Consells per organitzar actes virtuals segurs amb Zoom

Diputació Barcelona

Índex

Zoom

Zoom és la plataforma que usem a la Diputació de Barcelona per fer actes exclusivament en format digital. Les sales de la plataforma que gestionem a la Unitat de Comunicació Digital Corporativa tenen capacitat per acollir esdeveniments virtuals de fins a 300 participants.

Els assistents a aquestes sessions hi accedeixen a través d'un enllaç que se'ls ha facilitat en la convocatòria o en la invitació a la trobada o a l'acte. Un cop accedeixen a Zoom, habitualment han de passar per la sala d'espera, des d'on l'amfitrió de la sessió (*host*) els permet l'accés a la sala.

De vegades, alguns d'aquests actes virtuals poden patir *zoombombing* (assalts o boicots per part d'elements externs o desconeguts).

Amb el *zoombombing* els assistents no convidats es colen a la nostra sala de Zoom i boicotegen la sessió compartint les seves pantalles i fent sons estranys, amb un contingut ofensiu, brut o pertorbador. Aquests atacs fan palès un cop més que la seguretat completa no existeix, però que, no obstant això, cal prendre mesures per minimitzar els riscos i les vulnerabilitats dels nostres actes virtuals.

Habitualment, el *zoombombing* més comú que ens trobem a la corporació és el que ha atacat actes de contingut que podria considerar-se polèmic o d'actualitat política, de continguts dels àmbits de la igualtat, trobades internacionals, etc., per bé que cap àrea ni acte pot estar exempt d'endur-se un ensurt d'aquesta mena.

Com podem evitar els riscos del *zoombombing*?

1. NO FEU PÚBLIC EL VOSTRE ENLLAÇ DE ZOOM

Limiteu l'accés a l'enllaç de la sessió de Zoom i comuniqueu-lo amb la menor antelació possible. Si l'enllaç s'ha publicat en un web, a les xarxes socials o a qualsevol altre lloc públic, els boicotejadors poden trobar-lo fàcilment amb eines i bots programats amb aquesta intenció. Cerqueu altres maneres per donar a conèixer la manera d'accedir al vostre acte virtual (mitjançant una tramesa privada o anunciant que el trobaran en un web concret de www.diba.cat el dia de l'acte amb un registre previ obligatori, etc.).

2. CONTROLEU EL DESENVOLUPAMENT DE L'ACTE PER LIMITAR ELS PERMISOS

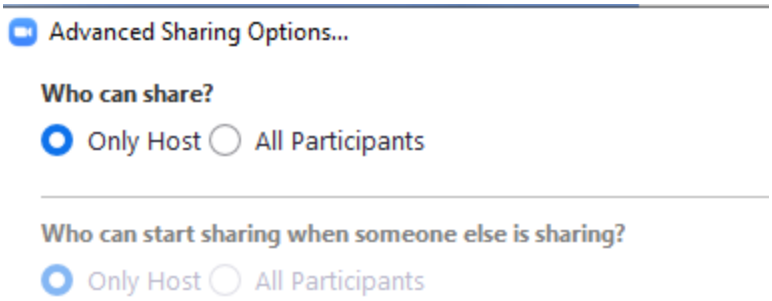
Abans d'un acte cal valorar bé les restriccions que aplicarem en funció de com s'hagi de desenvolupar. Tingueu en compte els punts següents, que cal decidir abans de cada esdeveniment:

Habilitar el xat: Si el xat està habilitat, qualsevol usuari hi podrà escriure el que vulgui. És el risc menor, ja que el xat només permet inserir-hi text i no imatges (també permet documents), però cal anar amb compte que cap trol no ens faci anar a un enllaç maligne. És important moderar la sessió i esborrar alguns comentaris si escau, però sense arribar a censurar en excés. Si s'escapa algun comentari una mica despectiu, tampoc no passa res. Pensem que el conferenciant sempre pot fer alguna broma sobre el tema i treure-li importància. És una estratègia molt aconsellable per no perdre el control sobre les intervencions i, alhora, mantenir l'espontaneïtat que funciona tan bé en aquesta mena d'actes.

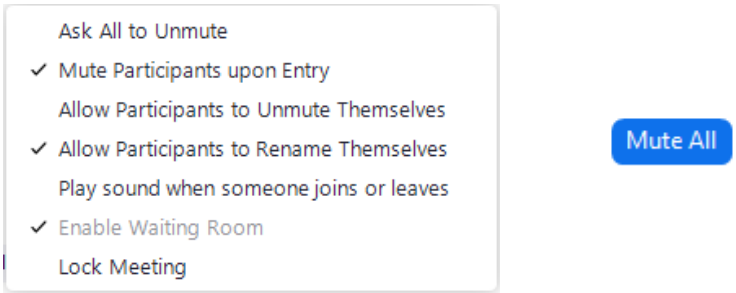
Permisos d'amfitrió: Cal limitar al màxim qui té permisos de coamfitrió (*cohost*). L'amfitrió té poders per poder admetre i expulsar usuaris de la sala, tancar el micròfon o decidir si vol deixar un usuari fixat. Idealment, només haurien de tenir aquest permís les persones que gestionen la sala i les que han d'intervenir a la

sessió. En alguns casos, aquests boicotejadors han arribat a entrar amb el mateix nom d'usuari que alguna de les persones de l'organització (perquè el coneixen prèviament o perquè, un cop dins, han vist qui gestiona la sala i aprofiten per demanar o obtenir el coamfitrió fraudulentament, fet que els fa tenir més permisos i, per tant, possibilitats de *zoombombing*).

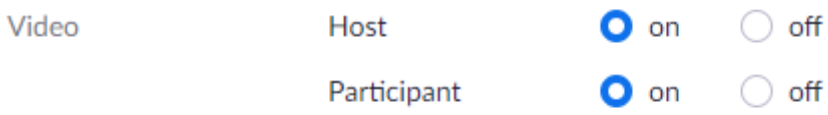
Restringir la compartició de la pantalla: Cal habilitar que només els amfitrions puguin compartir la pantalla. Així evitem que qualsevol altre usuari ens pugui donar un ensurt de *zoombombing* compartint continguts que no tinguin res a veure amb el tema de l'acte.



Tancar els micròfons: L'opció «Bloquejar micròfons» evita que cap usuari que no sigui l'amfitrió pugui intervenir durant la sessió. En cas que es vulgui autoritzar algun usuari a parlar, se li pot donar permís amb l'opció «Allow Participants to Unmute Themselves».



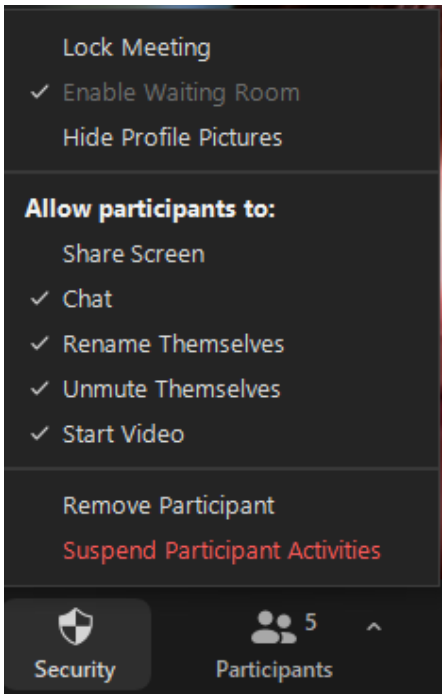
Desactivar el vídeo dels assistents: Potser no és necessari que els assistents, que només han de seguir la sessió, tinguin la càmera engegada. En aquest cas, a la configuració, podeu activar l'opció que només els amfitrions puguin activar el vídeo.

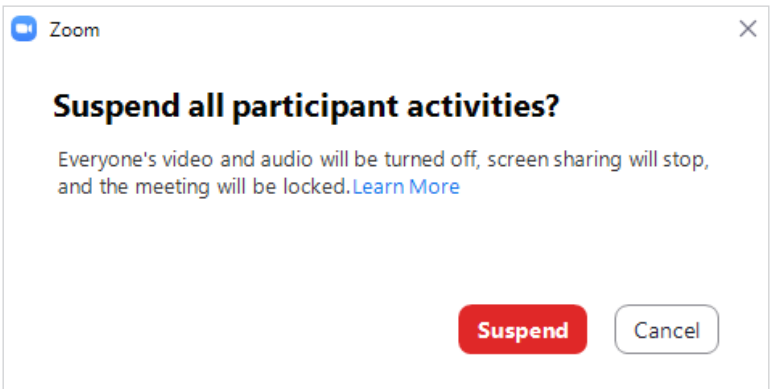


3. QUÈ PODEU FER EN UNA SITUACIÓ DE *ZOOMBOMBING*?

Si malgrat aquestes mesures preventives ens trobem que el nostre acte rep un atac de *zoombombing*, sobretot l'amfitrió i el coamfitrió han d'actuar de la manera següent:

1. Suspendre l'activitat de tots els usuaris. D'aquesta manera, amb un clic tots els usuaris de la sessió deixen de tenir permisos per a tot: no poden compartir pantalla ni xatejar ni activar el micròfon ni la càmera.
Per activar aquesta opció, cal prémer el botó inferior «Security» i escollir «Suspend Participant Activities». Seguidament, apareix una pantalla per confirmar l'acció.





2. Expulsar un usuari o diversos usuaris (normalment en són diversos) que estan boicotejant la sessió, en cas que els hàgim pogut detectar. Si no els detectem, cal seguir la sessió només amb la presentació i el permís de la persona que hi hagi d'intervenir. També podem assegurar-nos que no puguin tornar a unir-s'hi desactivant l'opció «Permetre als participants eliminats tornar a unir-se» a la pestanya «Configuració: Reunions - Bàsic».

3. Explicar als usuaris que un trol ha fet un atac, però que no s'han de preocupar per la seguretat dels seus equips, i que la sessió continua tot i que amb restriccions de participació per evitar que es torni a repetir.

4. Procurar continuar la sessió amb normalitat i les màximes mesures preventives: només qui hi hagi d'intervenir ha de tenir permisos de coamfitrió que li permetin obrir el micròfon i compartir la pantalla. La resta d'usuaris poden veure la sessió però no poden interactuar-hi.

MESURES PREVENTIVES EXTREMES

Si cal extremar al màxim les mesures preventives, Zoom permet tres opcions que dificulten l'accés a la sessió. D'entrada, no recomanem usar-les en els actes on volem, preveiem o desitgem una assistència massiva i diversa d'usuaris, perquè, si les activem, els podria dissuadir d'accedir-hi o podrien trobar-se que no poden accedir-hi. Tot i així, les exposem a continuació:

Demanar un registre previ: Un primer filtre seria demanar un registre previ als usuaris. Només qui s'hi ha registrat (per tant, ha donat una adreça de correu vàlida) podrà accedir a la sessió.

Posar una contrasenya: En aquest cas, Zoom requerirà un codi d'accés per accedir a la sessió. Si no s'introdueix aquest codi, no s'hi podrà accedir. El codi el pot fixar i personalitzar l'organitzador de l'acte i no compromet cap clau personal dels usuaris.

Bloquejar la sessió: Un cop la sessió s'ha iniciat i tots els participants ja són dins, es pot escollir l'opció de bloquejar la sessió («Lock meeting»). Ara bé, si s'activa aquesta opció, cap més usuari podrà accedir-hi.

Per adoptar les mesures més convenients en cada sessió, és clau pactar prèviament amb la persona de suport de la Unitat de Comunicació Digital Corporativa quin serà el desenvolupament de l'acte, per donar permisos només a qui sigui estrictament necessari, i saber qui agafarà les regnes en cas de patir algun atac.

RESUM D'ACTUACIÓ EN SITUACIÓ DE MÀXIMA PREVENCIÓ

Amfitrió: Només dues persones amb el nom d'usuari «Diputació Barcelona» i les tasques següents:

Amfitrió 1: Vigilar els accessos i permisos de cada usuari (i donar permís puntual a l'usuari que hagi de compartir pantalla, si escau).

Amfitrió 2: Coordinar la realització de pantalla.

Xat: Completament tancat.

Micròfons: Tancats.

Compartició de pantalla: Només l'amfitrió.