KPMG

Cybersecurity during Covid-19

Cybersecurity hygiene for audio and video conferencing

May 2020

Covid-19 measures are causing organizations to turn to video conferencing applications for remote working. Good cybersecurity hygiene can help keep out unwanted attendees, protect your employees and secure your data.

Require passwords for all meetings

Meeting IDs can be guessed, allowing unauthorized attendees to join even if they have not received an invite. Never share meeting IDs on public (including social media) unless you intend the meeting to be open to all. Set a meeting password, which can be communicated by other channels, to limit access.

The chairperson joins first

The chairperson or host of the conference should control admittance. Use the "waiting room" feature to manage those requesting to join and challenge unknown attendees before starting the conference.

Lock calls after everyone joins

Once invited attendees have joined, lock the meeting to keep out unknown attendees.

Be wary of unknown phone numbers

Beware of attendees dialing in from unknown phone numbers. Ask them to confirm their identity and expel them from the call if they refuse to do so. Check whether your conferencing application enforces passwords when dialing in.

Set up alerts when meetings are forwarded

Establish alerts, so you know when meeting invites are forwarded over email to others; check any secondary invitees are legitimate and challenge the forwarding of the invite if not. If necessary, schedule a new meeting with new dial-in details.

Limit file sharing in the chat

Restrict file sharing in the message column of a conference call, so that any unknown attendees aren't able to receive and open private documents, or send malware disguised as an attachment to other attendees of the call.

Prevent the recording of meetings

Block any attendees except for the chairperson or host from recording the meeting, or set up alerts to identify which attendee has started recording.

Use a business or enterprise license

Your employees need access to effective collaboration tools. Consider buying an enterprise license that allows you greater control over employee use, and helps ensure that default settings are secure and meet privacy needs.

Be a great listener

Make sure that every attendee speaks at the start of the call, maybe even on video. It helps deal with isolation and identifies unknown attendees.

Contacts

Tariq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/sa