



Guide pratique de cybersécurité n°1

« J'utilise Zoom en Sécurité »

De 5 à 30 participants connus de l'organisateur

Merci à W. qui a réalisé ce guide

1. Introduction

Dans le contexte de confinement lié au Covid-19, l'application Zoom s'est retrouvée très utilisée. Elle a démontré quelques failles de sécurité. Ce document centralise les bonnes pratiques à adopter dans l'utilisation de Zoom afin de garantir un maximum de sécurité.

Si vous n'avez pas correctement paramétré Zoom, vous pouvez être confronté à ce qu'on appelle un « zoombombing », c'est-à-dire l'intrusion d'une personne malveillante dans votre réunion virtuelle au vu et au su de tous les participants. **Le paramétrage de Zoom vous permet de vous prémunir des incidents précédemment rencontrés dans le monde et récemment en France.**

Ce document s'adresse, par exemple, aux professeurs désirant enseigner auprès de leurs élèves via Zoom de manière sécurisée. Pour suivre ce guide, vous aurez besoin :

- d'un ordinateur (Windows ou Mac) disposant d'une connexion internet ;
- d'un compte Zoom (vous pouvez en créer un en vous rendant sur <https://zoom.us/signup>).

Comment les *hackers* font-ils pour se connecter sur une session Zoom ?

Afin de bien vous protéger, il est indispensable de comprendre comment les *hackers* fonctionnent pour s'infiltrer dans vos conversations. La réponse est simple : ils empruntent les mêmes accès que les personnes que vous avez invitées, par les « portes » que vous avez laissées ouvertes...

Pour la grande majorité, ce ne sont donc pas des *hackers*, mais des personnes sans compétence informatique particulière.

Nous allons voir comment paramétrer correctement vos visioconférences afin de **poser un maximum de barrières tout en permettant une utilisation simple de zoom.**

2. Sécurisation des visioconférences

Si vous êtes l'animateur de la session Zoom, **nous vous conseillons tout d'abord de l'utiliser sur un ordinateur (Windows, Mac, Linux).**

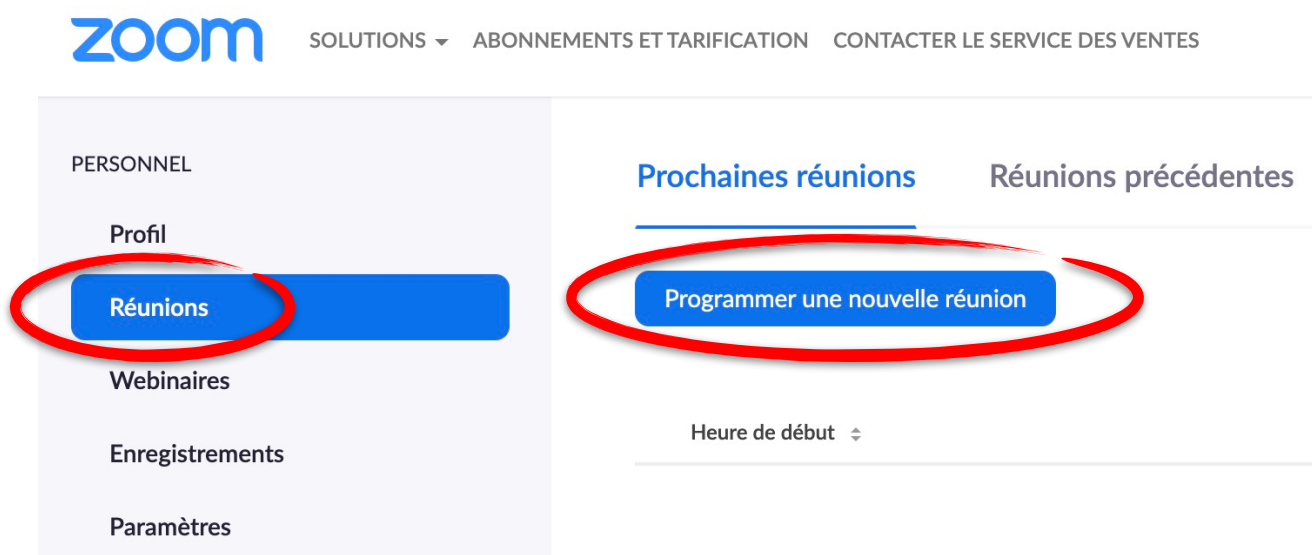
En effet, la taille des écrans des téléphones et tablettes étant plus petite, l'interface y est plus sommaire, ne vous permettant pas de voir et de gérer tous les participants en même temps. Nous parlerons donc uniquement de la version ordinateur de Zoom. Si vous n'avez pas d'autre choix que de l'utiliser sur une version mobile, les mêmes options y sont disponibles, mais sous une interface de gestion différente.

Comment créer et paramétrer une session sécurisée sur Zoom ?

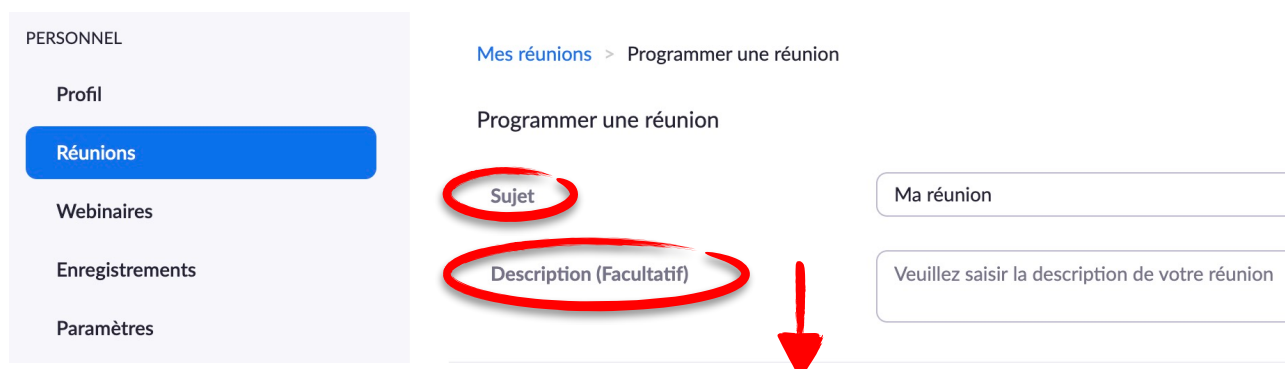
Tout d'abord, rendez-vous sur le site Zoom (<https://zoom.us>) puis sur « **SE CONNECTER** ».



Cliquez ensuite sur « **Réunions** » puis « **Programmer une nouvelle réunion** ».



C'est à partir de cette page que vous devrez paramétrer tous vos futures visioconférences. Nous allons passer en revue **les différents paramètres indispensables à activer ou désactiver**.

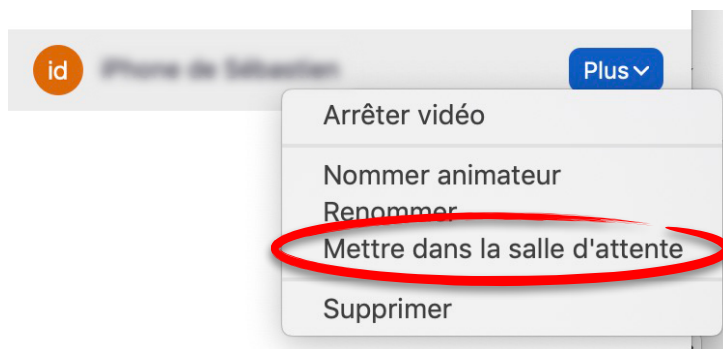


ID de réunion : Cette option vous permet de choisir si vous voulez créer une adresse différente pour chaque réunion. **Préférez l'option « Créé(e) automatiquement »**. Cependant, l'option « ID de réunion personnelle » est tout aussi sûre si elle est accompagnée des options ci-dessous.

Mot de passe de la réunion : Cette option vous donne l'opportunité de mettre un mot de passe à vos sessions. **Il est préférable d'activer cette option** même si elle seule ne vous protégera pas suffisamment (si vous partagez le lien de connexion au même endroit que le mot de passe, cela peut être une porte d'accès pour une personne mal intentionnée).

Options de la réunion :

- *Ouvrir l'accès à la réunion avant l'arrivée de l'animateur :* **option à désactiver** afin d'empêcher n'importe qui d'accéder à votre réunion avant vous. **Vous seul devez contrôler l'accès à votre visioconférence, et ce dès le début.**
- *Activer la salle d'attente :* **option à toujours activer. Ne décochez cette case sous aucun prétexte, c'est l'option la plus performante et la plus sûre pour contrôler votre visioconférence.** En effet, **lorsqu'une personne cliquera sur votre lien, elle sera dans un premier temps basculée dans une salle d'attente.** À vous de prendre ensuite la décision de l'autoriser ou non dans la visioconférence. Notez qu'il restera possible, tout au long de la visioconférence, de **basculer à nouveau un participant dans la salle d'attente.**



3. Bonnes pratiques et astuces à adopter

Avant de conclure ce document, nous allons vous parler de quelques bonnes pratiques à adopter afin de sécuriser davantage vos visioconférences.

Bonnes pratiques

- Dites aux participants de **mettre leur véritable identité** – et non un pseudonyme – afin de savoir qui vous allez accepter depuis la salle d'attente.
- Demandez-leur également d'**activer leur caméra** afin de vous assurer que la personne visible correspond bien à l'identité renseignée plus haut. Nous vous conseillons fortement que chaque élève la garde active. Si les ordinateurs de certains participants n'en sont pas équipés, rappelez-leur qu'ils disposent quasiment tous d'une tablette numérique et d'un téléphone, et donc d'une caméra.
- **Ne partagez pas les identifiants ou URL de réunion sur les réseaux sociaux.** Préférez un groupe Whatsapp, ou un autre groupe de discussion fermé.
- **Verrouillez votre réunion** : si tous vos participants sont présents à la réunion, utilisez le menu de sécurité de Zoom pour verrouiller votre réunion, empêchant ainsi toute nouvelle personne de s'y joindre.
- **Enregistrez votre réunion** : activez la fonction « Record » pour enregistrer l'ensemble de la visioconférence. Ainsi, si une intrusion malveillante se produit, l'enregistrement permettra d'avoir des éléments factuels pour une investigation et/ou des éléments de preuve pour un dépôt de plainte.
- **Signalez un compte problématique** via l'icône de sécurité présent dans la barre de menu.

Astuces

- **Soyez prudent avec le mode de présentation.** Bien que Zoom permette à plusieurs personnes de présenter un document en même temps, si vous n'avez pas besoin de cette fonctionnalité, ne l'utilisez pas. Elle est désactivée par défaut et devrait le rester.
- **Soyez prudent avec le partage d'écran.** Lorsque vous partagez un écran, choisissez de partager une fenêtre spécifique, plutôt que l'ensemble de votre écran. Cela peut éviter de partager accidentellement trop d'informations, ou d'avoir des notifications parasites qui interrompent votre réunion. De plus, lorsque vous partagez le contenu d'un navigateur, créez une nouvelle fenêtre avec seulement l'onglet ou les onglets que vous souhaitez partager.
- **Définissez une sécurité par défaut.** La plupart des conseils de sécurité partagés ici peuvent être définis comme paramètres par défaut pour toute nouvelle réunion, en allant par exemple sur zoom.us/profile/setting.

Signalez toute intrusion malveillante au SPCJ au 0 800 18 26 26.