UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Vademecum

Prevenire e contrastare attacchi informatici a eventi organizzati via web: il fenomeno del Bombing

Lo strumento della videoconferenza, specie col perdurare dell'emergenza pandemica, costituisce un supporto fondamentale alle attività didattiche e alla realizzazione di eventi a distanza privati o pubblici.
L'Ateneo supporta attualmente come piattaforme autorizzate per la realizzazione di videoconferenze **Microsoft Office 365/Teams, Meet di G Suite (licenza Edu e Enterprise), Zoom (licenza free e Edu).**

Se, da un lato, l'esponenziale aumento dell'utenza ha portato a notevoli migliorie e fondamentali accorgimenti tecnici da parte dei provider per migliorare e semplificare l'esperienza utente, dall'altro ha causato la comparsa di nuove tipologie di attacco e di azioni di disturbo alle sessioni di videoconferenza ad opera di sconosciuti.

Accedendo al link della videoconferenza pubblicato su siti pubblici, gli sconosciuti, sfruttando i canali audio, video e chat possono entrare nella riunione e interrompere le sessioni diffondendo immagini e messaggi, spesso illeciti, con l'obiettivo di disturbare, danneggiare o sfruttare a scopi pubblicitari questi canali. Questo tipo di incursioni e aggressioni, seppur virtuali, impediscono il corretto svolgimento degli eventi e accrescono il senso di insicurezza e incertezza verso l'affidabilità degli strumenti tecnologici da parte di quanti si trovano a subirli.

Il fenomeno ha preso il nome di **ZoomBombing** dal nome della piattaforma che per prima ha subito questi attacchi a livello mondiale.

Particolare attenzione deve essere quindi prestata dagli organizzatori di eventi aperti al pubblico sia nella fase di pianificazione dell'evento che nella fase di realizzazione e gestione dell'evento stesso.

È importante anche capire come scegliere, tra quelle autorizzate dall'Ateneo, la piattaforma più indicata per il tipo di evento che si intende pianificare e come configurare le opzioni dell'evento per consentire il pieno controllo da parte dell'organizzatore.

Di seguito riportiamo un breve vademecum delle strategie da mettere in atto per ridurre il rischio di intrusioni indesiderate.

Avvertenze nella realizzazione di eventi privati o a pubblico limitato

Generalmente il rispetto delle dovute accortezze per riunioni o eventi con pubblico limitato (studenti, partecipanti iscritti, etc.) è sufficiente e permette una scelta abbastanza libera della piattaforma da utilizzare.

Accortezze per il corretto svolgimento di un evento privato o a pubblico limitato, in generale, sono:

- **invitare singolarmente i partecipanti** durante la pianificazione dell'evento in Calendario, in questo modo riceveranno il link direttamente via mail e non sarà necessario pubblicarlo su un sito
- **chiedere di non partecipare in modo anonimo:** invitare i partecipanti a effettuare il login alla piattaforma con il proprio account istituzionale e/o creare un account
- **impostare la "sala d'attesa"** virtuale con successiva accettazione esplicita dei partecipanti autorizzati
- **consentire l'accesso solo con webcam e microfono spenti**
- **non pubblicare il link su siti pubblici o post pubblici sui social media**
- **impostare i relatori esplicitamente solo in corso di riunione**

Avvertenze nella realizzazione di eventi pubblici

Nel caso di eventi pubblici, senza iscrizione o ad iscrizione aperta è necessario scegliere opportunamente la piattaforma da utilizzare. Inoltre, nel caso di eventi per cui è prevista un'affluenza ingente è necessario prevedere una o più figure che si occupino dell'azione di moderazione dell'evento.
Accortezze per il corretto svolgimento di un evento pubblico, in generale, sono:

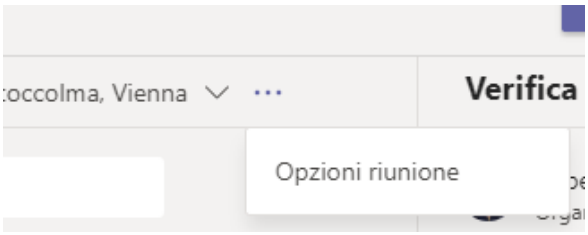
- **Creare un form di registrazione** che mandi il link via mail agli iscritti e concedere l'accesso solo agli indirizzi registrati
- **Evitare di pubblicare il link su siti pubblici o post pubblici sui social media**
- **Valutare la trasmissione solo in streaming dell'evento** con eventuale sezione domande/risposte privata o pubblica (eventi live di Teams)
- **Valutare l'attivazione della "sala d'attesa" all'entrata**
- **Se la piattaforma lo consente, impostare la password di accesso al meeting e comunicarla con modalità separata dal link**
- **Mettere in muto i partecipanti al momento dell'entrata**
- **Bloccare la possibilità di partecipare prima dell'organizzatore**
- **Bloccare l'ingresso nella riunione dopo che i partecipanti sono entrati**
- **Limitare al minimo l'interazione dei partecipanti**
- **Assegnare il ruolo di relatore a persone specifiche**: di norma può essere fatto sia durante la creazione dell'evento che durante l'evento stesso
- **Prevedere una figura che si occupi della moderazione della riunione**, nello specifico una figura che si occupi di:

    - **Ammettere i partecipanti**: nel caso sia stato attivato il form di registrazione controllare che gli stessi figurino nella lista degli iscritti
    - **Controllare costantemente la lista dei partecipanti** (e relatori) per disabilitare eventuali microfoni accessi (se ne fosse consentito l'utilizzo)
    - **Scollegare elementi di disturbo** ed evitare che gli stessi si possano riconnettersi rifiutando future richieste di accesso

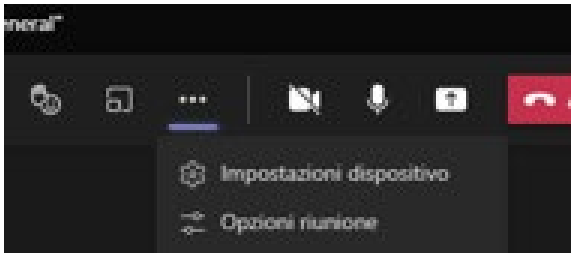
Suggerimenti per piattaforma

Proteggere una riunione di Teams

Teams consente lo svolgimento di riunioni (fino a 1000 partecipanti) e di eventi live (trasmissione in streaming, fino a 10000 partecipanti).
Nelle riunioni, modifica le impostazioni da Opzioni riunione dopo la pianificazione dell'evento in Calendario.



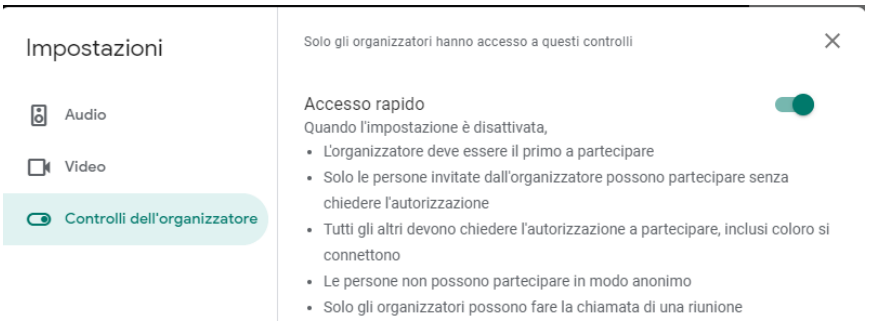
Durante la riunione clicca sui 3 puntini nella barra delle opzioni e poi *Opzioni riunione*



- **Attivare la sala d'attesa per i guest:** in *Opzioni riunione* imposta che possono evitare la sala d'attesa solo i membri dell'organizzazione che hanno fatto il login a Teams
- **Spegnere il microfono dei partecipanti all'entrata**
- **Controllare la lista dei partecipanti** durante la riunione alla ricerca di eventuali intrusi
- **Limitare il ruolo di relatore al solo organizzatore**: modificare l'impostazione in *Opzioni riunione*. Il relatore può condividere, mutare o rimuovere partecipanti, immettere guest dalla sala d'attesa, avviare la registrazione
- **Impostare eventuali altri relatori solo durante la riunione** cliccando sui 3 puntini di fianco al nominativo e poi *Make an attendee*
- **Rimuovere un eventuale intruso** cliccando sui 3 puntini di fianco al nome nella lista dei partecipanti e poi *Remove from meeting*

Proteggere una riunione Meet di G Suite

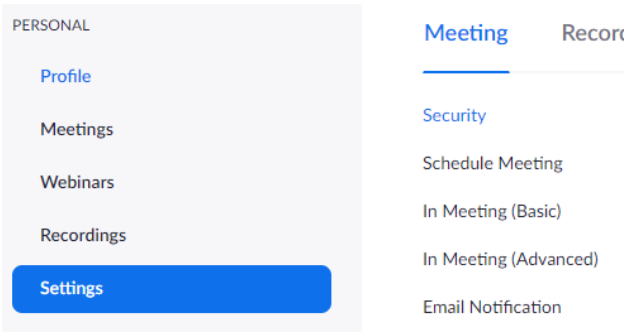
Meet consente lo svolgimento di riunioni fino a 100 partecipanti (licenza Education) e fino a 250 partecipanti (per chi dispone della licenza Enterprise).
Controlla le impostazioni della riunione cliccando sui 3 puntini in basso a destra, *Impostazioni, Controlli dell'organizzatore*.



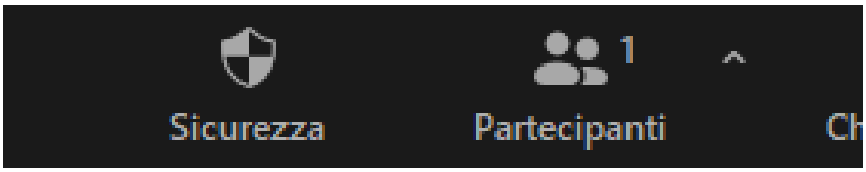
- Per default, tutte le persone invitate alla riunione che non fanno parte del dominio **@unimore.it** devono essere ammesse per partecipare (inclusi gli studenti)
- **Disabilitare l'accesso rapido**: in questo modo tutte le persone interne ed esterne alla tua organizzazione devono chiedere di partecipare alla riunione, chiunque venga invitato durante la riunione da altre persone oltre l'organizzatore deve chiedere di partecipare, potranno partecipare a nuove istanze della riunione con lo stesso codice solo le persone invitate esplicitamente, se si rimuove un intruso dalla riunione (interni o esterni al dominio **@unimore.it**) questi non potrà più richiedere l'accesso per partecipare nuovamente alla riuniuone.

Proteggere un meeting di Zoom

Zoom consente la realizzazione di meeting fino a 100 partecipanti (licenza free) e fino a 300 partecipanti (per chi dispone di licenza Edu).
Modifica le impostazioni nella sezione *Setting/In Meeting e In Meeting advanced* dopo l'accesso a **unimore-it.zoom.us**.



Durante il meeting modificare le impostazioni dal menu Sicurezza nella barra delle opzioni



- **Prevedere un form di registrazione** all'evento che consenta l'accesso solo agli iscritti
- **Impostare la password del meeting** e comunicarla su un canale diverso da quello in cui si comunica il link di accesso
- Chiedere ai partecipanti di **accedere con account Zoom**
- **Attivare la Sala d'attesa**
- **Impostare se possibile un co-host** che partecipi al controllo del meeting
- **Disabilitare** la possibilità per i partecipanti di condividere lo schermo
- **Disabilitare** la possibilità per i partecipanti di riattivare il proprio audio
- **Disabilitare** il Controllo Remoto
- **Disabilitare** il Trasferimento file cioè la possibilità di condividere file nella chat
- **Impedire** ai partecipanti di rinominarsi
- **Impedire** l'accesso prima dell'host
- **Disabilitare** la possibilità di riconnettersi ai partecipanti rimossi
- **Spegnere il microfono** dei partecipanti all'entrata
- Tenere in primo piano la barra degli strumenti di controllo delle riunioni in modo da agire rapidamente in caso di intrusioni

Indicazioni nel caso di attacco in corso

Nel caso in cui non si sia comunque riusciti a evitare lo ZoomBombing durante un proprio evento è necessario chiudere prontamente la riunione in atto e riorganizzarla avendo cura di condividere il link soltanto con i presenti interessati.
Segnalare inoltre tempestivamente il caso all'indirizzo dei Servizi Informatici **supporto.collaboration@unimore.it** condividendo, se possibile, la registrazione dell'evento al fine della valutazione di quanto accaduto e l'avvio di eventuali azioni legali.

Per approfondire

Sezione ONLINE www.unimore.it/online

Teams: https://support.microsoft.com/it-it/topic/configurare-i-ruoli-e-la-sicurezza-della-riunione-82a4fce1-1a07-4ded-80f1-3a380702364e

Meet: https://support.google.com/meet/answer/9852160?hl=it#zippy=%2Cmisure-di-sicurezza

Zoom: https://support.zoom.us/hc/it-it/articles/360041848151-Opzioni-di-sicurezza-nelle-riunioni?mobile_site=false

Esempio informativa tipo

INFORMATIVA EX ART. 13 ss. GDPR

I dati raccolti saranno finalizzati alla partecipazione all'**Evento** ……. organizzato con la collaborazione di …… e saranno conservati per un tempo non superiore alla finalizzazione delle attività organizzative connesse all'Evento (prima fra tutte l'attestazione di partecipazione). Ai fini dell'iscrizione all'Evento saranno trattati i Suoi dati personali identificativi e dati di contatto (nome, cognome, mail). Potrà essere trattata la Sua voce e immagine soltanto nel caso in cui, durante gli eventi (se possibile), chieda di intervenire mediante le apposite modalità messe a disposizione dall'Organizzatore. La **base giuridica** del trattamento – che ha natura essenziale per adempiere alle Sue richieste – è rinvenibile nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento [**art. 6 par. 1 lett. *e)* GDPR**], ed in particolare nella realizzazione delle finalità istituzionali identificabili nella c.d. "*terza missione*" universitaria. I dati potranno essere trattati sia in modalità cartacea che digitale. Potranno accedere ai dati personali da Lei forniti solo il p.t.a., dipendenti, collaboratori e docenti UniMoRe, tutti opportunamente formati ed istruiti. I dati saranno trattati solo da persone incaricate del trattamento dei dati, non saranno comunicati a terzi (ad eccezione di ……) e non saranno diffusi. Alle condizioni previste dal GDPR, Lei potrà esercitare i diritti di accesso, rettifica,

cancellazione, limitazione del trattamento, portabilità dei dati, opposizione al trattamento e di non essere sottoposto a processo decisionale automatizzato (**artt. 15-23 GDPR**). Allo scopo di verificare la sussistenza delle condizioni e le modalità per l'esercizio di tali diritti, si rimanda al testo integrale del GDPR, disponibile sul sito: www.garanteprivacy.it. La informiamo che, qualora ritenesse violati i diritti di cui sopra, la vigente normativa le consente di presentare reclamo presso l'Autorità GPDP nazionale. I predetti diritti potranno essere esercitati contattando: il Titolare del trattamento, l'Università di Modena e Reggio Emilia (**UniMoRe**) e per essa il Dip. di …… con sede a ……, via ……, reperibile all'indirizzo ……; Il responsabile della protezione dei dati (**DPO o RPD**) designato è reperibile all'indirizzo dpo@unimore.it.

☐ Ho preso visione della presente informativa

(*non sarà necessario raccogliere l'ulteriore tic / spunta su "Acconsento al trattamento dei dati personali"*)