Zoom and Security

CCSQ Data Guardian

10 April 2020

How To Make Your Zoom Teleconferences More Secure

The Zoom teleconferencing platform offers a myriad of benefits to those who have to work from home during this period of time. As with any tool, it is important to be aware of the possible risks, and use the functions available to you on the platform to communicate safely.

Zoom: not all doom and gloom!

There have been a host of vulnerabilities reported with Zoom. Many have been fixed or are being fixed, but protection against other threats relies on meeting hosts following sound security practices. Here are some of the main issues with Zoom, and advice on how to deal with them.

Zoombombing

Zoombombing is the number one threat, a technique whereby the “bomber” obtains the ID of an open meeting through phishing or other means – including use of Internet search programs like zWardial – and joins the meeting without authorization. Once in the meeting, bombers have been seen to display obscene and other unpleasant images on their screen, and to interrupt the meeting shouting objectionable insults and slogans. There are even bad guys out there planning Zoomraids – a term for coordinated, mass Zoombombers accessing a meeting, compounding the disruption through the sheer number of attackers. Of course, attackers may just be interested in listening to your meeting and stealing your information.

How To Protect Against Zoombombing

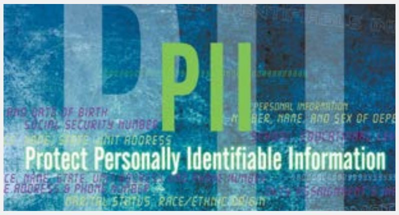
The issue here is that hosts have made invitations open to all who can find the Meeting ID, and can therefore enter the session without authorization. There are several steps[1] that hosts can take to prevent this by proper configuration of your meetings:

[1] Options marked with an asterisk require you to go to your Meetings settings on the web.

Questions!

Your IT Support should be your first port of call.

Useful information can be found on Zoom's Blog: Https://blog.zoom.us


PII
Protect Personally Identifiable Information
DATE OF BIRTH
SOCIAL SECURITY NUMBER
PERSONAL INFORMATION
NUMBER, NAME, AND SEX OF DEPENDENTS
MARITAL STATUS, RACE/ETHNIC ORIGIN

1. Generate the Meeting ID automatically. This is set by default in Zoom so don't disable the option and set your own Personal Meeting ID, which will often be easier to guess.

2. Require a login password. Zoombombing happens when an attacker obtains the meeting ID , and no password has been set. Hosts should generate and allocate their own unique password for each meeting. The password can be a mixture of letters and numbers. If you can, use a password generator to ensure you have a complex one.

3. Use the Waiting Room feature. This automatically turns off the facility for others to join the meeting before you, the host. It might seem a bit tedious to have to confirm each participant one by one to join the meeting, but it does mean you will be allowing in only legitimate attendees.

4. Mute participants upon entry – you can unmute attendees when they need to speak or when you are satisfied that only authorized folks are in the meeting.

5. Disable video by default for hosts and participants, Again, you can allow users to display video after the meeting has started.*

6. Screen sharing should be on, but initially for the host only, unless you are sure you know all the participants.*

Following these practices should eliminate the threat of Zoombombing completely.

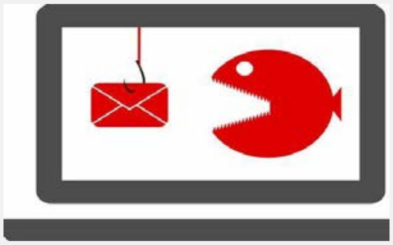
Some General Guidance

There are a number of potentially useful features of Zoom that bring with them their own risks:

- Do you need to really need to record the meeting? If you or other participants are going to display sensitive information – e.g. Personally Identifiable Information (PII), Personal Health Information (PHI) or private contract information – it may be better not to record.

- Don't assume that what happens in Zoom stays in Zoom. You have the option of saving recordings to a local computer, to Zoom's cloud, or to a shared platform on an information sharing cloud that may be open to other parties. Sharing to the cloud, either Zoom's or another instance, is problematic in that it may allow others to access your recording. A recent report found that a lot of

For update information, sign in to the Zoom desktop client, click on your profile picture at the top right of the screen (may just have an initial) and click Check for Updates

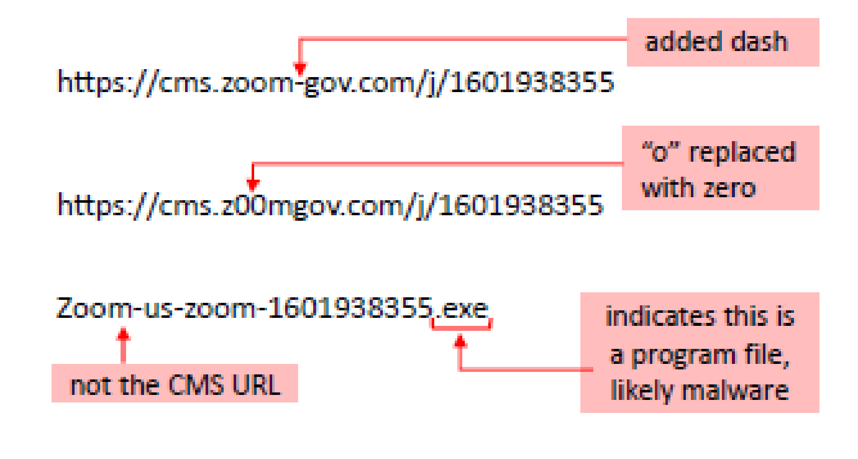


meeting recordings were open to search on the Internet and, therefore, available to anyone.

- Check regularly whether your Zoom client needs to be updated. And update it!

Phishing: A Continuing Threat

As you might expect, during this time of home working and the increased use of teleconferencing facilities, the delivery of fake Zoom invitations via phishing is growing exponentially. Hackers are using fake Zoom links to trick people into downloading malware to steal data, lock up your computer or compromise CMS and contractor networks. Hackers can create countless fake links and file names using any combination of keyboard characters. All will look different from a legitimate link, often just slightly. Here are a few CMS-related examples (NB. While these are CMS-focused, the same techniques may be used against you and your corporate networks):

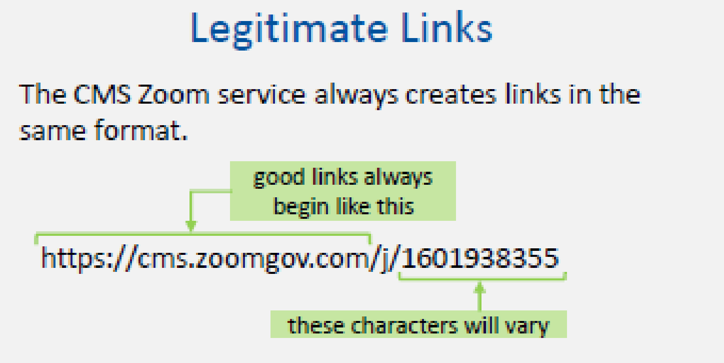


https://cms.zoom-gov.com/j/1601938355

https://cms.z00mgov.com/j/1601938355

Zoom-us-zoom-1601938355.exe

Legitimate links will look like this:



Legitimate Links

The CMS Zoom service always creates links in the same format.

https://cms.zoomgov.com/j/1601938355