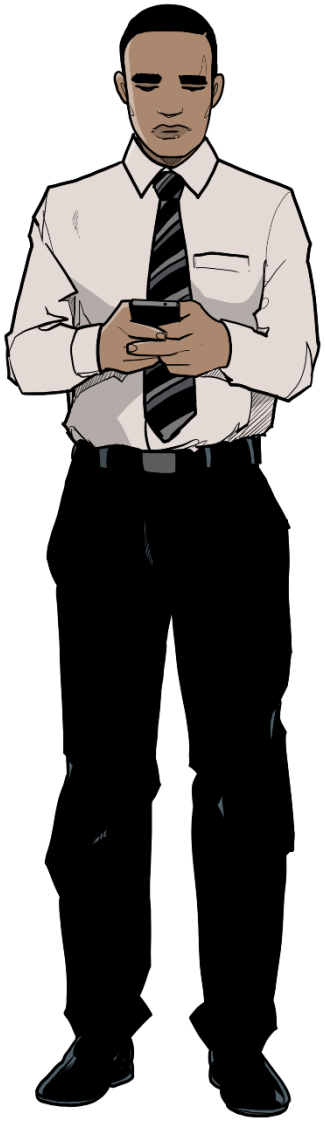
Secure Zoom

Zoom has emerged as a very popular tool for online meetings, training and other communication activities during the coronavirus pandemic of 2020, but there are risks associated with any such app…



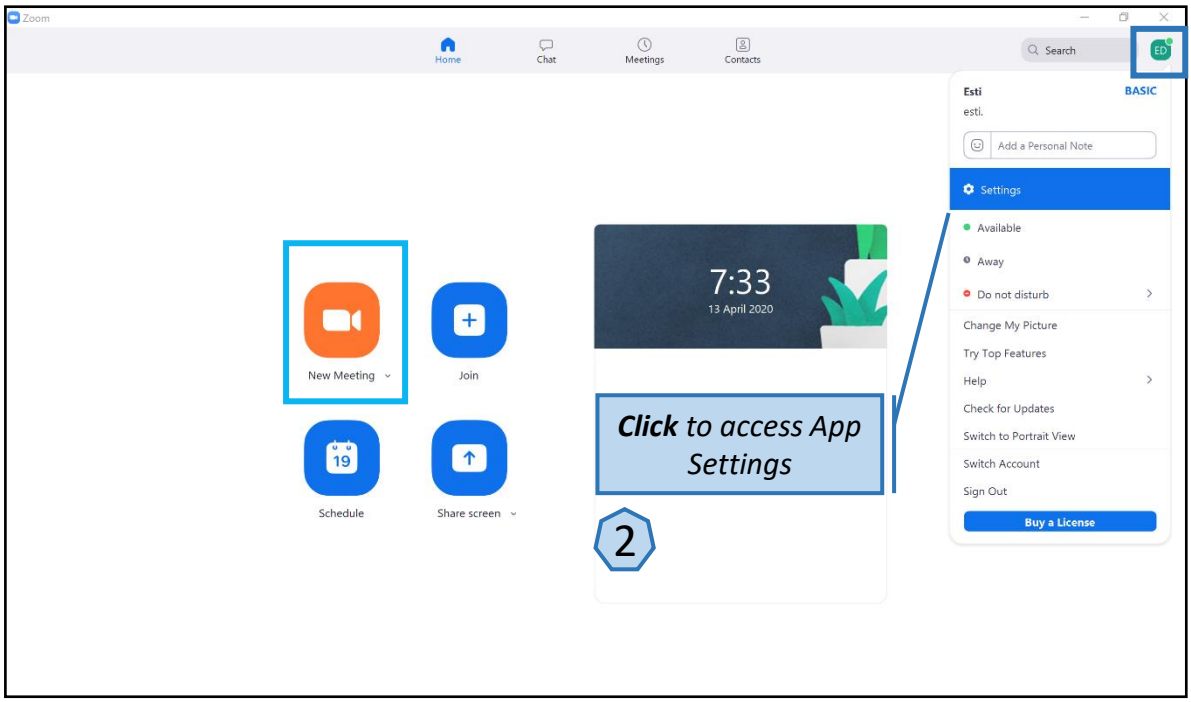
- **Phishing ploys**; messages inviting participants to click on *malicious links* to fake meetings, or uninvited guests sharing malicious links during a meeting.
- **Privacy risks**; users including *sensitive information* in their Zoom profiles, which can be viewed by meeting participants.
- **Live recording**; hosts allowing participants to *record the session*, or participants using mobile phones to record it surreptitiously.
- **'Zoom bombing'**; unauthorised participants *hijacking meetings*, often because password access was not setup or meeting passwords were shared insecurely.

This short guide outlines the main Zoom security controls and how to access them, *some in the App and others on the Zoom Webpage*…

Locating your Account Settings in the App

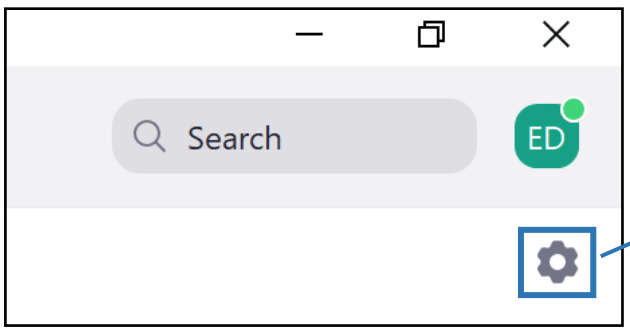
1

*First **click** on your initials here…*



***Click** to access App Settings*

2

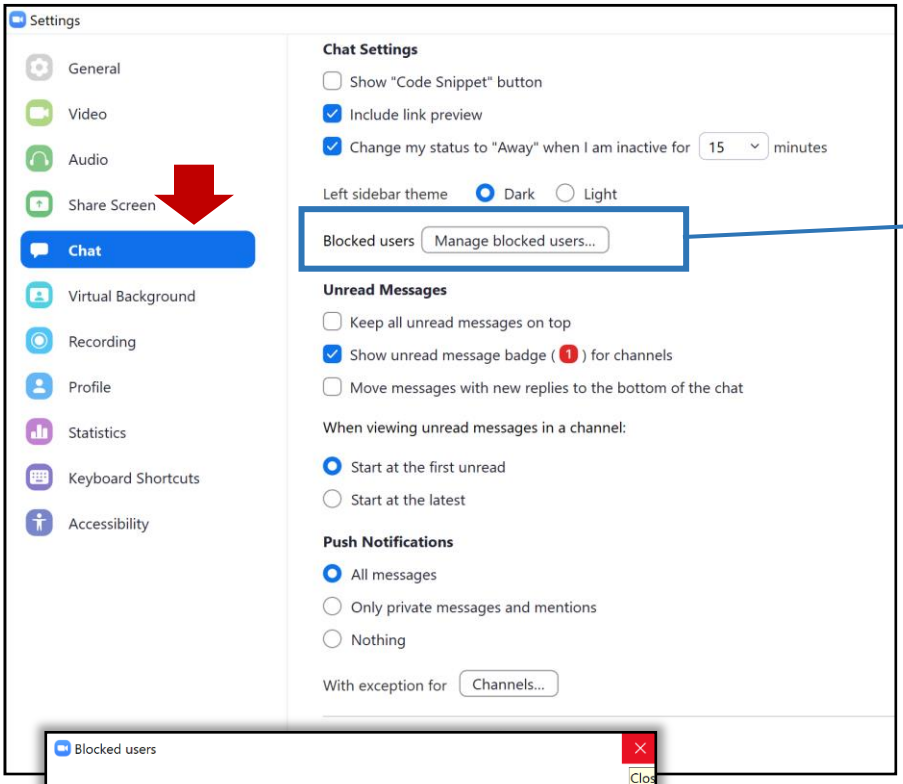


3

*You can also access **Settings** by clicking **this button***

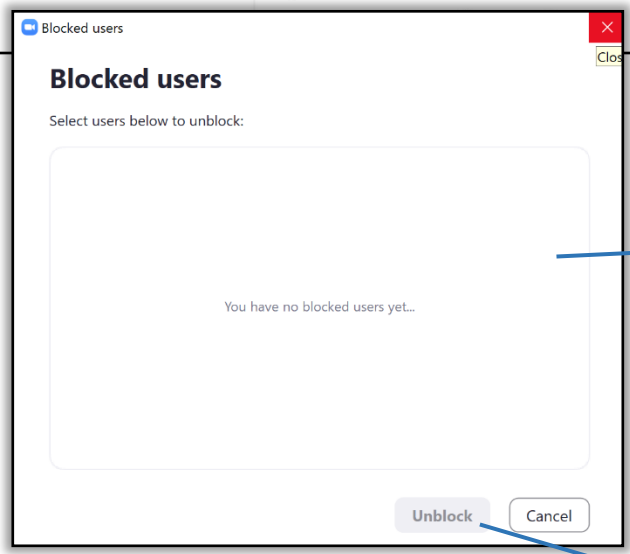
Note that some important Zoom settings are accessed via the website, while others are accessed from within the App. You will need to do both.

Blocking users in the App



1

*Block any **unwanted** users here*



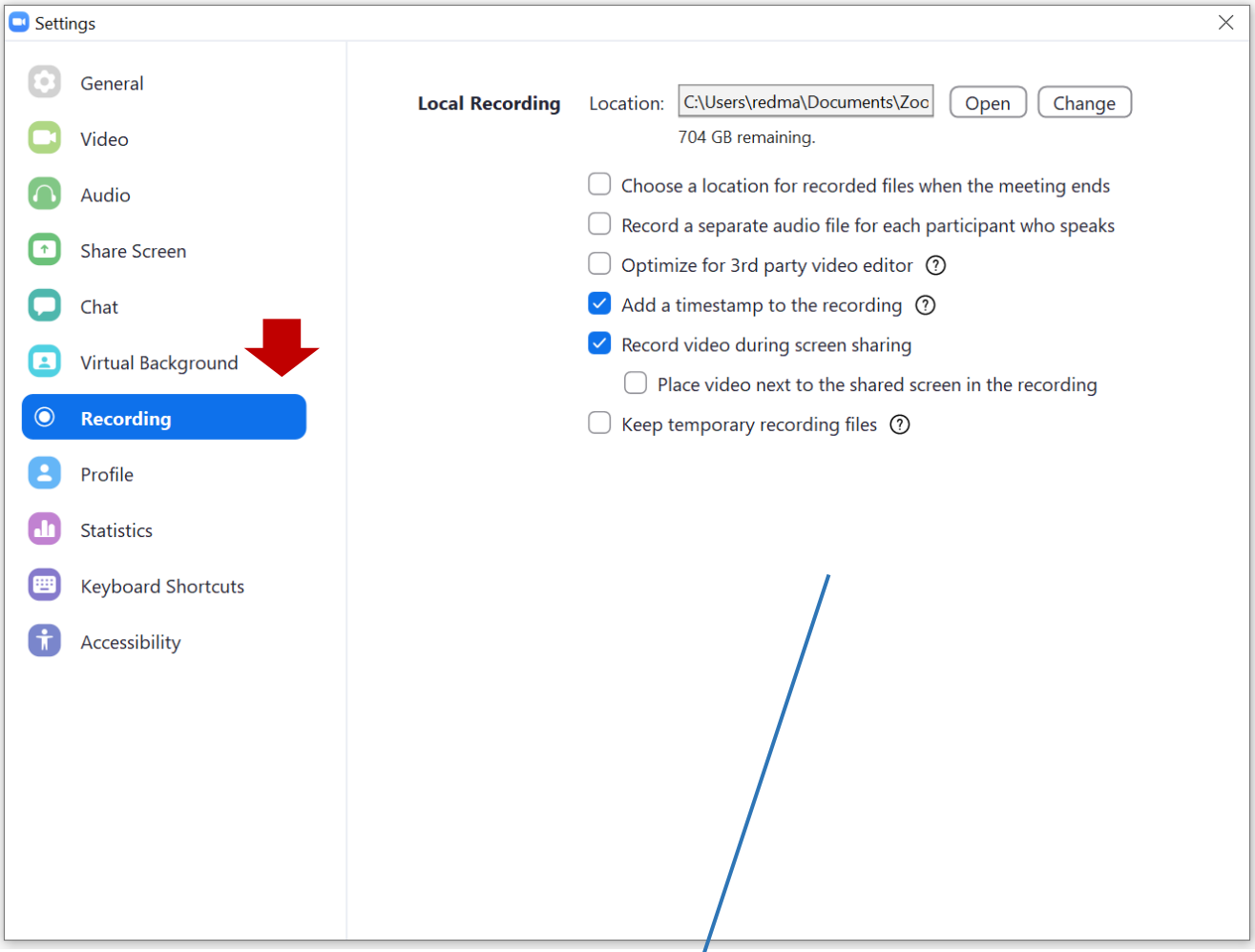
2

You'll see a list of blocked users

3

You can always unblock users later

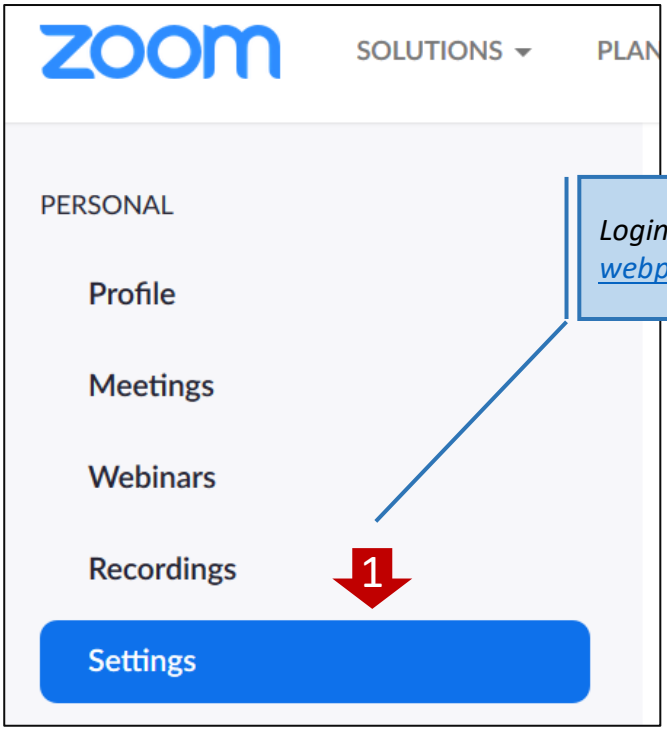
Adjusting recording settings in the App



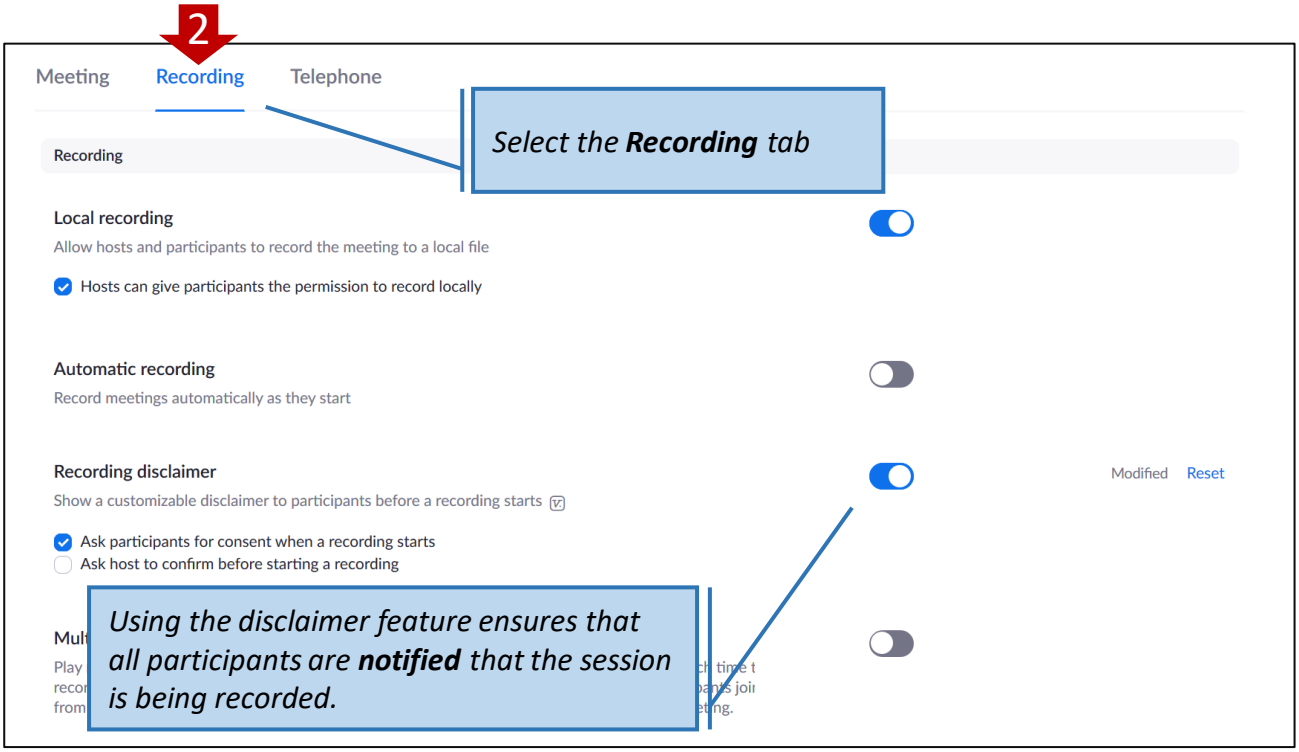
*Within the **Zoom App**, go to the **Recording** menu and choose the appropriate settings for your meetings.*

Adjusting recording settings via the webpage

*If you are hosting the meeting, you can access several advanced settings and **allow or block all recording** by logging in to your **web-based Zoom account**…*



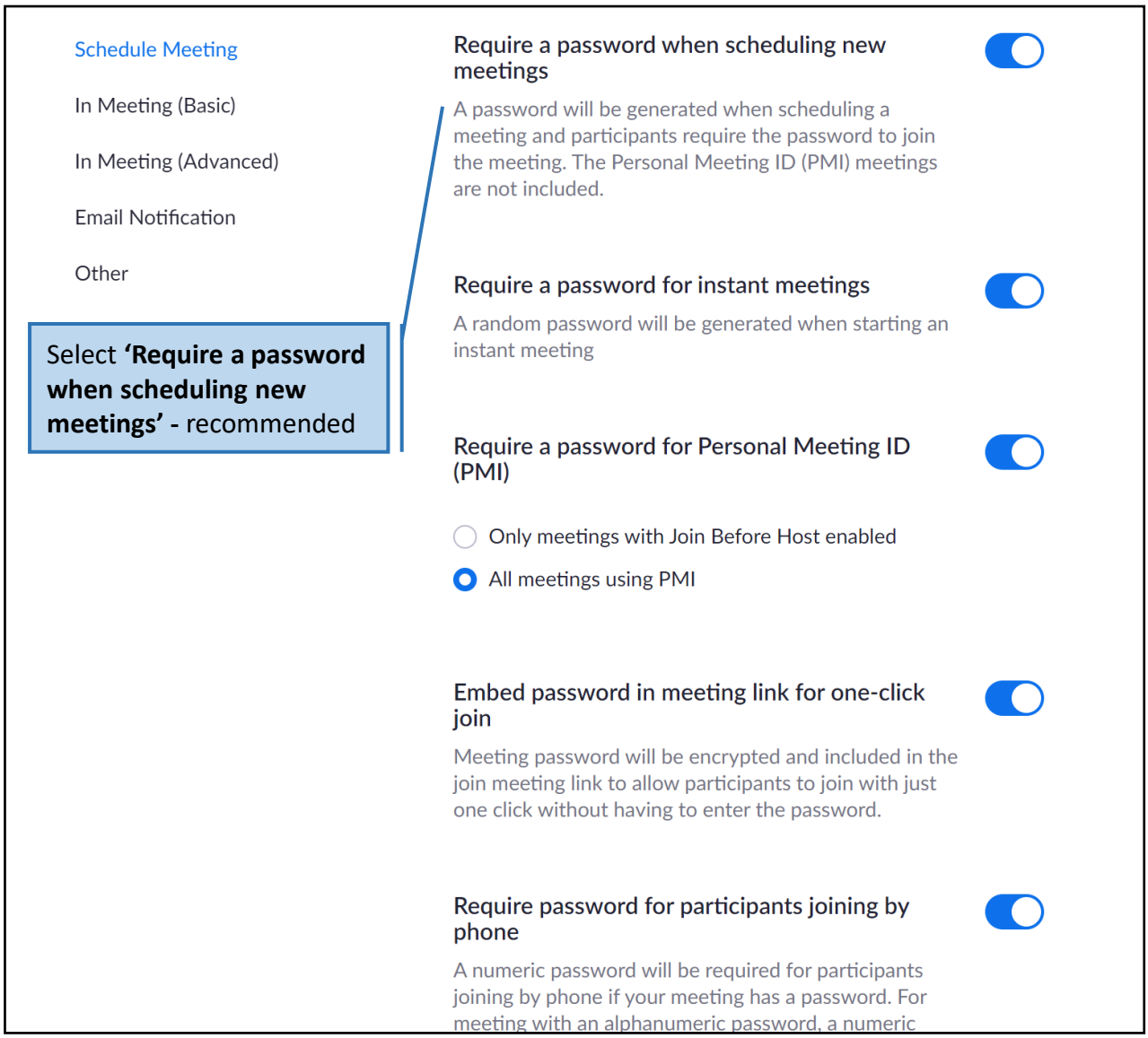
*Login to your account on the Zoom webpage, then select **Settings**.*



*Select the **Recording** tab*

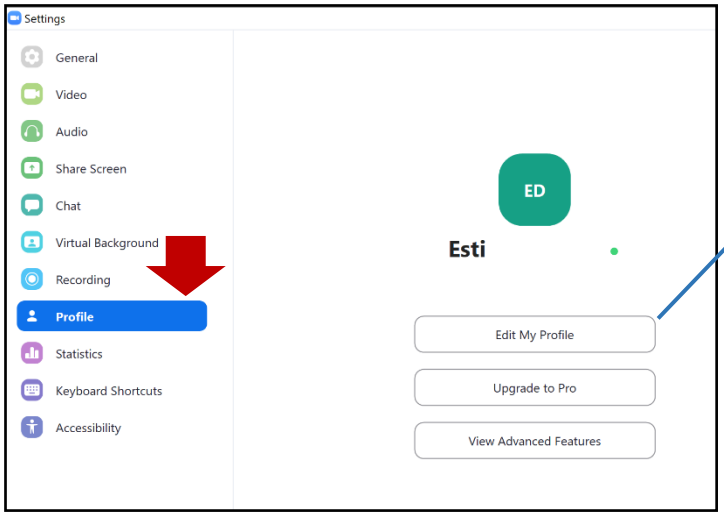
*Using the disclaimer feature ensures that all participants are **notified** that the session is being recorded.*

Managing your meeting settings via the web



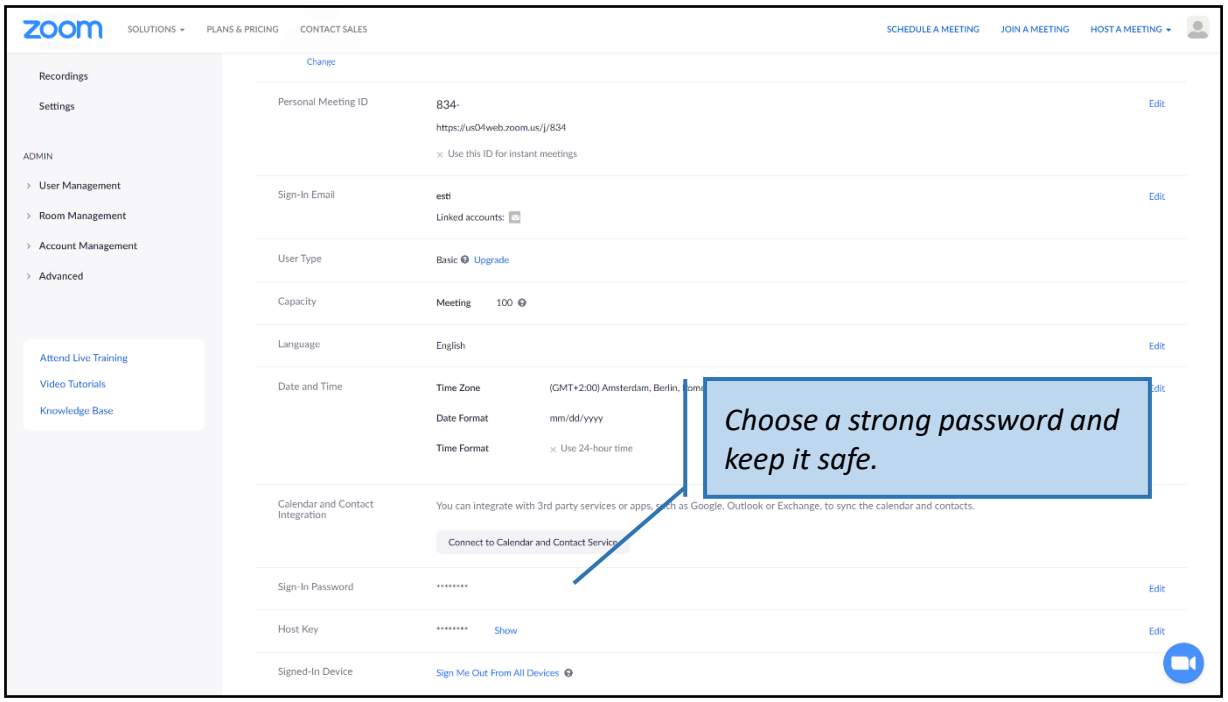
Once again, you can go to your web account to access advanced meeting settings. Make sure that you select **Require a password when scheduling new meetings** *if the nature of your role of the nature of the meeting requires this.*

Managing your profile



You can edit your profile here. ***The App takes you to the webpage.***

Do not include any unnecessary or sensitive information in your profile.

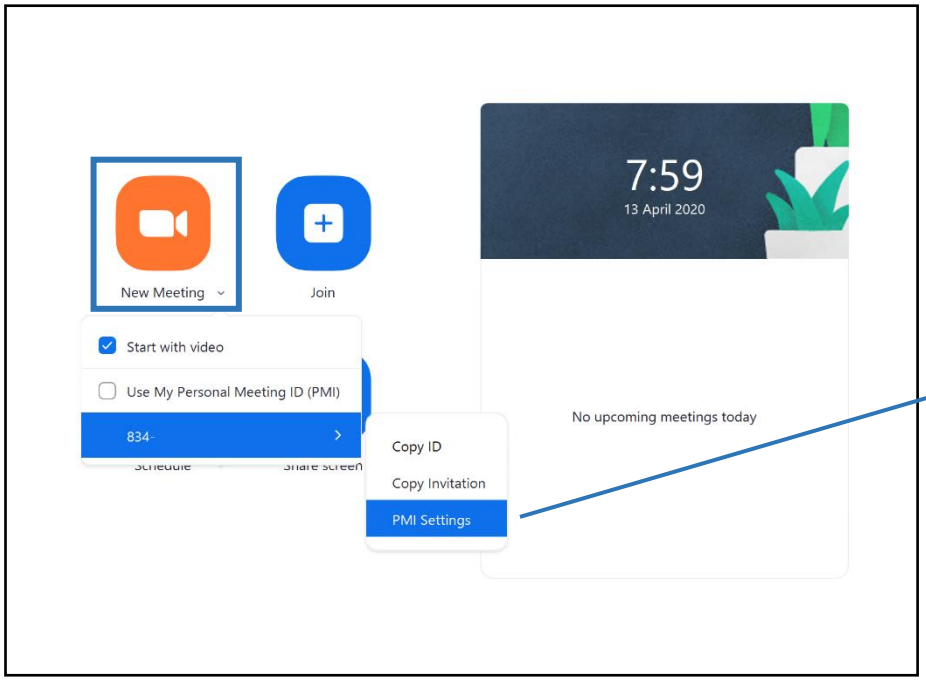


Choose a strong password and keep it safe.

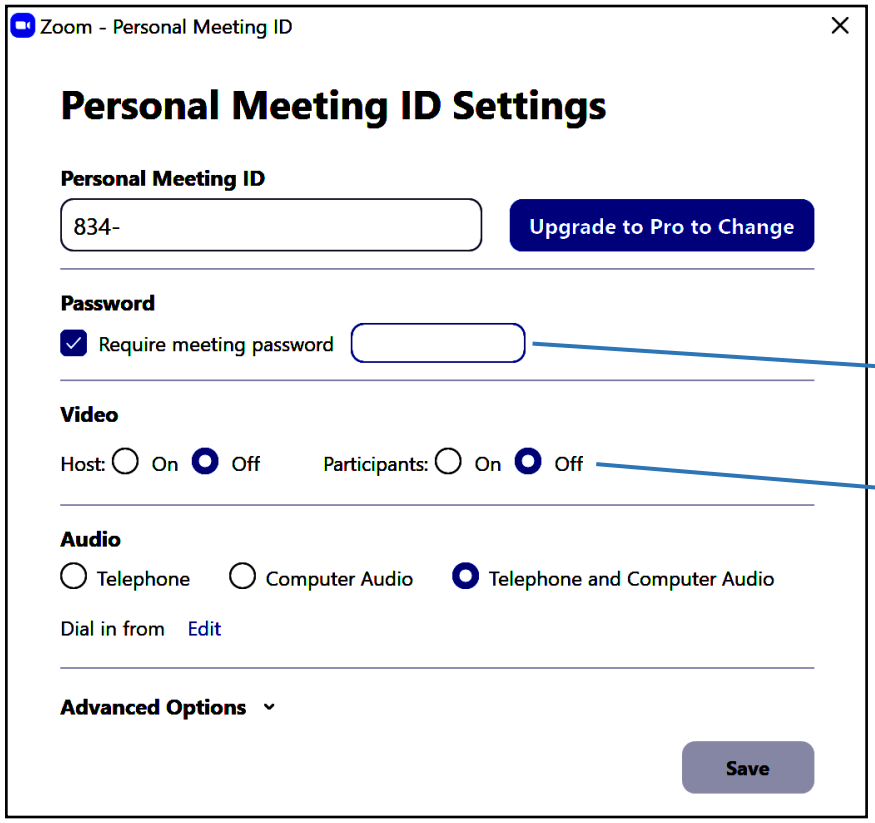
Password advice from the National Cyber Security Centre (NCSC)

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27!. Be creative and use words memorable to you, so that people can't guess your password.

Managing your meetings via the App



*Go back to the Zoom app homepage and click on **'New Meeting'.** Then choose your ID number and then access your Personal Meeting ID (PMI) settings*



Choose a unique password for each meeting you host.

*Think about how you will **share the password** with attendees. Encrypted email or secure messaging are both good options.*

*You have an opportunity to modify your recording options. **Blocking recording** by other participants is the more secure option, but you will need to assess the risks and needs for each session.*

Remember, regardless of the settings chosen, any participant can still record their screen using a mobile phone. Always consider the topic & whether Zoom is the appropriate medium.

Credits

Conceived and commissioned by the National Policing DCG Futures Group
Produced by The Risk Management Group (TRMG | www.trmg.biz)
OSINT Consultant, Esti Medynska, TRMG
Artwork produced on commission to TRMG by Nic Brennan

Disclaimer

Social Media, Browser, App and device security settings change constantly. Check your settings and options regularly to ensure that you are using the highest levels of security.

Neither the NPCC, nor TRMG, accept responsibility for any loss or breach arising from the use of this document. The document represents best efforts to encapsulate the common body of knowledge existing at the time of writing and is a guide to the security features available to users of online services and smartphones. This is not an operational guide and the reader is advised to consult his or her respective organisation for operational guidance on security and best practice.

Issued by the National Policing DCG Futures Group
DCGFutures@met.police.uk