4 April 2020

Using Zoom safely

Almost every piece of software has settings (or in Mac language, Preferences). Often we just accept the software as it comes 'out of the box'. But it's worth knowing about how to use Zoom in a way that reduces the risk of what's become known as 'Zoom-bombing' where a stranger joins your meeting and shares obscenities or pornography.

First, let me say that as a computer user for 30 years, and as a software trainer for 10 of those, I'm resigned to being hacked – that experience where people steal some of your information or even access private data. [Caveat: I'm not a 'techie' – I've trained people to use apps (we used to call them programmes) and my specialism is not IT security.]

I do a lot to minimise the risk of hacking – avoiding using public WiFi without using VPN, not using any of my several hundred passwords for more than one log-in. But clicking on a dodgy link in what appears to be a genuine email can undermine that – as someone seeks to gain access to address book. Unless your computer is never connected to the internet, there is risk. You need to minimise the risk.

So my approach to using Zoom is the same. **Use it wisely and minimise the risk**.

Zoom themselves are aware of the heightened misuse and on Friday 3rd April sent out an email to users. This is what they have done:

1. Zoom have turned on Waiting Rooms by default. This prevents anyone from entering your meeting without you seeing their name and approving them joining the meeting that you've started. So in a small group environment, where you know everyone, you should recognise their name.
    a. Of course, if someone doesn't enter their name, or uses a shortened version of a name which is common in your group, it doesn't help. Recently one retiree joined my meeting with the model of her phone as her name. Encourage people to complete the name info in the app.

   b. Here's an extract from Zoom's email:
   How do I admit participants into my meeting?
   It's simple. As the host, once you've joined, you'll begin to see the number of participants in your waiting room within the **Manage Participants** icon. Select **Manage Participants** to view the full list of participants**,** then, you'll have the option to admit individually by selecting the blue **Admit** button or all at once with the **Admit All** option on the top right-hand side of your screen. For step-by-step instructions, please watch this **2-minute video by following this link: https://bit.ly/2Xd0B6W** .

2. Zoom have turned on passwords by default. People who join directly from a meeting link don't need the password. Those who just enter the meeting ID number will need a password. Zoom have produced a video to demonstrate what you and your participants will see: **https://bit.ly/2ywhgYx** .

   a. UCAN[1] recommend "don't ever publish the meeting ID or password to publicly accessible social media. This is important information and therefore should be treated with appropriate caution. Share only via private groups, messages and emails where you have confidence in the recipient list."

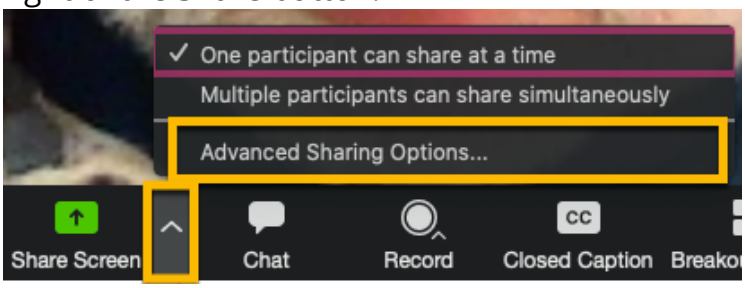
[1] UK Church Administrators Network

Some other suggestions

A. Don't use the Personal Meeting ID (PMI), but use the Generate Automatically feature to create a unique ID for each meeting.

B. For extra security, you could just give people the meeting ID number (they'd have to click 'Join Meeting' in the app) and send them the password by a different means (e.g. send one by email, the other by SMS or WhatsApp).

C. In settings, Find Screen Sharing, and change the default to 'Host Only'. If you have a meeting containing only trusted individuals, you can change this using the Advanced Sharing Options in the menu (up arrow) to the right of the Share button.



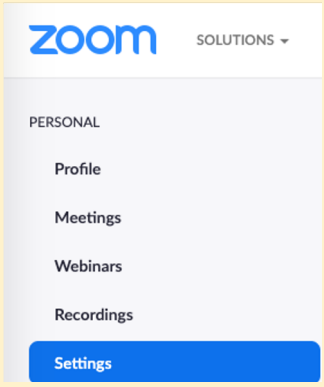
Adjusting the Settings

The settings are the rules that, by default, apply to each meeting you create. It is best to adopt cautious settings, which you can then relax for individual meetings.

Where to find the settings

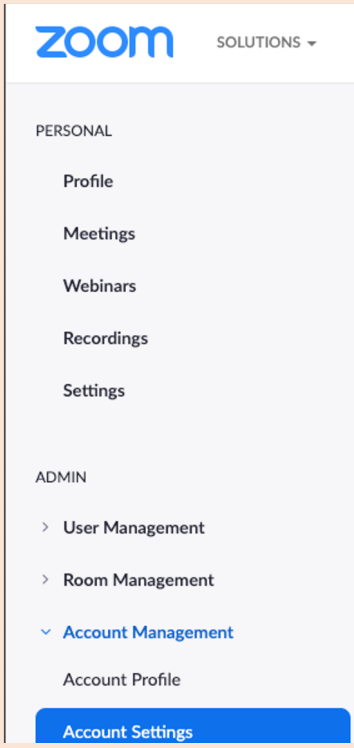
1. On your internet browser (e.g. Safari, Chrome, Microsoft Edge, Firefox) got to https://zoom.us .
2. If not already signed in, Sign In.

If you are using a Basic (free) Licence, the only choice of settings is on the left under **PERSONAL>Settings**



If you have a Pro License (for which you or your organisation are paying) you can also adjust the settings on the left under **ADMIN>Account Management> Account Settings**.

This also give you the ability to lock certain settings so that other hosts using your account (under a separate email address) can't override key settings.



Go through the settings. You'll discover more about Zoom. If you don't understand a setting, Google it by typing 'Zoom' followed by the setting description. There is loads of help online.

Zoom isn't perfect (yet)

Finally, be aware that Zoom does have some work still to do. **This article from the Guardian https://bit.ly/3e2t4SX** will frighten any reader**.** It may be mitigated by reading **this subsequent article: https://bit.ly/2xUetbe .** And **this article https://bit.ly/3aL9bxx** identifies some of the same issues but also reports on recent fixes.

So, speaking personally, I'm not going to use a Zoom meeting to share my confidential plans for world takeover. But I'm going to continue using Zoom elsewhere. Where I save the recordings, it will be on my encrypted hard drive on my computer, and I'll change the name of the file before I distribute it to anyone else.

Using Zoom within your church?

Part of my DNA is being a trainer. I can teach you sailing, the Bible, how to drive a computer or soft skills to use in business and life. Currently I'm in a position to help if you (or someone you know – even if a technophobe – could use some help to get up and running with Zoom for groups within your church. Do ask me for help. Contact details and an enquiry form are on the website where you find this document.

Disclaimer

This article is written to help users manage some of the security risks associated with using Zoom. It is not a comprehensive solution, and if you choose to follow the advice and opinions expressed within we exclude all liability for any loss or damage suffered by you as a resulting of doing so (including all consequential loss or damage howsoever caused and whether or not this was in your or our reasonable contemplation).