TRINUS
stress-free IT

You've Been ZoomBombed!

Some Interesting Video Conferencing Information as You Work Remotely

As we enter our third week of the new COVID-19 Work Paradigm for many of us, I want to make you aware of some limitations and pitfalls of Video Conferencing, as well as some tips for making remote conference calls more pleasant and productive.

Video Conferencing & Meetings - What Software to Use

We've had an explosion of client requests for video conferencing and remote meetings, as most of their staff members transition to working-from-home. We're doing the same thing ourselves, so it's appropriate to offer some perspective and advice on the subject.

There are several applications that offer video conferencing capabilities. But just like other software, there are business class applications, and ones designed for very casual or home use.

Best of Breed - especially for slightly larger organizations and municipalities - is **Microsoft Teams**. We've highlighted Teams many times before; it has built-in advantages for **work collaboration, messaging, organizing staff into teams** (groups), as well as robust **video/audio conferencing**.

Other applications that offer video conferencing are **Zoom, GoTo Meeting** and **Skype**. All fall into the (very) small business or home user category. These applications focus on video conferencing, and for the most part, they perform well. However, don't expect to collaboratively share files, message users, share calendars, or organize your staff into business groups. They're also more prone to Cyber Security problems.

As an example, I asked our ***Cyber Security Supervisor, Karl,*** to look specifically into the **Zoom** app, as it seems to be receiving most of the attention recently. He discovered something disturbing:

Right now, the biggest issue with Zoom is their Privacy Policy. It's strange, to say the least. They're allowed to collect "customer content", which means anything and everything that goes on in a meeting (shared files, video, audio, all of it.) They also empower the meeting's host to be able to do the same thing without notifying participants.

The encryption of the audio and video streams, while strongly implied by Zoom as being end-to-end, is less robust than users are led to believe, and it allows Zoom access to the information in the data stream. This means that ANY content shared during a meeting, including captured video, audio, shared files, or screen shots can be used by Zoom and/or the meeting host. Zoom is a US-based company, so this can present **major problems for organizations subject to Canadian Privacy and Information Security Laws**.

Karl goes on to say: ***During a meeting, if you use the private message function to communicate with someone else in the meeting (anyone), those messages can be seen when the chat is downloaded in the minutes folder after the meeting is over.*** Thus, Private messaging isn't private.

There are additional reports of Zoom meetings being hijacked (***ZoomBombed***), as hackers trolling for online video meetings use common techniques to take over moderator functions and disrupt the meeting with inappropriate content. The FBI reported they have ***"received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language."*** Most of this is preventable, but default settings for a Zoom meeting make it easy to be hijacked.

Still, other hackers are registering domain names that contain the word ***Zoom*** - or something similar - to catch unsuspecting persons, by re-directing them to a bogus website that contains malware. While the fake site appears to be a legitimate Zoom website, it downloads malware instead of the Zoom video conferencing software.

Finally, there is the matter of the Zoom business model. By offering a free version (with restrictions), Zoom are relying on harvesting user information to sell to advertisers, which potentially increases your exposure to SPAM. If you opt for the paid version without restrictions, you're equal in cost to a fully featured Microsoft Office 365 license with Teams, but Zoom are still harvesting your information.

GoTo Meeting, Skype, and others have their own issues to deal with, but I think you get the point.

Meeting Etiquette

If you're having a short meeting between you and one other work colleague, then the default settings for any meeting are enough. But as the number of users grow, some rules pertaining to the technology will go a long way in enhancing the experience for everyone - and helping the meeting to run faster.

Audio Headsets for everyone are a MUST-HAVE addition for any meeting with more than three participants. Laptop MIC's and those built into webcams, have poor fidelity, and inject a lot of noise into the meeting. This problem magnifies with more users. Users should test the MIC prior to entering the meeting and adjust the MIC level for the mid-scale on the sound level meter built into the software or computer; too soft, then no one can hear you - too loud and it will induce unwanted background noise and distortion. Headsets also produce a more consistent sound level, as the MIC is always at a fixed distance away from the speaker's mouth.

Participants should reduce the background noise in their room as much as possible. Turn off fans, heaters, radios, and other media devices. Mute your phone and notification ringer. Clear pets out of the room and close office doors.

Participants need to know how and when to mute their MIC. All meeting software has a mute function, but each person should control their own and not rely on the moderator to control mute functions. Depending on the meeting type and content, the moderator may ask - or force - all MIC's to be muted, when entering the meeting.

Video should be used only when required, as it takes additional Internet bandwidth, and could lead to an unstable meeting for everyone. If you require video, make sure the lighting is adequate. Avoid excessive lighting behind you, such as open window blinds, as it blacks-out the participant's face. Place a small desk lamp right in front of you - and to the side out of camera range - and turn it to a low setting. Overhead lighting will also work well. Video should be tested, and the camera zoom adjusted to produce a head-and-shoulders view of the participant. If possible, place the webcam at shoulder height, to reduce the ***from-the-grave*** look and excessive shadows. You might also pay attention to the background image and dress: offensive or highly personal images, bright contrasting colours, wall-art, and shiny objects reflecting light, can distract from a business-like image, as can your pajamas.

Finally, avoid excessive movements and look at the camera when speaking or being spoken to. Have a notepad off to the side to record important information from the meeting, as typing on your laptop keyboard while on camera is noisy and distracting; I've seen too many finger and knuckle closeups.

We are all learning from the new experience of remote computing and video conferencing. I do suspect many of us will be using these new-found tools and skills long after COVID-19 has faded from memory, so we are best served by doing it properly from the start.

Please let me or your Account Manager know if you would like more information about ***stress-free*** Video Conferencing.

Thanks.

Dave White
TRINUS
stress-free IT
dwhite@trinustech.com
trinustech.com

Did you find this page through Social Media?

Join Our Mailing List!

If you are having troubles viewing this email, please contact us.

TRINUS Technologies
#110, 3806 - 49th Avenue
Stony Plain, Alberta T7Z 2J7
Phone: (780) 968-1333
Toll Free: 1-877-489-9985