KEEPING VIRTUAL EVENTS FREE FROM HATE

MUSLIM ADVOCATES

TIPS & BEST PRACTICES

Over the last several weeks, an unprecedented number of meetings and events have taken place virtually as we continue to grapple with the realities of a global pandemic. While virtual events enable communities to stay connected during this time, the increase in online gatherings also comes with growing concerns about digital safety.

In just the last few weeks, a Muslim Student Association virtual meeting was attacked by a disrupter, a health forum organized by a Muslim public health organization was interrupted, and Jewish community events including funerals have been disrupted by racists and white supremacists.

As our community members and houses of worship prepare for virtual gatherings during Ramadan this year, we hope this guide will provide useful tips and best practices for securing your virtual events.

What type of platform should be used for our virtual events?

There is a wide range of platforms available for hosting events. Some platforms offer both a meeting function, where participants can interact with one another, and a webinar or broadcast function, where participants listen to one or more presenters. Unless your event requires significant interaction from participants, consider structuring your events as webinars to minimize security breaches. Regardless of which platform you choose, we recommend reviewing and becoming familiar with the security features available.

BEST PRACTICES FOR SECURING VIRTUAL EVENTS

Require registration

Rather than hosting a public event that is open to everyone, ask participants to register in advance. A simple registration process that requires registrants to share their names and contact information not only gives institutions the opportunity to review and vet the participant list, it also serves as a deterrent for bad actors intending to disrupt an event.

Limit access to event links

Take steps to ensure that URLs or links to your meetings or events are not posted publicly, and instead are shared only with those who register to participate. When possible, make events password protected and send out the password shortly before the event starts.

This document is for informational purposes only and should not be interpreted as legal or IT advice. The information is not a substitute for expert legal or other professional advice tailored to your specific circumstances.

Continued on next page.

Create unique event links

Create unique links or meeting IDs for each individual event rather than repeatedly using the same one for multiple events. This measure adds a layer of security—any potential bad actors or disruptors who gained access to links from previous events will be unable to use the same link over and over again.

Enhance restrictions for public events

If events must remain open to the public, consider turning off features that allow participants to speak, share screens, customize their background, rename themselves, annotate or chat/comment during the event.

Assign a host or co-host

Assign at least one host for the event who can monitor any potential disruptions and immediately engage security controls and features as needed. Consider assigning more than one host for larger events.

Enable security controls and features

Ensure a thorough review of all security controls and features on the platform before an event begins. Consider turning on or enabling as many features as possible to increase security, and remember that these features can be adjusted throughout the event. Make sure that you have the latest version of whichever platform you are using, so that all security features are current.

Prepare for disruptions

Hope for the best, expect the worst. Always have a plan for what to do if your event is disrupted.

What steps should we take if our virtual event is disrupted?

- **Assign** individuals on the host team responsible for enabling and disabling features throughout the event.
- **Document** any disruption as best as possible through recording features on the platform or taking screenshots of any offensive comments or chats.
- **Lock** or stop the event as quickly as possible while the disruption continues. This includes turning off any live stream to social platforms, if applicable.
- **Report** disruptions to the platform and consider sharing with law enforcement as well. Here is more information from the U. S. Department of Justice about reporting these types of incidents to local or federal law enforcement officials.

Additional Resources

How to keep uninvited guests out of your Zoom event
Cisco Webex Best Practices for Secure Meetings
Best Practices for Safe and Secure Meetings with AnyMeeting

For more information/questions, contact Madihha Ahussain at madihha@muslimadvocates.org

This document is for informational purposes only and should not be interpreted as legal or IT advice. The information is not a substitute for expert legal or other professional advice tailored to your specific circumstances.

MUSLIM
ADVOCATES