Tips för säkrare Zoom-möten

Antalet videomöten har ökat den senaste tiden nu när många sitter hemma och jobbar. Obehöriga känner också till detta.”Zoom bombing” är termen för när oinbjudna gäster dyker upp i ditt möte och uppsåtligen saboterar genom att t.ex. spamma chatten eller dela störande bilder via funktionen skärmdelning. De flesta av dessa intrång sker när möteslänkar av misstag gjorts tillgängliga offentligt.

Obs! Vid användning av Zoom inom Umeå universitet är det viktigt att du förhåller dig till universitetets riktlinjer. Kommunikationen i Zoom är krypterad och eventuella personuppgifter som hanteras sker inom EU. Tjänsten är dock, på samma sätt som de flesta centrala IT-system inom Umeå universitet, inte avsedd för att hantera känsliga personuppgifter eller sekretessbelagd information.

Rekommenderade inställningar

Nedan listas rekommenderade skyddsåtgärder som du som mötesvärd kan vidta för att skydda dina möten från oinbjudna gäster.

Ta för vana att:

- Lägg inte ut möteslänkar offentligt, exempelvis på sociala medier. Skicka istället länken direkt till deltagaren.
- Inte göra mötet offentligt. Det kan ske på två sätt: genom att sätta lösenord på mötet, eller att låta användare vänta ”utanför” för att bli insläppta.
- Begränsa möjligheten för deltagare i mötet att dela skärm, skriva i chatten m.m. ”*Host only*”-inställningar ger dig bättre kontroll över vad som visas i ditt möte.
- Se till att din installation av Zoom är uppdaterad till den senaste versionen. Zoom uppdaterar sina säkerhetsfunktioner med jämna mellanrum.

Få bättre koll över vilka som ansluter till ditt möte

Det finns olika inställningar för att få bättre koll och reglera vilka som ansluter till ditt möte. Välj det som passar bäst utifrån ditt mötes syfte.

- Begränsa möten med ditt personliga mötes-id

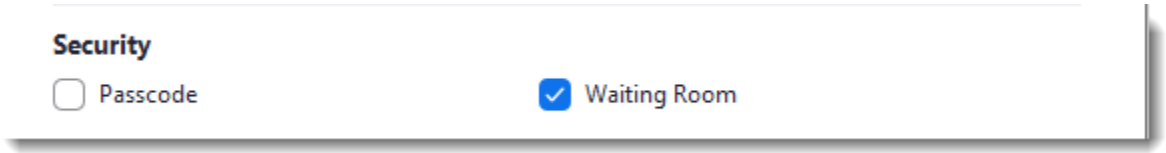
Genom att använda ditt personliga mötes-id så är länken för att ansluta till dina möten alltid densamma. Fördelen med detta är att t.ex. kollegor som du ofta har kontakt med har enklare att hitta ditt möte, men det innebär också att utomstående som fått tillgång till din länk också kan ansluta till dina möten.

Vid undervisning där man vill använda samma möteslänk under en längre tid lämpar det sig därför bättre att använda andra mötesrum och istället skapa ett ”Recurring Meeting” med ett slumpat mötes-id. Detta bidrar bland annat till att du undviker att bli störd i andra sammanhang där du använder ditt personliga mötes-id.

- Lösenordskydda ditt möte

För att förhindra att obehöriga deltar i ditt möte kan du lösenordsskydda det. Det innebär att endast deltagare som har mötes-id samt lösenord kan ansluta till mötet. När du schemalägger ett möte kan du skapa ett lösenord genom att bocka i “*Passcode*”. Bocka i rutan och skapa ett eget lösenord eller låt Zoom slumpa ett. När en deltagare ska ansluta till mötet kommer deltagaren bli ombedd att skriva in detta lösenord.

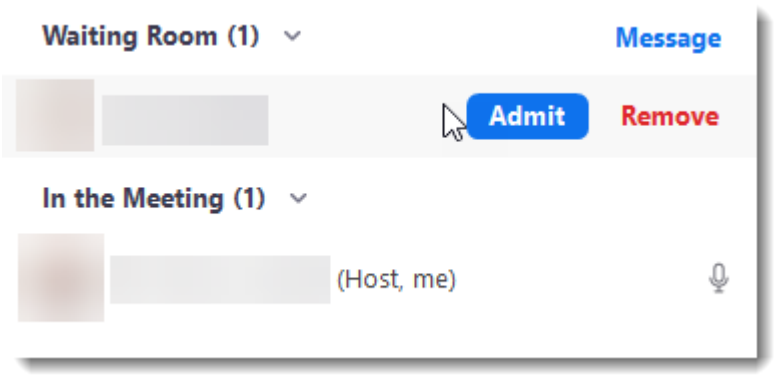
- Väntrum för anslutande mötesdeltagare



Denna funktion är bra för att få kontroll över vilka deltagare som ansluter sig till mötet och när de ska ansluta sig. Som värd för mötet, *host*, kan du

manuellt tillåta deltagare att ansluta en i taget via väntrummet till mötet eller lägga in alla samtidigt. Detta kan kräva lite mer arbete av dig som värd men möjliggör att du får bättre överblick av vilka deltagare som är med i mötet.

Notera att om en student ansluter sig för sent till ett möte kommer du att få ett pop up-meddelande om detta för att göra dig medveten. Du kan därefter släppa in deltagaren direkt ifrån pop up-fönstret eller genom att gå till Participants i mötet.



I väntrummet kan du lägga till ett personligt meddelande som deltagarna får när de ansluter sig, detta kan vara exempelvis information om mötets upplägg. Detta gör du genom att navigera till Meetings och sedan till Security-fliken i dina Zoom-inställningar.

- Only authenticated users can join meeting

Med denna inställning kan du välja att aktivera att endast ”authenticated users” kan ansluta till ditt specifika möte. Det innebär att alla deltagare måste logga med antingen UmU-id eller Zoom-konto för att komma in i mötet. Inställningen finns under ”Advanced options” när du schemalägger ett nytt möte.

- Inaktivera ”Join before Host”

Om denna inställning är inaktiverad kan inte deltagare ansluta till mötet förrän du som värd har startat mötet. Deltagare som väntar, kommer automatiskt in i mötet så fort mötet startas av dig som är värd.

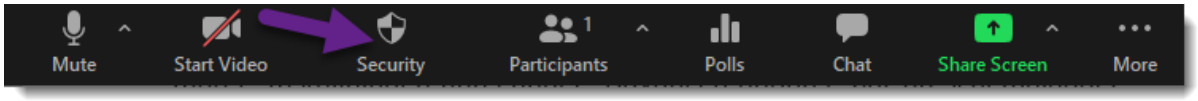
Denna inställning kan du ändra under “*Meeting options*” när du ska schemalägga ett möte. Om du vill ändra denna inställning för alla

schemalagda möten framöver finner du detta under "*Settings*" och "*Schedule meetings*".

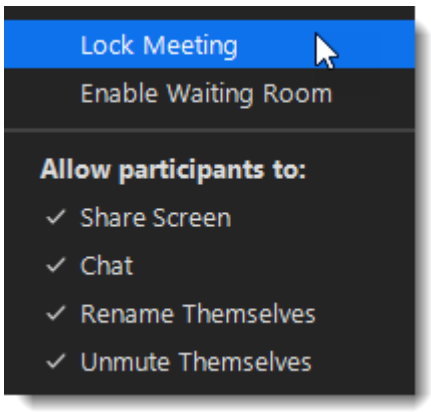
Kontrollfunktioner under pågående möte

- Lås ditt möte

Som värd för ett möte har både du och "*Co-Host*", medvärd, möjlighet att låsa mötet. Om du låser mötet kan inga fler deltagare gå med även om de har tillgång till länken.



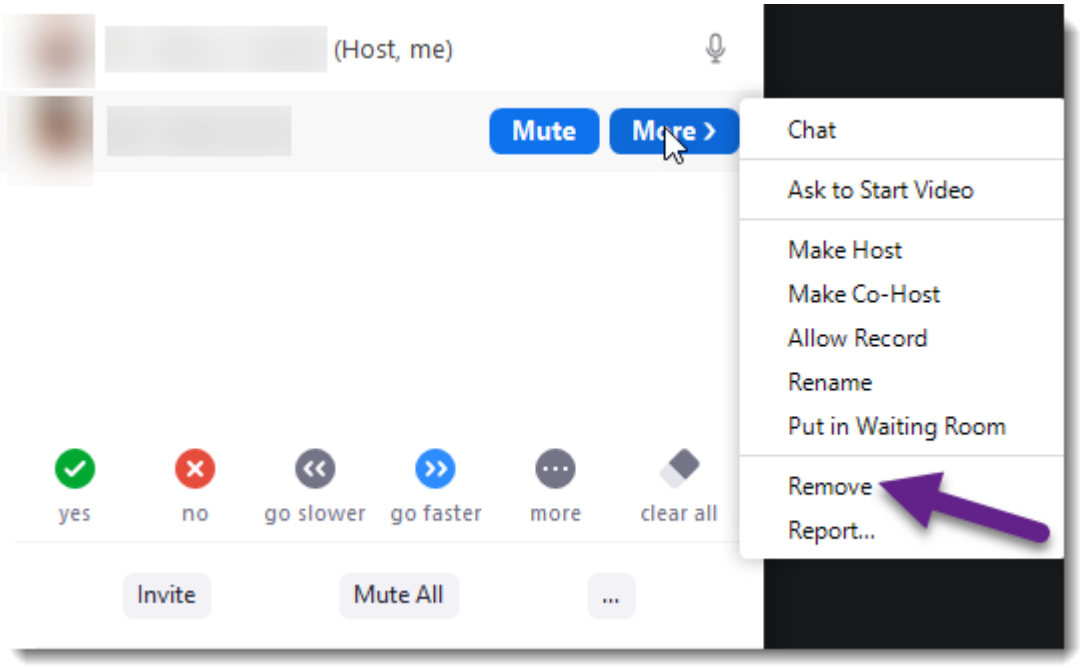
För att låsa mötet klickar du först på "*Security*" i menyn under mötets gång.



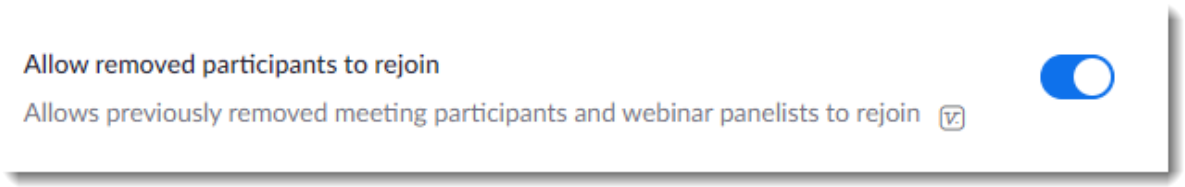
Klicka därefter på "*Lock Meeting*" för att låsa mötet. För att låsa upp mötet är det bara att klicka igen.

Om någon försöker att gå med i mötet när det är stängt får du ingen notifikation om detta. Det är därför viktigt att inte stänga mötet förrän alla som ska vara med har hunnit ansluta sig.

- Ta bort deltagare från möte



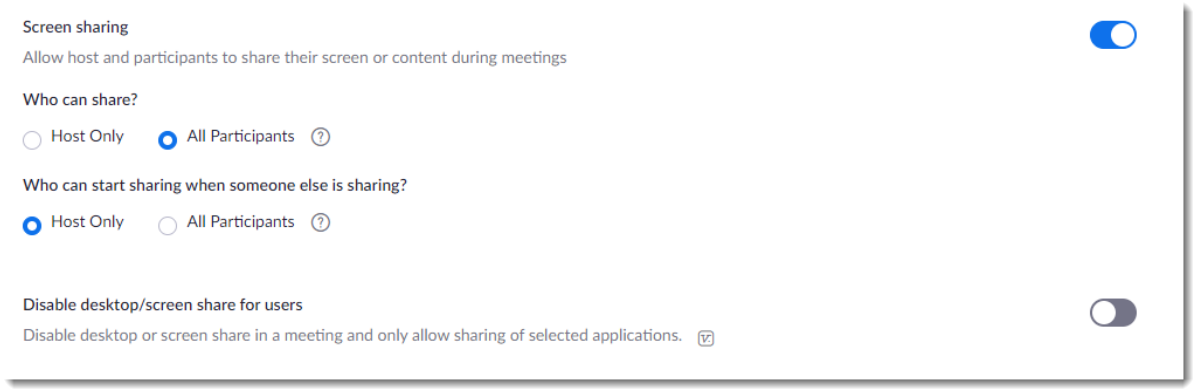
Om du under ett möte upptäcker en oönskad deltagare så kan du ta bort denne igenom att klicka på *"Participants"* och därefter *"More"* bredvid deltagarens namn. Ifrån menyn som dyker upp kan du välja *"Remove"*, vilket tar bort deltagaren från mötet.



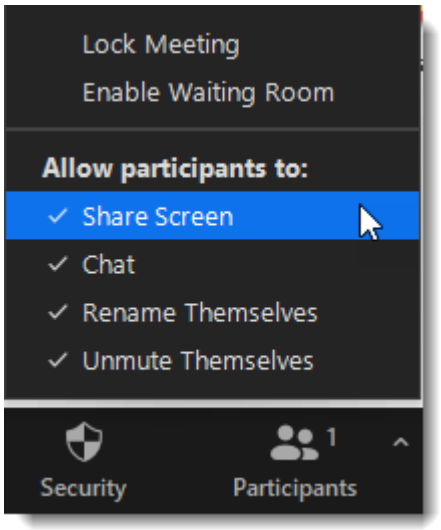
Om du av misstag tagit bort fel person kan du ändra detta genom att gå in på ditt konto, klicka på "*Settings*" och sedan "*In meeting (basic)*". Därefter scrollar du ner till "*Allow removed participants to rejoin*" och aktiverar den.

- Begränsa vem som kan dela skärm

Som värd kan det vara viktigt att du inte ger över kontrollen för vad som ska visas på skärmen till andra. Du vill inte ha någon i ditt möte som delar med sig av opassande och oönskat innehåll med deltagarna. Både innan mötet och under pågående möte kan du begränsa skärmdelningen till att endast du som värd kan dela skärm. Notera att standardinställningen innebär att både du och andra deltagare kan dela sin skärm.



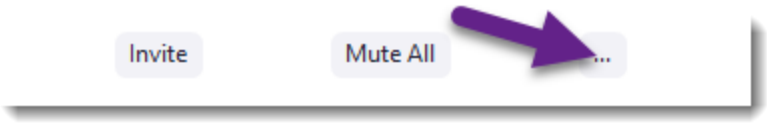
Om du vill begränsa vilka som kan skärmdela redan innan ditt möte påbörjas kan du gå in på ditt Zoom-konto. Därefter klickar du på "*Settings*" och under "*In meeting (basic)*" får du möjligheten att välja om endast värd eller även deltagare ska kunna skärmdela. Bilden ovan visar vilka valmöjligheter du har och du klickar i det alternativ du önskar för ditt kommande möte.



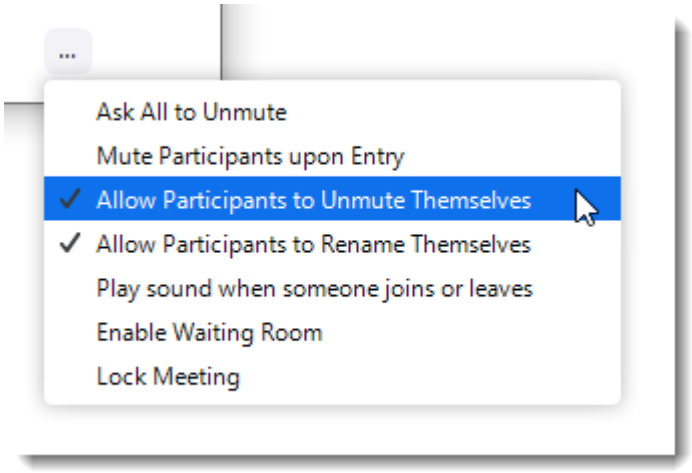
Vill du under pågående möte begränsa möjligheten för deltagare att dela skärm så klickar du på *"Security"* i mötesmenyn, och därefter bockar du ur *"Share Screen"*. För att låta deltagare dela skärm igen så är det bara att bocka i igen.

- Stäng av deltagarnas kamera och/eller mikrofon

Som värd för ett möte kan du själv kontrollera huruvida deltagare själva ska kunna aktivera sina kameror och mikrofoner.



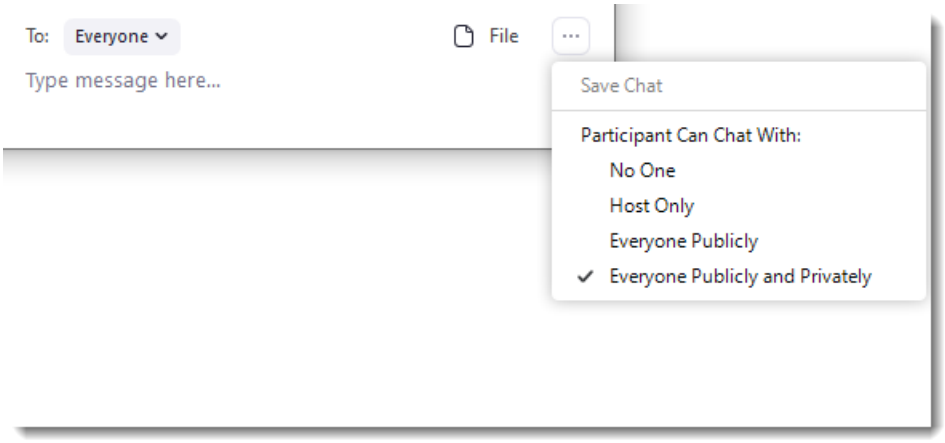
Du gör detta genom att klicka på *”Participants”* och därefter knappen med de tre punkterna längst ner i fönstret för att se fler valmöjligheter. Bredvid finns även *”Mute All”*-knappen, vilken slår av mikrofonen för alla deltagare.



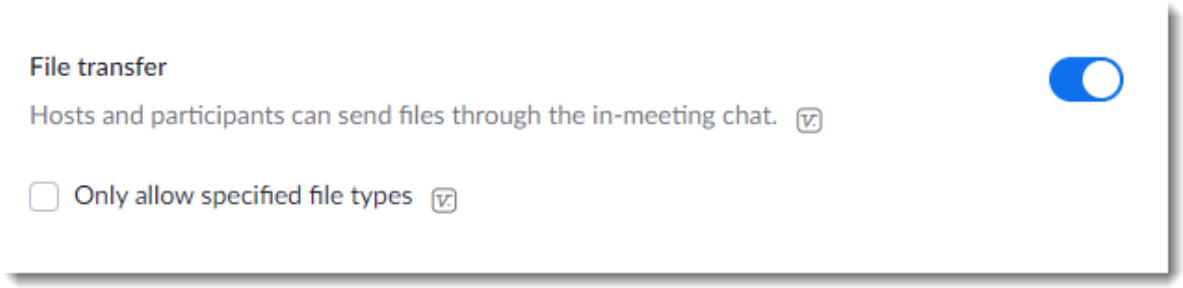
Om du inte vill att deltagarna i ditt möte ska kunna använda sina mikrofoner så kan du bocka i *”Mute Participants upon Entry”* och bocka ur *”Allow Participants to Unmute Themselves”*. Du kan även använda *”Mute All”*-knappen från föregående meny för att snabbt tysta deltagare och därefter bocka ur möjligheten för dem att ”avtysta” sig själva. Genom dessa valmöjligheter kan du som värd bestämma vem som har möjlighet att dela ljud, och när.

- Begränsa chatt och filöverföring under möte

Den förvalda inställningen i Zoom är att alla i mötet (deltagare och värd) kan skriva både publika och privata meddelanden. Du som mötesvärd kan redigera dessa inställningar vid behov. En säkerhetsåtgärd kan vara att slå av möjligheten för privata konversationer eller helt slå av chatten vid behov. Du kan göra inställningen under pågående möte.



Du hittar inställningarna för chatten genom att klicka på *"Chat"* och därefter klicka på knappen med de tre punkterna för att se menyn. Härifrån kan du bestämma huruvida deltagarna i mötet kan chatta med varandra, offentligt eller privat och så vidare.

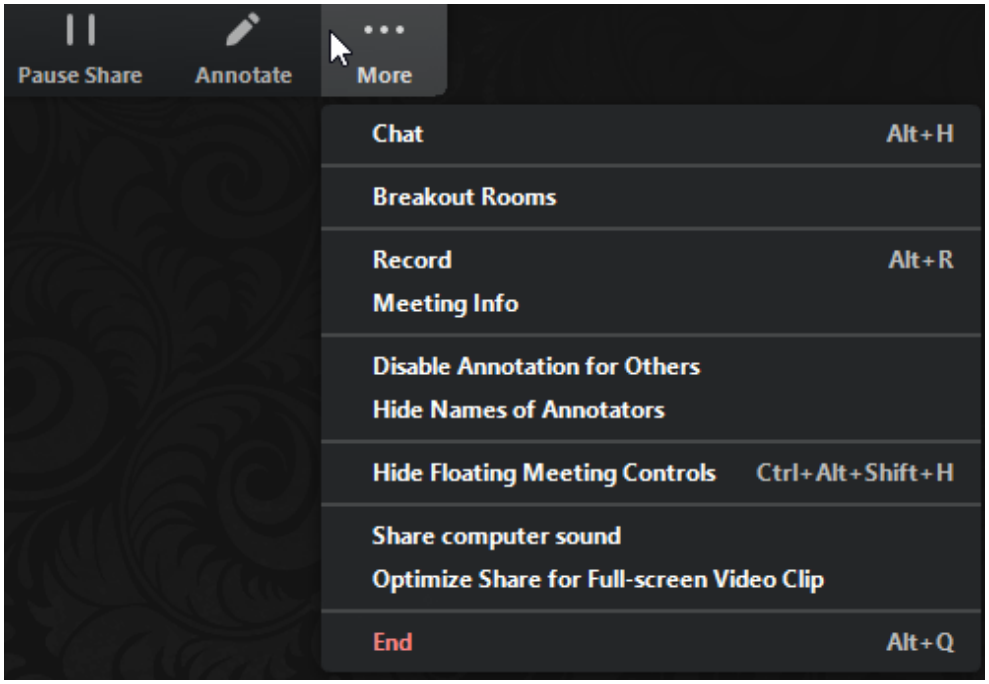


Filöverföring i chatten tillåter deltagarna att skicka filer till varandra under mötets gång. Vid händelse av opassande filer eller meddelanden i chatten kan det vara aktuellt att inaktivera funktionen för filöverföring.

Gå in på ditt konto, "*Settings*" och "*In meeting (basic)".* Där hittar du "*File transfer*" som du kan välja att aktivera eller inaktivera. Du kan även klicka i "*Only allow specified file types*" där du kan kontrollera exakt vilka typer av filer som är går att dela i mötet. Där skriver du in varje format som är tillåtet med ett kommatecken emellan för att skilja dem åt.

- Begränsa användning av annoteringsverktyg

Du och dina deltagare kan göra annoteringar och markera innehåll tillsammans med kommentarer under skärmdelningen. Du kan inaktivera kommentarfunktionen i Zoominställningarna för att förhindra att folk skriver över hela skärmarna. Vid behov kan du slå av deltagarnas möjlighet att göra annoteringar.



När du delar din skärm och vill slå av möjligheten för deltagare att kommentera så klickar du på *”More”* och sedan *”Disable Annotation for Others”*.

Fler rekommendationer för säkerhet i Zoom

- https://blog.zoom.us/teachers-top-features-for-securing-virtual-classrooms-enhancing-student-learning-experiences/
- https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-securing-zoom