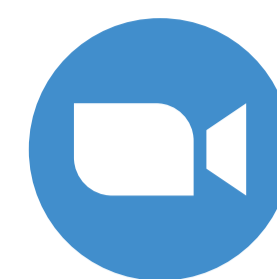



How to Avoid Video Calls Cyber Attacks



What are video calls attacks, or else called, Zoom Bombing, Microsoft Teams Bombing, etc?


The term bombing, as in "photo bombing", for example, suggests an unwanted disruption. In reference to video calls, people with bad intentions, or Internet trolls hijack the meeting and expose offensive, abusive, or uncensored content to participants.

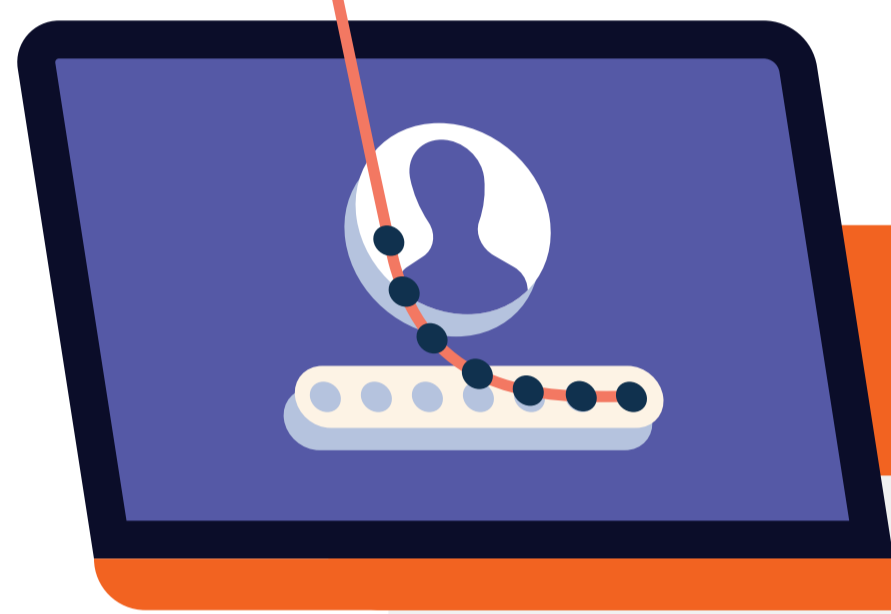
Last but not least, an uninvited attendee can act as a spy overhearing your private conversations.

It's questionable whether this kind of attack is planned by hackers or by people with no special technical knowledge or a desire to steal.

An interesting fact:
In 2020, one of the most popular virtual conferencing platforms, Zoom, surpassed 300 million daily meeting participants.



How do attackers manage to access a meeting they're not invited to?




By finding public links posted on social media

By exploring recycled video calls links

By taking advantage of default settings

Another interesting fact:
90% of people find it easier to get their point across on video.



If you follow these precautions, you might be a target to attackers but they will never succeed in compromising your meetings.

- 1 Generate a unique link every time 
- 2 Request registration with a meeting ID 
- 3 Update your video communication software regularly 
- 4 Use options like private rooms 
- 5 Lock your meetings 
- 6 Switch on and off Screen Sharing, Translation, Unmuting, Renaming, and Starting Video 

As a host of a meeting, you can also take advantage of privileges, such as:

- 1 Create Invites only meeting 
- 2 Mute participants 
- 3 Remove somebody you don't know 
- 4 Disable someone's camera 
- 5 Restrict control over presentations 
- 6 Turn off file transfer 



Last curious fact:
Businesses reduce their travel costs by 30% thanks to video calls.



And REMEMBER:
Don't share your links and IDs for video calls on social media and in general office mailboxes.