Zoom's Security Flaws: How Churches Can Respond

Other options for connecting and what to do if you continue using this popular online meeting tool.

Nick Nicholaou, Church IT Consultant

FImage: Alistair Berg | Getty Images

Most organizations were a bit unprepared for the increased remote work forced on us by the current pandemic. Churches and ministries are communication-focused, and most organizations are letting staff use communication tools they normally might not work with.

Church IT experts Nick Nicholaou and Jonathan Smith discuss some simple approaches for communicating online with church staff and with the entire congregation.

Many people are using Zoom, but this online meeting tool has a reputation for poor security. Is it valid? And if you want to use Zoom anyway, how should you?

Why is Zoom so controversial?

Zoom has had a number of security vulnerabilities come to light—including password breaches, takeover of webcams, data mining, multiple security flaws, and uninvited people joining meetings and doing unwelcome things on camera. Even federal law enforcement has recommended not using it.

But many of its users don't care! Zoom is fun and easy! So much so that those responsible for running churches and ministries are having a hard time reining in its use.

What to use instead of Zoom

There are better solutions than Zoom. Solutions that don't come with security warnings! Here's what I recommend and why:

- *FaceTime*. It is free, secure, easy, and fun, but it only works on Apple devices (which is why it is secure—Apple strongly controls their ecosystem). The downside is that everyone has to have an Apple device to participate, and that's often not the case.

- *Microsoft Teams*. Anyone with an Office 365 account has free access to Teams. It is secure and easy to use—you can create a meeting in Outlook and send it to everyone you want in the meeting, and they'll be able to join easily. It is free, even to those without Office 365 accounts.

- *GoToMeeting*. Secure and pretty easy to use. It is free for 30 days.

Zoom usage recommendations

Our organization does not recommend Zoom because of its many security vulnerabilities but is allowing it until we select an organization-wide solution.

If you have decided to use—or let team members use—Zoom, I recommend you communicate the following to each participant in advance of their next Zoom meeting:

- When setting up a Zoom meeting, use the password and waiting room options, and *do not* post your meeting invite details or meeting screenshots online.

- *Do not* use a user ID and password combination you use for any other website, database, etc. Make certain your user ID and password in Zoom are unique to your Zoom account. Doing so will ensure that if Zoom's user base gets hacked again, you won't be vulnerable.

    - While in a Zoom call, please *do not* talk about:
        - Any financial specifics (your financial institutions, account numbers, etc.);
        - Family structures and names, ages, etc.—nor the schools your children attend.
        - Missionaries or pastors of churches in closed countries; or
        - Anything else you would not want to be made public.

That may seem like overkill but is appropriate.

Adapted from an article that first appeared in MinistryTech *magazine. Used with permission from the author.*