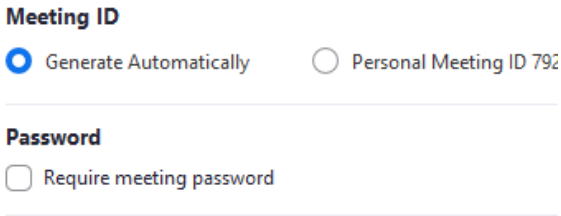
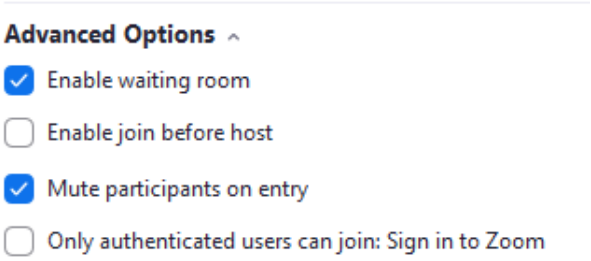
Basic Computer and Zoom Security

Staying Safe with Zoom

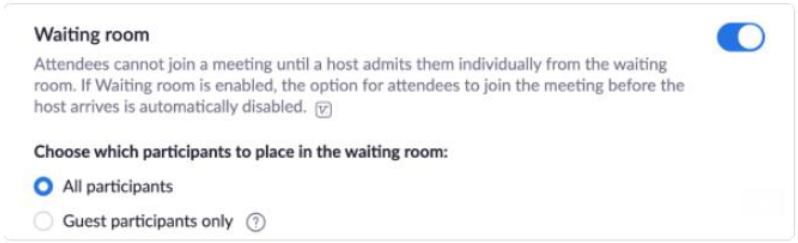
Using personal ID numbers to book meetings is useful because it is the same number every time, so once you have given out the ID number, then people joining a regular meeting don't have to look far. However, if someone other than the intended attendee gets hold of the number, they can join your meeting and potentially cause havoc. Automatically generating a new ID # each time can help to avoid unwanted guests. Passwords used for meetings can help keep your meeting private and avoid anyone randomly picking up a number and joining your meeting.



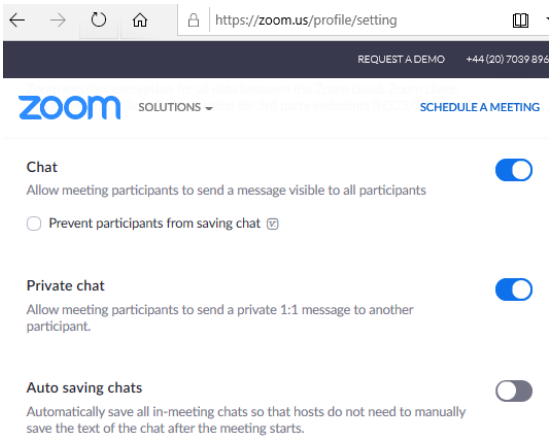
Meetings joined via a link will take the attendee into the meeting directly as the Link will include the password. Anyone joining manually, via the 'join meeting' option, entering an ID# will require to enter a password. The password is part of the invitation, or for instant meetings in the URL (meeting address https://zoom.us...), would also contain the password.



"Join before host" enables people to chat and socialise before the meeting and is useful for regular club meetings. However, setting up "waiting rooms", which should now the default status, means that before a meeting you can see who is attending before you open the meeting, in case there are some uninvited attendees. Attendees can be admitted via 'Manage Participants'.



More information on 'How to' see the Zoom tutorials or on Link manage your waiting room and Link Secure your Meeting.



It is probably a good idea to disable; "screen sharing for non-hosts", You can make your speaker a co-host, and they will be able to share their screen. Also, you should disable the "remote control" function, file transferring" and the "autosave feature" in chats. Disabling these features will restrict the ability of any uninvited attendees from doing harm and adds a level of security.

Once a meeting starts and all attendees are present, there is the ability to "lock the meeting". It is always useful to have one or two co-hosts that can help with a meeting, in case your computer or your Link stops.

How Do They Get Access

Using a random number generator and attempting to open a meeting, Once successful, the meeting can then be hacked. Prevented by passwords and the Link, including the password. (password protocols)

Personal Meeting ID and Regular meetings. Often used and word gets about. Prevented by Auto-Generated IDs

Word of mouth or publicised Meeting IDs (careless talk costs embarrassment). Prevented by Nothing.

Essential Roles of the Co-host

Allocate co-hosts as the first attendees admitted.

- If the host computer goes down the meeting should continue.
- They can admit people they know.
- Able to monitor people in the meeting and e.g.
  - Mute extraneous noise.
  - Admit latecomers

    - Lock the meeting.
    - Field questions and Highlight raised hands.
- Setting up a meeting for someone else - Allocate a co-host who knows the attendees to be admitted from the waiting room.

How To Stop Unwanted Participants.

Registration

- Approval methods
    - Automatic - Large numbers approved immediately
    - Manual - Smaller number, check on approval, have to keep checking and responding.
- Participants report generated before the meeting for checking and information.

Waiting Room allows for checking who is waiting. You can then:

- Check waiting room participants against the registration report.
- Quick and easy to admit from the waiting room. Beware admit all.
- Develop a Strategy for unknown or unrecognised attendees?
- Message and ask to leave and re-join with Attendee name = Club and Full name
- Check against DMS
- Encourage all attendees always to enter their details as Club and Full name.
- A message with contact detail, to enable closer checking., care with this one.

What to do if you get uninvited attendees

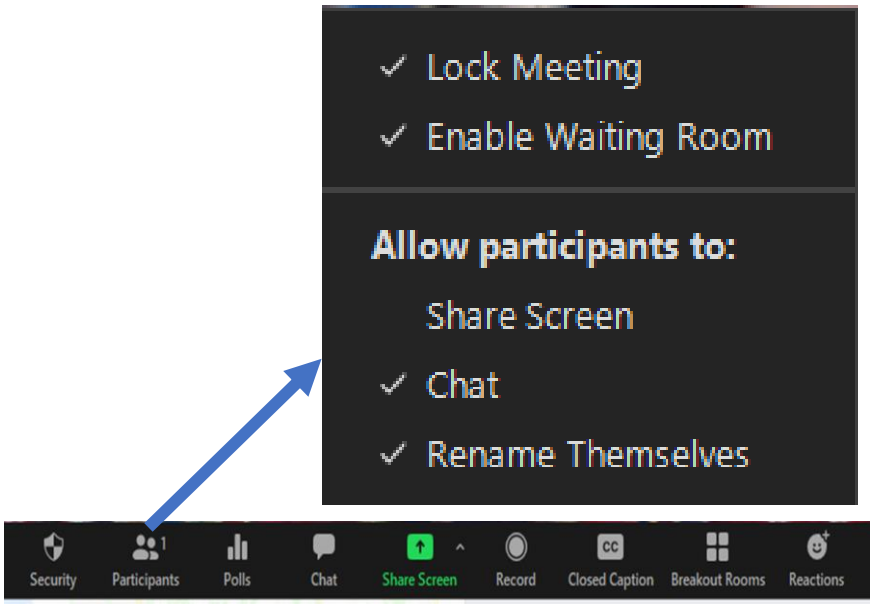
Zoom Meeting hacks are only disruptive and annoying; there is no harm to your computer, just your blood pressure.

Procedure

- Host and co-host have specific pre-determined roles should a zoom bomb occur.

- Share screen 'host-only' should already be actioned. If not change the share screen option to host-only.
- Immediately lock the meeting.
- Mute all and prevent unmuting.
- Look for a culprit(s) and remove or return to the waiting room.
  - Beware someone could be sitting there and look innocent, waiting for another opportunity.

The image shows the optimal settings for an uninterrupted meeting. Double-check the attendees the only way an unintended guest can now get in is if you let them in!

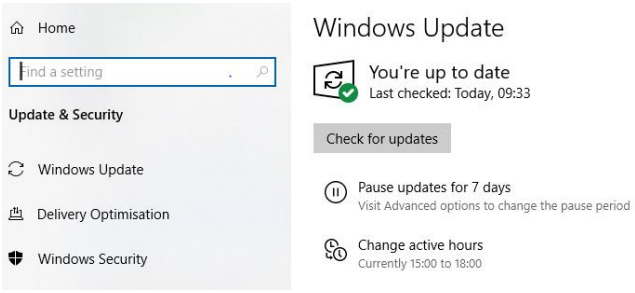


Keeping Your Computer Safe

The most important aspects of keeping your computer secure are quite simple.

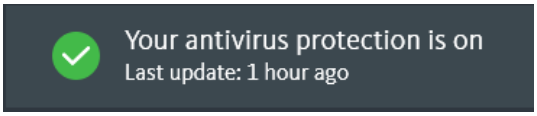
Update Your Computer Regularly

All software that we use every day, including significant players have many security issues. The main operating systems, such as Windows and iOS, provide automatic updates that solve many of the latest security issues. Updates are an essential part of keeping safe against online threats. Check that your automatic updates are enabled and now and then perform a manual update. Updates can often be found by typing "update" into your search bar.



Update your Virus Checker

While you are looking at your automatic updates, check that your virus checker is also up-to-date, turned on and functioning.



Malware

Windows Defender is free and as long as it is up to date provides excellent protection, including against Malware, which is another threat in addition to viruses

Windows Defender Firewall with Advanced Security
App

Passwords

You are familiar with passwords and the differences between strong and weak passwords; however, how many of us use the same passwords for many things? If one password gets compromised, then every login that uses the same password will also be compromised. Make it a habit of having different passwords for different applications and changing them regularly. If you keep a notebook of your passwords it is easy to keep track. Remember to keep your notebook safe. Many password "vault" programs will generate and keep your passwords can be found online. A facility often provided by your security provider as part of the package.