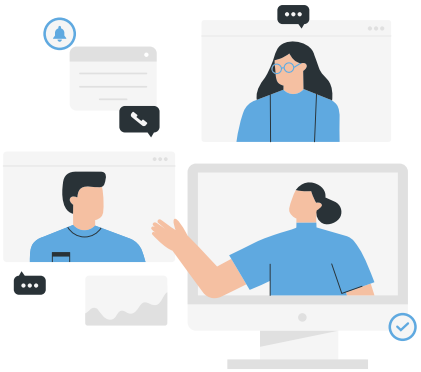
Protect Your Video Meetings



Use business-grade platforms

Programs such as Microsoft Teams follow industry and IT data protection standards such as HIPAA, ISO 27001, ISO 27018, SSAE16 SOC1, and SOC2.

Restrict meeting access

Password-protect meetings and limit the reuse of access codes. Also, allow only invited and signed-in users to join. Once the guests arrive, lock the meeting so new participants cannot join.

Don't overshare

Don't show your screen if you do not need to. Similarly, hide anything in your camera view that you do not want anybody to see. If possible, use a virtual background instead of showing your live workspace.

Update regularly

Update the meeting software regularly and make sure attendees do the same. Hackers can exploit security holes in older software versions.

Join secure Wi-Fi networks

Using unprotected networks, especially public Wi-Fi signals that do not require a password, leaves meetings accessible to hackers.

Watch out for phishing emails

Bad actors are impersonating video conference vendors and sending out malicious emails. Look at the email address and confirm it is from a trusted sender.

Create an online meeting policy

Require employees to review a document outlining meeting security and etiquette best practices. This can include using the company-approved meeting platform only and securing the meetings with passwords.

SwiftTech SOLUTIONS
INFORMATION TECHNOLOGY GROUP

If you are interested in more information about a business-grade video conferencing platform, you can contact us at info@swifttechsolutions.com.

swifttechsolutions.com