Comment sécuriser vos évènements et formations en ligne sur la plateforme Zoom ?

Introduction :

Le confinement a amené les associations à adapter leurs activités et à développer plus d'évènements à distance. En articulation avec ses travaux développés sur les cyberviolences à caractère sexiste, le Centre Hubertine Auclert recense ici différents conseils afin d'éviter tout risque d'intrusion ou de piratage d'évènements.

Zoom est une plateforme permettant l'organisation de réunions en visio-conférence et proposant différentes offres.

- Une offre gratuite, qui limite les discussions à partir de trois participant·es à 40 minutes,
- Une série d'offres payantes, donnant accès à des options supplémentaires (sondages, sous-groupes,…) et permettant d'accueillir des groupes plus ou moins importants (le premier tarif permet d'accueillir de 3 à 99 personnes sur un temps illimité),

La plupart des options de sécurisation sont disponibles dans les versions gratuites et payantes

Pour sécuriser vos évènements, trois niveaux peuvent être à prendre en compte :

1. Des réflexes que vous pouvez mettre en place à votre niveau.
2. Les options Zoom qui existent dès la première option payante, pour sécuriser vos évènements.
3. La modération pendant l'évènement

1. Les réflexes à avoir

Au-delà des options de sécurité mises à disposition par l'outil Zoom, il nous apparait nécessaire de lister une série de réflexes à avoir, complémentaires de ces outils, pour éviter toute intrusion et sécuriser au maximum son évènement.

En amont de l'évènement :

- ✓ Mettre en place un système d'inscription à l'évènement (formulaire en ligne), collectant les informations de base (nom, prénom, organisation représentée), afin de pouvoir faire un premier contrôle et, éventuellement, prendre contact avec des inscrit·es qui pourraient vous poser question,
- ✓ Ne jamais communiquer publiquement l'identifiant et le mot de passe de la réunion ; ces informations doivent être exclusivement envoyées aux personnes inscrites à l'évènement et le plus tard possible, pour minimiser tout risque de fuite,

Pendant l'évènement :

- ✓ Avoir une ou deux personnes en charge de la gestion technique et de la sécurité de l'évènement et les visibiliser auprès des participant·es, dans le cas où certain·es seraient visé·es individuellement, afin qu'ils et ellent puissent intervenir à distance,
- ✓ Prévoir une personne en permanence à l'interaction avec les participant·es, dans la salle d'attente et pendant l'évènement, afin notamment que chacun·e se renomme,

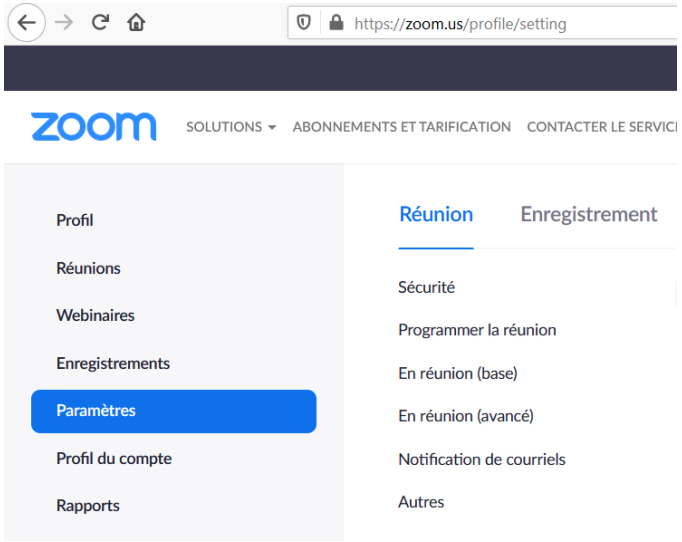
Attention ! Il est important de noter que certain·es participant·es n'ont pas l'habitude d'utiliser ce type d'outils. Il leur sera peut-être difficile d'interagir avec vous via le tchat. Il en est de même pour les personnes rejoignant les évènements à partir de leur smartphone, pour qui le tchat n'apparaît pas automatiquement, l'écran étant plus réduit que celui d'un ordinateur.

2. Les options Zoom

En vous connectant à votre compte en ligne, vous avez accès, à votre profil et aux différents paramètres pour programmer une réunion, mais aussi pour enclencher les options de sécurité proposées par l'outil.

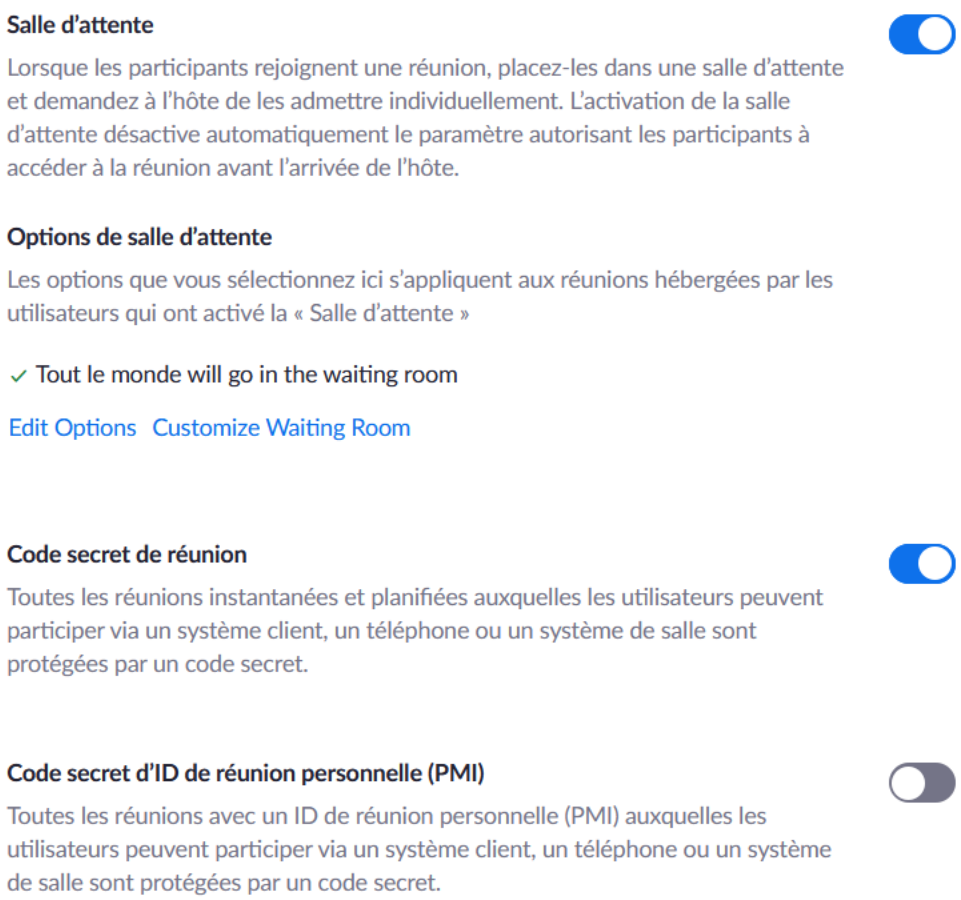
Pour y arriver :

Mon compte > Paramètres > Sécurité



Il arrive que les options soient déjà cochées ou non, il est important de s'en assurer pour sécuriser au maximum son évènement.

Les options sont cochées lorsqu'elles apparaissent en bleu et décochées lorsqu'elles apparaissent en gris.

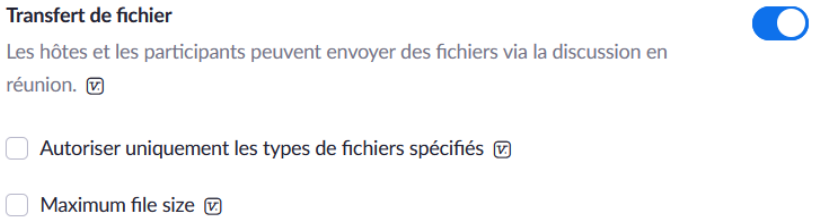


Salle d'attente : Cette option évite que toute personne qui se connecte à votre évènement n'arrive directement dans la salle virtuelle. Une salle d'attente apparaît dans l'onglet *Participants* de l'administrateur ou administratrice de l'évènement. Un aperçu est alors possible des personnes en attente et donc d'admettre progressivement les participant·es afin d'éviter l'entrée de personnes non inscrites. Il est également possible de communiquer avec les personnes en attente et de leur passer des messages (exemple : « *merci de vous renommer et d'indiquer la structure que vous représentez afin que nous vous admettions dans la salle* »). Cette modération à l'entrée est plus difficile pour des évènements réunissant un grand nombre de personnes. En cliquant sur **Options de la salle d'attente**, vous pouvez décider si tout le monde doit y passer ou si certain·es peuvent entrer directement. Il est recommandé de décider que tout le monde y attende et que, si certain·es doivent entrer avant les autres (les intervenant·es pour un test…), vous les admettiez un·e par un·e.

Code secret de réunion : Cette option doit être cochée, elle impose ainsi à vos participant·es de renseigner un code secret que vous leur enverrez. Deux possibilités existent, lors de la création de votre évènement (voir ci-dessous), donner un identifiant aléatoire (option plus sécurisée) ou proposer aux participant·es de se

connecter avec votre **PMI**, l'identifiant personnel de votre compte. Dans ce cas, le code est le même à chaque fois qu'une personne extérieure souhaite se connecter à un évènement que vous organisez à partir de votre compte. C'est donc moins sécurisé.

Transfert de fichier : Dans les paramètres, vous pouvez décider si vous ouvrez cette fonction aux participant·es et pour quel type de fichiers. Attention, hôtes et participant·es sont considérés pour cette option de la même manière, si vous ne la sélectionnez pas, ni vous, ni eux ne pourront en envoyer.



Lorsque vous ouvrez l'application Zoom pour *Programmer une réunion*, la fenêtre à droite s'ouvre.

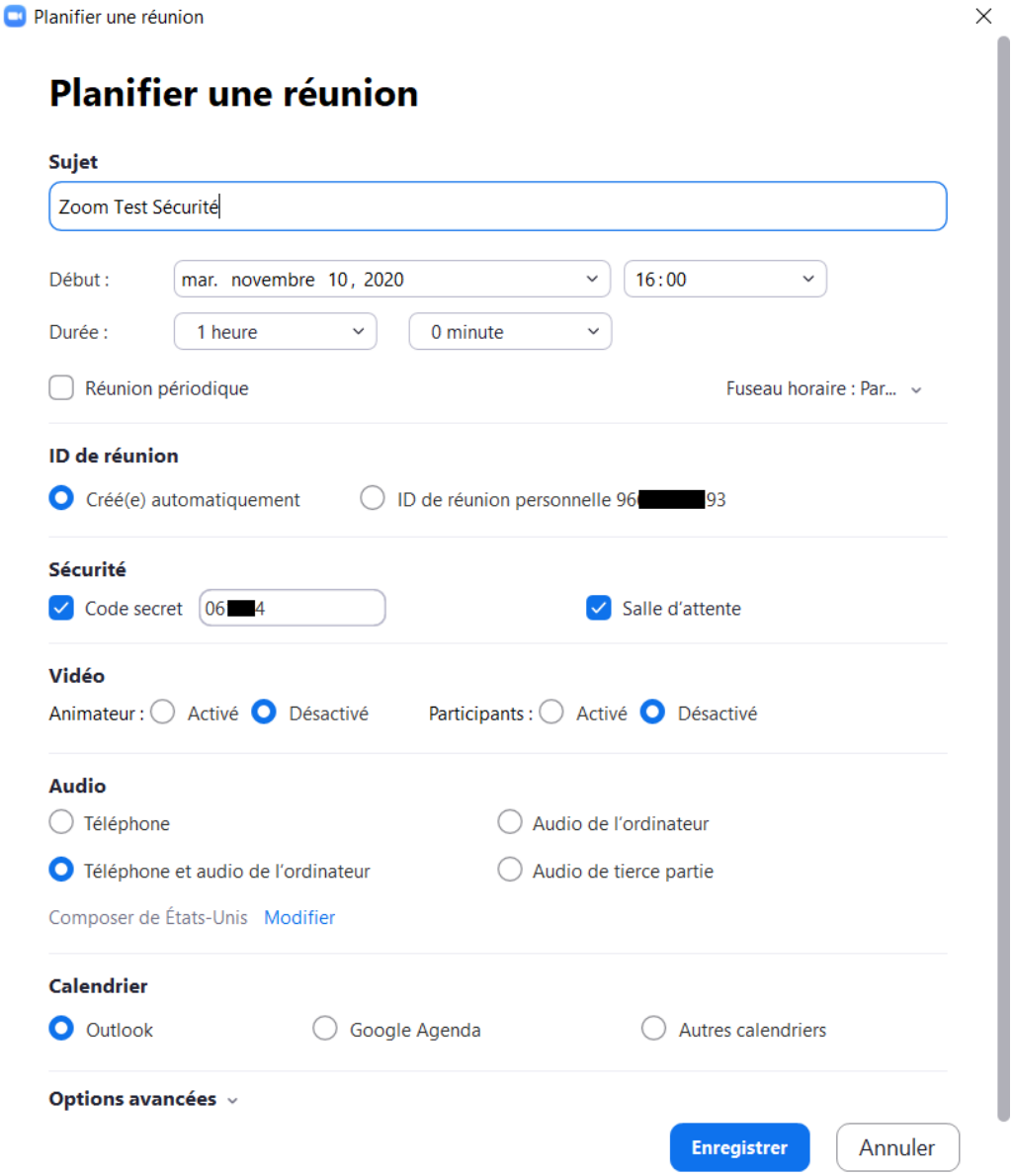
Il est indispensable, pour la sécurité de votre évènement, de vous assurer que :

- Un code de réunion est automatiquement créé (un nouveau à chaque fois, votre ID personnel est toujours le même),
- Un code secret à 6 chiffres est bien indiqué et coché,
- La case Salle d'attente est bien cochée,

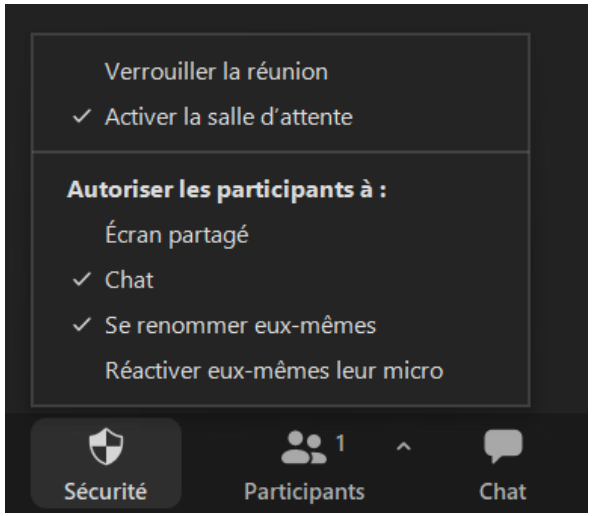
Ces options sont disponibles dans l'offre payante et dans l'offre gratuite.

Dans les *Options avancées*, vous pouvez renforcer la sécurité en cochant :

- *Coupez le son des participants à leur entrée* > cela évitera toute prise de parole intempestive
- *Seuls les participants authentifiés peuvent participer* > cela contrôle que les participant·es ont bien un compte Zoom, mais cela peut être une contrainte, l'idée étant que chacun·e peut se connecter, avec ou sans compte.



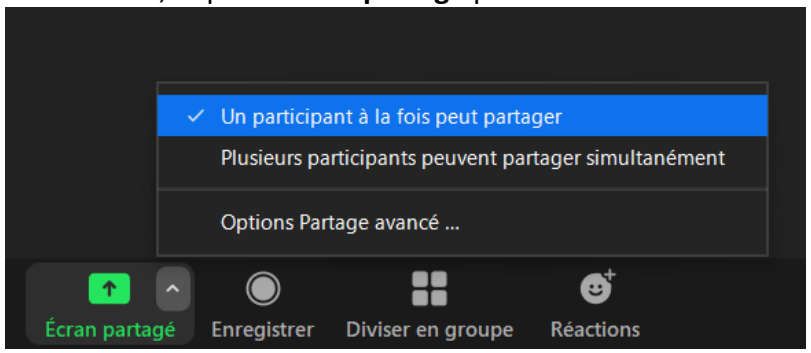
3. La modération pendant l'évènement

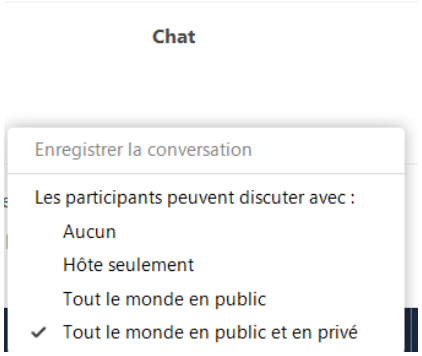


Une fois la réunion lancée, vous avez plusieurs actions ou contrôles que vous pouvez activer ou En cliquant sur le pictogramme **Sécurité** dans la barre de menu en bas de votre écran, vous avez la main sur toutes les options de sécurité que vous pouvez donc, si nécessaire faire évoluer pendant l'évènement. Nous vous conseillons de conserver les options telles qu'elles s'affichent sur l'image ci-contre.

En cas d'urgence, vous pouvez **Verrouiller la réunion**, plus personne ne pourra rentrer dans la salle.

Il est recommandé de ne pas autoriser les participants à partager leur écran, pour éviter la diffusion de contenus inappropriés. Néanmoins, l'option **Ecran partagé** peut être nécessaire dans le cas où un·e intervenant·e a une présentation PowerPoint à partager par exemple. Dans ce cas, il est nécessaire de modifier l'option soit en **Plusieurs participants peuvent partager simultanément** (avec le risque que d'autres partagent) ou via les **Options Partage avancé** > Un participant à la fois peut partager > Qui peut partager ? > Tous les participants.





Quel que soit le choix fait, il vous est possible, de suspendre le partage d'écran d'un participant·e (dans l'onglet *Participants*).

Sur le **chat**, vous pouvez avoir la main sur le type de partage que vous souhaitez privilégier pendant les échanges. Pour cela : Chat > … (Plus)

Vous avez accès à une nouvelle fenêtre (ci-dessus) vous proposant le mode de discussion dans le chat. Plus il est ouvert, plus il y a de risques. Il est possible de le modifier pendant l'évènement >> Le fermer pendant les interventions et l'ouvrir pendant les temps d'échange.