OnceHub Support

Microsoft Teams security best practices

Last Modified on Oct 18, 2022

At OnceHub, we designed our native Microsoft Teams integration with security at the forefront of our minds. Many of our integration features help you secure your meetings from uninvited guests.

Unique meeting IDs and links for every session

If you're used to offering a static link, break that habit fast and connect our native Microsoft Teams integration instead. It may be simpler to use the same customized meeting link to everyone meeting with you, but that opens a huge vulnerability for uninvited guests. Each session needs its own meeting created, with its own meeting ID.

There's no need to waste time signing into Microsoft Teams, creating the meeting, and sending a separate email with the conferencing information. When a customer books with you, OnceHub automatically creates a meeting in Microsoft Teams and includes all conferencing information in the booking confirmation notification and on the calendar event.

Note: Once you have a unique meeting ID, be sure only to share the conferencing information with those you want to join. Many make the mistake of including a joining link on publicly available posters or websites. This increases the risk of an insecure meeting.

Using the lobby

If you're concerned for uninvited guests, be sure to use the lobby feature in Microsoft Teams. This allows you to authorize individuals before they're able to access your meeting. Uninvited guests may have guessed your link or password, but they still won't be able to join your session without your express permission.

If you have many people joining, we recommend defining an additional co-host to watch the waiting room notifications and grant people access.

Learn more about changing Teams participant settings, including the lobby feature

Educate your team members before they go live

Be sure not to skip a dry run for each team member giving meetings. That dry run is one of the most important steps helping them maintain professionalism in their video meetings. Especially if they've not used the video conferencing app much, there's a learning curve they'll need to adjust to in order to feel comfortable leading their session.

They should have a high awareness of all their available features. Notable settings that help them control the experience include:

- Lobby features
- Chat features, including disabling private chat
- Muting participants
- Disabling video
- Managing the Whiteboard

© Copyright OnceHub 2021. All rights reserved.

- Managing screen sharing of fellow attendees
- Removing participants

If they'll be occupied with meeting content and a number of people will be present, it may be worth having another person from your organization join. The team member leading the meeting can designate this additional team member as a co-host. The co-host can control the above listed features while the original host leads the meeting.

Team members should also ensure they've downloaded the correct software version before their session and join a few minutes early, just in case they encounter technical difficulties. These can be challenging to predict, so their best bet is always to join four or five minutes early, so they can address any unexpected issues.

With a strong handle on the features available to them, they'll be able to lead the session with authority and be prepared to shut down any unanticipated security issues that come their way. For most sessions, they won't need to use this knowledge, but everyone (except the uninvited guests) will be grateful they're ready if a security breach occurs.

© Copyright OnceHub 2021. All rights reserved.