones first.
- If you have sensitive data stored in other fields, change that data if applicable.
- Update the LastPass default iteration setting of 100100. Directions for changing that are here -- 310,000 is now recommended.
- Remove LastPass entries for services you are no longer using.
- Be on the lookout for suspicious spam/phishing messages from attackers pretending to be LastPass

Because your email address and the sites LastPass stores passwords for may have been accessed, there is an increased risk of phishing attacks impersonating LastPass itself or targeting LastPass users. Please remain alert for these types of attacks. If you are unsure of the legitimacy of any email, please reach out to your support team.

Questions?

Faculty & PhD Students: Academic Distributed Representatives

Staff: Administrative Support

Students: Wharton Computing Student Support

For more information regarding LastPass password management, you can also reach the Wharton Information Security Office at security@wharton.upenn.edu.

Zoom Meeting Security

The best way to deal with disruptive behavior in a Zoom meeting is to prevent it from happening in the first place. This article details several ways to secure your Zoom meetings and how you can quickly deal with disruptions in an active Zoom meeting.

Before You Start
You will need:

- An activated Penn Zoom Account before completing any of the tasks in this article.
- Have the host or co-host role in the Zoom meeting.

Best Practices

Zoombombing, wherein participants join Zoom meetings to cause a disruption, can derail any meeting. There are some things that you can do to thwart potential Zoombombers before they even have the chance to enter your meeting.

Don't post meeting information publicly

Only share the Zoom meeting details with attendees. Avoid posting them on a publically accessible website (Canvas sites are only accessible to those people explicitly granted access).

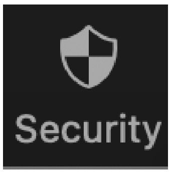
You should also consider not using your Personal Meeting ID. This is a permanent meeting that has set login information. While your PMI is great for sharing with students and co-workers because the login information remains the same, it is less secure since that login information could be shared with others without your knowledge. We recommend setting up individual Zoom meetings for regular work/classes.

Enable Waiting Room

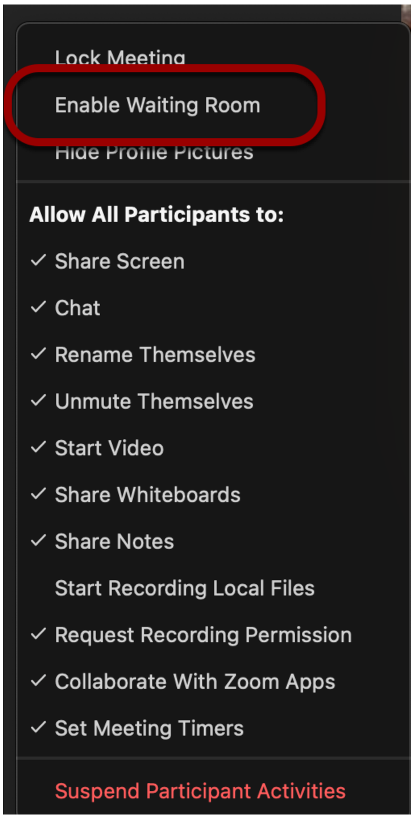
In a Zoom meeting with Waiting Room enabled, the meeting host/co-host has to admit people into the meeting. This allows you to control exactly who can join your meeting.

To enable the Waiting Room for a Zoom meeting as it is taking place (and the host/co-host of):

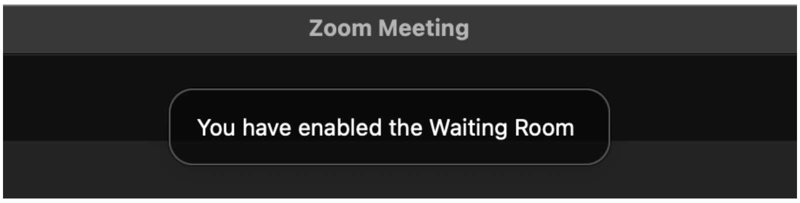
1. Click the **Security** icon at the bottom of your Zoom meeting window.



2. Click **Enable Waiting Room** on the Security menu.



3. You'll see an alert that lets you know the waiting room has been enabled for the meeting.

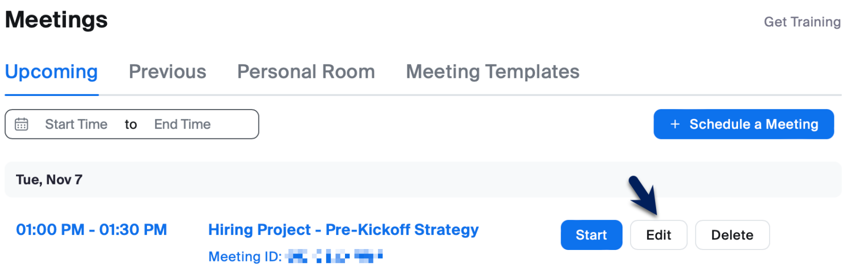


You have enabled the Waiting Room

You'll get an alert whenever someone enters the Waiting Room. You can read more about Waiting Rooms in Zoom's documentation.

To enable the Waiting Room for a meeting scheduled in the future:

1. Log into .us with your PennKey username and password.
2. Click on **Meetings** in the left sidebar.
3. You will see a list of your upcoming meetings. Hover over the meeting you want to change and click the blue **Edit** button.

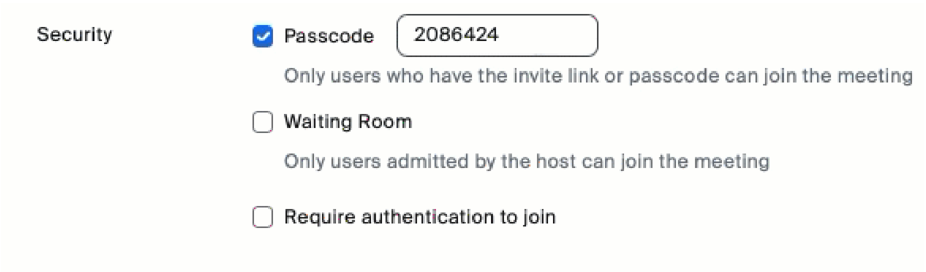


Tue, Nov 7

01:00 PM - 01:30 PM Hiring Project - Pre-Kickoff Strategy

Meeting ID: [redacted]

4. Scroll down to the Security section and **check the box** next to Waiting Room.


Security

☑ Passcode 2086424

Only users who have the invite link or passcode can join the meeting

☐ Waiting Room

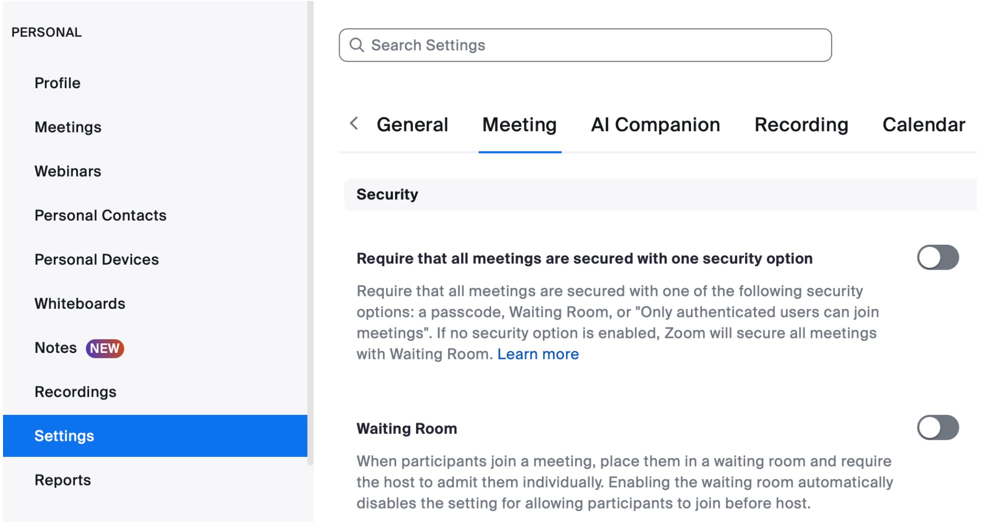
Only users admitted by the host can join the meeting

☐ Require authentication to join

5. Click **Save**, and your meeting is updated.

To have all of your new Zoom meetings have Waiting Room enabled by default:

1. Log into .us with your PennKey username and password.
2. Click on **Settings** on the left sidebar.
3. This should open the Meeting settings, with Waiting Room near the top.



Security

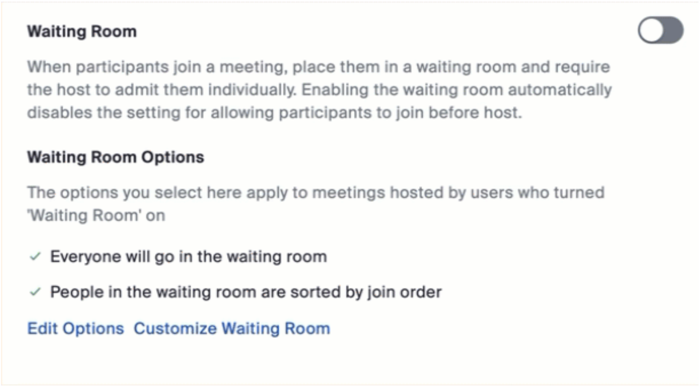
Require that all meetings are secured with one security option

Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. Learn more

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

4. Toggle Waiting Room on.


Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

✓ Everyone will go in the waiting room

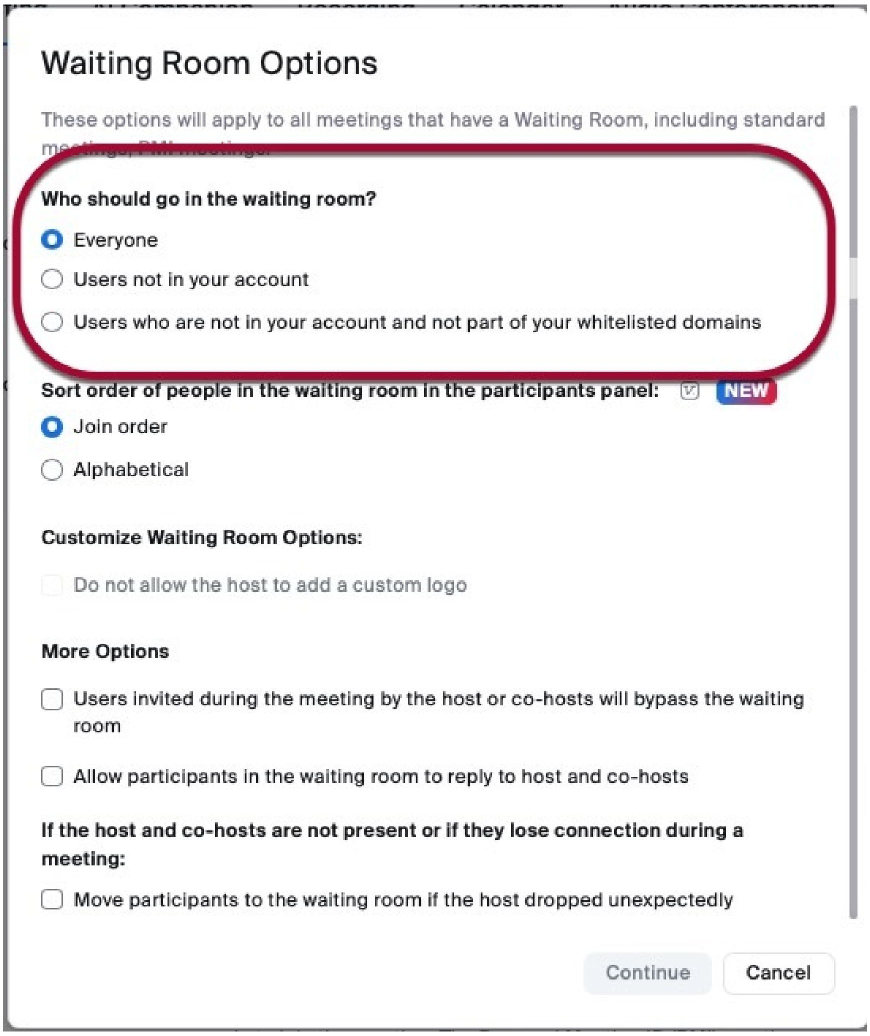
✓ People in the waiting room are sorted by join order

5. Click **Edit Options** if you'd like to change who should go into the waiting room ("users not in your account" means non-Penn users), among other things.
6. Changes are saved automatically, so any meetings you create going forward will have a Waiting Room.

If you enable "Allow Authenticated Users Only" (see the next section for more information on this setting), you can allow authenticated users to skip the Waiting Room and be automatically allowed into the meeting by following these directions after logging into .us with your PennKey username and password:

> **Note**: This is a global setting for your account, which will impact all of your Zoom meetings with both Waiting Room and Authenticated Users enabled.

1. Click **Settings**.
2. Click **Security**.
3. Under the Waiting Room section, click **Edit Options**.
4. Change "Who should go into the waiting room" to "Users not in your account." This will allow Penn users to skip the Waiting Room whilst, non-Penn users, or unauthenticated Penn users, will need to be allowed into the meeting from the Waiting Room.



Waiting Room Options

These options will apply to all meetings that have a Waiting Room, including standard meetings, PMI meetings.

Who should go in the waiting room?

● Everyone
○ Users not in your account
○ Users who are not in your account and not part of your whitelisted domains

Sort order of people in the waiting room in the participants panel:

● Join order
○ Alphabetical

Customize Waiting Room Options:

□ Do not allow the host to add a custom logo

More Options

□ Users invited during the meeting by the host or co-hosts will bypass the waiting room

□ Allow participants in the waiting room to reply to host and co-hosts

If the host and co-hosts are not present or if they lose connection during a meeting:

□ Move participants to the waiting room if the host dropped unexpectedly

5. Click **Continue**.

Authenticated users only

You can require that all attendees be logged in with their Penn accounts or a Zoom account before they can join your meeting. You can limit it to (the following list goes from least to most inclusive and is additive):

- Penn users only
- Anyone with a Zoom account

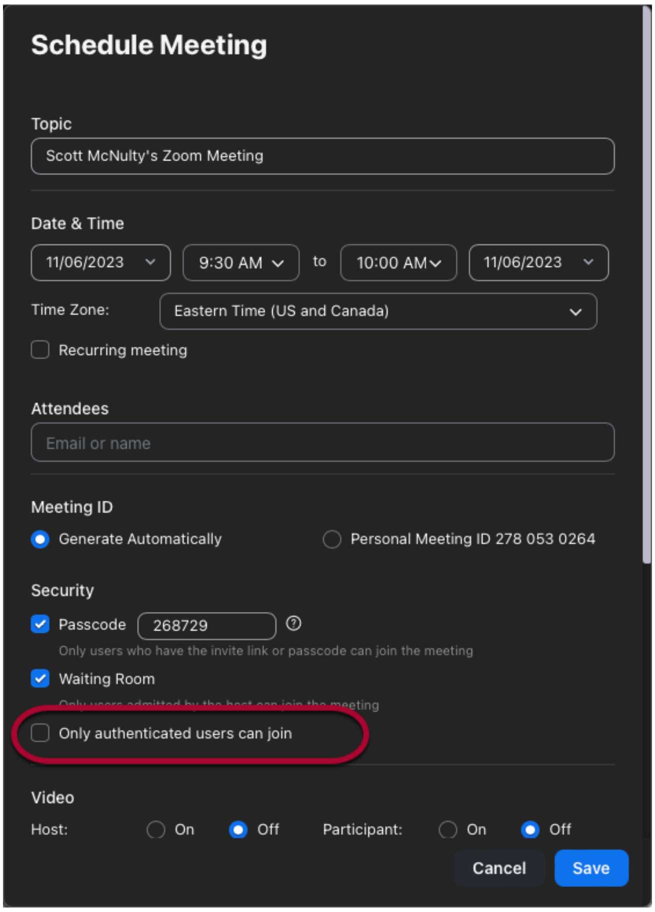
- Specific exceptions can be added per meeting (i.e.,santa@northpole.com can join without having to authenticate, but everyone else has to since they might be naughty).

You can require authentication on a per-meeting basis or by default for all meetings:

On an individual meeting

New Meeting

1. Launch Zoom.
2. Schedule a new meeting.
3. Scroll through the Schedule Meeting window and **check the box** next to "Only authenticated users can join."



Schedule Meeting

Topic

Scott McNulty's Zoom Meeting

Date & Time

11/06/2023 9:30 AM to 10:00 AM 11/06/2023

Time Zone: Eastern Time (US and Canada)

□ Recurring meeting

Attendees

Email or name

Meeting ID

● Generate Automatically ○ Personal Meeting ID 278 053 0264

Security

☑ Passcode 268729

Only users who have the invite link or passcode can join the meeting

☑ Waiting Room

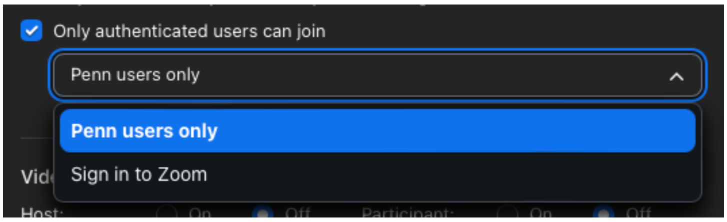
Only users admitted by the host can join the meeting

□ Only authenticated users can join

Video

Host: ○ On ● Off Participant: ○ On ● Off

4. Select either **Penn users only** (the default) or **Anyone with a Zoom account** from the dropdown.



☑ Only authenticated users can join

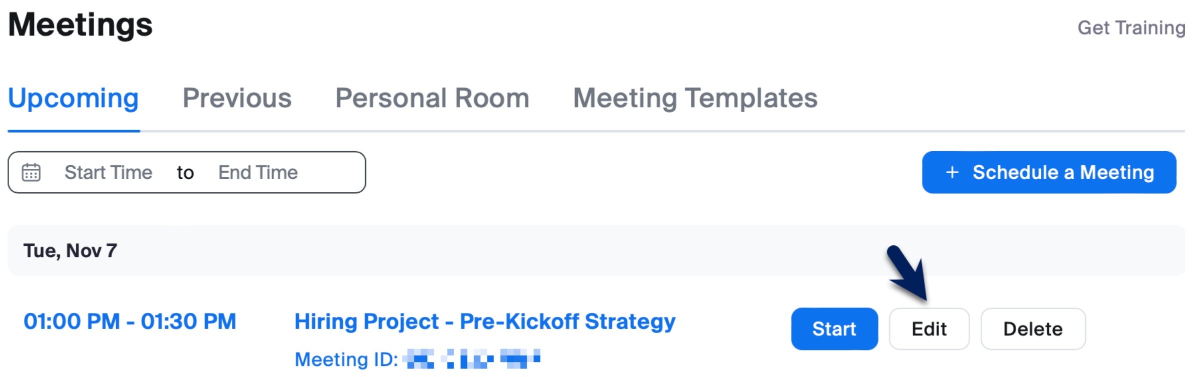
Penn users only

5. Continue scheduling your meeting as usual.

Existing Meeting

The best way to force authentication on an existing meeting is to edit the settings via .us:

1. Log into **.us** with your PennKey username and password.
2. **Hover over the meeting** you'd like to edit from your Upcoming Meetings.
3. Click the **Edit** button that appears as you're hovering over the meeting.

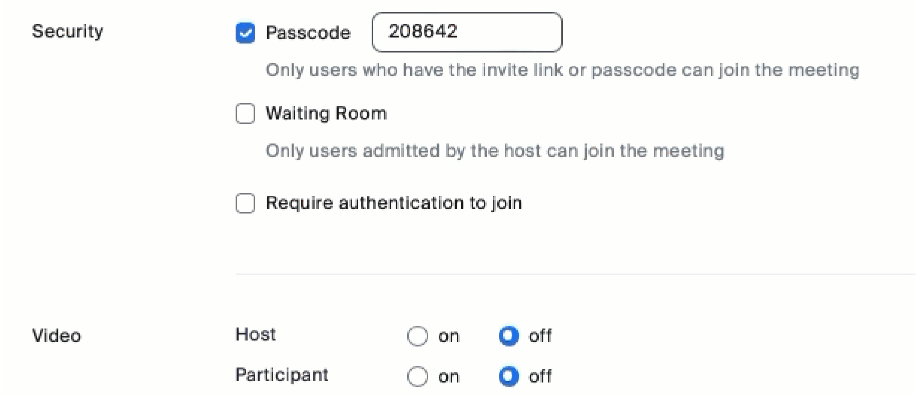


Tue, Nov 7

01:00 PM - 01:30 PM Hiring Project - Pre-Kickoff Strategy

Meeting ID: [redacted]

4. **Check** "Require authentication to join" in the Security section.
5. Select either **Penn users only** (the default) or **Anyone with a Zoom account** from the dropdown.



Security

☑ Passcode 208642

Only users who have the invite link or passcode can join the meeting

□ Waiting Room

Only users admitted by the host can join the meeting

□ Require authentication to join

Video

Host ○ on ● off

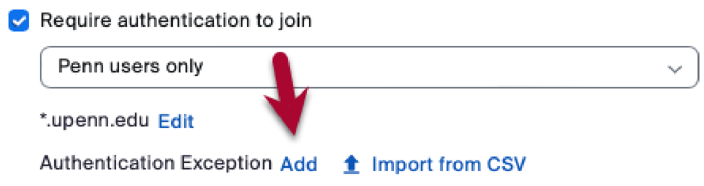
Participant ○ on ● off

6. Click **Save**.

Allowing Exceptions

Authentication Exceptions allow you to list people who don't have to authenticate to enter a meeting that requires it. This allows you to limit your attendees to Penn folks (or people with a Zoom account) but include non-Penn guest speakers. Here's how:

1. Log into **.us** with your PennKey username and password.
2. **Hover over the meeting** you'd like to edit from your Upcoming Meetings.
3. Click the **Edit** button that appears as you're hovering over the meeting.
4. Click **Add** next to "Authentication Exception" under "Require authentication to join" in the Security section.



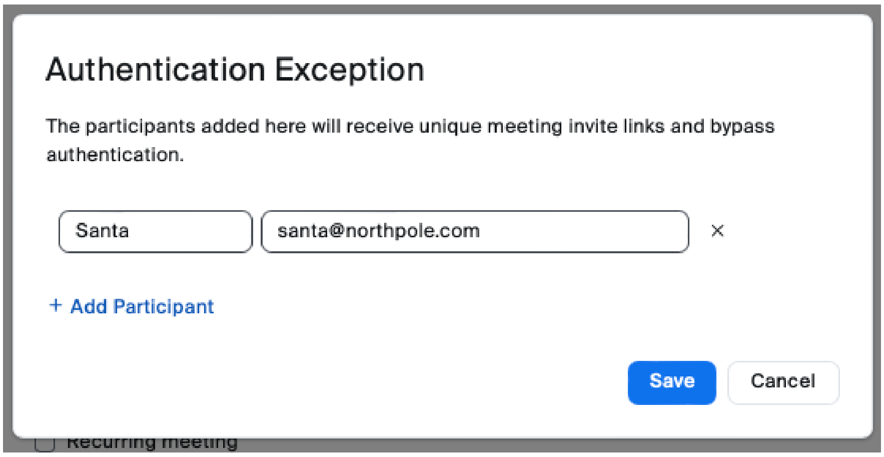
☑ Require authentication to join

Penn users only

*.upenn.edu Edit

Authentication Exception Add Import from CSV

5. Type the exception's full name and email address.



Authentication Exception

The participants added here will receive unique meeting invite links and bypass authentication.

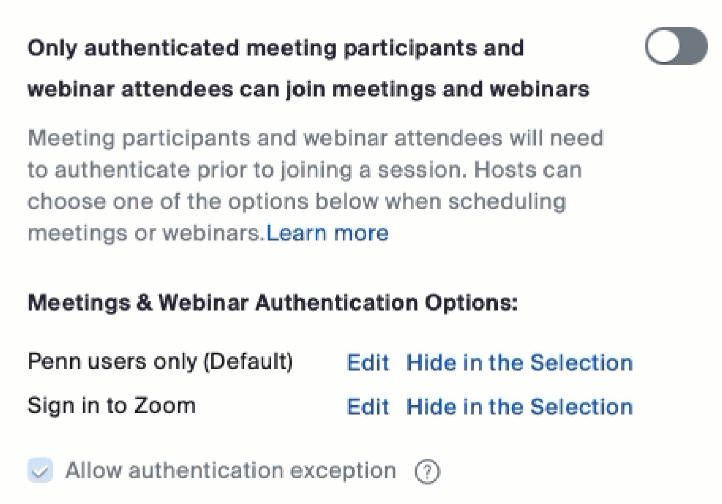
Santa | santa@northpole.com ×

6. Click **Add Participant** to add more exceptions.
7. Click **Save** to save the exceptions.
8. Click **Save** to save the settings for the meeting.

Making this a Default Setting

You can require authentication for all your Zoom meetings going forward by logging into.us with your PennKey username and password and following these directions:

1. Click **Settings**.
2. Click **Security**.
3. Scroll down until you see "Only authenticated meeting participants and webinar attendees can join meetings and webinars."
4. Click the toggle next to that section to turn it on (the toggle displays blue when a feature is active).



Only authenticated meeting participants and webinar attendees can join meetings and webinars

Meeting participants and webinar attendees will need to authenticate prior to joining a session. Hosts can choose one of the options below when scheduling meetings or webinars.Learn more

Meetings & Webinar Authentication Options:

Penn users only (Default) Edit Hide in the Selection

Sign in to Zoom Edit Hide in the Selection

☑ Allow authentication exception ?

5. Your settings are automatically saved, and now, each Zoom meeting you schedule will require attendees to authenticate.

> **Note**: Penn users only is the default and recommended authentication setting. You can change this by clicking **Edit** next to "Sign in to Zoom" under "Meetings & Webinar Authentication Options" and checking the default box.

During Your Meeting

Despite following all of our best practices, disruptions could occur in a Zoom meeting in which you're the host (or co-host). There are a few Zoom tools that make it easy to deal with a disruptive participant quickly:

- **Remove Participant** - Disruptive participants are easy to remove once identified.
- **Lock Meeting** - Locking your meeting stops any further participants from joining.
- **Suspend All Participant Activities** - The most severe option of the bunch; this will stop all activity in the meeting so you can gather your thoughts and identify the disruptive participants who should be removed.

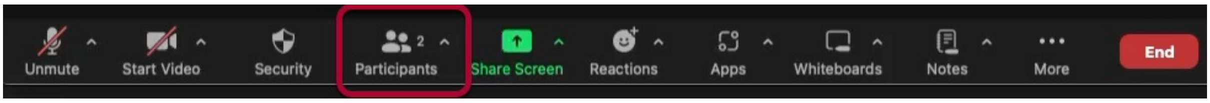
The following three sections detail each of these features in turn.

> Remember - Keep your cool; all of these tools are only a few clicks away!

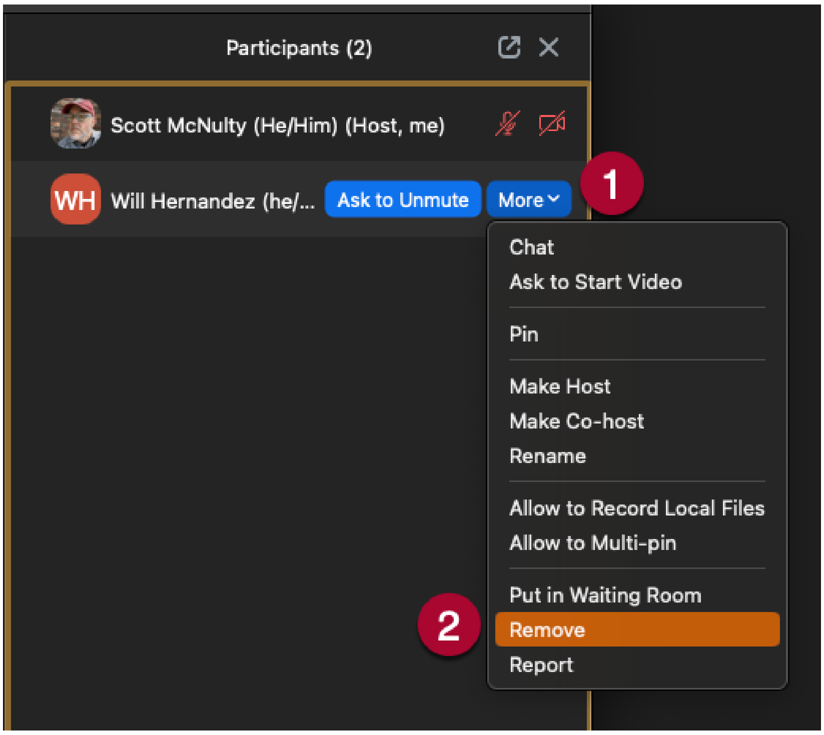
Remove Participant

If you can identify the disruptive participants, you can remove them from your Zoom meeting:

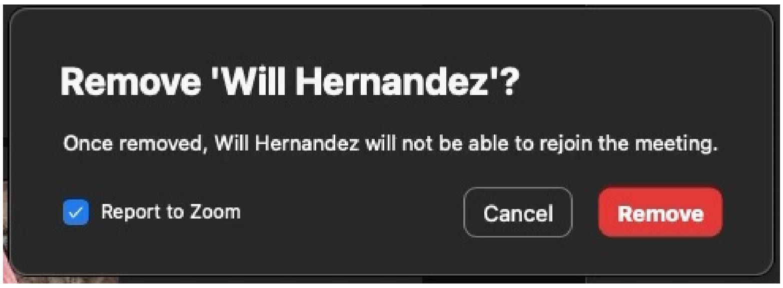
1. Click on the **Participants** icon at the bottom of the Zoom window to show the Participants list if it isn't already showing.



2. Find the person you'd like to remove and hover over their name in the list.
3. Click on **More** to reveal a list of options.



4. Click on **Remove** to remove the selected participant.
5. A confirmation popup appears. We recommend **unchecking** "Report to Zoom."


Remove 'Will Hernandez'?

Once removed, Will Hernandez will not be able to rejoin the meeting.

☑ Report to Zoom

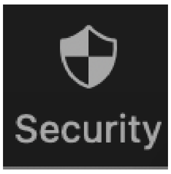
6. Click **Remove**, and the participant is removed from your meeting and will not be able to rejoin.

7. Repeat for each participant you'd like to remove.

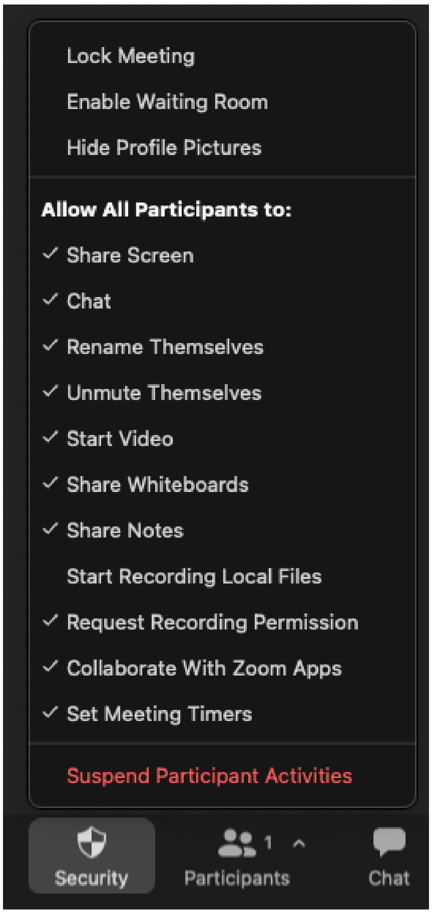
Lock Meeting

You may want to stop additional people from joining your meeting for some reason. To do this, you need to "Lock" your meeting:

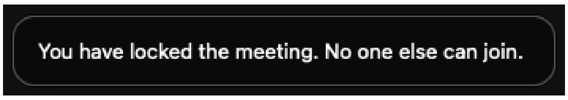
1. Click the Shield icon labeled **Security** at the bottom of your Zoom meeting window.



2. A list of all the in-meeting security controls available to you appears. Click **Lock Meeting** at the top of the list.



3. An alert appears, letting you know that no one else can join the meeting.



You have locked the meeting. No one else can join.

Note: To allow people to join, unlock the meeting by clicking the Security Icon and then clicking "Lock Meeting" again.

Suspend All Activities

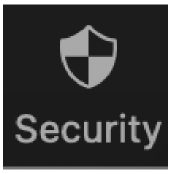
If there is a significant disruption in your meeting, you can suspend all participant activities with a few clicks. Be warned that this turns off most of the functionality of your Zoom meeting. Suspending all participant activities does all of the following:

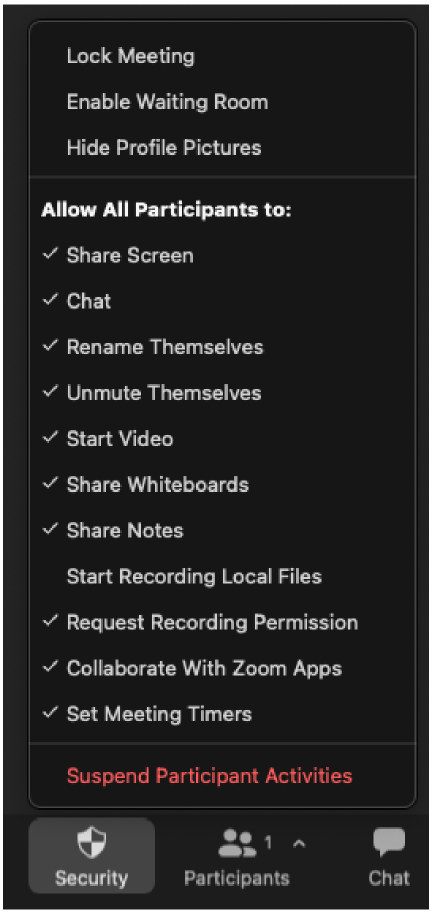
- Mutes all video and audio.
- Hides all profile pictures
- Stops all active screenshares and turns off screensharing.
- Closes all breakout rooms.
- Stops the meeting recording if the meeting is being recorded.
- Turns off any Zoom apps active in the meeting.
- Locks the meeting, preventing anyone else from joining.

Once all activity has been suspended, you can use the "Remove Participant" directions above to remove the disruptive participant(s).

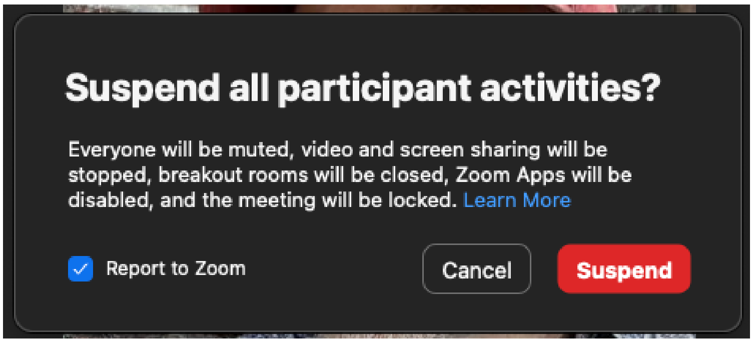
Warning: If you suspend all activity, you'll need to restart your Zoom recording.

To Suspend All Participant Activity in a meeting:

1. Click the Shield icon labeled **Security** at the bottom of your Zoom meeting window.


2. Click **Suspend Participant Activity** at the bottom of the list in red.


3. **Uncheck** "Report to Zoom" in the notification, which also reminds you that you're about to turn off all the functions in your Zoom meeting.

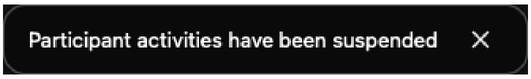


Suspend all participant activities?

Everyone will be muted, video and screen sharing will be stopped, breakout rooms will be closed, Zoom Apps will be disabled, and the meeting will be locked. Learn More

☑ Report to Zoom

4. Click the red **Suspend** button.
5. You'll get a confirmation message that all activity has been suspended in the meeting.



Participant activities have been suspended

Once you've dealt with the disruption, you can turn on individual features by clicking the Security icon and enabling each feature individually.

After Your Meeting

If any of your Zoom meetings are disrupted besides using the features above, report the incident to the Wharton Information Security Office (security@wharton.upenn.edu). They can engage additional resources, if needed, and offer any help you may require.

Questions?

Contact your Wharton Computing Representative or the Wharton Information Security Office for more information.