* [How to Schedule a Zoom Meeting](https://rcpi.sharepoint.com/:v:/s/Wiki/EfAwWcSLJXJMuCHa5K-aJCUBZqLHjPArGtjTPFo37ISW5A?e=ztJLGs)
* [How to Set your Default Dial in Options](https://rcpi.sharepoint.com/:v:/r/infohub/Wiki/Shared%20Documents/Zoom/How%20To%20Set%20Your%20Default%20Country%20Dial-In%20Options.mp4?csf=1&web=1&e=g34EfZ)
* [How to Join a Zoom Meeting as a Participant](https://rcpi.sharepoint.com/:v:/r/infohub/Wiki/Shared%20Documents/Zoom/Join%20A%20Meeting%20As%20A%20Participant.mp4?csf=1&web=1&e=bV3Mfh)
* [How to Start a meeting Host](https://rcpi.sharepoint.com/:v:/r/infohub/Wiki/Shared%20Documents/Zoom/Start%20Meeting%20As%20Host.mp4?csf=1&web=1&e=e2vqss)
* [How to set a virtual background for your profile in Zoom Meeting](https://rcpi.sharepoint.com/:w:/r/infohub/Wiki/Shared%20Documents/Zoom/Zoom%20Virtual%20Background%20Steps.docx?d=w5ab30851665b4147afbb6770f1f23875&csf=1&web=1&e=yw73ef)
* [Keeping unwanted guest out of your Zoom Meetings](https://rcpi.sharepoint.com/infohub/Wiki/SitePages/Zoom-Security.aspx)

**Zoom Security**

Zoombombing has been causing problems all over the world, but this handy guide will help ensure your meeting stays as secure as possible.

With more and more people staying at home throughout the Covid-19 crisis, many have resorted to connecting with others using popular video conferencing tool Zoom.

But, as is the case with most online tools, it is not impervious to privacy issues, especially with so many people using it for the first time.

This week, a Dublin GAA club fell victim to ‘Zoombombing’ when an online coaching session for young children was [hacked](https://www.independent.ie/world-news/coronavirus/dublin-gaa-club-apologises-to-parents-after-kids-online-coaching-session-is-zoombombed-with-inappropriate-content-39103093.html) with inappropriate content shown to participants. This is [just one of several examples](https://www.siliconrepublic.com/enterprise/zoombombing-illegal-zoom-call-hijacked-hacked) where Zoom calls have been hijacked, which has led to the US Department of Justice stating that Zoombombing qualifies as a federal offence.

Zoom has already started putting [additional security measures](https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms-default) in place to reduce the risk of Zoombombing. However, it’s worth noting that these new measures are mainly based around setting features that already exist within the platform as the default, such as password requirements and waiting rooms.

Users of the platform have a responsibility to ensure their own meetings are as secure and private as they can be. Speaking on RTÉ’s Six One News yesterday (6 April), Siliconrepublic.com editor Elaine Burke said if users create a Zoom link that’s open for anyone to join and share it on public platforms such as Facebook or Twitter, it creates a risk.

“It can be quite easy to set up programmes to search for these links online or they might be shared in groups that are just built to cause havoc,” she said.

So, while Zoom continues to beef up its own security measures, here is what you need to know when using the platform to ensure your calls are as secure as possible.

**Know about your Zoom package**

There are several different Zoom account types available, each with different privileges and powers. For example, a basic account is free and allows you to have unlimited one-to-one meetings, but for meetings with three or more people, there is a 40-minute time limit.

A pro account is the next tier up and it gives the user administrative abilities such as enabling and disabling recording, and it extends meeting limits to 24 hours.

Whatever package you’re on, it’s important that the host of each meeting is familiar with the settings that will maximise security of each meeting and minimise disruption.

**Don’t share Zoom details on public forums**

This is probably the most crucial tip for ensuring your meeting is secure. As Burke said, sharing a link to a meeting on a public forum makes it much more susceptible to hackers. Most Zoom meetings have a public link that, if clicked, allows anyone to join.

This makes it easy for trolls and hackers to collect these links and share them with groups with the specific intention of Zoombombing or causing other problems. The same goes for sharing meeting IDs. Therefore, avoiding putting your meeting link in public places helps to mitigate these risks.

**Be mindful of using meeting IDs**

If you’re using meeting IDs instead of links to host public events, make sure you use a randomly generated ID, rather than your personal meeting ID.

If you share your personal meeting ID in public, it allows anyone who sees it to not only join that initial meeting, but to crash your personal virtual space at any other time.

You should think of your personal meeting ID like your own phone number and then think about the privacy and security issues around sharing that number on Facebook or Twitter.

You should also be mindful about this before sharing a screenshot of you and your colleagues having a Zoom call. The novelty of conducting business completely remotely is still strong and many people are eager to show off their social events and work meetings on social media.

However, if the picture includes the Zoom ID, it leaves the meeting exposed to crashers. This is worse again if that happens to be someone’s personal meeting ID, which is the equivalent of sharing a private phone number.

**Set passwords on your meetings**

Password protection is now being rolled out as a default by Zoom, but it’s important to ensure users are exercising this practice anyway. All Zoom meetings should have both an entry link or ID and a password in order to get in.

Remember, security measures such as these are only as effective as the users who enable them, so just as you should not publicly share open meeting links, meeting passwords are rendered useless if they are shared on public platforms alongside a corresponding link or ID. Trolls and hackers can find them too and then you’re back to square one.

**Set up a registration system**

Another way to avoid putting up a public link or meeting ID is by using a registration system instead. Tools such as Eventbrite can be used to register the details of those who want to attend a session, and then the registered attendees can be sent a private message with the link and password in order to gain entry to the meeting.

This definitely adds some extra steps but essentially enables additional safety gates for event hosts to monitor who is being added to the meeting, particularly with so many large and public events going virtual. It also helps moderators double-check participants during the next step.

**Set up a waiting room**

The waiting room is another feature that will become a default setting as part of Zoom’s latest security measures, and it is an excellent way of monitoring who is coming into your meeting.

When scheduling a meeting, go to your settings and click advanced options. Here you will have the ability to ‘enable waiting room’, which means that when participants do join the meeting, they will be added to a virtual waiting room, where the host of the meeting can vet participants before allowing them to join the call.

The waiting room also gives you a chance to set up your meeting properly before participants enter, such as having the right screen shared if necessary and ensuring participants’ powers are managed in advance.

**Restrict participant powers**

You can restrict the powers of your participants during meetings, which can often be good practice in general but, more importantly, will restrict the powers of any troublesome entrants.

For example, you can mute all attendees upon entry to ensure that there are no disruptions. This can be done while scheduling the meeting, under advanced options in the same place you set up the waiting room, or it can be done once you have entered the meeting.

The bar along the bottom of the screen allows you to manage participants. You can mute everyone on the call or prevent them from unmuting themselves. You can also ensure that only the host has the ability to share their screen by clicking the arrow next to ‘share screen’. You can also restrict chat options if chat is not needed, or limit chatting to the host only.

Screenshot: Zoom

Depending on how large your Zoom meeting is, you may need to give other people hosting permissions to allow them to moderate, mute or monitor participants’ behaviour. This is particularly important if the original host is also the one who will be busy speaking during the meeting. However, co-hosting will require at least a Pro Zoom account.

**Lock the meeting**

Another helpful feature is locking a meeting once it has started as an additional security measure, just like you would lock your front door once everyone is in the house at night.

Once the meeting has started, you can select ‘manage participants’ and choose ‘more’ at the bottom of the side bar. This will give you the option to lock the meeting, which will prevent any further participants from joining.

For private meetings, this could be done once everyone has entered the meeting, and for more public virtual events, it could be done 10 minutes after the event has begun, for example. Think of it like a theatre in which late entries will not be permitted once the show has started.

**Set out best practices at work**

For companies using Zoom regularly to conduct meetings, the above tips will help provide as much security as possible, but it’s essential that employers inform employees of these practices too.

Inform them not to share meeting IDs, links or passwords anywhere that isn’t secure. Make sure they know not to share screenshots of Zoom calls.

If you want to show off your Zoom call, at least make sure everyone who is visible is comfortable with the photo being shared and make sure the meeting ID is not visible.

It’s also important that users know about the chat function. For example, if a Zoom call is recorded, all chats, [even private chats between two participants](https://www.forbes.com/sites/kateoflahertyuk/2020/03/31/are-your-zoom-chats-private-heres-why-you-should-think-before-opening-the-app/#2b99ffb19791), will be downloaded into a ‘minutes’ folder once the call ends.

It’s crucial that everyone on your team is comfortable with using Zoom and is aware of its security settings if you’re going to use it for business purposes.