As remote working becomes part of our day-to-day lives, the use of the remote conferencing technology Zoom, has been implemented.

Conference calls by their nature are an open and not always secure environment, by virtue of the fact you are never entirely sure to whom you are speaking, particularly in larger meetings.

Security advice for all Zoom meeting participants (incl. meeting hosts)

- Discussions of a confidential or classified nature should not be conducted over these means and due care and attention should be taken when it comes to the management of remote video conferences

- It should also be borne in mind, that meeting recordings (if enabled) and chat/instant message (if enabled) logs are processed and stored in Zoom’s cloud after the meeting has ended, and as such may be subject to FOI, as per other digital communication tools such as emails

- A good rule of thumb is: "Assume what goes on a Video Conference will not always stay on a Video Conference."

- Keep the version of the Zoom client application updated at all times, on all devices. The current version is 4.6.10
  (Detail of vulnerability addressed and changes to existing features from two latest updates on screen shot included below)

- Use the Web Browser, rather than Desktop or mobile application, to access your web conferencing application or virtual meeting

Additional security advice for Zoom meeting hosts

- Do not Use Personal Meeting ID for Public Meetings
  - for public meetings, you should always schedule new meetings with randomly generated meeting IDs. That way, only invited attendees will know how to join your meeting

- Use the password function when scheduling meetings, and only share it with those scheduled to attend the meeting

- When scheduling a meeting use the "Waiting Room" function (screen shot included below).
  - As meeting attendees arrive, Zoom can notify you and provide you a list of those in the meeting, and those still in the waiting room, so you have total control of who joins your meeting.
  - Once you’ve admitted an attendee into your meeting, you can easily push them back to the Waiting Room or remove them from the meeting all together, and can even prevent their return.

- You can take meeting security even further when scheduling a meeting, you can require attendees to register with their e-mail, name, and custom questions.

- Before starting a meeting, make sure to check who exactly is on the call from the Participants menu

- Meeting hosts have a Security icon in the toolbar for quick access to essential in-meeting security controls (screen shot included below)

- Select "Lock Meeting" function once all expected guests have joined the meeting

- Manage screen sharing. Do not give control of your screen unless you know and can verify the individual you are passing control to.
  - To prevent participants from screen sharing during a call, using the host controls at the bottom, you can click the arrow next to Share Screen and then Advanced Sharing Options.
  - Under “Who can share?”, you can choose “Only Host” and close the window.

- Minimise the use of the chat function or disable entirely if not required

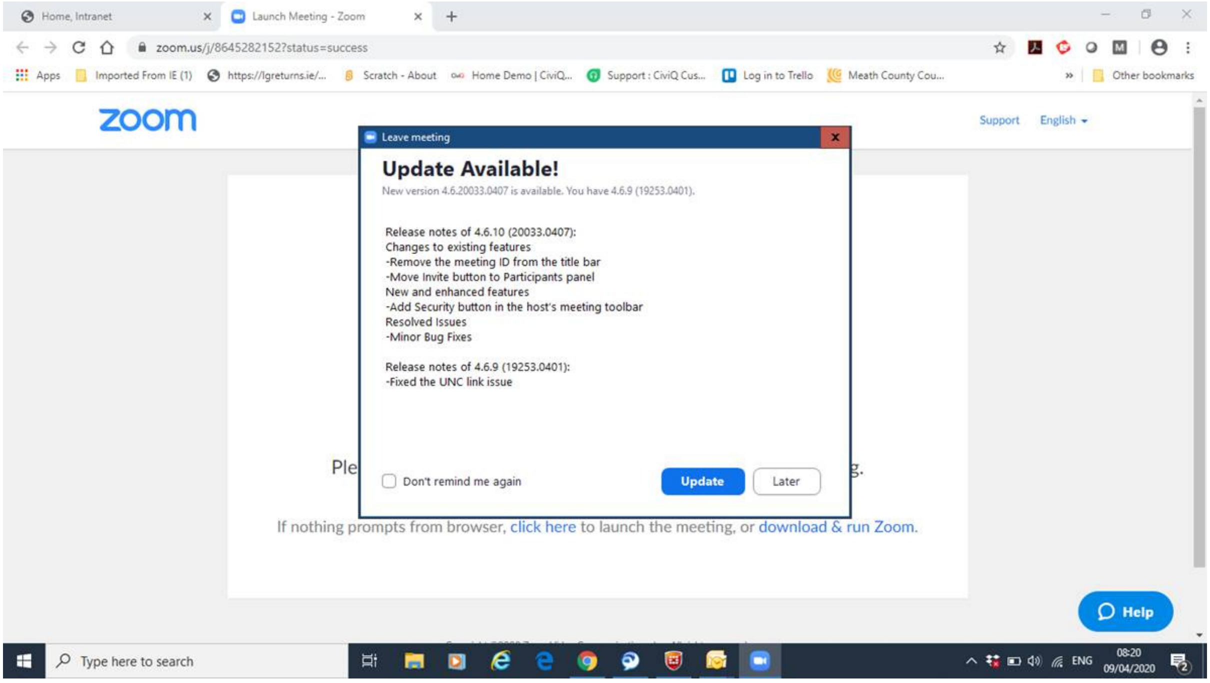
- Minimise the use of the file sharing function through the in-meeting chat, or disable entirely if not required

- Do not record meetings unless it is strictly necessary

- **Password Advice**

  - Use ‘complex’ passwords
  - Do not reuse passwords across multiple accounts
  - Do not sign-in via web-mail or other social media platforms such as using Gmail or Facebook credentials to log in – in particular do not re-use existing passwords which you may use for accessing other social media services
  - Remember the importance of secure password hygiene, not just with work accounts but also with personal accounts

Updates introduced with latest versions



Update Available!

New version 4.6.20033.0407 is available. You have 4.6.9 (19253.0401).

Release notes of 4.6.10 (20033.0407):
Changes to existing features
-Remove the meeting ID from the title bar
-Move Invite button to Participants panel
New and enhanced features
-Add Security button in the host's meeting toolbar
Resolved Issues
-Minor Bug Fixes

Release notes of 4.6.9 (19253.0401):
-Fixed the UNC link issue

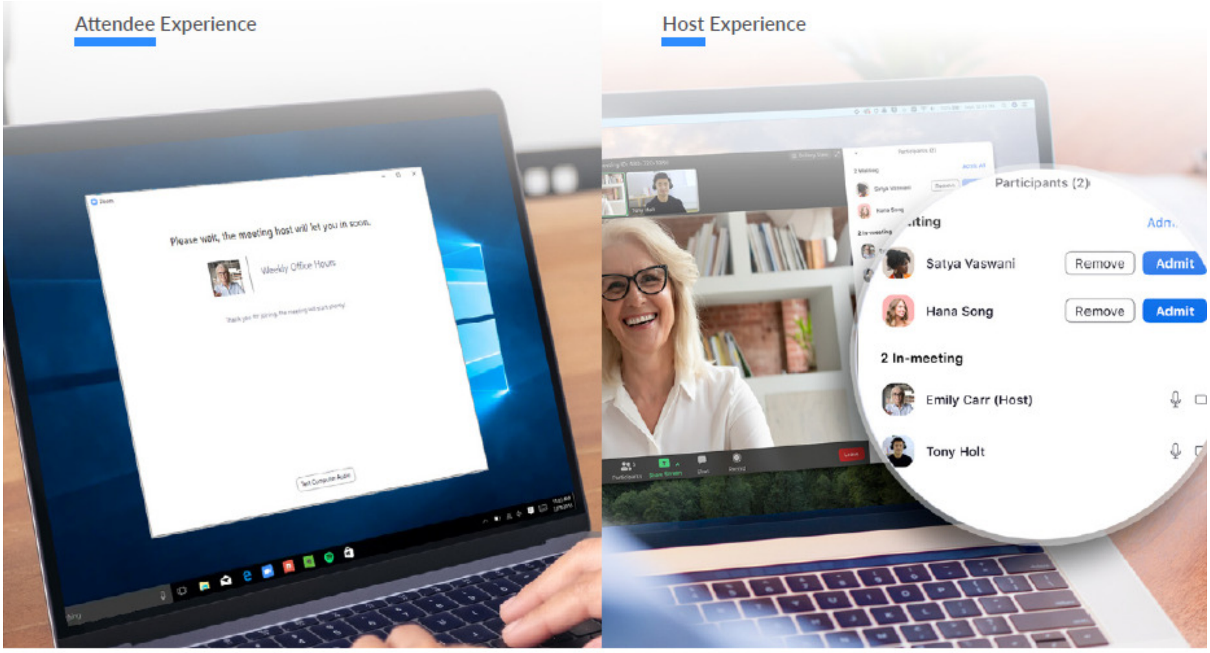
□ Don't remind me again

Update

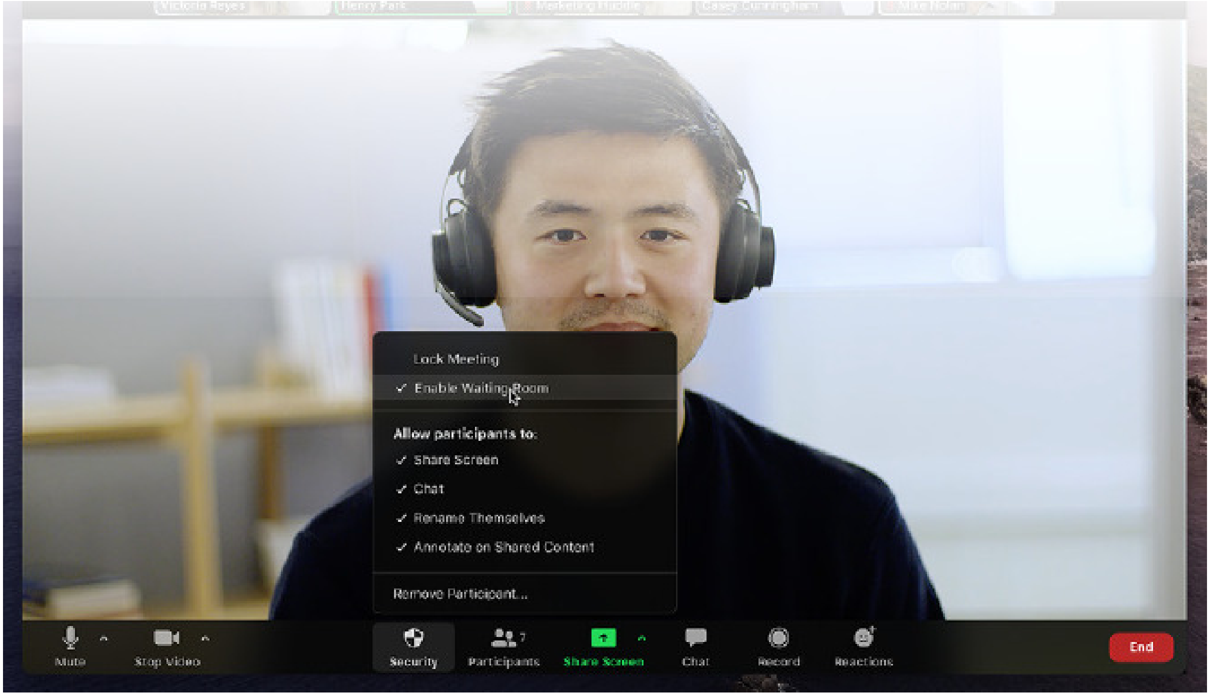
Later

If nothing prompts from browser, click here to launch the meeting, or download & run Zoom.

Waiting Room



Security icon options in the toolbar



Lock Meeting
✓ Enable Waiting Room

Allow participants to:
✓ Share Screen
✓ Chat
✓ Rename Themselves
✓ Annotate on Shared Content

Remove Participant...

Zoom Security and Privacy Documentation

- Zoom Video Communications GDPR Compliance - https://zoom.us/gdpr
- ZOOM TERMS OF SERVICE - https://zoom.us/terms
- Privacy Policy - https://zoom.us/privacy
- Zoom_GLOBAL_DPA - https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf