UNIVERSITÀ di VERONA

Direzione SISTEMI INFORMATIVI E TECNOLOGIE
Area Sistemi Informativi

VIDEOCONFERENZE CON ZOOM (e non solo): NOTE IMPORTANTI SULLA SICUREZZA

Premessa

In questo periodo di emergenza dovuta al Covid-19 è diventata fondamentale l'interazione fra le persone attraverso le videoconferenze, sia per la didattica a distanza fra docente e studenti sia per le riunioni di lavoro con i propri colleghi.

Il presente documento riguarda l'applicativo ZOOM anche perché ultimamente anche la stampa ha veicolato notizie relative a rischi nel suo utilizzo.

Si puntualizza però che tanti consigli sono applicabili a tutte le piattaforme di videoconferenza che devono essere tenute sempre aggiornate, non si devono diffondere sui social i link alle riunioni e fare attenziona a chi viene ammesso alla riunione.

L'applicazione ZOOM è al momento una delle più utilizzate, non solo in Italia. Questa improvvisa popolarità ha destato l'attenzione di hacker e troll che in modo inopportuno si sono inseriti in videoconferenze o hanno utilizzato i contatti degli utenti.

La violazione delle policy del servizio riguardanti le misure di sicurezza adottate da Zoom sono state segnalate dai maggiori esperti di cybersecurity di aziende e istituti i quali hanno evidenziato la necessità di seguire alcune accortezze per evitare di esporre gli utenti al rischio di intrusione o hackeraggio.

La Direzione Sistemi informativi e Tecnologie ritiene importante darne comunicazione a tutti coloro che stanno utilizzando Zoom, riportando alcuni consigli fondamentali elencati anche sulla pagina specifica del blog di Zoom e aggiornati continuamente dal produttore. Si consiglia pertanto di consultare sempre le ultime informazioni che sono comunicate sulla home page del blog.

Si avvisa che Zoom ha rilasciato una versione aggiornata ed ha reso pubblico il programma delle azioni intraprese in un messaggio rivolto ai propri utenti sul blog ed in particolare l'impegno dell'azienda a concentrare i propri sforzi di sviluppo sulla sicurezza della piattaforma, piuttosto che all'introduzione di nuove funzionalità.

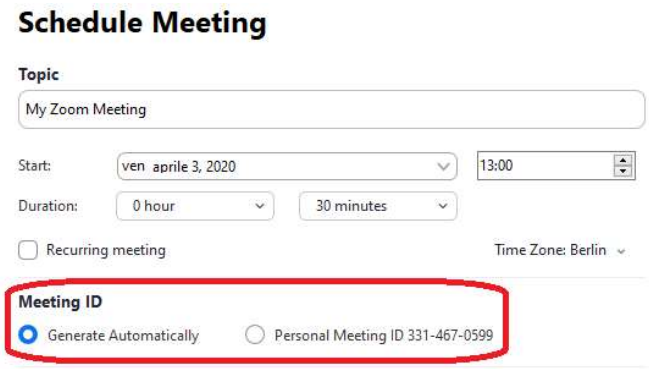
Consigli per gli utenti utilizzatori di Zoom

1) **Aggiornare sempre il client Zoom all'ultima versione rilasciata.**

Qualora si utilizzi l'applicazione client Zoom, si raccomanda di assicurarsi di avere installato l'ultima versione disponibile. In particolare, per i sistemi Windows e macOS è disponibile ad oggi la versione 4.6.9 rilasciata il 02 Aprile 2020, che ha risolto una falla sulla gestione dei path UNC, oltre ad altre problematiche inerenti la sicurezza.
L'aggiornamento all'ultima versione parte in automatico nel momento in cui si lancia l'applicativo installato.

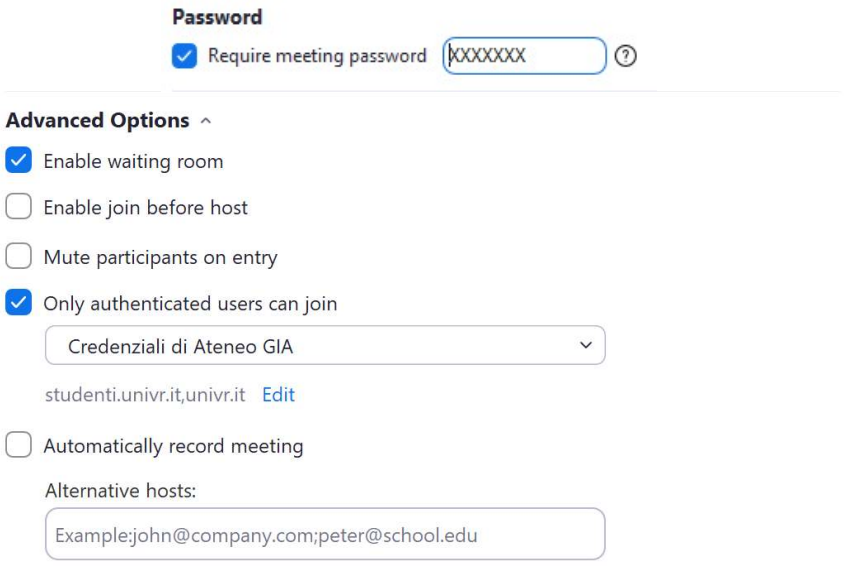
2) Nella programmazione di un nuovo meeting, evitare di utilizzare il Personal Meeting ID.

Il Personal Meeting ID (PMI) è, di fatto, un meeting sempre attivo, il cui identificativo non cambia nel tempo. Nelle opzioni di schedulazione di un meeting, è quindi consigliato di utilizzare l'opzione di generazione automatica del meeting ID.



3) Proteggere il meeting con una password o attivare la funzionalità di "waiting room"

E' sempre consigliato indicare una password per l'accesso al meeting, al fine di evitare accessi non consentiti. Si tenga comunque presente che per impostazione predefinita, il link ai meeting contiene al suo interno la password di accesso. E' pertanto consigliato inviare il solo meeting ID e la relativa password in due comunicazioni separate. E' possibile attivare anche la funzionalità "waiting room", che consente al creatore del meeting di accettare o rifiutare i partecipanti prima che essi accedano al meeting. Infine è anche possible far sì che solo gli utenti in possesso delle credenziali GIA possano partecipare al meeting, settando la funzionalità "Only authenticated users can join"

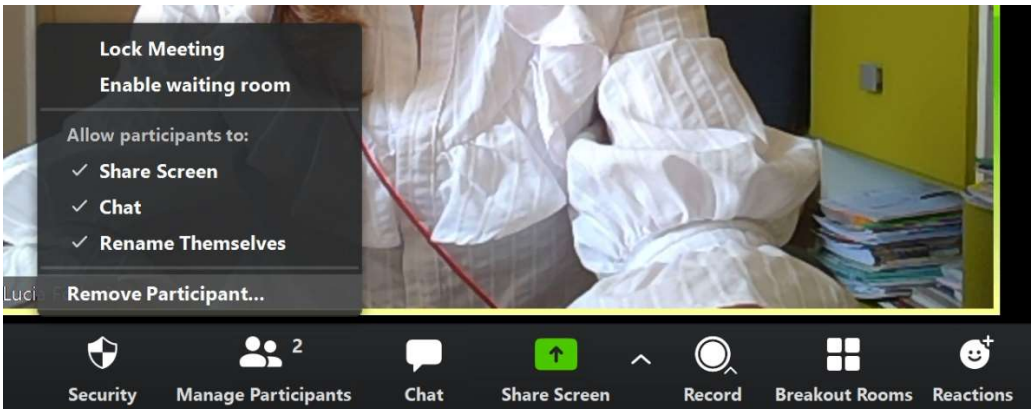


4) Non diffondere mai il link del meeting su canali pubblici (es. Social Network o altro)

Se il link completo del meeting viene pubblicamente diffuso, questo diventa accessibile a chiunque possieda il link. E' pertanto importante condividere puntualmente il link con i partecipanti specifici.

5) Utilizzare l'icona Security introdotta nella barra degli strumenti

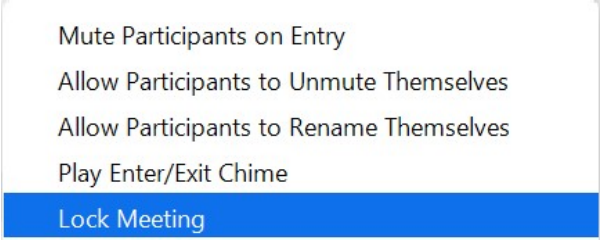
Selezionando l'icona suddetta è possibile impedire l'accesso al meeting (Lock Meeting), abilitare anche in corso di meeting la waiting room e inibire alcune funzionalità ai partecipanti (Share Screen, Chat e Rename).



Tutte le opzioni sopra descritte sono configurabili per default su tutti i meeting nell'area riservata del portale Zoom, cliccando sul menù "Settings"

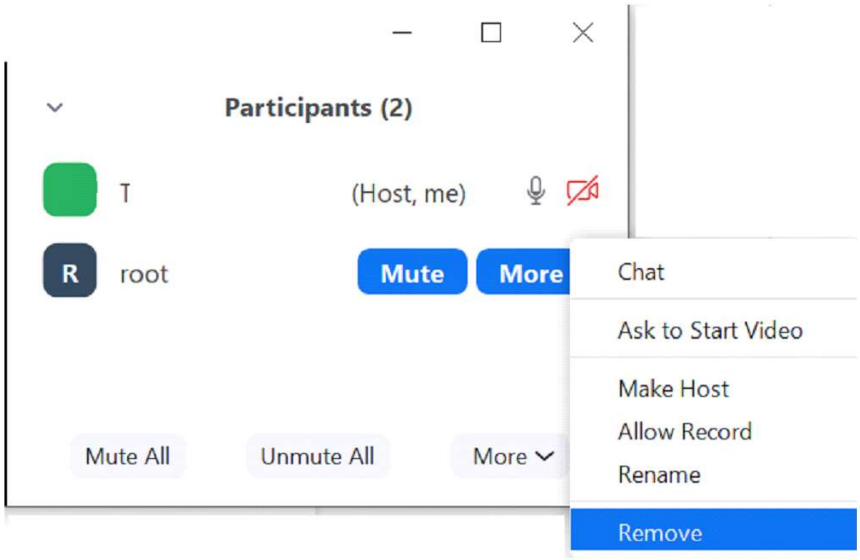
6) Bloccare il meeting una volta che tutti i partecipanti hanno fatto accesso

Quando il meeting è stato avviato e tutti i partecipanti hanno avuto accesso, è possibile bloccare il meeting affinché nessun nuovo partecipante possa avere accesso. Per far questo, è necessario cliccare sul bottone “Manage Participiants”, cliccare sul bottone “more” e selezionare l’opzione “lock meeting”



7) Rimuovere dal meeting eventuali partecipanti non voluti:

Dal menù “Participants”, è possibile selezionare il nome di un partecipante non voluto e cliccare il tasto “remove” affinché abbandoni il meeting.



8) Disattivare le chat, le chat private e altre funzionalità non desiderate

Accedendo al portale Zoom, nella sezione “Settings”, sono disponibili molti settaggi che possono aiutare a gestire in sicurezza un meeting e a disabilitare opzioni potenzialmente non volute quali chat e chat private. Si invitano gli utenti a verificare queste impostazioni prima della creazione di meeting.

Per eventuali comportamenti anomali o problemi di sicurezza si possono inviare segnalazioni direttamente a Zoom https://support.zoom.us/hc/en-us/requests/new

Per informazioni più dettagliate sulla gestione di un meeting, è possibile far riferimento anche alla guida ufficiale Zoom: https://support.zoom.us/hc/en-us/articles/115005759423-Managing-Participants-in-a-Meeting

9) Registrazione lezioni

Si ricorda che è necessario evitare che la registrazione parta in automatico ed è inoltre indispensabile - anche agendo sui settings del proprio account - garantire sempre il rispetto della privacy dei partecipanti, rifacendosi alle disposizioni della normativa esistente in termini di privacy.

Si ricorda in ogni caso che - per default - le registrazioni delle lezioni sono disponibili solo agli iscritti a uno specifico insegnamento nello spazio moodle e non sono scaricabili.

Per dubbi e/o informazioni in merito si rimanda all'ufficio competente della privacy.