

Founded in 2011, Zoom is one the world's leading video conferencing software providers. It has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and





What parents need to know about



ZOOM BOMBING

RISK OF PHISHING

PRIVACY CONCERNS

LIVE RECORDINGS

PRIVATE ZOOM MEETINGS

'LIVE STREAMING' RISKS





Safety Tips For Parents





REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel ancomfortable or upset then they need to talk about it and report it. Parents can report unwented activity, heteomery, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see repetition for accountable.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and Sessitively to be hacked. It's important to never share meeting IDs with anybody you don't know and always set-up a password function to allow other people to sign-in.

This should already be a default setting that is applied on Zoom.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number, etc. Create your child's account under a fabe name or pseudonym and always set a custom background to help hide details in your home. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not freedulent. Signs of a phishing small include an unrecognizable email address, an unofficial demain name or a slightly distorted logo. The email itself might also be poorly written or contain countries a star-horsest. 0



TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can furn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chats can feelp to limit the risk of receiving any malicious attachments or receiving any inappropriate messages in addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE VIRTUAL WAITING ROOM FEATURE

The realting room feature on Zoom means that anybothy who wants to join a meeting or live session carned automatically join and must wait for the host to screen them before entering. This is now a default function and adds another layer of

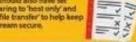
KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest wersion of Zoom available and always update it if you get a prompt. These updates are usually to fix security holes and without the update you will be more valuerable to an attack. Check the efficial website to see what the latest version is and

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then its important to make sure that the host is abiding by Zocen's Terms of Service, This includes the fact that they have gained everybody's permission for the session to be recorded.

The host should also have set screan sharing to host only and disabled file transfer to help keep the five stream secure.



Meet our expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.





SOURCES: https://icoom.uc/privacy | https://icoom.au/ | https://icoom.au/ https://icoom.au/ https://icoom.uc/privacy | https://icoom.au/ https://www.theguardian.com/technology/2020/apr/02/2coom-technology-security-coronavirus-video-conferencing



www nationalonlinesafety com

Twitter - @natonlinesafety

Facebook - / National Online Safety Instagram - @ National Online Safety