Office of the Chief Information Security Officer

Virtual Collaboration Tools Security Tips

How to Securely Work and Learn Remotely

As more people are working and learning remotely, many are turning to virtual collaboration tools such as WebEx, Zoom, and Teams to share video, audio, and screen content.

A nationwide trend of disruption or hijacking these meetings, sometimes called "Zoom-bombing" is emerging. Individuals scheduling, hosting, and attending meetings using these tools should remain cyber aware to protect their content and meeting. DIR recommends the following:

CONNECT WITH CARE, BE CYBER AWARE

Secure

- Use your organization's provided services and devices.
- Require participants to enter an access code.
- Avoid reusing access codes or meeting pins.
- Use a privacy shield or cover over your webcam when it is not in use.
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting.

Share

- Avoid adding your meeting to any public calendars or posting it on social media.
- Distribute the meeting link and access code directly to the intended participants.
- Remind invited guests not to share the access code.
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information.

Manage

- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing.
- Muting users on entry can prevent potential disruptions.
- Prevent users from sharing video by default; allow video sharing only when necessary.
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting.
- Do not trust the safety of links shared in meeting chats.

Always follow your organization's policies addressing virtual meetings, information security, and records retention.

STOP

Be Aware of Potential Disruptions!

Scammers and disruptors are targeting and "hijacking" unsecured online meetings.

It is tempting to share screenshots of coworkers collaborating, but you may unintentionally share the meeting ID or session details, which provides potential disruptors uninvited access to your meeting.

Case Study: In late March 2020, a high school reported that while a teacher was conducting an online class using a virtual collaboration tool, an unidentified individual joined the virtual classroom and yelled potentially upsetting phrases and caused a general disruption to the students learning.

Security Tips for Common Virtual Collaboration Tools

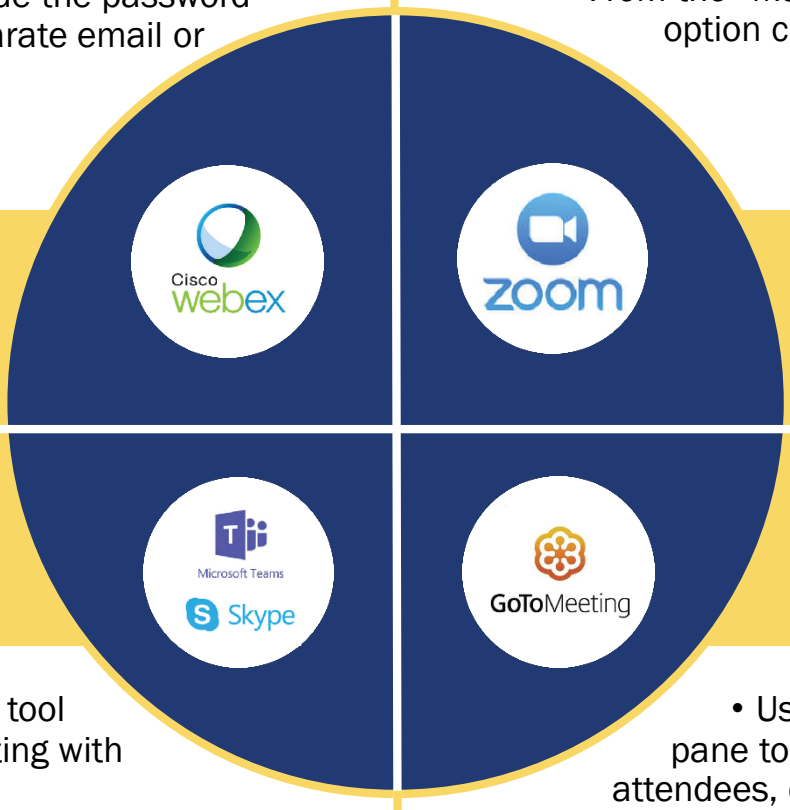
If you use a different system, please consult your IT department or the tool's help section for guidance.

WebEx

- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time.
- Do not allow attendees to "Join Before Host."
- Set up each meeting to require all attendees to enter a password.
  - Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting.
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone.

Zoom

- Make meetings "Private" by requiring a strong meeting password.
- Select the "Enable Waiting Room" option to control the admittance of guests.
- Before a meeting begins, set screen sharing to "Host Only."
- Check your workspace for unwanted objects, documents, or notes in view of attendees..
- Prevent unauthorized access by locking the meeting after all participants have joined. From the "Manage Participants" option click "Lock Meeting."



Teams/Skype

- Use the "Chat Pinning" tool to ensure you are chatting with the correct recipients.
- Understand that chat, channel, and files data are retained forever unless the system admin has actively modified retention policies.
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile.

GoToMeeting

- Use the "Attendee List" pane to view all meeting attendees, change their presenter rights, or revoke attendee privileges.
- When sharing content select "Show Only" to share the desired information from your computer. This selection will show an animated gray frame indicating what attendees will see if selected.
- Require attendees who join via telephone to enter their Audio PIN. This gives the organizer audio controls for each participant.
  - If users did not enter their audio PIN, right-click the person's name and select "Send Audio PIN".