BlueOrange Alert:

Teleconference Hijacking

In response to the COVID-19 pandemic, there has been a significant increase in the number of organizations and educational districts relying on video-teleconferencing (VTC) solutions to facilitate remote work and learning, including Zoom. Unfortunately, there has also recently been an increase in instances of uninvited users hijacking or crashing these online meetings, often referred to as "Zoom-bombing". While this activity most often appears intended to simply disrupt the video conference and upset the invited participants with offensive video or audio, there is the potential for an uninvited user to attempt to go unnoticed in the conference and access restricted information.

Most of these hijacking/intrusion incidents appear not to be due to underling security flaws in the Zoom application, but rather a lack of sufficient configuration of the application's privacy settings. If a Zoom meeting is set to the "Public" level of availability, anyone that locates the meeting's "zoom.us" address can click the link and join the meeting. As malicious actors find these meeting addresses, they are typically sharing them on dedicated forums. While websites like Reddit have worked to remove these forums and lists, the incidents have continued to occur.

Here are a few steps to help you properly configure and share your Zoom meeting information with invited users:

- Do not share meeting links publicly. Your organization and your users should never post internal Zoom meeting information on social media such as Facebook or Twitter. Meeting links should only be distributed through a private internal method such as email and should restrict attendees to only those users who are logged in to Zoom using their organization email address. Internal meeting invitations should not be forwarded to any unauthorized parties.
- Set your Zoom meetings to the "Private" setting. The minor inconvenience of intended participants having to enter a password is preferable to having uninvited parties accessing the meeting.
- Meetings should not be set up with a user's Personal Meeting ID (PMI), which is a static credential that can carry over from meeting to meeting. While Zoom may prompt for this ID to start an "instant" meeting, opting to create a "scheduled" meeting will generate a one-time meeting ID, significantly reducing the risk of future misuse.
- Restrict video sharing in your meetings. If the meeting host will be the only user expected to share video, change the screen-sharing setting for the meeting to "Host Only."
- Utilize the "Waiting Room" feature to hold invited users from joining the meeting until the host has approved them.
- Ensure that your organization's users are using the most up-to-date version of the Zoom application.
- Ensure that your organization's telework policy or guidelines address your requirements for physical and information security.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.