GUIDANCE FOR SECURING VIDEO CONFERENCING

Four principles and tips to secure video conferencing

1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home.

Mitigation: Change default passwords for your router and Wi-Fi network. Check that you are using Wi-Fi encrypted with WPA2 or WPA3. Verify your video conferencing security settings and use encrypted video conferencing tools whenever possible.

Tips: Here are some simple actionable tips for connecting securely at home.

- Change default password to strong, complex passwords for your router and Wi-Fi network.
- Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
- Ensure your home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum, and that legacy protocols such as WEP and WPA are disabled. See CISA's Tip on Home Network Security for additional information.
- Avoid using public hotspots and networks.
- Only use video conferencing tools approved by your organization for business use.
- Enable security and encryption settings on video conferencing tools; these features are not always enabled by default.

GUIDANCE FOR SECURING VIDEO CONFERENCING

Four principles and tips to secure video conferencing

2. CONTROL ACCESS

Risk: Uncontrolled access to conversations may result in disruption or compromise of your conversations, and exposure of sensitive information.

Mitigation: Check your tool's security and privacy settings. Enable features that allow you to control who can access your video chats and conference calls. When sharing invitations to calls, ensure that you are only inviting the intended attendees.

Tips: Here are some simple actionable tips for connecting securely at home.

- Require an access code or password to enter the event. Try not to repeat codes or passwords.
- Manage policies to ensure only members from your organization or desired group can attend. Be cautious of widely disseminating invitations
- Enable "waiting room" features to see and vet attendees attempting to access your event before granting access
- Lock the event once all intended attendees have joined.
- Ensure that you can manually admit and remove attendees (and know how to expeditiously remove unwanted attendees) if opening the event to the public. Be mindful of how (and to whom) you disseminate invitation links

GUIDANCE FOR SECURING VIDEO CONFERENCING

Four principles and tips to secure video conferencing

3. MANAGE FILE AND SCREEN SHARING AND RECORDINGS

Risk: Mismanaged file sharing, screen sharing, and meeting recording can result in unauthorized access to sensitive information. Uncontrolled file sharing can inadvertently lead to users executing and clicking malicious files and links, which could, in turn, lead to system compromise.

Mitigation: Disable or limit screen and file sharing to ensure only trusted sources have the capability to share. Users should be aware of sharing individual applications versus full screens.

Tips: Here are some simple actionable tips for connecting securely at home.

- Toggle settings to limit the types of files that can be shared (e.g., not allowing .exe files).
- When recording meetings, make sure participants are aware and that the meeting owner knows how to access and secure the recording. Consider saving locally rather than in the cloud. Change default file names when saving recordings. Consult with your organizational or in-house counsel regarding laws applicable to recording video conferences.
- Consider sensitivity of data before exposing it via screen share or uploading it during video conferences. Do not discuss information that you would not discuss over regular telephone lines
- See CISA's Tip: Risks of File-Sharing Technology for more information.

GUIDANCE FOR SECURING VIDEO CONFERENCING

Four principles and tips to secure video conferencing

4. UPDATE TO LATEST VERSIONS OF APPLICATIONS

Risk: Outdated or unpatched video conference applications can expose security flaws for hackers to exploit, resulting in a disruption of meeting privacy and potential loss of information.

Mitigation: Ensure all video conferencing tools, on desktops and mobile devices, are updated to the latest versions. Enable or opt-in to automatic update features, or else establish routine updates (e.g., once weekly) to check for new versions and patch security vulnerabilities.

Tips: Here are some simple actionable tips for connecting securely at home.

- Enable automatic updates to keep software up to date.
- Develop and follow a patch management policy across the organization that requires frequent and continual application patching
- Use patch management software to handle and track patching for your organization.
- See CISA's Tip: Understanding Patches and Software Updates for more information

OKLAHOMA
Office of Management
& Enterprise Services