MBDH Events—Zoombombing

As we all have adopted the virtual event or workshop over the last few years, the Midwest Big Data Innovation Hub would like to provide some recommendations to make sure your Zoom event is as secure as possible for upcoming and future events. Although these items reference the Zoom meeting and Webinar web conferencing services, these recommendations may be updated in the future to reflect new ways of handling unwanted Zoom visitors, also known as “Zoombombing.”

**Obfuscation:**

Avoid making the URL easy to find through basic web searchers and making it prominent on advertisements. We recommend hiding the session's URL by creating a shortened URL to help disguise the Zoom link.

**Registration:**

Register attendees ahead of time to collect names and emails of all participants. Doing this allows for vetting of registrants before they receive the link to the session. Once approved, the registrant receives a link to join the session. We recommend for webinar hosts to uncheck the “Allow registrants to join from multiple devices” option to prevent disruptive attendees from using the link to make multiple connections.

**Authentication:**

Zoom offers the option of requiring authentication via <https://zoom.us>. This authentication allows for limited disruptive incidents.

**Waiting Room:**

Waiting rooms are suggested if registration is not required. The waiting rooms allow for vetting by the host and co-host. Hosts and co-hosts can admit attendees at their discretion. We highly recommend the Waiting Room feature to be used for all sessions, especially any session without registration.

**Telephone Calls:**

This feature allows users to dial in and make audio-only connections. We highly recommend collecting phone numbers at registration if you are going to allow attendees to dial in. Encourage attendees to download the Zoom app on their smartphones.

**Screen Sharing:**

This feature allows attendees to share content from their display. We recommend configuring the session such that only the host and co-host/panelist can share. We recommend configuring the session settings beforehand to select “only the user who is sharing can annotate” option on the session creator’s account settings. This will prevent display sharing from unwelcome guests.

**Recording:**

This feature records audio, video, and shared content. We recommend recording all sessions. In the event of a disruption, this can provide valuable information for the investigation. We also recommend displaying participants’ names in the recording to help identify disruptive attendees.

**How to respond to a disruptive event:**

The host should immediately end the session and notify all attendees who were there why the session was canceled. After a Zoom disruption of a discriminatory nature, the host institution should issue a statement detailing the event and the institution’s planned response.

**Report the incident:**

Report the disruptive behavior to your institution’s Offices of Diversity and Ethics and the Midwest Big Data Innovation Hub ([info@midwestbigdatahub.org](mailto:info@midwestbigdatahub.org)).