



April 4, 2020

Dear CFC Family,

Blessings to all! Our prayer goes to all families and we hope that everyone is safe and in good health. While our community of Couples for Christ and the world is under order to remain in their homes for the foreseeable future, teleconferencing tools like Zoom provide a vital opportunity to conduct meetings, business and continue education remotely, but it has rapidly become apparent maybe opening users up to new security risks.

Video conferencing surged in March as nonessential businesses across the country to help prevent the spread of COVID-19. The sudden expansion has revealed some unexpected security and privacy concerns and has given rise to a new phenomenon called "Zoom-bombing" as resourceful "trolls" find their way into meetings to interfere and bring fear to users.

In the last couple of weeks, widely reported Zoom-bombing cases have ranged from distasteful but harmless pranks to more troubling disruptions involving racism, sexual harassment, and revealing the identities of Alcoholics Anonymous members. Cyber security cases like this could be avoided if host choose **to require a password**.

People must not just jump in right away because it is easy and friendly to use. Be careful and take slower steps to adopt the platform. Read the documentation, and make sure your settings are correct. The big thing is to **avoid making meetings on public, and to keep links to meetings as private as possible by selecting private as an option**.

Many casual users, Zoom-bombing poses minimal personal risk. A troll interrupting a class or a meeting can be annoying and offensive, those conducting more sensitive meetings via videoconference must be more careful because an unknown entity listening in could present a serious threat. With social distancing guidelines, shelter in place and lockdown likely keeping people at home for at least another month, Zoom with the latest cybercrime exposed announced several steps the company is taking to reassure and protect users, including conducting a comprehensive third-party review of security and holding weekly webinars to update the community.

Zoom has deactivated some features that sparked controversy, including one that it said inadvertently shared user data with Facebook. It is also highlighting tools already available that can limit unwanted intrusions like waiting rooms, passwords, muting controls, and limiting screen sharing. To credit, Zoom has done an admirable job of recognizing its flaws and working to address them, particularly compared to other online and app technology companies that have neglected privacy complaints. Zoom has really leaned forward to communicate their understanding of the issues and the effort they are doing to close the gaps to fix the problem.

To note, as other companies also have experienced different forms and ways of cybercrimes, consumers must be vigilant and proactive to protect their privacy at home and business as there are always vulnerabilities in every software package developed, and new vulnerabilities are always being found after the older ones are detected and fixed but not necessarily terminated.

As Zoom and other online platforms works to tighten security and privacy protections on its end, there are also actions users of its service and other videoconferencing programs can take to defend themselves against cybercrimes. Please see attached TIPS to take in consideration to help prevent future cybercrimes not only "Zoom-Bombing".

There are also more secure services that are out there, but they can be less user-friendly and much more expensive like Microsoft Teams and Cisco's WebEx. Please check if these options will be worth to invest on.

As a final note and a friendly reminder, please be reminded of the two immediate protocols to do. **For host to require a password to all attendees. Secondly, Select PRIVATE as an option for meeting. Avoid making meetings on public, and to keep links to meetings as private as possible. Lastly, avoid posting meeting links in your social media platforms.**

God bless the world and God bless Couples for Christ!

Thank you,  
NITT USA