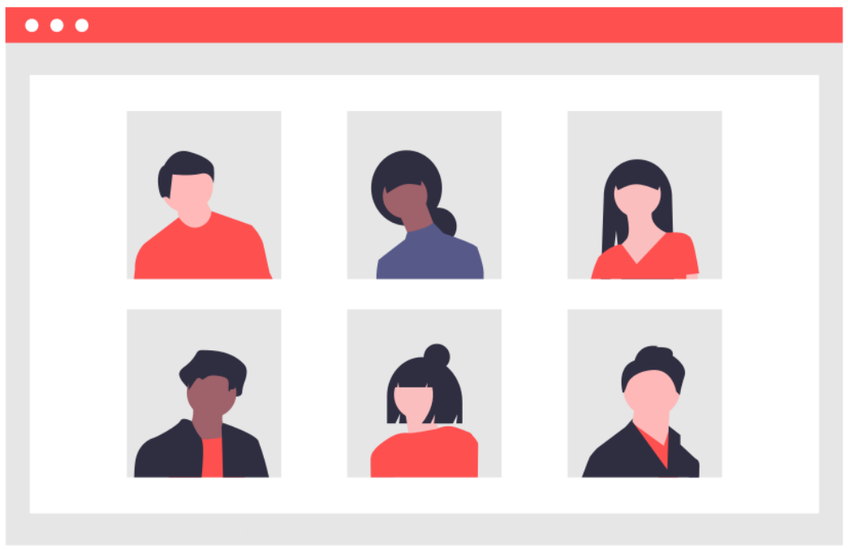
Hosting Cyber Fit Zoom Meetings



Zoom has quickly become the de facto standard for online business meetings. With the rapid rise in adoption, an equally rapid rise in attention from security researchers and privacy advocates has surfaced a range of concerns for those hosting and participating in Zoom meetings.

It's exceptionally easy for people to connect online using Zoom, a fundamental need we're all facing as we lock ourselves away at home. To make connections super easy, Zoom's default configuration goes without a number of security and privacy controls.

Learn more at our website cynch.com.au

Watch out for

Un-invited guests | Noisy participants | Bad behaviour | Privacy disclosure

THE GOOD NEWS Simple measures can help your Zoom meetings stay secure and private.

Before your meeting

- [ ] Secure your Zoom account with a strong password and Multi-factor authentication if you're using a business account.
- [ ] Check that Zoom is compatible with all your privacy obligations.
- [ ] Establish and share ground rules for the meeting ahead of time:
  - [ ] Is the meeting open to the public or will access be limited?
  - [ ] What details will need to be shared (e.g. Full name) to join the meeting?
  - [ ] Will attendees be permitted to use video / audio or screen sharing?
  - [ ] What will happen if someone behaves inappropriately?
  - [ ] How should chat be used?
  - [ ] How should someone report inappropriate behaviour or concerns?
  - [ ] How will links to sites or documents be shared with participants?
- [ ] Set a unique meeting ID for each meeting and avoid reusing the same ID.
- [ ] Don't publish the meeting details publicly.
- [ ] Be up front if and how the meeting is going to be recorded or streamed.
- [ ] Take some time to check over the meeting settings:
  - [ ] Set a password for the meeting that can't be easily guessed.
  - [ ] Enable the waiting room and admit people as they come in.
  - [ ] Set the meeting to not allow rejoining.
  - [ ] Set the meeting to require registered accounts if possible.
  - [ ] Restrict who can share their screen.
  - [ ] Restrict who can turn on video and microphone.
- [ ] Host a practice meeting to make sure you're familiar with how to control attendees:
  - [ ] Test kicking people out.
  - [ ] Test the meeting lock feature.
  - [ ] Test disabling video, audio and screen sharing.
  - [ ] Test what someone needs to do to join.
  - [ ] Test if someone can rejoin.
- [ ] Share advice with attendees on how they can stay safe and private.

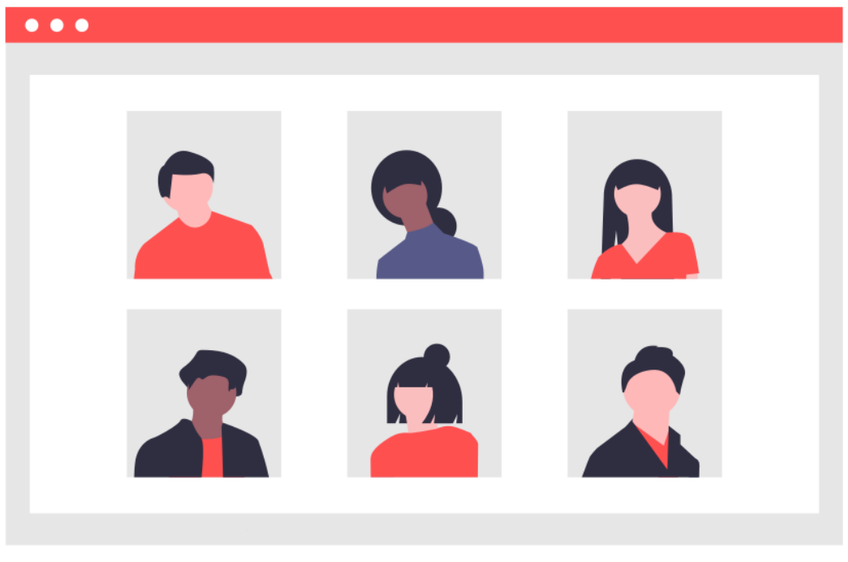
During the meeting

- [ ] Reiterate the ground rules.
- [ ] Ensure all attendees are aware of and consent to recording or streaming before you start.
- [ ] Review each person joining and deny access to anyone that shouldn't be there.
- [ ] Use the meeting lock feature once everyone has joined.
- [ ] Have someone else in the meeting monitoring chat and attendee behaviour.
- [ ] Call out anyone behaving inappropriately and kick them out following the ground rules.
- [ ] Carefully check what's visible before you share your screen.
- [ ] Take care when discussing anything personal or confidential.

Afterwards

- [ ] Download and delete any cloud recordings.
- [ ] If the meeting is recorded, review it for anything confidential before sharing.
- [ ] Review your ground rules and update them for next time if appropriate.

Staying Secure and Private in Zoom



Zoom has quickly become the de facto standard for online business meetings. With the rapid rise in adoption, an equally rapid rise in attention from security researchers and privacy advocates has surfaced a range of concerns for those hosting and participating in Zoom meetings.

It's exceptionally easy for people to connect online using Zoom, a fundamental need we're all facing as we lock ourselves away at home. To make connections super easy, Zoom's default configuration goes without a number of security and privacy controls.

Watch out for

🤫 Sensitive discussions

☠️ Dodgy software

😈 Bad behaviour

🙊 Privacy disclosure

THE GOOD NEWS Simple measures can help you stay secure and private in Zoom meetings.

Before joining meetings

- [ ] Make sure emails appearing to come from Zoom are legitimate.
- [ ] If possible join using the browser version only.
- [ ] If you need to install the software, make sure you're installing it from a trusted source: https://zoom.us/download
- [ ] Regularly check for software updates to make sure the latest security bugs are fixed.
- [ ] Familiarise yourself with any meeting ground rules.
- [ ] Find a private location for meetings if confidential information is being discussed.

During meetings

- [ ] Limit the personal information you share when entering or during a meeting.
- [ ] Take care when clicking on links or attachments shared during the meeting.
- [ ] If you're not participating in the meeting, disable your camera and microphone.
- [ ] Consider using a webcam shield or tape over your camera if you don't need it.
- [ ] Carefully check what's visible before sharing your screen.
- [ ] Be mindful that the meeting host can tell if you click away from the meeting window.
- [ ] Flag any inappropriate behaviour with the meeting host or moderator.

After meetings

- [ ] Contact the host if you have any concerns about your privacy or security.
- [ ] Uninstall Zoom software from your device if you no longer need it.