Zoom Security

You may have read that Zoom have experienced some security issues in their past. This is not a surprise, especially following the unprecedented demand for their service. Zoom's popularity is due in part to its ease of use which often means it's not as secure as some harder to use packages. The following notes explain how to make it more secure.

Keep Zoom client updated

- Always install the latest update to your device.
- If you are prompted to update your Zoom client, please install the update.
- The latest Zoom updates enable Meeting passwords by default and add protection from people scanning for meeting IDs.
- With Zoom being so popular at this time, more threat actors will also focus on it to find vulnerabilities. By installing the latest updates as they are released, you will be protected from any discovered vulnerabilities.

Can Zoom be hacked?

A lot of online apps and services are vulnerable to being compromised through attacks like phishing, whereby login information is elicited through duplicitous websites and emails.

One attack method has become so widespread that it has led to a new term being coined: 'Zoom-bombing'. This is where strangers join conference calls and hijack them by broadcasting pornographic images, shouting profanities, or issuing threats to the people involved in the call.

While there will always be risks with most online app, there are ways to ensure the maximum level of security by adjusting the platform's settings.

To try and prevent the possibility of these issues here are some tips on what you can do to secure Zoom so that you and your friends or colleagues can meet safely.

Securing Zoom meetings with passwords

You can add Zoom passwords at the individual meeting level, or they can be enabled at the user, group, or account level for all meetings and webinars. Account owners and admins can also require passwords for all meetings and webinars on their account. The advice is making passwords your default for all meetings.

To do this for your account, take the following steps:

1. Log into your account via the Zoom web portal.
2. As the owner or admin, select Settings.
3. Navigate to the Meeting tab and verify that the password settings that you would like to use for your account are set properly.

For your groups (if using Pro):

1. Sign in to the Zoom web portal as the owner or admin and click on User Management then Group Management.
2. Click the Group Name from the list and then click the Settings tab.
3. Now, navigate to the Meeting tab and verify that the password settings that you would like to use for this group are enabled.

If you want to require everyone in your group to use these password settings, click the lock icon, and then click Lock to confirm that you want everyone to use passwords.

For your meetings and webinars, once more:

1. Sign in to the Zoom web portal.
2. Head to Settings
3. Navigate to the 'Meeting' tab and verify that the password settings that you would like to use for your meetings and webinars are enabled.

No matter whether you're setting up passwords for your account, groups, or specific meetings and seminars, you'll see essentially the same choices. For maximum safety, it is recommended that you activate passwords for new meetings, instant meetings, personal meetings, aka PMI, and people joining by phone.

Important Tips:

Zoom recommended users read this guide which covers precautions for keeping their meetings safe… https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

Most importantly, **Zoom users should not share meeting links publicly**. This is perhaps the single most obvious precaution you can take. Rather than posting a meeting link to a Facebook group or in a promotional tweet, distribute information via a more private method, such as email.

Second, **set your meetings to "private."** Zoom now sets all new meetings to "private" by default, requiring attendees to provide a password for access. But users often opt to make meetings public for the sake of convenience. Given the wave of Zoom bombings, the inconvenience of requiring a password is probably worthwhile in keeping your meeting safe.

Also, **don't use your personal meeting ID**. Every registered Zoom user has a personal meeting ID, linked to what is essentially a permanent virtual meeting room. Because that ID doesn't change, sharing it publicly increases the chance that future meetings using your personal ID might be Zoom bombed.

To avoid the risk of Zoom bombing, **share your personal meeting ID only with your most trusted contacts**. Generally, while Zoom will prompt you to use your personal ID for "instant" meetings, scheduled meetings will use a one-time meeting ID, reducing risk. If you're concerned that you may have already shared your personal meeting ID in an insecure way.

Finally, **restrict video sharing**. If the meeting host is the only person who needs to share video, such as in a seminar or presentation, the host should change Zoom's screen-sharing setting to "Host only."

How you can protect your data

As Zoom becomes more popular, there are some steps you can take to keep your data safe.

- **Use two devices during Zoom calls:** If you are attending a Zoom call on your computer, use your phone to check your email or chat with other call attendees. This way you will not trigger the attention tracking alert.
- **Do not use Facebook to sign in:** It might save time, but it is a poor security practice and dramatically increases the amount of personal data Zoom has access to.
- **Keep your Zoom app updated:** Zoom removed the remote web server from the latest versions of its apps. If you recently downloaded Zoom, there's no need to be concerned about this specific vulnerability.
- At the end of a Zoom session make sure you close the Zoom program and close the browser window.

In terms of data protection Zoom are GDPR compliant in the way that they use your data.

https://zoom.us/security