QBE

Your guide to cyber safe *video conferencing*

As a result of COVID-19, working from home has become the new normal. And with this sudden global shift in remote working, we're using video conferencing solutions like Zoom, WebEx and Microsoft Teams to connect with colleagues, business partners and clients more than ever before.

Unsurprisingly, there's been a huge spike in new user numbers across video conferencing platforms in recent months. For example, Zoom has grown from 10 million daily participants per day in December 2019, to more than 300 million in recent weeks.[1]

During any rapid technology adoption, hackers often follow the masses, attempting to find security holes in the technology. That's why it's increasingly important to know how to keep your business information safe. Here are a few video conferencing security recommendations.

1 **https://blog.zoom.us/wordpress/2020/04/22/90-day-security-plan-progress-report-april-22/**

Select a secure provider

When choosing a secure video conferencing provider, it's important to do your research to make sure the solution they are offering is secure and meets your needs.

Typically, this means making sure they have documented and comprehensive security and privacy policies.

They should also have ISO 27001 certification and, or a current SOC2 certification. You should be able to find these on providers' websites.

Always check for updates

Always check you're using the very latest version of your video conferencing application and update it before use. Video conferencing providers regularly release updates to address security issues or privacy concerns so updating regularly is key.

You should also update all other applications and devices. Having the latest software on your device not only gives you the latest features – it provides the best protection for you and your personal data.

Be careful with links, files and recording

If you receive any unexpected invitations for online meetings, check the legitimacy of the email and invite, and don't click on any links or attachments that seem suspicious.

When you connect to a meeting, don't accept requests to take control of your screen, or open any links or files shared within the session, especially if you don't know the participants on the call.

Remember, videoconferencing sessions can be recorded, so be careful with information you share verbally and on-screen. And when hosting a meeting, make sure you're not accidentally sharing any confidential information on your screen or in your background.

Tips for hosting a meeting

1. Lock meetings and use strong passwords

To make sure only invited attendees can join a meeting, set a strong password or long phrase. This will stop unwanted attendees gaining access and keep your information private. Also, don't share the password unnecessarily, and use a different password for each meeting. You can also restrict forwarding when you send out your invitation.

2. Always use waiting room features

Use 'waiting room' features if they're available. This lets you verify attendees, and make sure only invited participants join the meeting.

3. Lock down your meeting

Once all of the participants have joined your meeting, lock it down so no one else can get access.

4. Disable file sharing

If you want to share sensitive information, use your company's file-share technologies, rather than sharing files within the meeting itself.

5. Protect meeting recordings

Importantly, if you plan on recording your session, make sure you get permission from all your attendees as a first step.

If you do decide to record, make sure the recordings are protected and stored securely – just like you would for any other files containing confidential business information. You can password-protect recordings using an encryption tool like Bitlocker, FileVault or WinZip.

Additionally, only share files with people who need access – that means recordings shouldn't be shared online or made publicly accessible.

6. Use a business VPN

A business virtual private network (VPN) can help better secure internet connections, and keep private information secure via encryption. If you need any specific help or advice, please consult with your IT provider.

Need more help?

To learn more about using video conferencing tools safely, see the **government's eSafety guide**, which takes you through security tips that apply to a range of video conferencing solutions.