

## SÉCURISER VOS ÉVÈNEMENTS CONTRE LE « ZOOMBOMBING »

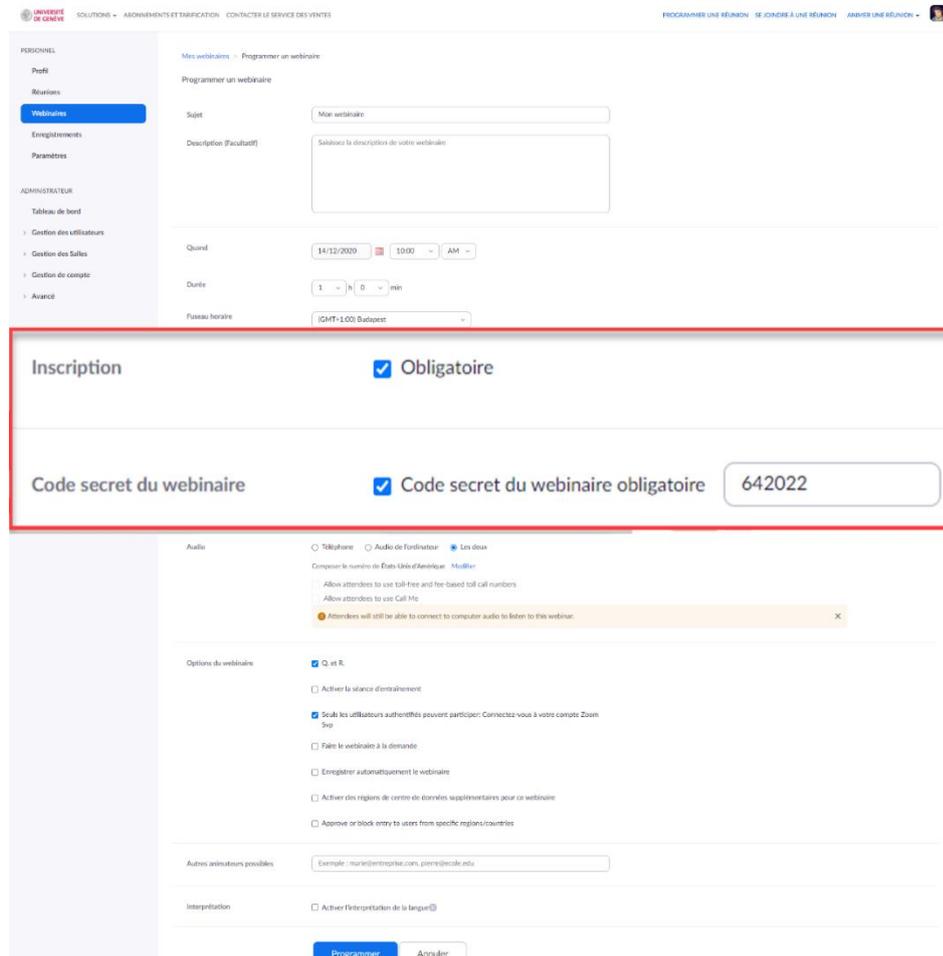


### 1. Introduction

Les événements publics, réalisables avec la fonction Webinaire de Zoom, sont des cibles de choix pour les connexions indésirables. Pour limiter les risques de ces phénomènes (aussi appelés [Zoombombing](#)), il est indispensable de vérifier les paramètres présentés dans cette fiche.

### 2. Vérifications à effectuer lorsque vous programmez le webinaire sur Zoom :

- ✓ Connectez-vous sur votre compte Zoom UNIGE et allez dans la section « Webinaire » ;
- ✓ Ne désactivez aucun des paramètres activés par défaut, ils vous garantissent le plus haut de niveau de sécurité ;
- ✓ Activez l'option **Inscription**, qui vous permettra de communiquer un formulaire d'inscription à vos participant-es sous forme de lien que vous pouvez partager dans la publication de votre événement.



The screenshot shows the Zoom webinars configuration interface. A red box highlights the 'Inscription' (Registration) section, which includes the following settings:

- Inscription** (Registration):  Obligatoire (Mandatory)
- Code secret du webinaire** (Webinar Passcode):  Code secret du webinaire obligatoire (Mandatory webinar passcode) with the value **642022** entered in the adjacent field.

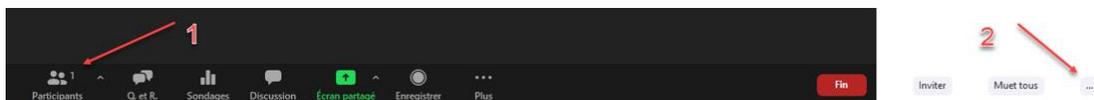
Below the highlighted section, other settings are visible, including 'Audio' (set to 'Les deux'), 'Options du webinaire' (with 'Q, et R' checked), and 'Autres utilisateurs possibles' (with an example email address).

- ✓ Une fois votre Webinaire paramétré, vous pouvez accéder au lien d'invitation afin de l'inclure dans la publication en ligne de votre évènement :

The screenshot shows the Zoom management interface for a webinar. The 'Invasions' tab is selected, displaying the webinar size (100 participants) and the registration link: [https://unige.zoom.us/webinar/register/WN\\_L7LsWB3TR\\_WX-Qf160D-qg](https://unige.zoom.us/webinar/register/WN_L7LsWB3TR_WX-Qf160D-qg). Other tabs include 'Paramètres de l'e-mail', 'Valorisation de l'image de marque', 'Sondage/Enquête', 'Q, et R.', and 'Plus'.

### 3. Options à activer/désactiver pendant votre webinaire :

- ✓ Dans la mesure du possible, **verrouillez la réunion en suivant les étapes 1, 2 et 3.** Une fois le webinaire verrouillé, il n'est plus possible d'y admettre d'autres participant-es, ce qui réduit le risque d'intrusion ;



- Demander à tout le monde la réactivation du micro
- ✓ Désactiver le son des panélistes lors de leur arrivée
- ✓ Autoriser les panélistes à réactiver leur son
- Autoriser les panélistes à se renommer
- ✓ Émettre un son lorsque quelqu'un rejoint ou quitte la réunion
- Verrouiller le webinaire ← 3
- Autoriser les panélistes à démarrer la vidéo

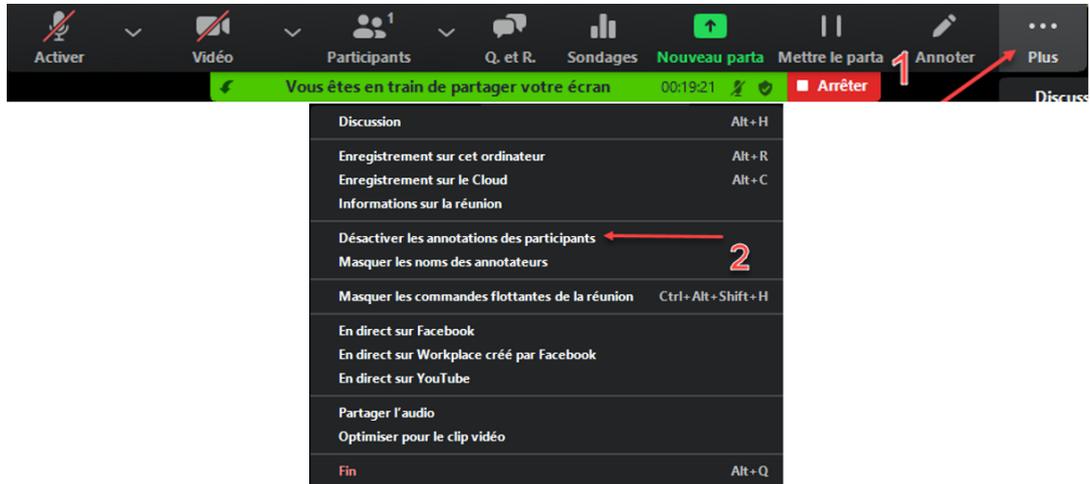
#### Autoriser les participants à :

- ✓ Lever la main
- Afficher le nombre de participants

#### Configurer la disposition de la vidéo pour les participants :

- ✓ Suivre le mode d'affichage de l'animateur
- Affichage de l'intervenant actif
- Affichage galerie

- ✓ Si vous n'avez pas prévu d'inviter vos participant-es à intervenir pendant le webinaire en annotant votre présentation, il est préférable de désactiver les annotations des participant-es ([en savoir plus sur les annotations](#)) :



- ✓ Evitez les pollutions sonores en décochant la permission aux participant-es de réactiver eux-mêmes leur micro. Cela forcera ces derniers à utiliser la fonction Main Levée pour prendre la parole.



### Remarque :

**L'ajout d'un-e co-hôte à votre événement permet de fournir un degré de modération supplémentaire et ainsi vous permettre d'agir rapidement en cas d'attaque.**