You may have heard that Zoom has been in the news in the past few days not from the surge of new users but from security and privacy concerns. Here's a quick update and how you can protect yourself / users:

Here's what you can do to protect yourself.

1. Zoom has released a patch to fix the vulnerability and secure the bugs allowing people to control your Mac computers.
2. Zoom's new release has also fixed the privacy flaw that shared user information with third party sites.
3. You can take steps to stop Zoombombing by following the below steps:

Securing your Zoom meetings

1. *Add a password to all meetings!*
   When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6 digit password.

   You should not uncheck this option as doing so will allow anyone to gain access to your meeting without your permission.

2. *Use waiting rooms*
   Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.
   This feature can be enabled during the meeting creation by opening the advanced settings, checking the 'Enable waiting room' setting, and then clicking on the 'Save' button.

   When enabled, anyone who joins the meeting will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."

   The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.

   You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.

3. *Keep Zoom client updated*
   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.

4. *Do not share your meeting ID or better yet use an autogenerated meeting ID*
   Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.

If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.

Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary.

5. *Disable participant screen sharing*

To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen.

As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options' as shown below.

When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'Only Host'.

You can then close the settings screen by clicking on the X.

6. *Lock meetings when everyone has joined*

If everyone has joined your meeting and you are not inviting anyone else, you should Lock the meeting so that nobody else can join.

To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.

7. *Do not post pictures of your Zoom meetings*

If you take a picture of your Zoom meeting than anyone who sees this picture will be able to see its associated meeting ID. This can then be used uninvited people to try and access the meeting.

For example, the UK Prime Minister Boris Johnson tweeted a picture today of the "first even digital Cabinet" and included in the picture was the meet ID.

This could have been used by attackers to try and gain unauthorized access to the meeting by manually joining via the displayed ID.

Thankfully, the virtual cabinet meeting was password-protected but does illustrate why all meetings need to use a password or at least a waiting room.

8. *Do not post public links to your meetings*

When creating Zoom meetings, you should never publicly post a link to your meeting.

Doing so will cause search engines such as Google to index the links and make them accessible to anyone who searches for them.

As the default setting in Zoom is to embed passwords in the invite links, once a person has your Zoom link they can Zoom-bomb your meeting.

9. *Be on the lookout for Zoom-themed malware*

Since the Coronavirus outbreak, there has been a rapid increase in the number of threat actors creating malware, phishing scams, and other attacks related to the pandemic.

This includes malware and adware installers being created that pretend to be Zoom client installers.

To be safe, only download the Zoom client directly from the legitimate Zoom.us site and not from anywhere else.

10. *Check your current version of Zoom.*
    Find and open the Zoom app from your workstation. You can find the version at the bottom center of the application login screen.

    4.6.9 is the current version for Windows and MacOS. Either way, if you open the client and log in (may need to create an account) you will be prompted to update. You should also be able to download the latest version from here: https://zoom.us/download#client_4meeting. The manual update will overwrite the installed copy.