sbrcentre.co.uk

Zoom

Etiquette and Security

Scottish Business Resilience Centre

Contents

Zoom

Zoom is the worlds most popular Video Conferencing software. Access to calls is governed by meeting IDs instead of user accounts; greatly simplifying the process of joining meetings. In addition Zoom offers a wide variety of settings to really tailor meetings to host needs.

Installation

You can install Zoom by visiting https://zoom.us and downloading the installer appropriate to your Operating System. Once downloaded you can install the program by double-clicking and working through the prompts. If you see a Windows pop-up asking if you want to run the setup as an Administrator click yes.

Setup

Once installed Zoom has a variety of options that you can enable to enhance your meetings, control access to them and increase your overall security. Basic settings can be found clicking the icon with your initials on in the top right.

From here you can adjust the settings of your Zoom client. You can change your background, adjust your audio, see what resources Zoom is using and even touch up your appearance when on camera!

Further settings can be found by clicking **View More Settings** in the Settings menu. This will take you to your account on the Zoom website. This is where the most powerful settings for Zoom hosts can be found.

Joining a Meeting

There are two ways to join a meeting in Zoom. The first is to use a meeting ID. You will be prompted for this after selecting **Join** or when launching Zoom. You may also be asked for a password - if you do not know the password you will need to contact the meeting host and ask for it. One way that you can do this is with the **Chat** feature, which you can use to **Instant Message** your zoom contacts.

The other way to launch a Zoom meeting is to click on an invitation link. These bypass the need to enter a password so you won't be prompted to enter one. Clicking the link will first open your web browser and take you to a **zoom.us** webpage. Zoom will either launch automatically or your web browser will ask if you want to allow Zoom to be launched. Click **Yes** or **Allow** and you will enter the Zoom meeting.

Hosting a Call

If you're hosting a call there can be quite a lot to consider. One key decision is wether you want to run a meeting or a webinar. Running a webinar gives the host far more control over what happens but obviously comes at the cost of audience participation. As it's your meeting you will ultimately be responsible for what happens so consider this carefully. Ensure that attendees are aware of the behaviour that's expected of them and be sure to keep things as professional as you can. How you start a meeting will usually set the tone for the rest of it so take some time on your opening statement when appropriate.

As host you will also be moderating and probably dealing with technical issues so take some time to familiarise yourself with zoom and its features.

Below is a checklist of things to consider before and during your meeting.

Important Zoom Settings for Hosts

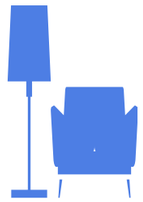
Within your Zoom account there are a number of incredibly useful settings that can greatly enhance your control over your meetings and improve the experience for your attendees.

If you want to enforce these settings for all users in your account click the lock icon and then click **Lock** to confirm your selection.

Meeting Password

Ensure that all your meetings are locked with a Password. This should be enough to prevent "Zoombombing".

Waiting Rooms



Waiting rooms allow you to admit attendees individually, ensuring that only invited guests can participate.

Disable File Transfer

This will stop participants from being able to send malicious files to other attendees.

Host Only Screen Sharing

Helps ensure that attendees will only see what you want them to see.

Mute Participants Upon Entry

This will eliminate annoying feedback and other undesired audio.

Prevent Removed Participants from Rejoining

Ensures that disruptive attendees will not return and lessens the burden on moderators.

Disable Annotations

Prevents attendees from drawing on the screen for all to see.

Disable Private Chat

This should help prevent attendees from being harassed without moderators being able to see.

Zoom Host Checklist

Hosting a Zoom meeting can be a little daunting if you haven't done it before. This checklist should help you set everything up smoothly and ensure that your attendees have the best experience possible.

Before the Meeting

- ✓ Create the event, schedule the meeting and ensure a password is applied.
- ✓ Create an Eventbrite event to secure registration and authenticate email subscribers prior to admittance.
- ✓ Invite your speakers and designate them as Co-Hosts.
- ✓ Immediately prior to the event host a practice Zoom call so all your presenters can familiarise themselves with the application.
- ✗ Never disclose the Meeting ID number or publicly advertise the direct Zoom Link.

The Host and Presenters

- ✓ Remember this is as if you presenting in public, preparation is key.
- ✓ Look directly at the camera, not at something on the screen.
- ✓ Consider your camera position and what your audience will see.
- ✓ Consider your background , a busy bookcase or multiple family photos in the background will distract your audience.
- ✗ Refrain from other activity that may show disinterest to other speakers.

During the Meeting

- ✓ Ensure your waiting room option is initiated to preclude unwanted visitors.
- ✓ Disable the File Transfer capability, Annotations, Private Chat and set mute attendees on arrival.
- ✓ Initiate screen share for Presenters, Co-hosts and Hosts only.
- ✓ Once the presentation has commenced, lock down the meeting. This will help prevent Zoombombers from crashing the event.
- ✓ Please request that participants to refrain from photographing screen without permission as it can breach GDPR.
- ✓ Please encourage questions and comment via the share command.
- ✓ Should an attendee wish to raise an urgent point; they can select **Raise Hand** otherwise all questions will be answered as the host sees fit.
- ✓ If doing so, inform your participants that the event will be recorded and/or slide decks will be shared.

Zoom Security

As Zoom has grown in popularity a number of questions have been raised regarding its security. There have been many worrying stories and some large organisations have chosen to ban the platform altogether. The section below will explore some of the raised issues.

Overall though Zoom is a reasonably secure application and is fine for casual use and most business cases. However if confidentiality is of the utmost importance then Zoom should be avoided.

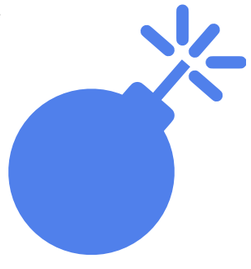
Encryption

Zoom calls are not fully end-to-end encrypted. They are encrypted from users to Zoom servers. These servers act as switchboards and therefore need access to the unencrypted data to function properly.

A hacker cannot eavesdrop on calls in transit but if they gained control of a Zoom server they could be able to see and hear everything. This isn't terribly likely but should be considered if you wish to have a highly confidential conversation.

It should be noted that as of April 2020 Zoom's encryption keys are not distributed in the most secure way possible, adding another small vulnerability.

Zoombombing



Zoombombers gatecrash meetings in order to disrupt them for their own amusement. Password protecting your meetings and not sharing Meeting Invitations on public forums should protect you from these individuals.

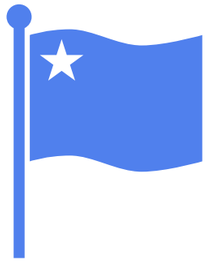
It's also advisable to never use your Private Meeting ID (PMI) as this cannot be changed and if leaked will make it bit easier for Zoombombers to access your meetings.

User Details Sent to Third Parties

Until recently Zoom would send some data to Facebook and Google servers when any user logged in. This was due to Zoom using Google and Facebook's SDK to allow users to log in with their Facebook and Google accounts.

This code has now been stripped back and Zoom will only contact these servers when absolutely necessary.

Zoom Calls Routed Through Chinese Servers



There have been reports of Zoom routing traffic through Chinese servers and thus have exposed customer data to surveillance by the Chinese security services. This is likely an oversight as Zoom has been rapidly acquiring server space to keep up with an explosion in demand from users.

Zoom has stated that this will not happen again and paid users can now choose specific countries that they would their Zoom calls to be routed through.

Zooms Stance on Security

Zoom have stated that all their updates for the foreseeable future will be focused on improving the security of their application.

As such it's critical that users keep their Zoom client up to date in order to benefit from the enhanced security features being offered. If a new update is made available your client will download and apply it at launch. If you wish to update Zoom manually you can do so from the settings menu.

Scottish Business Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27