

Zoom: utilizzo sicuro

- Assicurarsi che Zoom sia sempre aggiornato all'ultima versione in modo da beneficiare di tutte le patch e aggiornamenti in materia di sicurezza e privacy.
- Nel caso di creazione di un nuovo account Zoom con email @unimi.it non utilizzare Facebook o Google sign in ma creare login/password con l'email di ateneo come login e una password *diversa* da quella di ateneo.

Prima del meeting

- Assicurarsi che le preferenze sul sito prevedano l'uso della password per tutti i meeting e che l'opzione di inglobarla nei link sia attiva (per convenienza dei partecipanti)

passcode1.png

.

- Assicurarsi che sia l'host che i partecipanti ad un meeting siano identificati con nome e cognome (modificabile dall'utente sul proprio account sul sito zoom.us). Eventualmente l'host può modificare l'identificatore di un partecipante dopo essersi assicurato della sua identità.

- Se possibile, evitare l'utilizzo dell'opzione "Join before host" nell'impostazione dei meeting.

joinbeforehost.png

- Nel caso di meeting ristretti e con audience conosciuta l'host/organizzatore assicurarsi che sia abilitata la waiting room (questo permette di verificare chi chiede di partecipare ed ammettere singolarmente o in gruppo i partecipanti).

meetingroom.png

- Nel caso di lezioni o conferenze (molti partecipanti): se possibile utilizzare comunque la waiting room eventualmente utilizzando un moderatore (co-host) che possa gestire l'ingresso dei partecipanti. In ogni caso, l'host deve assicurarsi che l'uso di password sia abilitato e distribuire preventivamente ai partecipanti link/invito con un canale sicuro raccomandandosi di mantenere la confidenzialità dei dati per l'accesso al meeting.

- Per le attività didattiche fornire link al meeting (con password inglobata) su un sito ad accesso ristretto (Ariel/Moodle) e raccomandare agli studenti di non condividere il link. Chi utilizza Moodle con il plugin per Zoom si assicuri di pianificare il meeting da Moodle selezionando l'opzione per l'uso di password.

Durante il meeting

Condivisione schermo

- Quando solo l'host (per esempio il docente durante una lezione) deve condividere lo schermo, deve impostare la configurazione in modo che non preveda condivisione dello schermo da parte dei partecipanti (durante il meeting da menu a tendina a fianco della funzionalità di "share screen" scegliendo "advanced settings" e selezionando "only host").

share_only_host.png

- Se un numero limitato predefinito di persone devono condividere lo schermo (per esempio consigli di dipartimento o riunioni) si suggerisce di eleggerli dinamicamente al ruolo di co-host nella finestra dei partecipanti.

make_co_host.png

- Quando è indispensabile la condivisione da parte di arbitrari partecipanti impostare a "only one sharing at a time". In questo modo l'host arresterà la propria condivisione per permettere al partecipante designato di attivare la propria.

share_only_one.png

- Gestione audio/video. Nelle lezioni e nei meeting aperti è opportuno impostare le preferenze in modo che tutti i microfoni dei partecipanti siano in "mute" (senza possibilità dei partecipanti di riabilitare il microfono) e il video disabilitato.

mute_all.png

Registrazione

- La registrazione da parte dei partecipanti deve essere disabilitata.

no_rec.png

- Ove sia necessaria la registrazione da parte dell'host, avvisare esplicitamente i partecipanti e salvare la registrazione in locale (poi eventualmente caricabile sulle piattaforme di ateneo) e non su cloud Zoom. E' anche possibile abilitare un avviso audio in inglese che è comunicato automaticamente a tutti i partecipanti una volta che una registrazione inizia: tale impostazione è attivabile dalle [impostazioni](#). [rec_privacy.png](#)

- Se viene effettuata la registrazione della lezione (da parte del docente) le impostazioni di cui sopra diventano necessarie e qualora fossero previsti interventi in audio/video, il docente deve interrompere la registrazione e poi abilitare il microfono del partecipante. In alternativa si può prevedere una sessione specifica di domande e risposte in cui la registrazione sia disattivata oppure utilizzare la chat.

- La registrazione di sessioni d'esame è attualmente vietata dall'ateneo.

Ulteriori informazioni utili alla sicurezza

- <https://blog.zoom.us/best-practices-for-securing-your-virtual-classroom/>
- <https://zoom.us/docs/doc/Tips%20and%20Tricks%20for%20Teachers%20Educating%20on%20Zoom.pdf>
- <https://support.zoom.us/>

In relazione al continuo aggiornamento di funzionalità messe a disposizione da Zoom, si precisa che le indicazioni contenute nel seguente documento potranno essere modificate e aggiornate nel corso del tempo.

Aspetti riguardanti la privacy

Gli host e in generale i partecipanti ai meeting sono invitati a leggere la privacy policy corrente sul sito di [Zoom](#) per quanto riguarda l'esposizione dei dati alla piattaforma.

Gli host devono sapere che usando l'account universitario (account @unimi.it associato al dipartimento) gli amministratori dell'account possono vedere alcuni dati relativi ai meeting da loro organizzati, tra i quali i più rilevanti sono: Titolo del meeting, orario di inizio e durata, id dei partecipanti, tempo speso nel meeting da ciascuno, OS utilizzati, IP address.

Gli host devono avvisare i partecipanti che:

- il loro identificatore (spesso Nome e Cognome), IP, orari di entrata e uscita dal meeting vengono acquisiti da Zoom e registrati in un report a disposizione dell'host e dell'amministrazione universitaria.
- che la chat viene registrata e che nel caso di videoregistrazione (segnalata dall'host e da apposito simbolo) verranno ovviamente registrati anche i loro interventi.

From:

<https://servizi.di.unimi.it/> - **Servizi Tecnologici**
Dipartimento di Informatica

Permanent link:

<https://servizi.di.unimi.it/servizi:servtec:zoom:zoomsecurity>

Last update: **2024/01/16 12:55**

