Virtual Meeting Best Practices

With so many people working from home, webinars and conference calls have become the standard method for holding meetings or working collaboratively. But even though we have all become more security conscious when working online, we often overlook the security concerns of these virtual meetings. Given the current climate, it's helpful to take a step back and think about the platform itself as well as what is to be discussed when you are hosting an online meeting.

TABLE OF CONTENTS

Tips & Tricks

As the world adapts to working remotely, cyber criminals are also adapting. A new trend is emerging known as "zoom-bombing" where hackers take advantage of holes in collaboration tools. Below are some tips to get you started on securing your meeting space:

- Only use a platform supported by your organization to host your meeting. If you are unsure which platform to use, contact your agency help desk.
- Never share your moderator pin with anyone and only provide meeting passwords to attendees. If the topic is particularly sensitive, consider waiting until just before the meeting begins to share the pin. Be sure to take attendance before your meeting begins. Conferencing platforms often have a dashboard where the moderator can view everyone logged in. If there are users you do not recognize, consider removing them from the meeting.
- Consider using video. This will not only allow you another way to validate participants but will also give your meeting a more "personal" feeling. Particularly in a time when most users are remote, it can be nice to talk to someone "face to face" rather than just talking to a screen or phone.
- Don't record a meeting unless it's necessary. Keep in mind that many states (including Massachusetts) require that you notify all attendees that a meeting will be recorded.
- If you must record a meeting, consider removing the recording from the platform and encrypting, particularly when discussing confidential or restricted data.
- Disable features you do not need or like such as chat or screen sharing.
- When sharing screens, remind participants to hide sensitive information before doing so. Many applications will allow you to share parts of your screen only, such as just the word document you are discussing and not the spreadsheet containing financial data you also have open.

Commonly Used Collaboration Tools

As we try to navigate this challenging time and find our way to the “new normal”, conference calls and webinars can enable us to collaborate with our colleagues as if it’s just another day at the office. But as with all technologies, conferencing systems must be managed as to not expose any sensitive information or data.

WebEx (https://help.webex.com/en-us/v5rgi1/Cisco-Webex-Best-Practices-for-Secure-Meetings-Site-Administration)

- Schedule "unlisted" meetings. Unlisted meetings require participates to know the meeting number and password rather than displaying the meeting on the site's calendar.
- Require a meeting password. Refer to **our password guidance** (/guides/password-best-practices-and-recommendations) on suggestions for creating a strong password.
- Exclude the password from your meeting invite. Provide the password to participants in a separate email or over the phone.
- “Lock" your room once your team is on the line to prevent anyone else from joining.

Zoom (https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/)

- Require a meeting password.
- Create a "waiting room" for attendees. This will allow the host to admit participants to the meeting.
- Set screen sharing permissions to "host only".
- Only allow individuals with a given e-mail domain to join.
- Expel a participant or all participants.

GoToMeeting *(by LogMeIn)* (https://blog.gotomeeting.com/5-best-practices-staying-secure-gotomeeting/)

- Use the "Attendee List" to view all meeting participants. Through the attendee pane, the moderator can give or revoke additional rights such as chat features or screen sharing.
- Require users connecting through telephone to enter their audio pin. This allows the host to verify participants and control the audio (e.g. when a user is muted).

Microsoft Teams (https://support.office.com/en-us/article/manage-meetings-ba44d0fd-da3c-4541-a3eb-a868f5e2b137?ui=en-US&rs=en-US&ad=US)

- Note that many of the security and privacy settings are set by company administrators. This can simplify the process for hosts but also may mean some features are not available.
- Verify external participants in the waiting room before giving them access.
- Turn off incoming video for large meetings.
- Remember that files shared within the meeting and chats may be retained on servers indefinitely.

Contact

Cybersecurity and Enterprise Risk Management

Online

Cybersecurity questions: **CommonwealthCISO@mass.gov** (mailto:CommonwealthCISO@mass.gov)

Risk management questions: **ERM@mass.gov** (mailto:ERM@mass.gov)

Report cybersecurity or data breach: **eotss-soc@mass.gov** (mailto:eotss-soc@mass.gov)

Address

McCormack Building
1 Ashburton Place, 8th Floor
Boston, MA 02108

Directions (https://maps.google.com/?q=1+Ashburton+Place%2C+8th+Floor%2C+Boston%2C+MA+02108)

(/)

All Topics (/topics/massachusetts-topics)

Site Policies (/site-policies)

Public Records Requests (/topics/public-records-requests)