GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Zoom Security Advice for Public Servants

Purpose

1. This paper sets out the Government Chief Information Security Officer's advice to public servants on important security settings when using Zoom remote conferencing services for official New Zealand Government business, either within a public sector organisation, or when collaborating with partner agencies.

2. Under no circumstances should Zoom be used when dealing with information classified above RESTRICTED.

3. This paper sets out the recommended security measures individuals should take when using Zoom.

4. Note that this paper follows on from more detailed technical advice to government CISOs and security teams on 27 March 2020.

Context

5. This advice applies only during COVID-19 alert levels 3 or 4. In normal circumstances agencies will have conducted security reviews and accreditation and assurance processes for the technology they use. Due to the exceptional circumstances as a result of COVID-19 we are relaxing these requirements for video conferencing during alert levels 3 and 4. If your agency intends to continue to use Zoom it will need to conduct a standard C&A process as per the requirements of the NZ Information Security Manual.

6. If your organisation already uses another video conferencing tool (for example Microsoft Teams or Skype for Business) you should continue to use that video conferencing tool for internal meetings, in line with your organisation's policies. You should still familiarise yourself with this advice as you may be asked to join a Zoom meeting when engaging with other agencies.

What is Zoom?

7. Zoom provides a video and audio-conferencing toolset, based on the premise of joining meetings from anywhere, on any device, at any time. This functionality allows for increased remote working capability, collaboration, and video calling functionality for practically all situations a public servant might attend or chair a meeting for.

8. Agencies have begun using Zoom, therefore we have moved to provide advice to assist agencies making good security decisions when using Zoom. There have been security issues with Zoom over the past 18-24 months and it is not risk-free. If you are going to use Zoom, we need you to follow this advice and help protect the government's information during these unprecedented times.

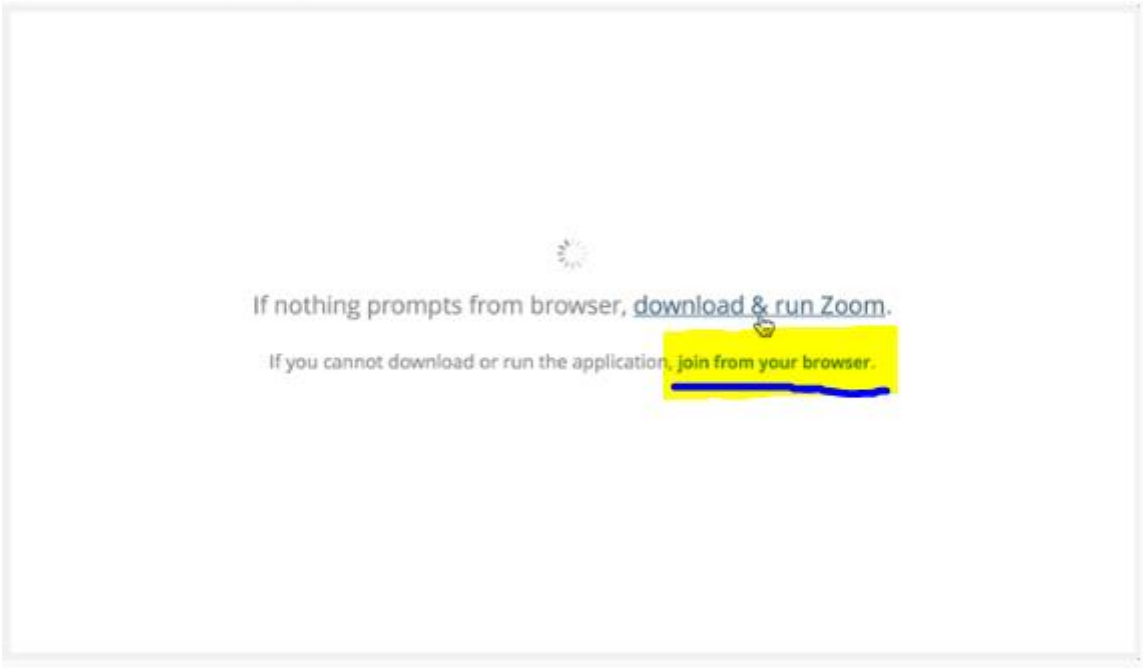
Our advice when attending a meeting using Zoom

9. You should use the Zoom desktop application and avoid using the Zoom smartphone app if at all possible. Our preference (in order) is for you to use:
    a. the Zoom desktop application (on your laptop)
    b. Zoom's in-browser functionality (from a laptop or mobile device)
    c. the Zoom mobile app (this should be avoided if at all possible).

10. There has been public reporting about Zoom's record of enabling user tracking on its mobile applications, and a permissive privacy policy. Given the urgent need to support agencies to move to remote working, we have not been in the position to undertake our own independent technical analysis of Zoom yet.

11. If you are on a mobile device, we suggest you use Zoom's in-browser option if possible. Note that when joining a Zoom on mobile, Zoom will try to guide you to download the app instead of proceeding to use it in the browser. As per figure one (below) there will be smaller text "join from your browser". Click on this link, sign in and join the meeting this way. However, this may not be possible on all mobile platforms.

Figure one: Zoom joining screen on mobile phone[1]



[1] For more information visit: https://support.zoom.us/hc/en-us/articles/214629443-Zoom-Web-Client

12. You need to be signed into Zoom (your organisation should have a Zoom account for you). If you are attending a multi-agency meeting, you should add your agency name or acronym into your screen name (e.g. Andrew Hampton, GCSB) to clarify which organisation you are representing.

13. If you are a senior official, or have a public profile, you are at greater risk from targeted phishing attempts to acquire your Zoom account details. Globally there have been significant criminal efforts to capitalise on, and profit from, COVID-19 related technology changes. We recommend that all users enable multi-factor authentication (MFA) on Zoom accounts[2], however at present Zoom is only able to provide MFA to its web browser users. MFA does not apply to the Zoom desktop client or mobile app.

Our advice when hosting a meeting using Zoom

14. The Zoom smartphone app preferably should not be used for ***hosting*** meetings or presentations, and where possible should not be used by staff attending calls or presentations hosted by third parties.

15. You should use the Zoom desktop application to host calls or presentation.

Setting up the meeting

16. When creating the invite and sending it out, you should:

    a. generate a random meeting ID, rather than sharing a link

    b. allow only signed-in users to join the meeting

    c. disable the "join before host" feature (if your administrator has not already disabled it)

    d. enable the waiting room feature

    e. only send the meeting invite information to required people

    f. send the password to the call via a separate method (i.e. send the meeting invite information via an email and the password via Signal message).

17. If recording of the video or audio is required, then the local recording feature within Zoom must be used and the recording should be uploaded into the agency's records system as soon as practicable.

Once the meeting has started

18. When you start to host the meeting:

    a. check who is on the call before sensitive information is discussed

    b. only accept/open attachments you are expecting from call recipients

---

[2] For more information on Zoom account multi-factor authentication visit: https://support.zoom.us/hc/en-us/articles/360038247071-Setting-up-and-using-two-factor-authentication

c. only allow remote control of the screen-sharing session from a call recipient you know and trust (note that this feature should not be used in a webinar scenario)

d. lock the session when everyone you were expecting to join the meeting has joined (at the bottom of the participants panel in the meeting, click "More" and then "Lock Meeting").

19. More information about Zoom host controls can be found here: https://support.zoom.us/hc/en-us/articles/201362603-What-Are-the-Host-Controls-.

Need more advice on information security?

20. For further information about Government use of Zoom, or any other information security matter, please email us at: info@ncsc.govt.nz.