USING VIDEO CONFERENCING TOOLS WISELY

As more organisations move to remote work, many employees now rely on video conferencing tools to stay connected and productive. Here, we share our tips for using these tools safely and securely.

ACCESS CONTROL

Check video conferencing tool's security and privacy settings and enable features that allow you to control who can access your video chats and conference calls.

Be cautious of widely disseminating invitations. Only invite intended attendees to meetings. Manage policies to ensure only members from your organisation or desired group can attend meetings.

Add an extra level of security by requiring a password or code to enter the event (and try not to repeat these).

Ensure that you can manually admit and remove attendees (and know how to expeditiously remove unwanted attendees) if opening the event to the public.

Enable "waiting room" features to check attendees attempting to access call before granting access. Lock the event once all intended attendees have joined.

SECURE CONNECTION

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

Change your router and Wi-Fi network default password to strong, complex passwords.

Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.

Ensure home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum and ensure that legacy protocols such as WEP and WPA are disabled.

For more information or advice on securing your video conferencing tools, get in touch with us at contact@ka2.io

USING VIDEO CONFERENCING TOOLS WISELY

FILES, RECORDINGS AND SCREEN SHARING

Mismanaged file sharing, meeting recordings and screen sharing can result in unauthorised 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.

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 organisational 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

Toggle settings to limit the types of files that can be shared (e.g., not allowing .exe files).

USE LATEST VERSIONS OF APPLICATIONS

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.

Enable automatic updates to keep software up to date.

Use patch management software to handle and track patching for your organisation.

Develop and follow a patch management policy across the organisation that requires frequent and continual application patching.

For more information or advice on securing your video conferencing tools, get in touch with us at contact@ka2.io