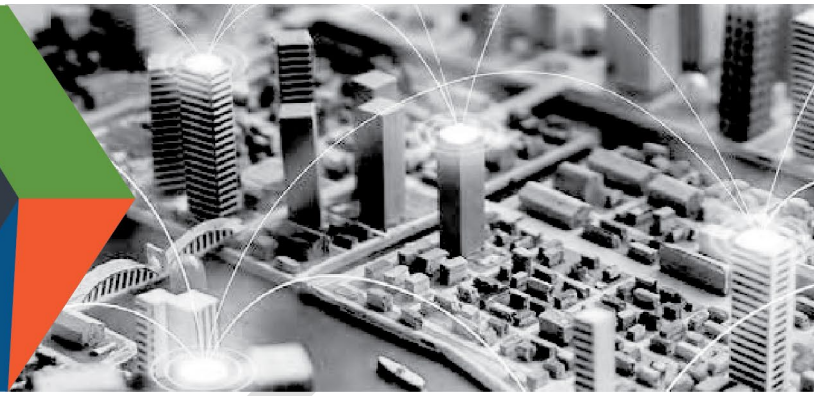
CISA
CYBER+INFRASTRUCTURE
DEFEND TODAY, SECURE TOMORROW



CYBERSECURITY RECOMMENDATIONS FOR K-12 SCHOOLS USING VIDEO CONFERENCING TOOLS AND ONLINE PLATFORMS

This videoconferencing product is for school district and campus IT administrators and staff charged with securing their IT networks, as well as end users such as teachers to help them think through cybersecurity issues.

RAPID INCREASE IN ADOPTION AND DEPLOYMENT OF VIDEO CONFERENCING

K-12 school districts are increasingly incorporating distance learning tools as a means of delivering curricula. Advances in information technology as the increased availability of video conferencing software and video conferencing capabilities incorporated into other products have rapidly made distance learning more feasible. However, schools and school districts must balance the convenience, usability, speed, and stability of these platforms with increasing risks to both school IT networks and individual users.

The following advisory guidance is intended to support the incorporation of cybersecurity considerations when adopting or expanding the use of video conferencing software and related collaboration tools. The guidance also includes recommendations for other school staff using these tools to host and attend meetings—information that is particularly critical as schools increasingly broadcast sensitive discussions over these platforms.

As the authority for providing information and risk management support to secure IT systems, including distance learning, the **Cybersecurity and Infrastructure Security Agency (CISA)** established this product line with cybersecurity principles and practices for more secure video conferencing. We plan to continue refining it and consider releasing additional products related to the secure use of online collaboration tools and video conference solutions to further support the ongoing efforts of cybersecurity leaders during this period of increased reliance on distance learning. Please send your feedback to CyberLiaison@cisa.dhs.gov.

POTENTIAL THREAT VECTORS

Cyber adversaries, from nation-state actors to insiders and criminal organizations, seek to acquire information on research and development, critical infrastructure, and personally identifiable information. Additionally, some actors, seek to disrupt the operations of American institutions and misuse systems for politically motivated causes. Some tactics include cyber actors:

- Actively exploiting unpatched vulnerabilities in client software to gain access to organizational networks and carry out cyber exploitation and cyberattacks;

- Exploiting communication tools to:
    - Take users offline by overloading services, or
    - Eavesdropping on meetings or conference calls;
- Hijacking video-teleconferences by inserting pornographic images, hate images, or threatening language;
- Compromising applications (used in some distance learning solutions to enable screen sharing for collaboration and presentations) to infiltrate other shared applications; and
- Attempting to penetrate sensitive meetings by using social engineering to deceive individuals into divulging information (e.g., meeting links) or by inferring meeting links from other links that use a common structure (e.g., school_name_YYYY_MM_DD).

Some video conferencing products may unintentionally expose information to nefarious cyber actors. For example, some of these products may share or sell customer information to third parties or target users to integrate product use with their personal social media accounts. This data sharing can unintentionally expose student and school information beyond intended recipients.

RECOMMENDED SECURITY PRACTICES FOR K-12 ORGANIZATIONS

1. Assess your organizational needs and determine the appropriate product to use for your institution or district. Also consider the mission need for your institution or district to collaborate with outside entities. Examine supply chain concerns (e.g., vendor reputation, data center locations) and whether the service under consideration addresses your institution's or district's other security, legal, and privacy requirements.
2. Establish an organizational distance learning and/or virtual meeting policy or recirculate the policies if they already exist. Ensure that your organization's remote work and distance learning policies or guides address requirements for physical and information security. Ensure updated guidance is continuously available. Develop easy to understand (e.g. one-page) summaries of policies applicable to distance learning and/or virtual meetings that are easily digestible by end users (e.g. teachers, students, and parents).
3. Limit and minimize the number of collaboration tools authorized for use by the organization to reduce the attack surface and the overall amount of vulnerabilities. Develop a list of approved collaboration and videoconferencing tools for your organization. Review and update security settings continuously. (In managed environments: Scan for and remove all unauthorized collaboration tools and associated clients from managed devices. Centrally manage authorized clients and configuration settings enterprise wide. Maintain the latest version by promptly updating client software and removing all obsolete versions from managed devices.)
4. When an outside entity initiates a meeting using a collaboration tool not on an approved product list, instruct users to join web (browser) based sessions that do not require installation of client software. (In managed environments: Prohibit end users from installing client software on school- or district-managed devices (including removing local administration rights).
5. Prevent system administrators from using collaboration tools on the system while logged on with administrative privileges. Administrators should not perform non-privileged operations on the systems they are administering (e.g., using email, browsing the internet, performing office automation tasks, engaging in recreational use).
6. Prohibit the use of collaboration tools and features that allow remote access and remote administration. While

not the main purpose of collaboration tools, some vendors may advertise remote access software as collaboration tools and some collaboration tools may allow remote access and remote administration.

7. Clearly articulate to employees the legal, privacy, and document retention implications of your organization's collaboration tools, including any data sharing or utilization of participation or attention tracking features.

BEST PRACTICES FOR END USERS

The below practices are provided as recommendations you can make to your end users to better secure their use of video conferencing tools.

1. Only use organization-approved software and tools for school-related work, including school-provided or -approved distance learning and collaboration tools to host/initiate and schedule meetings.
2. Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows and consider turning off alerts for incoming messages (e.g. emails and direct messages). If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting are intended participants.
3. When joining meetings initiated by third parties that use collaboration tools not approved by your school, do not attempt to install software—join web (browser) based session instead. Do not use school email addresses to sign up for unauthorized/free tools.
4. Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g., confirm that whiteboards and other items on the wall are cleared of sensitive or personal information; confirm that roommates or family members are not within earshot of sensitive conversations). If available, make use of background replacement or blurring options in the collaboration tool.
5. Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your space or in a public area. Consider using headphones.
6. If using a personal device:
    a. Require passwords to log into the device, use strong passwords, and change frequently (including passwords for other accounts accessed from the same device);
    b. Only use non-privileged profile for daily activities and only use elevated privileges when administering the device;
    c. Close all other, non-school-related windows and applications before and during school-related use of the personal equipment;
    d. Keep the operating systems and all relevant applications up-to-date, and fully patched; and
    e. Turn on automatic patching and run Anti-Virus software.
7. Check and update your home network. Change default settings and use complex passwords for your

broadband router and Wi-Fi network and only share this information with people you trust. Choose a generic name for your home Wi-Fi network to avoid identifying who it belongs to or the equipment manufacturer. Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

8. Tailor security precautions to be appropriate for the intended audience and content of a meeting. Do not make meetings "public" unless they are intended to be open to anybody. For meetings that will be broadly attended, ensure you have the capability to mute all attendees and limit the ability of attendees to share screens. Consider giving participants an option to participate by audio only if they have privacy concerns.
9. Particularly when conducting meetings with a large audience, have a preestablished plan that details:
    a. The circumstances in which a meeting will be terminated if it is disrupted,
    b. Who has the authority to make that decision, and
    c. How the meeting termination will be executed.
10. For private meetings and lessons, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them. Do not share a link to a meeting on an unrestricted, publicly available, or social media post. If possible, disable the ability of participants to join a meeting before the host and automatically mute participants upon entry.
11. Provide the link to the meeting directly to specific people and share passwords in a separate email. If possible, require unique participant credentials, monitor meeting members as they join, and lock an event once all desired members have joined. Use features to permit removal of any meeting guest during the course of the meeting. The host may consider staying in a meeting room until all participants have signed off.
12. Manage screensharing, recording, and file sharing options. Limit who can share their screen to avoid any unwanted or unexpected images. Consider saving locally versus to the cloud based on the specific circumstances (e.g., need to share the recording with a wide audience or the public, using school-issued equipment versus personal equipment). Change default file names when saving recordings. Make sure to consult with your organization or district's counsel about laws applicable to recording videoconferences and sharing materials through them. Set participant expectations on session recording, screen recording, and screen shots.
13. If logging into a collaboration tool via a web browser, be careful to accurately type the domain name of the website. Be wary of links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.
14. Do not share student credentials or links, with strangers who may use them to disrupt classes or steal information. Do not share passwords with anyone.
15. Carefully review meeting invitations sent for sessions. Check to see if the meeting originated from a known teacher or other school employee. Verify that the address has the district's or school's name in the URL.

REPORTING

To report a cyber incident, call CISA at 1-888-282-0870 or visit www.cisa.gov.