Zoom : 4 conseils pour une utilisation sécurisée

Les plateformes de communication en ligne sont devenues essentielles pour les interactions personnelles et professionnelles avec le reste du monde. Avec près de 20 % de part de marché mondiale, Zoom est l'une des plateformes les plus populaires.

Comme pour toute technologie populaire, outre les avantages évidents, il existe également des risques. Nous avons entendu parler de l'utilisation abusive de l'application, comme l'a signalé Check Point Research au début de l'année. Des tiers pourraient écouter des réunions et des conversations privées, conduisant à des fuites de données personnelles ou de l'espionnage.

Comment pouvons-nous donc profiter des avantages de Zoom sans être vulnérables à ces menaces ? Voici quelques conseils :

1 – Restez à jour

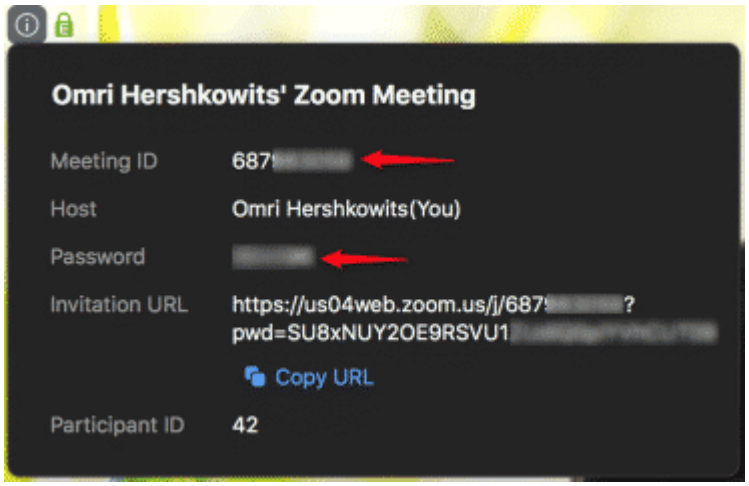
Pour que la sécurité soit efficace, le logiciel Zoom doit être mis à jour fréquemment. Les mises à jour proposées par les entreprises technologiques pour leurs produits n'ajoutent pas seulement de nouvelles options et fonctionnalités, mais corrigent également des bugs et des failles de sécurité, notamment la possibilité de découvrir et d'écouter les réunions que nous avons mentionnée plus haut.

Il est important de comprendre que, contrairement à la croyance populaire, la fenêtre d'opportunité des pirates ne se referme pas lorsqu'une faille de sécurité est corrigée, mais seulement après que les utilisateurs aient installé une mise à jour ou des correctifs pour s'en protéger. Cela signifie que les utilisateurs qui n'ont pas mis à jour le logiciel restent vulnérables.

2 – Utilisation d'un mot de passe de connexion

Notre enquête sur la sécurité des réunions Zoom a montré comment un pirate pouvait deviner les numéros aléatoires attribués aux URL des réunions Zoom et y entrer sans alerter les hôtes.
La faille de sécurité touchait les réunions pour lesquelles aucun mot de passe n'était défini. Zoom a corrigé la faille de sécurité et a adopté nos recommandations : toutes les réunions déjà programmées ont été automatiquement protégées par un mot de passe.

L'obligation de fournir un mot de passe avant d'entrer dans une réunion, en plus de l'affichage du numéro d'appel, offre une sécurité suffisante. Mais pour être pleinement protégé, il faut faire attention à la manière dont nous invitons les différents participants d'une réunion.



Outre la méthode sécurisée, qui consiste à envoyer l'identifiant de l'appelant et le mot de passe de la réunion, il existe une option moins sûre. Cette option vous permet de cliquer sur le bouton « Inviter » en bas de l'écran, puis sur « Copier l'URL » ou « Copier l'invitation » pour l'envoyer à quiconque devant participer à la réunion.

Comme ce lien ne nécessite pas de fournir un mot de passe, faites bien attention à la façon dont il est partagé, et avec qui, car **toute personne disposant du lien peut entrer dans la réunion sans avoir à fournir de numéro d'appel ou de mot de passe.** Nous vous recommandons également de vous connecter à Zoom via SSO (authentification unique) si votre entreprise intègre cette possibilité.

Une autre façon de contrôler les participants est l'option « Salle d'attente », dans laquelle le responsable de la réunion crée une « Salle d'attente » par laquelle les participants peuvent se connecter, mais seulement si le responsable de la réunion confirme les participants un par un ou en groupe. Vous pouvez utiliser cette fonctionnalité via le menu déroulant « Options avancées » lorsque vous programmez une réunion.

3 – Pendant la réunion, gérez les participants

Même si nous décidons d'utiliser l'option moins sécurisée de partage de lien, nous pouvons empêcher les participants d'afficher des contenus inappropriés en limitant l'utilisation de la caméra par les participants.

Le responsable de la réunion peut décider qui peut utiliser sa caméra et son microphone en cliquant sur « Gérer les participants ».

4 – Partez du principe que ce qui se passe dans Zoom ne reste pas dans Zoom

Zoom vous permet d'enregistrer des réunions vidéo et les exporter sous forme de fichiers vidéo dès la fin d'une réunion. C'est un outil très utile lorsque vous souhaitez informer des personnes qui ne pouvaient participer à la réunion. Le problème de sécurité associé à l'utilisation de cet outil est

presque évident : puisque les participants à la réunion peuvent exporter le fichier enregistré, celui-ci peut en fait se retrouver entre des mains malveillantes.

Pour réduire les dangers éventuels liés à l'utilisation de l'outil d'enregistrement, le responsable de la réunion peut décider qui des participants peut enregistrer la réunion, via la fenêtre de gestion des participants en cliquant sur « Autoriser l'enregistrement ».

Notez également que les participants peuvent enregistrer la réunion à l'aide d'un logiciel externe d'enregistrement de l'écran. Par conséquent, partez du principe que vous pourrez toujours être enregistré, et agissez en conséquence.

Après la réunion, si vous l'avez enregistrée, assurez-vous de ne pas télécharger l'enregistrement sur une plateforme de partage d'informations dans le Cloud ouverte à d'autres tiers.

La plateforme Zoom offre une myriade d'avantages à ceux qui doivent travailler à domicile pendant cette période. Comme pour tout outil, il est important d'être conscient des risques possibles et d'utiliser les fonctions à votre disposition pour communiquer en toute sécurité.