How to secure your online meetings

Advice for small and medium-sized organisations on choosing, setting up and using online meeting services safely

Online meetings rely on digital tools to support collaboration, but they also introduce security risks. This guidance – aimed at small and medium-sized organisations – outlines steps to keep your online meetings secure; to protect sensitive information and reduce the risk of cyber attacks.

For broader support on securing your organisation, you should visit the NCSC's Cyber Action Toolkit.

If you use an IT provider, refer to our Managed Service Providers (MSP) guidance to ensure your devices are being secured effectively.

Protecting your online meeting services

Follow these steps to secure your online meeting services.

Choosing a service

- Choose a service that works for you:
  - For personal use, free versions often provide enough security.
  - Organisations typically need paid plans to provide the security and controls required for business needs - such as managing multiple users securely and ensuring compliance and data protection.
- Only download apps from trusted sources like the Apple App Store, Google Play, or the provider's official website. Avoid clicking on ads and unsolicited links, which may lead to malicious sites.
- Once you've selected your service, it's important to secure your account and control who can join your online meeting by following the below steps. For specific instructions, refer to the vendor support website of the service you're using.

Securing your admin account

- Use a strong, unique password.
- Enable two-step verification (2SV).
- Use passkeys – explained in this NCSC blog: Trusting the tech: using password managers and passkeys to help you stay secure online – where the provider makes them available.
- Keep your app up to date.

Controlling meeting access

- Only allow direct access to authenticated users and invited guests.
- Require passcodes for unauthenticated users.
- Use a waiting area (often referred to as the 'lobby') to verify participants before admitting.
- Consider blocking calls from outside your organisation and from unknown contacts.
- Never share meeting links or passwords in public spaces. If someone joins and you don't recognise them, politely ask who they are before continuing.

Controlling what you share: data and privacy tips

- Check your surroundings before joining a call and consider using a background blur or an image for privacy.

- Get familiar with basic controls like muting your microphone, turning off your camera, and spotting when a meeting is being recorded.
- Review and adjust privacy settings to suit your needs before use.
- Know where recordings, transcriptions, chat logs and shared files are stored.
- Be aware of AI attendees - these tools may record, transcribe, or analyse meeting content. Understand what data they collect, how it's used, and whether you can opt out.
- Check who has access to your data and how long it is retained. Only individuals and systems who genuinely need the information should be able to access it, and you should only keep personal data for as long as you have a clear reason to.

PUBLISHED

19 March 2026

WRITTEN FOR

Small & medium sized organisations