CMSD ALL
Excellence for ALL
OPPORTUNITY | EQUITY | SUCCESS

Cyber Security Internet Safety

GUIDELINES FOR EDUCATORS

As we increasingly use video conferencing for meetings and for remote education, cyber intrusion and crime has also increased, targeting video conferencing technologies and their users. As we approach the first quarter in a Remote Learning environment, we can expect to see the kind of activity that some of educators have already experienced. It is therefore important that you have these guidelines to prepare for and to manage any unwanted visitors to your parent, staff or classroom meetings.

- **Meeting "Bombing" –** In this type of attack, an uninvited guest joins a video conferencing meeting either to listen in on the conversation or to disrupt the meeting by sharing inappropriate media. These incidents are possible when:
  - you do not require a password.
  - the attacker is able to discover or guess the meeting ID, known as "war dialing."
- **Malicious Links in Chat –** Once attackers gain access to your meeting room, they can trick participants into clicking on malicious links shared via the chat, allowing attackers to steal credentials. This reinforces that it's more critical than ever to require passwords for all meetings.

How to avoid being "bombed" or hacked during a virtual class or meeting

- The recommended platform for remote learning is through Microsoft Teams. Cyber Security and IT Risk Management through an Enterprise license control the security of teams.
- In April, The State Department sent an email to employees saying that the free version of Zoom "is not authorized for the conduct of official business or on official Department devices used to access the OpenNet" (Internet). Additionally, the FBI has warned Zoom users of how vulnerable it is to hacking.
- If an educator uses a personal Zoom account to host virtual classes at the District level, security settings cannot be enforced. Educators can implement security settings at the user level.

Zoom Security Settings

1. Turn on your Waiting Room
One of the best ways to secure your meeting is to turn on Zoom's Waiting Room feature, which provides a virtual waiting room for your attendees and allows you to admit individual meeting participants at your discretion.

2. Manage Screen Sharing
To prevent participants from screen sharing during a call, using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options. Under "Who can share?" choose "Only Host" and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.

3. Mute participants
Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting or inappropriate noise from other participants. Enable 'Mute Upon Entry' in your settings.

4. Turn Off File Transfer
In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

5. Disable Private Chat
Zoom has in-meeting chat for everyone, or participants can message each other privately. Restrict participants' ability to chat amongst one another while your event is going on to cut back on distractions. This is to prevent anyone from getting unwanted messages during the meeting.

6. Turn Off Annotation
Like screen sharing and in-meeting chat, annotation can be a great tool when you need it, but it can also be an opportunity for mischief when you don't. To avoid unwanted annotation, Zoom allows you as the meeting host to remove all participants' ability to annotate during a screen share. Disable this for the entire meeting, or just temporarily.

7. Don't Use Personal Meeting ID for Public Meetings
Your Personal Meeting ID (PMI) is the default meeting that launches when you start an ad hoc meeting. Your PMI doesn't change unless you change it yourself, which makes it very useful if people need a way to reach you. For public meetings, you should always schedule new meetings with randomly generated meetings IDs so that only invited attendees will know how to join your meeting. Turn off your PMI when starting an instant meeting in your profile setting.

8. Require a Passcode to Join
Take meeting security even further by requiring a passcode to join your meetings. This feature can be applied to your Personal Meeting ID, so only those with the passcode will be able to reach you, and to newly scheduled meetings.

9. Make Someone a Co-Host
Promote a trusted meeting attendee to Co-Host, allowing them many of the same privileges and control features available to the meeting host themselves.

10. Join Before Host
Do not allow others to join a meeting before you, as the host, have arrived.

11. Lock the Meeting
When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the Lock Meeting button.

12. Remove Unwanted Participants
From the Participants menu, hover your mouse over a participant's name; several options will appear. Click 'Remove' to exit a participant from the meeting.

What you should do if your meeting is hacked

- Take a screenshot of the disruptive behavior; then shut down the video conferencing (class) immediately.
- Call 216.838.0440 to report the incident immediately to the Cyber Security and IT Risk Management Department or email a message to CyberITSecurity@clevelandmetroschools.org
- Report the incident to the FBI Internet Crime Complaint Center (IC3). Provide a detailed description of the incident and how you were victimized.
- If you or someone within your meeting clicked on a phishing link in the chat, immediately inform the Cyber Security and IT Risk Management department.
- Cyber Security and IT Risk Management will request a meeting via Teams to review the security settings of the video conferencing platform with the teacher.
- If you see something concerning in the home environment of a student while on a video conference report it to the proper authority.

In a separate guidance document, parents and students have been advised to:

- refrain from commenting in a chat or from clicking on any links.
- leave the meeting (class) immediately.
- to log onto their District Email (Office 365) and wait for further instruction from their teacher.

How to Support Students in Internet Etiquette

1. **Teach Digital Citizenship.** If you have not joined the professional learning group on Teams titled Digital Citizenship Resources, send an email message to Sec.Admin@ClevleandMetroSchools.org requesting access. The Teams group has several resources to assist in educating your students.
2. **Connect with families & caregivers.** Encourage caregivers to stay involved in their students' online lives by asking questions, being open with their children and monitoring their online activity. It is the caregiver's decision how they raise their children, but teachers can share what they know and are seeing.
3. **Empower Student Leaders.** Educators can help. Students should be empowered to be leaders who stand against mean online behavior. Encourage students to report abuses, stand against bullies and comfort those who are attacked. Anti-bullying groups and organizations are helpful and should be encouraged, but the greatest impact comes when students feel empowered to stand against bullying in their own social circles.