

A group of diverse people in a meeting, looking at a screen together. The image is dark and serves as a background for the text.

Working effectively & securely online

Technical advice for e-therapy via ZOOM

John Kavanagh

bluePANGOLIN



Embrace • Connect • Energise

info@bluePANGOLIN.CO.UK

www.bluePANGOLIN.co.uk

Agenda

- Background
- Digital Security – what does it mean
 - Operating system
 - Virus protection
- Introduction to Zoom Security Features
 - Before a session
 - During a session
- Things to consider
- Q&A

Background

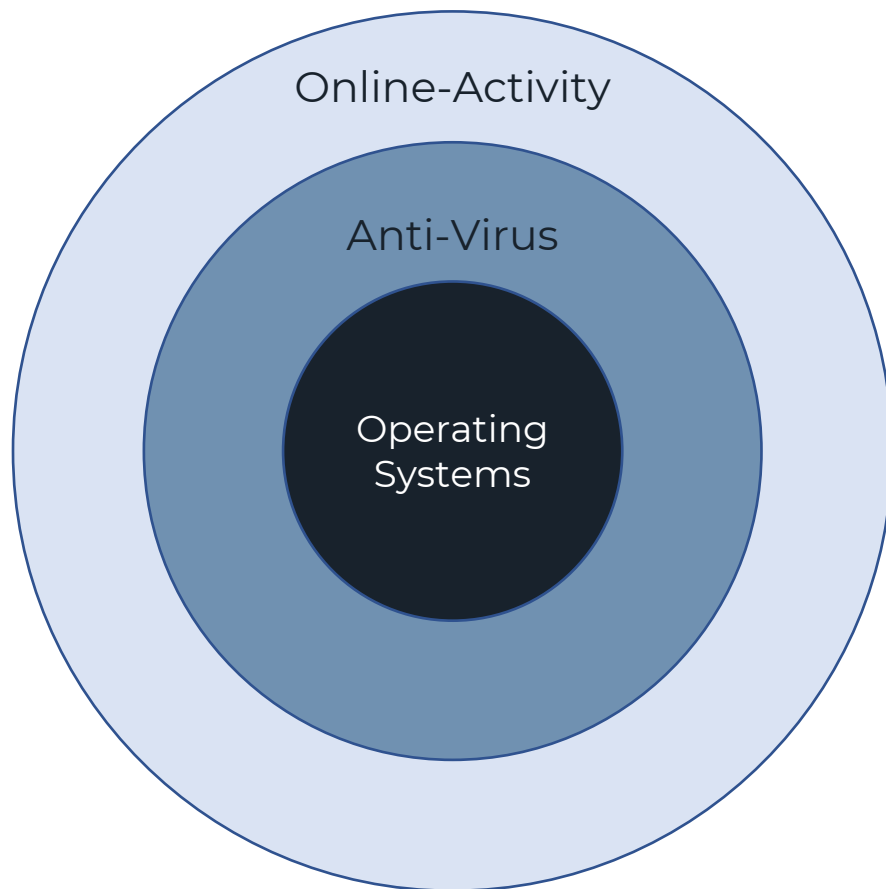
- Why this webinar?
- Who is it aimed at
- What will you get from it
- Ask questions

Digital Security!

What does it (practically) mean

- Protecting your digital activities from malicious intent by 3rd parties
- Types of Threat
 - Software (*Virus*)
 - Data (*Documents, videos, personal information*)
 - Physical (*digital interruption and access*)
- Note of Realism
 - This is not the movies
 - Need to be secure but need to be accessible

Digital Security - Good Practice



Operating System

- Update regularly

Ant-virus

- HAVE (at least)ONE!
- Keep it up to date

Online Activity

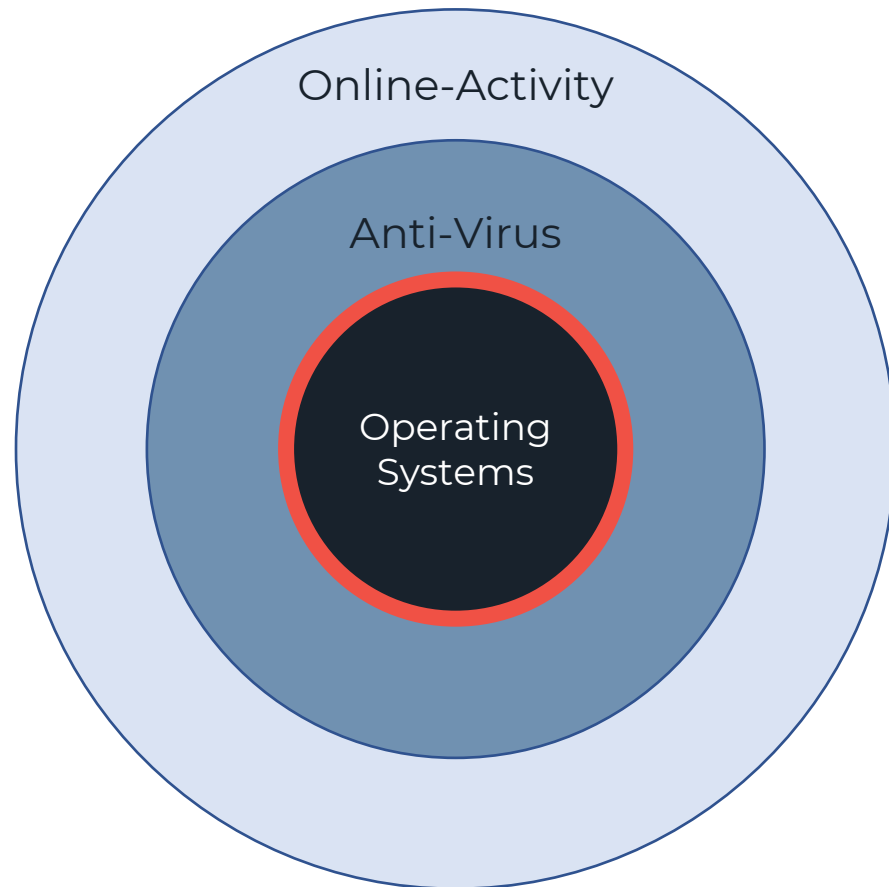
- Don't open the unknown
- Keep passwords safe
- Use app security features

Question?

How confident are you with your computing knowledge?



Operating System - Good Practice



Operating System

- Update regularly

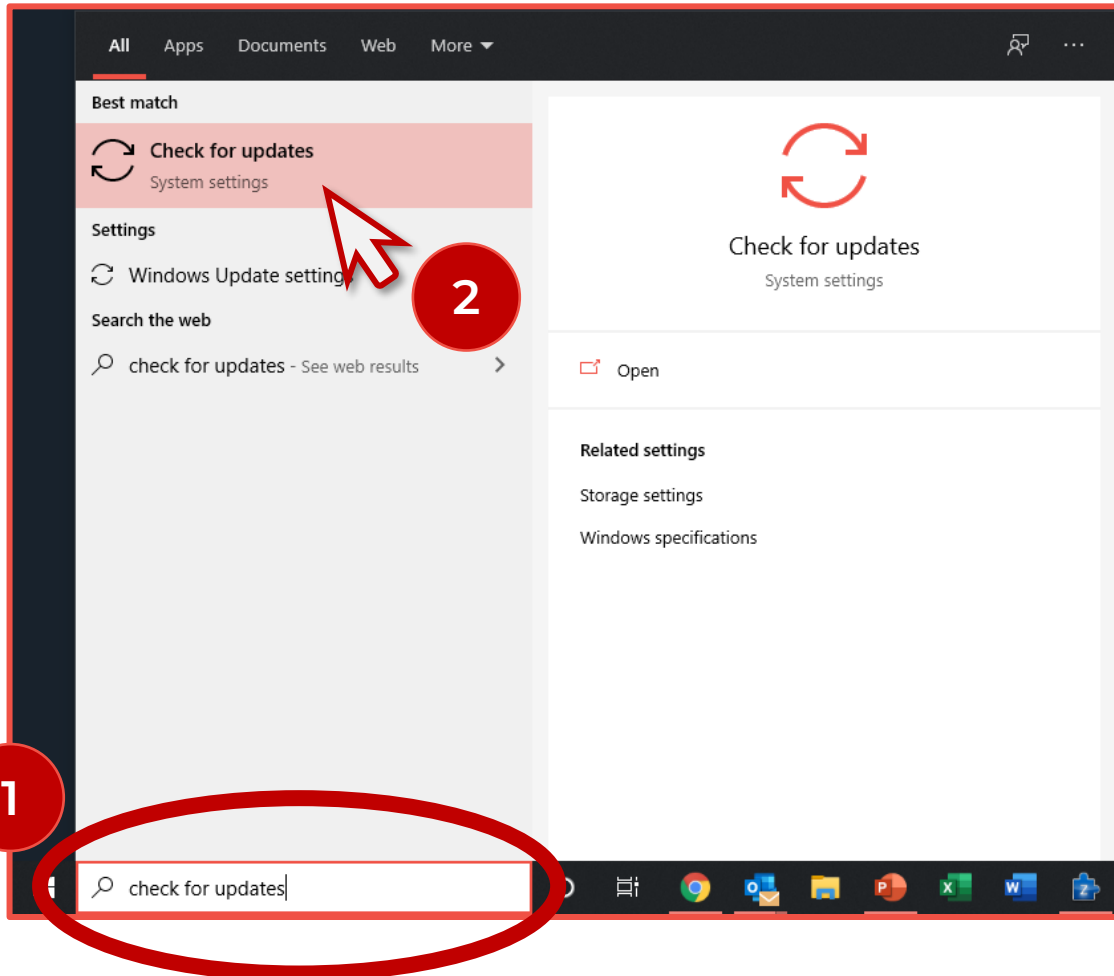
Ant-virus

- HAVE (at least) ONE!
- Keep it up to date

Online Activity

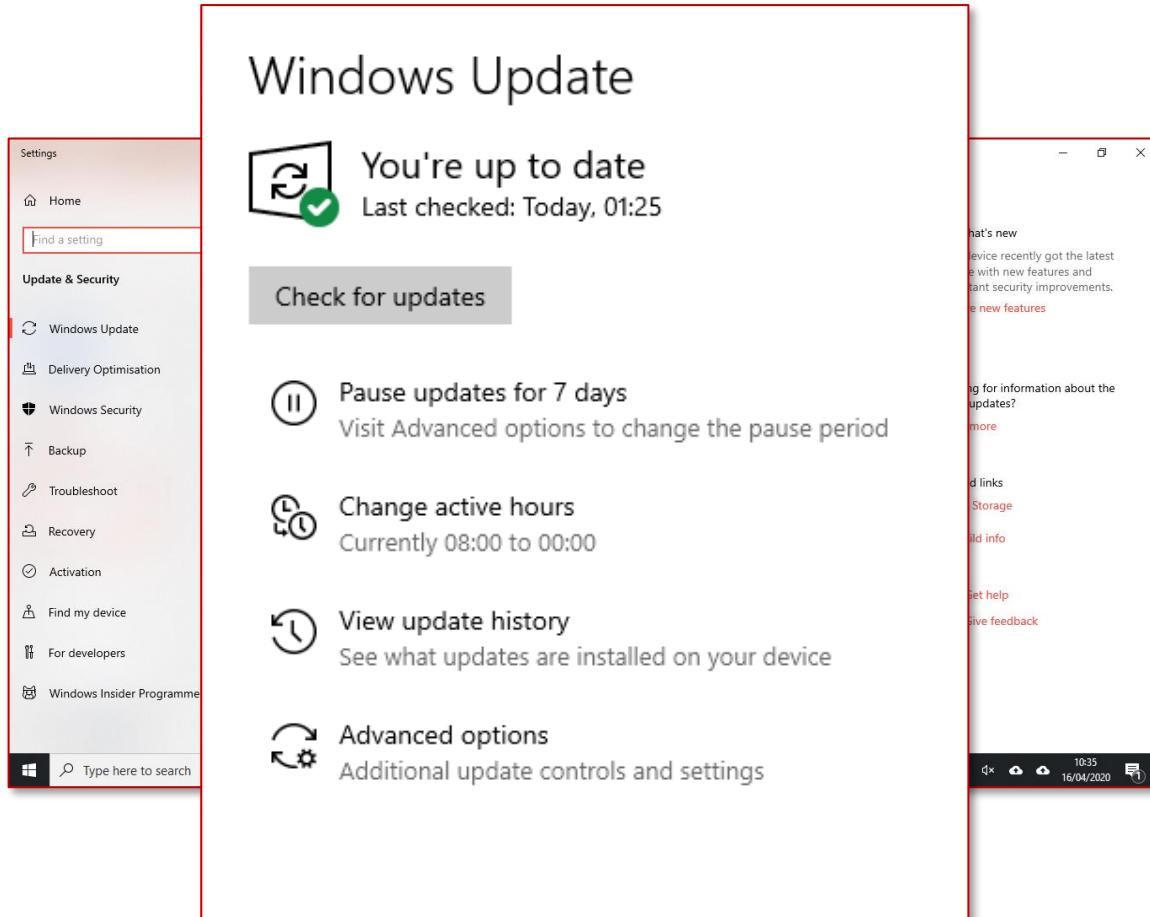
- Don't open the unknown
- Keep passwords safe
- Use app security features

Operating System - Good Practice



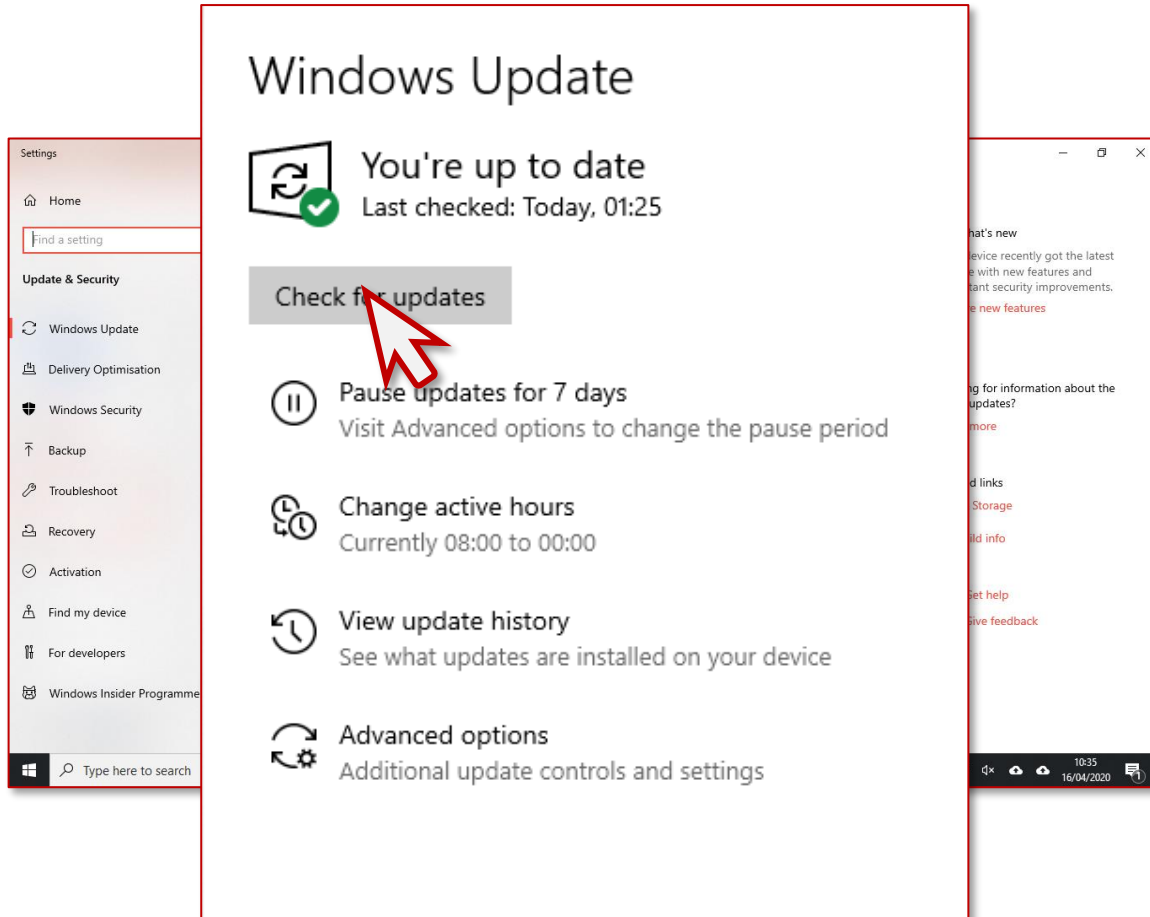
1. Go to windows search bar:
 - Type *"check for updates"*
2. Open the systems settings

Operating System - Good Practice



1. Status of last updates
2. Check now for updates
3. Additional & Advanced options

Operating System - Good Practice



1. Click “Check for updates”
2. Download and install updates
3. Encourage you to do this regularly

Operating System - Good Practice

Windows Update



Updates available

Last checked: Today, 10:40

Security Intelligence Update for Windows Defender Antivirus - KB2267602 (Version 1.313.1638.0)

Status: Installing - 0%



Pause updates for 7 days

Visit Advanced options to change the pause period



Change active hours

Currently 08:00 to 00:00



View update history

See what updates are installed on your device

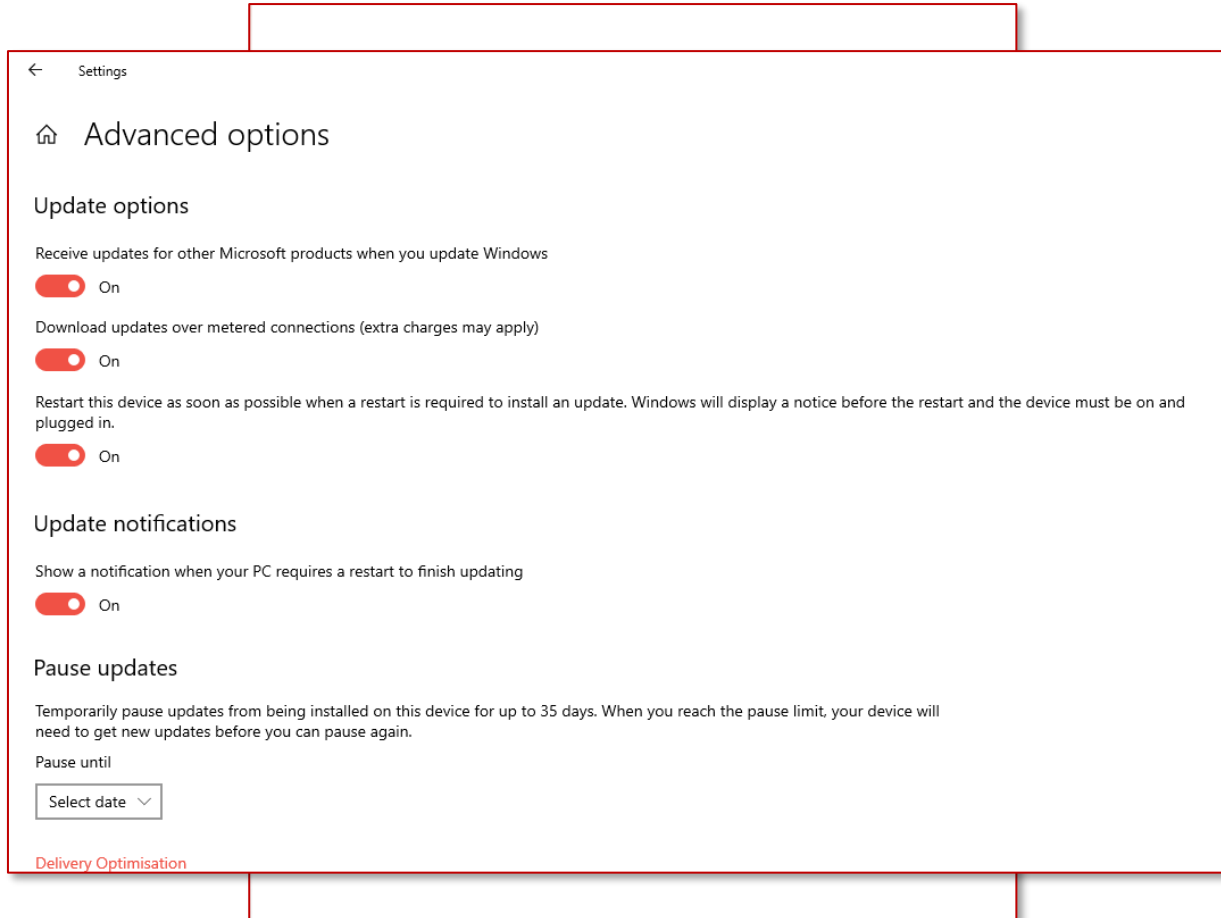


Advanced options

Additional update controls and settings

1. My system was up-to-date at 01:25
2. At 10:40 another update was available
3. Status changes to show Windows Defender updating

Operating System - Good Practice



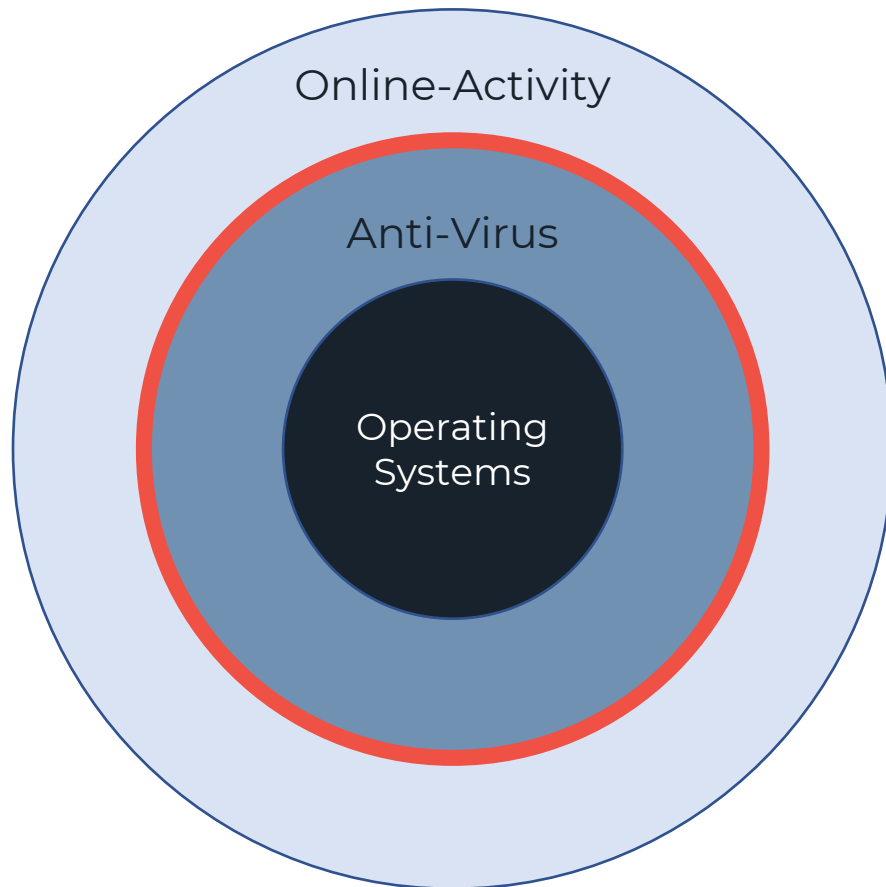
1. Select “Advanced options”
2. Enable all options

Question?

How confident are you with the topic of Computer Virus protect?



Anti-Virus - Good Practice



Operating System

- Update regularly

Ant-virus

- HAVE ONE! (*at least*)
- Keep it up to date

Online Activity

- Don't open the unknown
- Keep passwords safe
- Use app security features

Anti-Virus / Anti-Malware

(or both)



- Large choice – make an informed choice
- Protect against all malicious software (*not just virus*)
- Only pay for what you need
- Keep up-to-date

Different Types of Threat



Spyware

Captures your activity and data and transmits it to a 3rd party without your permission



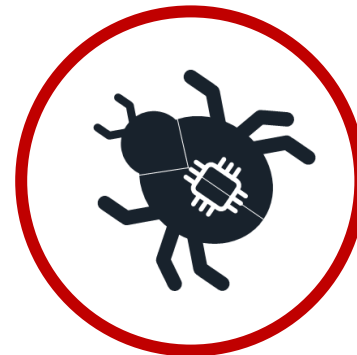
Ransom Ware

Access to your computer and files is locked until a ransom is paid and a release-code is issued.



Adware

Programmes that continually display adverts or directly to targeted sales websites



Virus

Code that will infect your computer and attempt to spread to other computers (e.g. Trojans, worms)

Recommendation

Free Solution



Windows
Defender




Malwarebytes
ANTI-MALWARE

Microsoft Defender provides a high standard of “traditional virus” detection with minimal performance impact

Malwarebytes provides latest Malware detection



Paid Solution



Norton
by Symantec

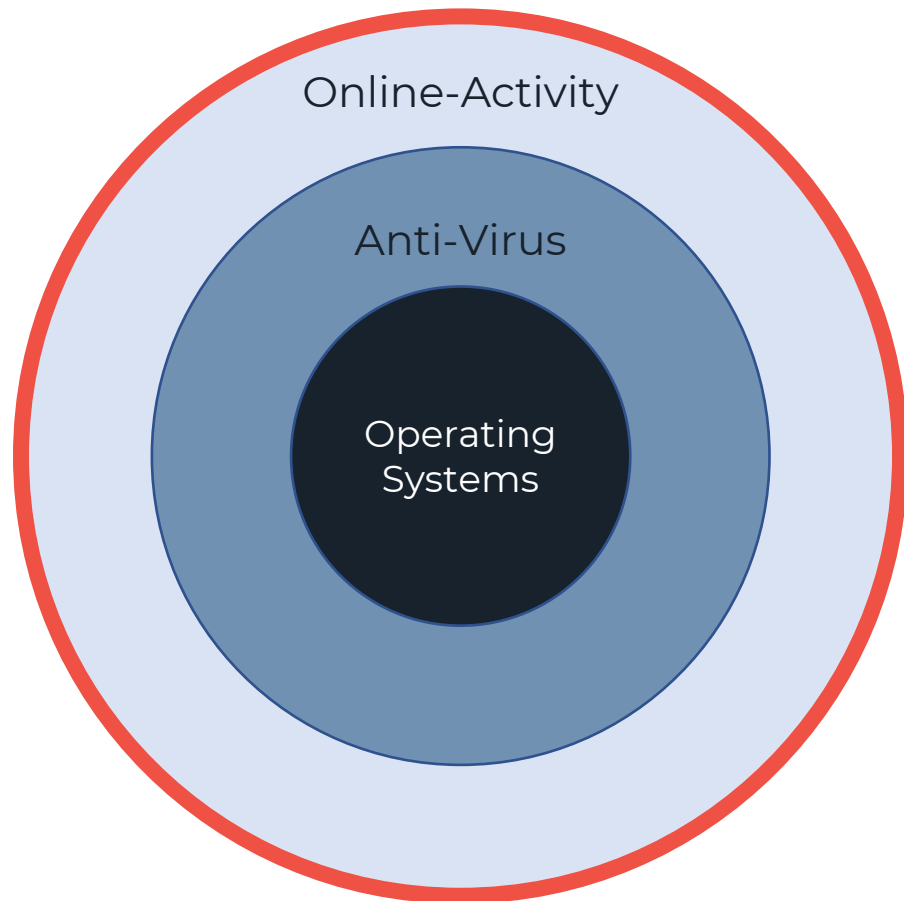
All Norton product range offers good protection for both Virus and Malware protection with a clear pricing structure.

Question?

How confident are you at configuring Zoom security?



Digital Security - Good Practice



Operating System

- Update regularly

Ant-virus

- HAVE (at least) ONE!
- Keep it up to date

Online Activity

- Don't open the unknown
- Keep passwords safe
- Use app security features

Video Conferencing tools



Signal




jitsi.org

- Once again here is lots of choice.
- Needs to work for you AND your clients
- Pay attention to the settings!!!



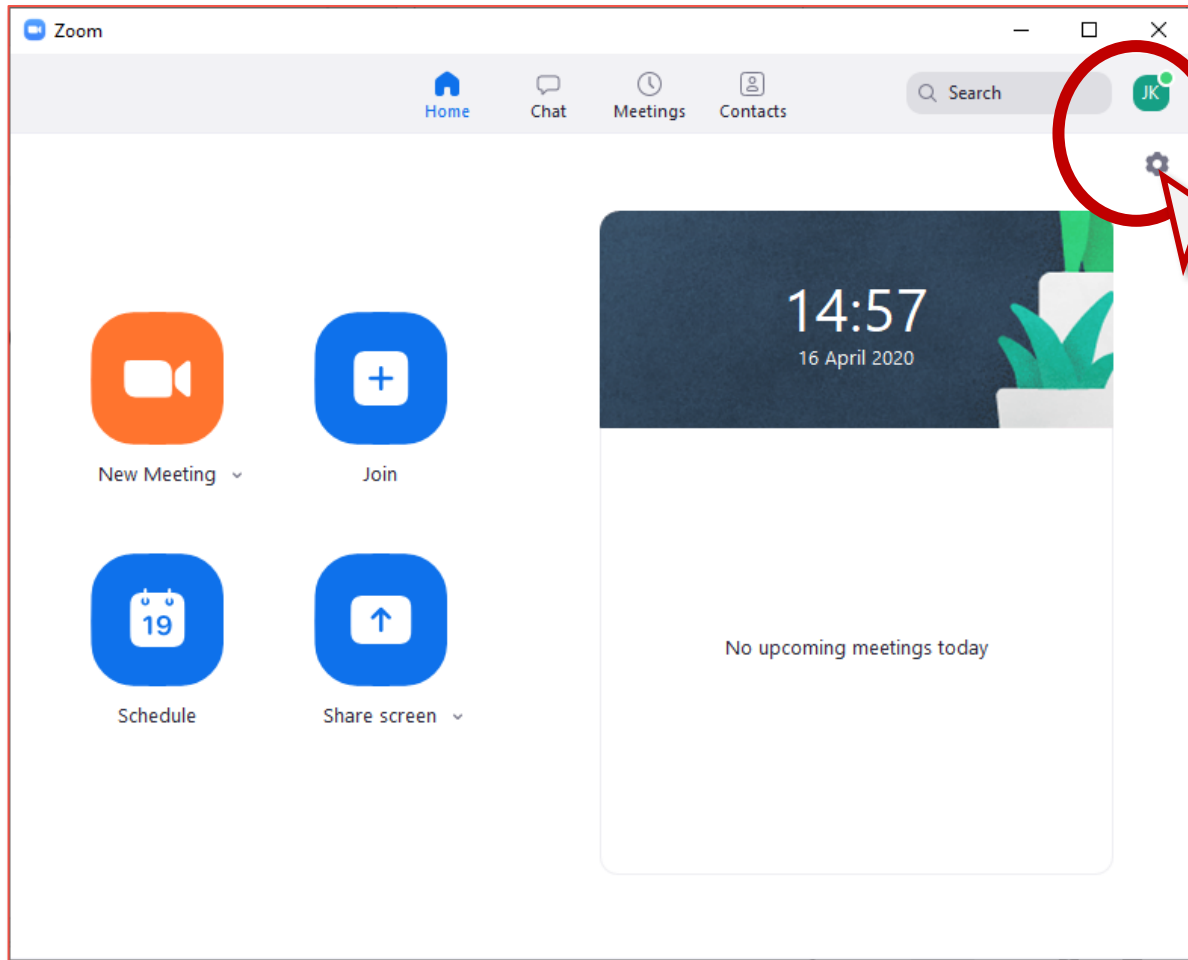
Zoom Security

How to setup a secure meeting using Zoom.



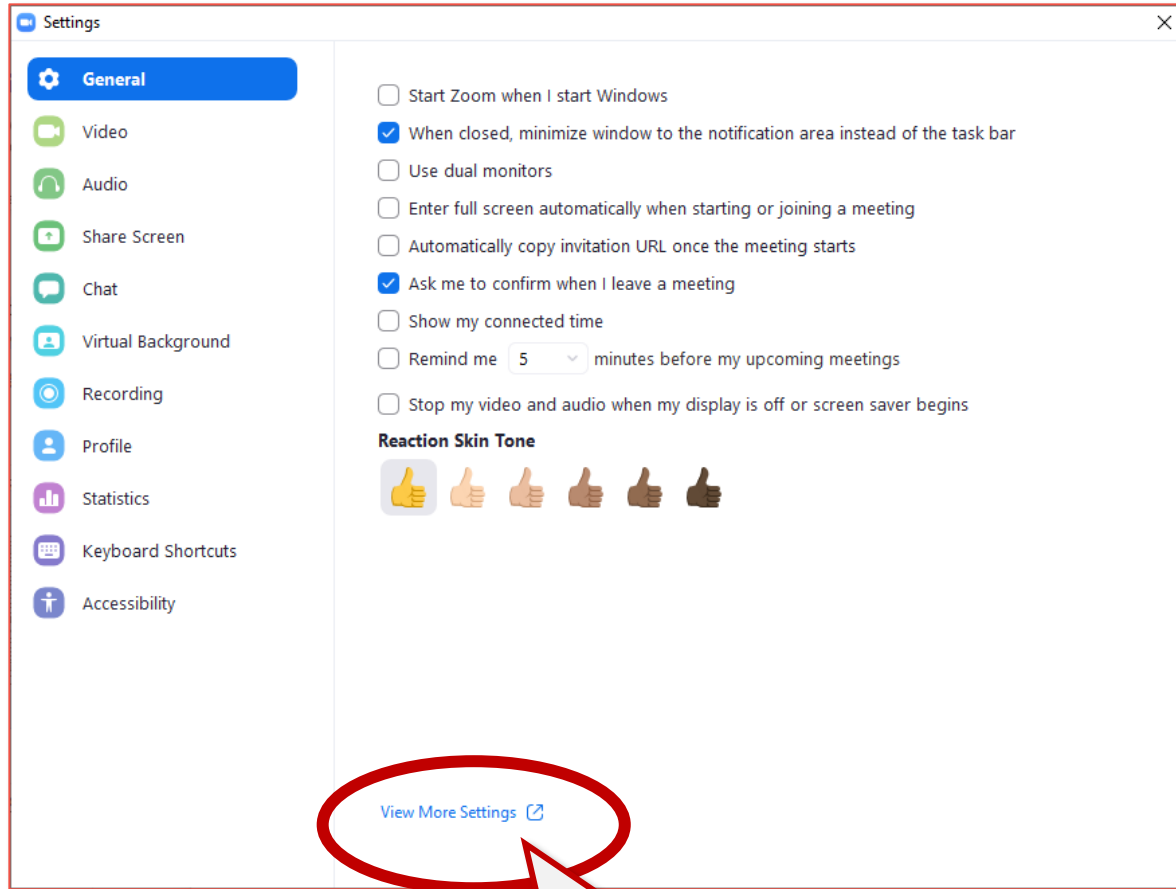
**Before creating any
meetings...**

Zoom: Setup



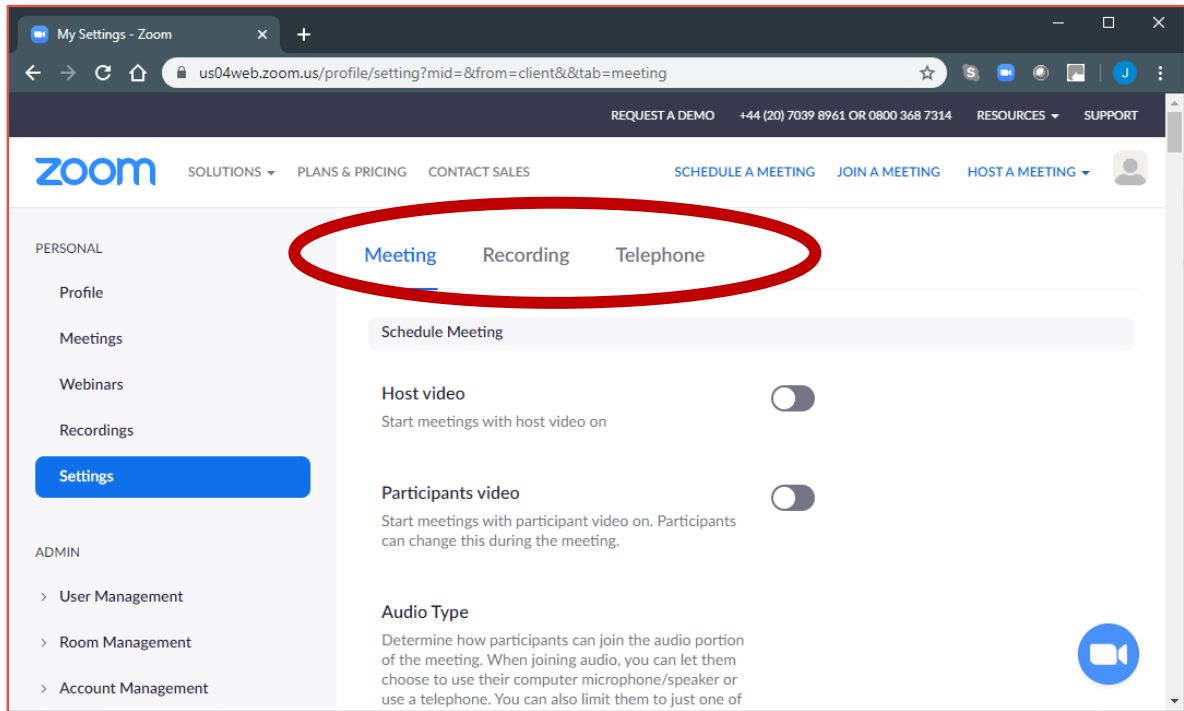
- Review your setting before starting any professional meetings
- Default settings are very open.
- Pay particular attention to block “Zoom-bombing” and unauthorised recording

Zoom: Change your settings



- The initial settings page only shows high-level settings.
- Use the link indicated to access detailed settings

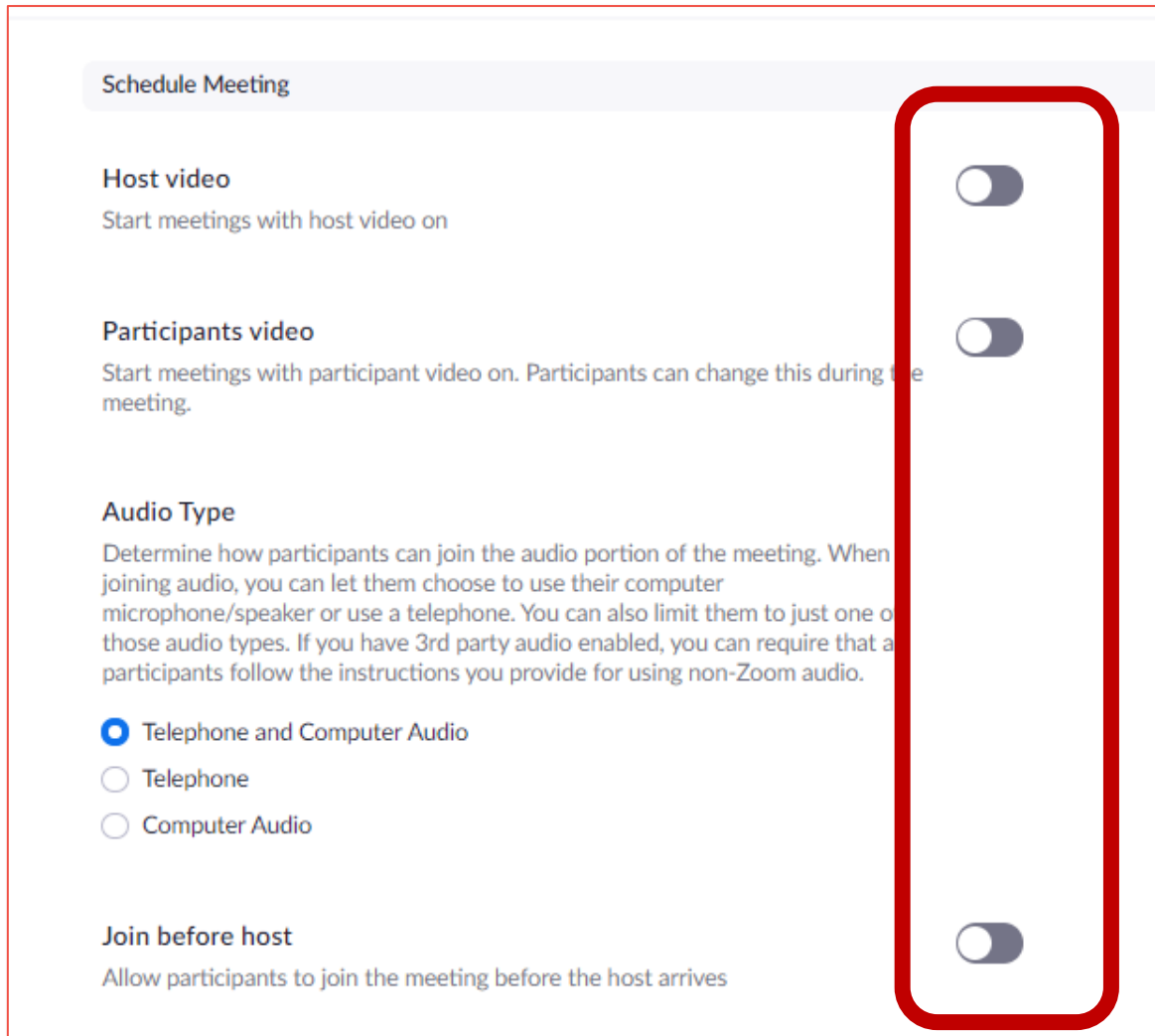
Zoom: Detailed settings



- Settings are broken down into three main categories
- The “Meeting” section is further divided into:
 - Schedule Meeting
 - In Meeting (Basic)
 - In Meeting (Advanced)
 - Email Notification
 - Other

Zoom: Detailed settings

Scheduling Meeting



Schedule Meeting

Host video
Start meetings with host video on

Participants video
Start meetings with participant video on. Participants can change this during the meeting.

Audio Type
Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that participants follow the instructions you provide for using non-Zoom audio.

Telephone and Computer Audio
 Telephone
 Computer Audio

Join before host
Allow participants to join the meeting before the host arrives

- As the “Host” you should control all aspects of the meeting.
- As standard, everyone should join with video turned-off (*they can turn this on once they are in the meeting*)
- Clients should NOT be allowed to join before the host

Zoom: Detailed settings

Scheduling Meeting

Only authenticated users can join meetings from Web client
The participants need to authenticate prior to joining meetings from web client

Require a password when scheduling new meetings
A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a password for instant meetings
A random password will be generated when starting an instant meeting

Require a password for Personal Meeting ID (PMI)

Only meetings with Join Before Host enabled
 All meetings using PMI

Embed password in meeting link for one-click join
Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

- All meetings you arrange should be password protected.
- You should not allow “one-click join” for your meetings

Zoom: Detailed settings

Scheduling Meeting

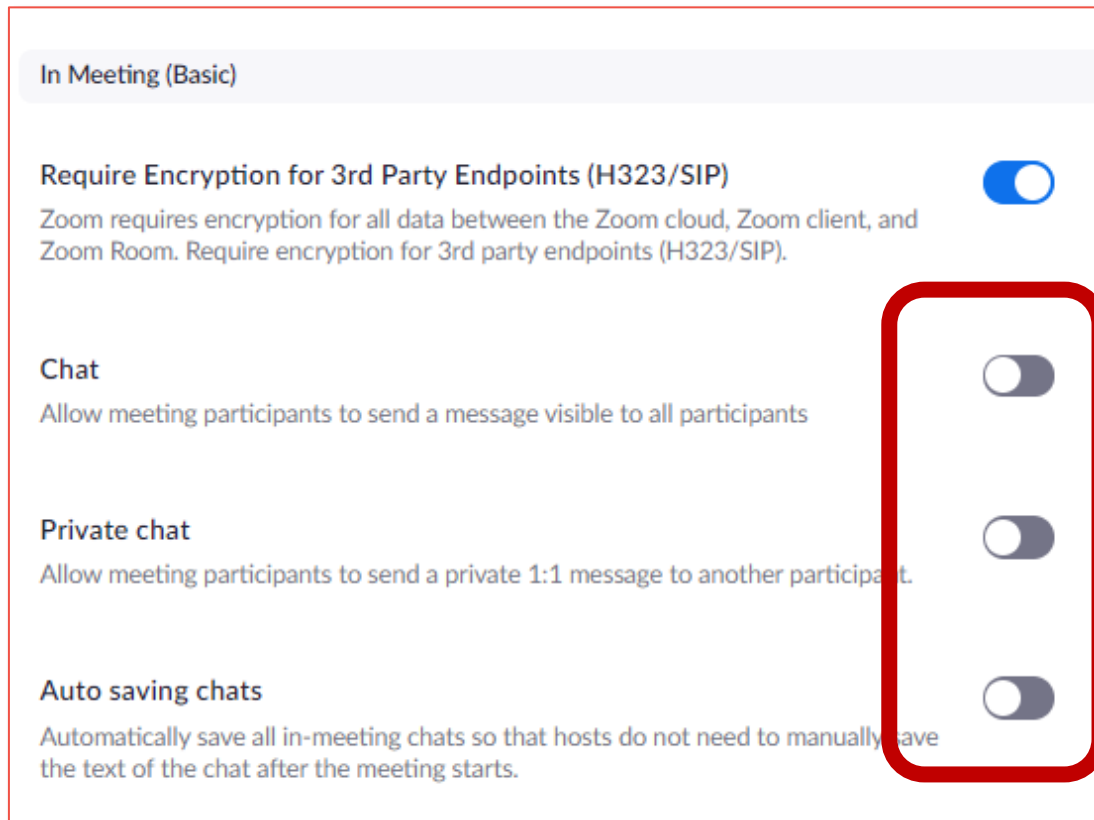
Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.



- As standard, everyone should join with audio turned-off (*they can turn this on once they are in the meeting*)

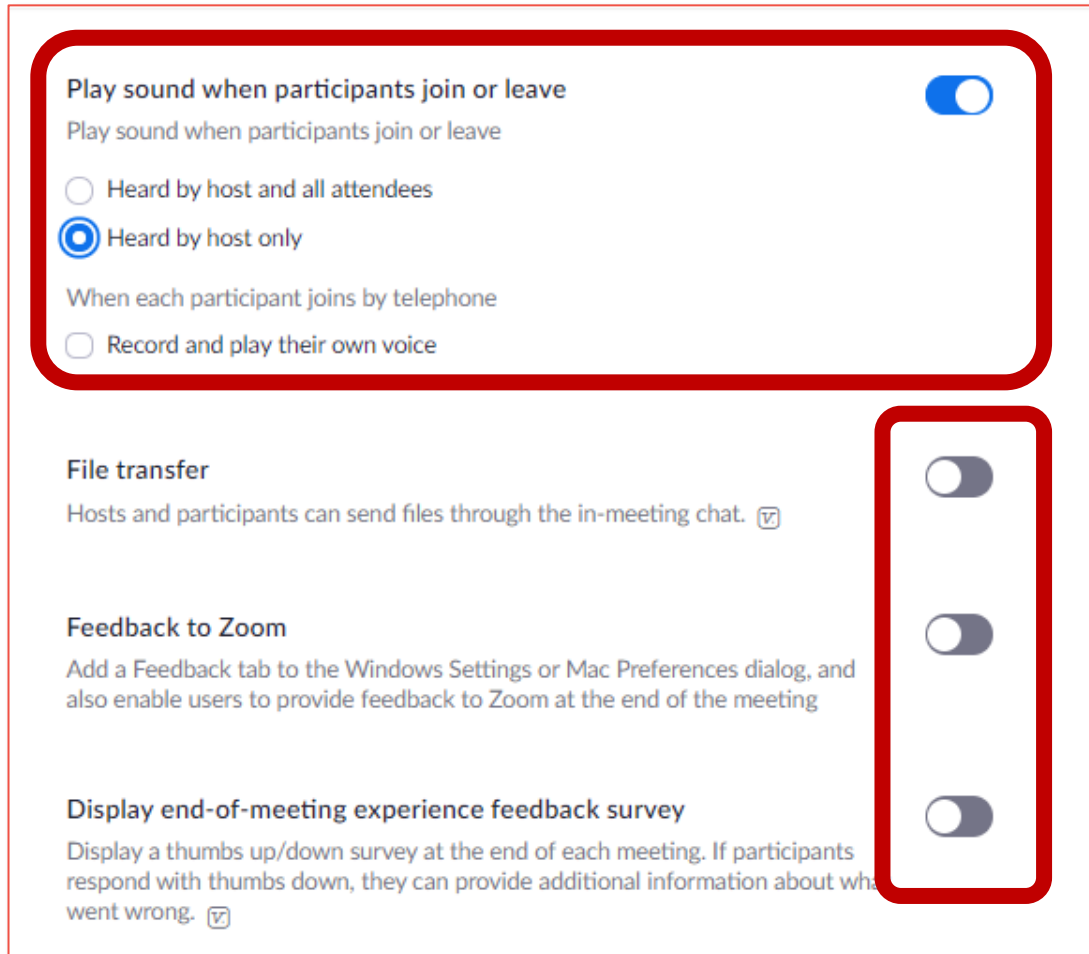
Zoom: Detailed settings In Meeting (Basic)



- One method of Zoom-bombing is to send inappropriate “Chats”
- *You can disable chats (both public and private)*
- *Prevent “Auto-saving”*

Zoom: Detailed settings

In Meeting (Basic)



- As the host of the session, you should be aware if anyone joins during your session.
- Transfer of files or information should be locked.

Zoom: Detailed settings

In Meeting (Basic)

The image shows a screenshot of the Zoom 'In Meeting (Basic)' settings. A red rounded rectangle highlights the 'Screen sharing' section, which includes a toggle for 'Screen sharing' (turned on), radio buttons for 'Who can share?' (set to 'Host Only'), and radio buttons for 'Who can start sharing when someone else is sharing?' (set to 'Host Only'). Below this, another red rounded rectangle highlights the 'Annotation' and 'Whiteboard' sections. The 'Annotation' toggle is turned off, and the 'Whiteboard' toggle is turned on. There is also an unchecked checkbox for 'Auto save whiteboard content when sharing is stopped'.

Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

Host Only All Participants ?

Who can start sharing when someone else is sharing?

Host Only All Participants ?

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications

Annotation

Allow participants to use annotation tools to add information to shared screens

Whiteboard

Allow participants to share whiteboard during a meeting

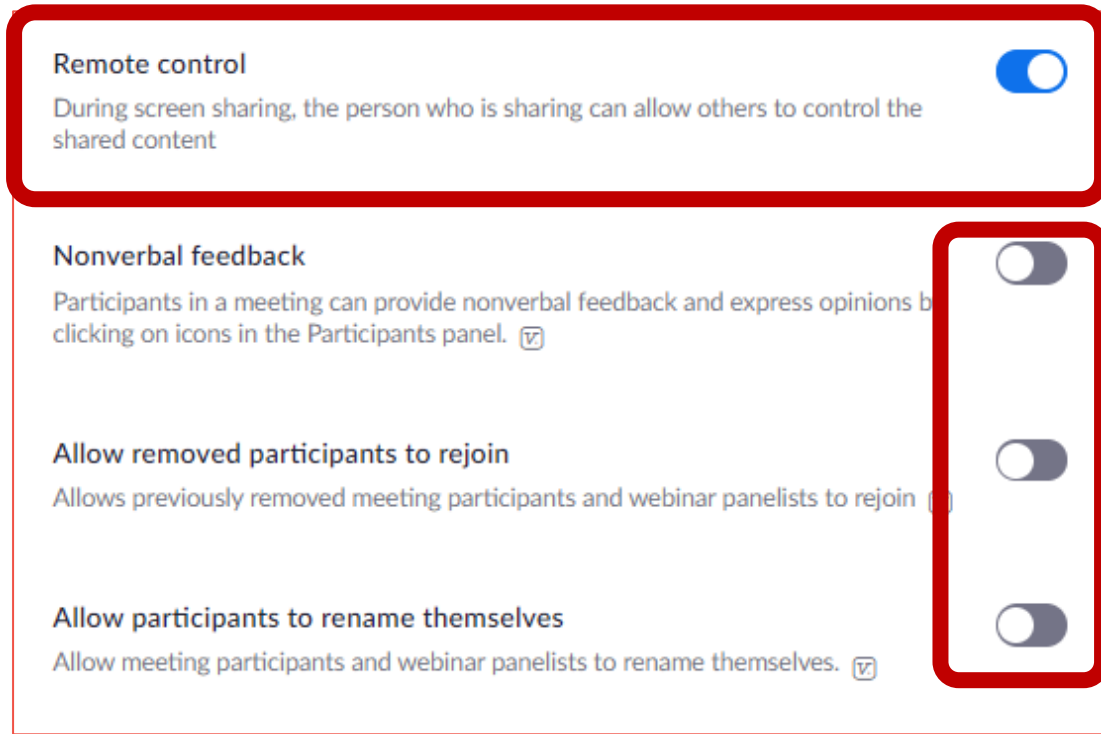
Auto save whiteboard content when sharing is stopped

- Screen sharing allows you (or your client) to display files from their computer to everyone on the call
- Annotation & Whiteboard are methods of working on a shared screen

Is this appropriate for your sessions?

Zoom: Detailed settings

In Meeting (Basic)

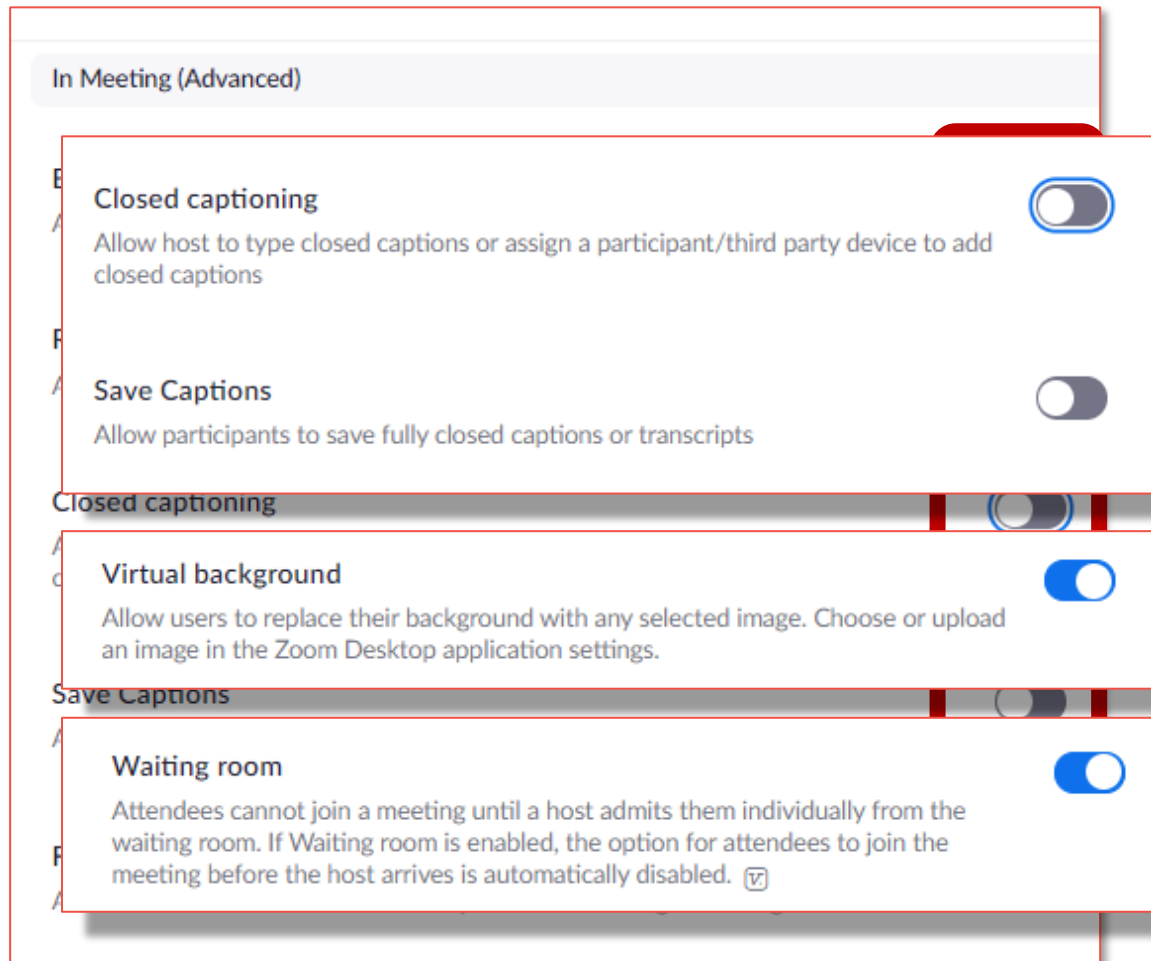


- Remote control allows others to take over a shared computer
- How can participants express themselves in a session?

Is this appropriate for your sessions?

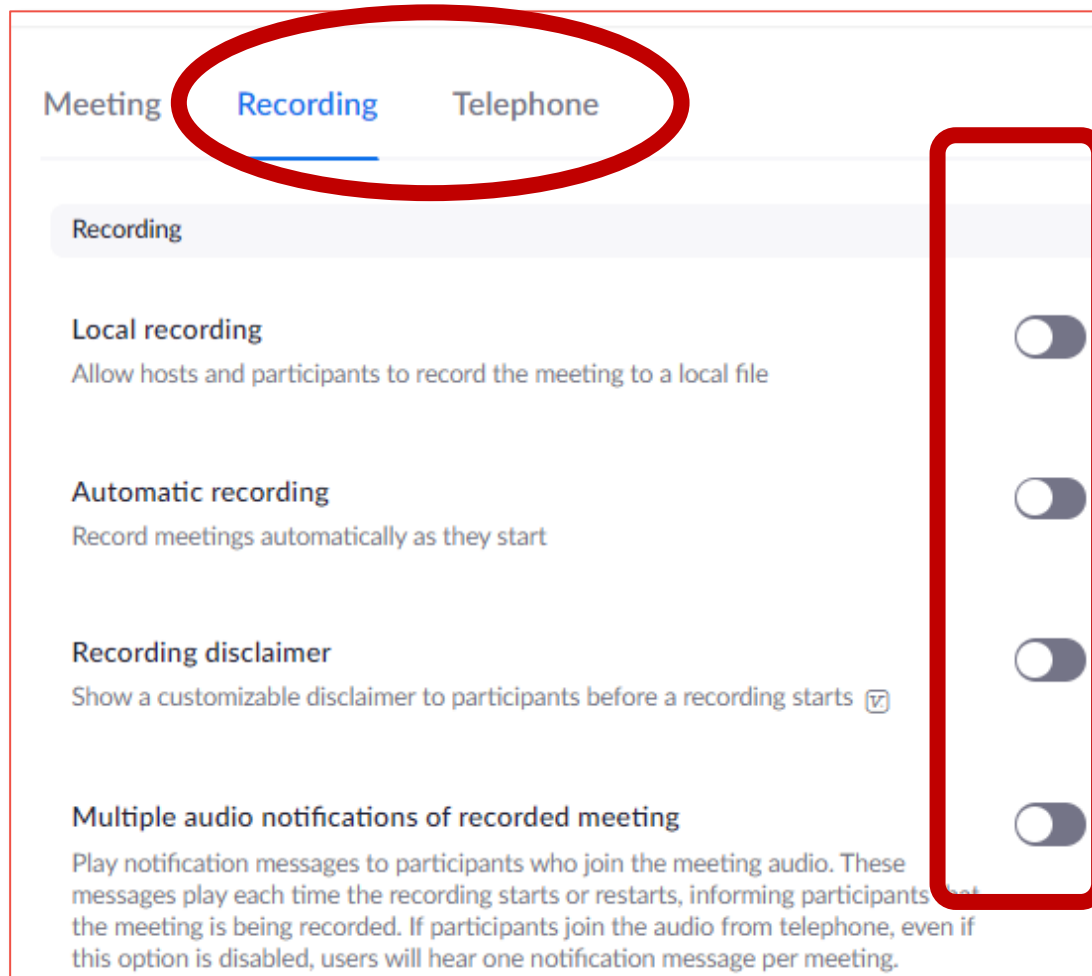
Zoom: Detailed settings In Meeting (Advanced)

- In the “Advanced” section I recommend all settings to be OFF.
- There are some notable exceptions:
 - Closed Captioning?
 - Virtual Background?
 - Waiting Room.



Zoom: Detailed settings

Other settings



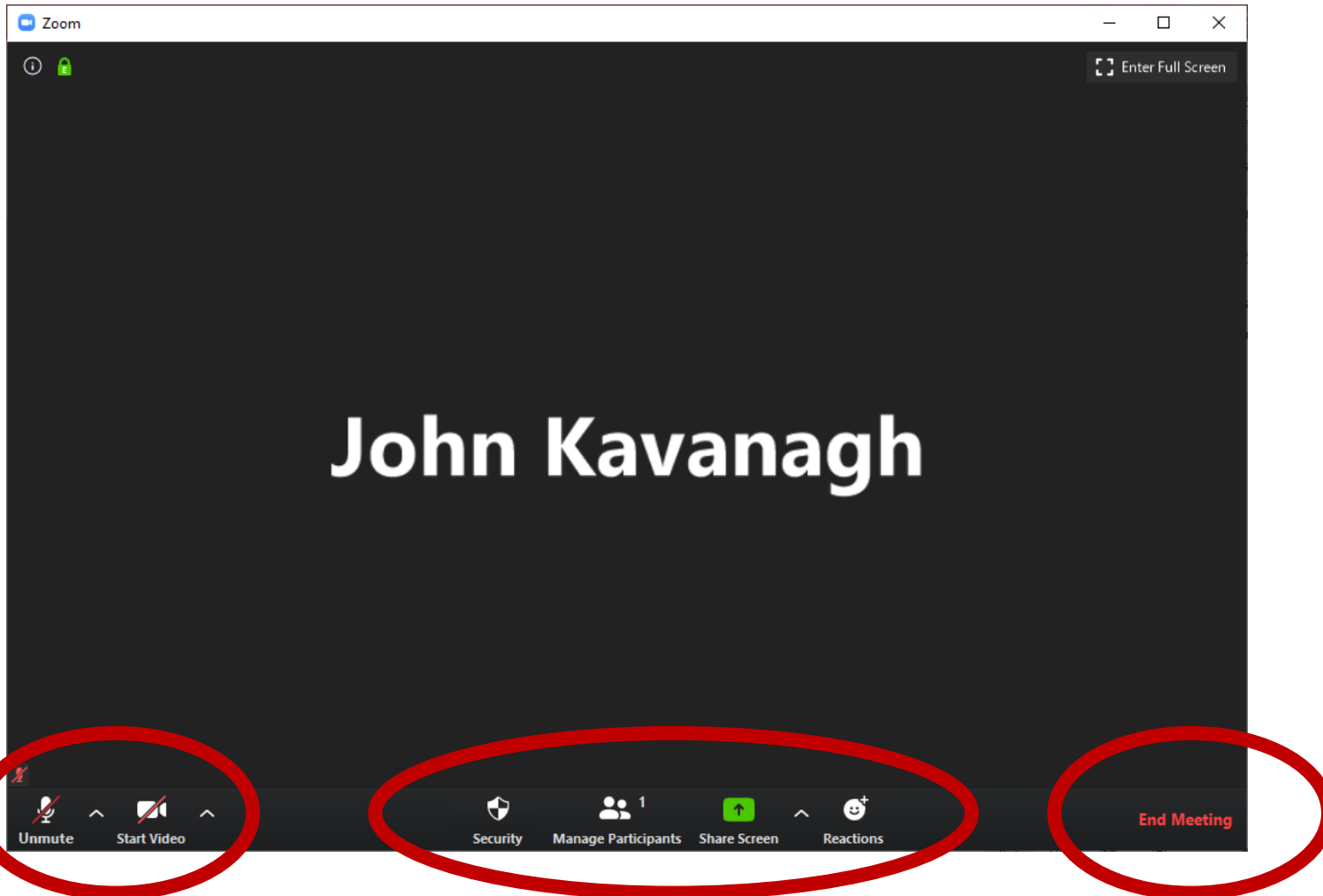
- In the “Recording” section I recommend all settings to be OFF.
- The “Telephone” section can be left as the default options.



During a meeting...

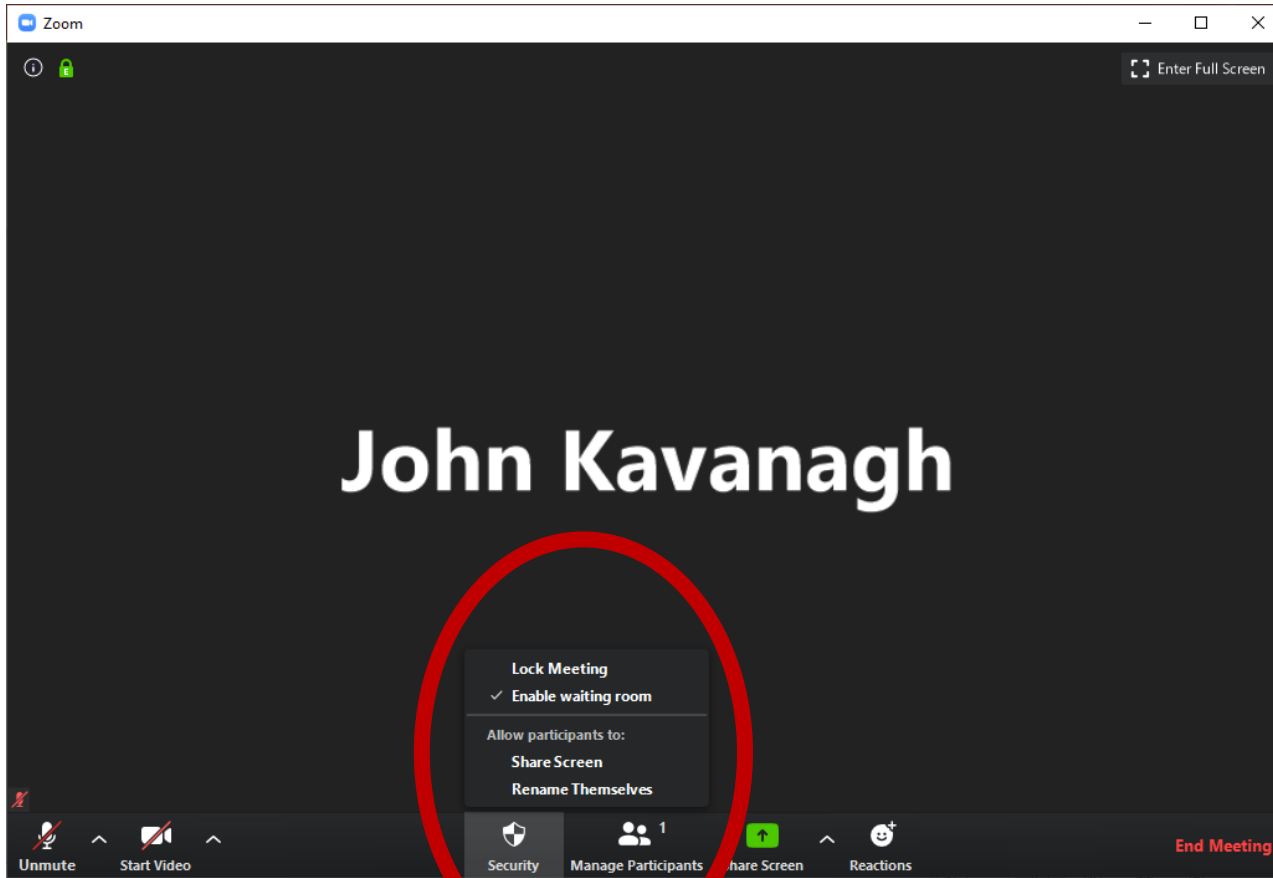
During a Session

Three key areas to control the session



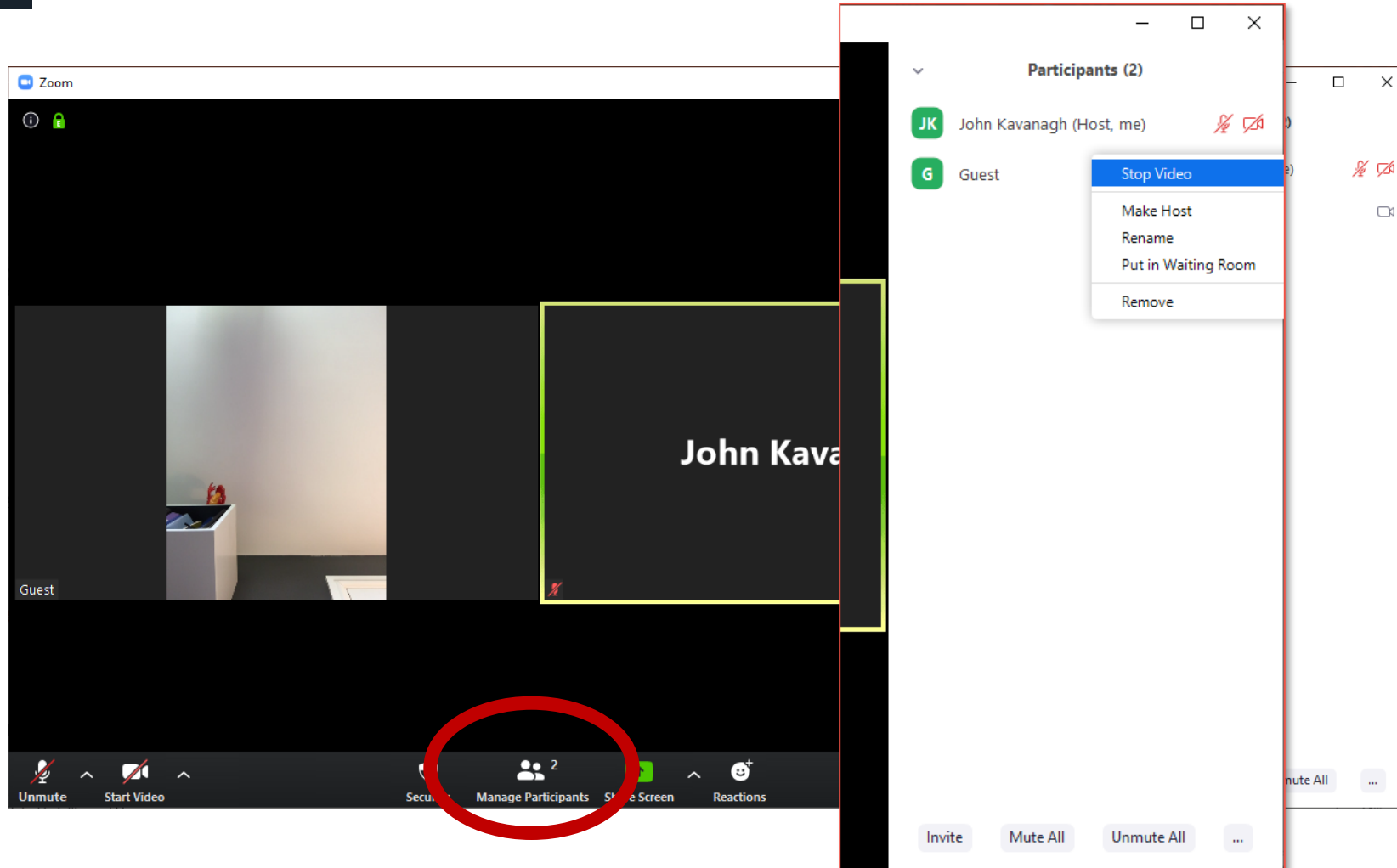
- Switching audio & video on and off
- Ending the meeting
- Controlling participants and content

Security features



- These features have already been set in the settings
- “Lock Meeting” will prevent anyone else from joining the meeting
- What happens if client is disconnected?

Participant list & Controls



- Control participants within the session
- You can remove a participant from the session



That's all, except ...

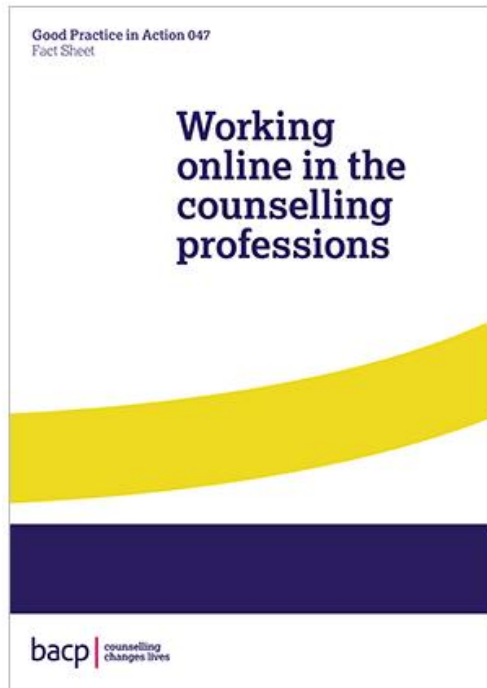
Things to consider in general

- It is video conference – people can see you!
 - Don't wear your pyjamas
 - Remember your facial expressions and body language
 - Pay attention
- It is video conference – people can see your room!
 - Remove personal items from the background
 - Try using “virtual background”
- Avoid being over-heard
 - Use headphones

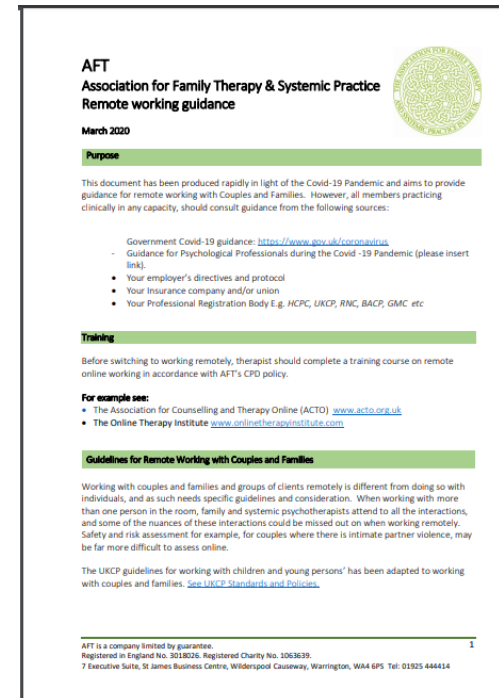
Things to consider as a Therapist

- Is your video conference provider GDPR compliant?
- Is an online platform appropriate for your clients age range
- What will you do if there is a technical interruption during your session?
- Is your client VC environment suitable?
- Can a 3rd party (parent or carer) eavesdrop or record your session?
- Do your policies and Terms & Conditions cover remote therapy?
- Does your insurance cover remote therapy?
- Do you have sufficient e-therapy supervision or peer support?

Additional Guidelines



BACP: Working online in the counselling professions



UKCP: Guidelines for online training.

Q&A

Ethernet cable connection



WiFi box probably came as part of your internet packages

On the back of the box will be a number (usually 4) "Ethernet ports" you can use to connect your computer directly to the internet with an Ethernet cable.



Ethernet cables have "RJ45" connectors on both ends and can be bought in lengths ranging from 0.5m up to 100m.

It should be rated as "Cat5e" as a minimum. Higher spec cables are available (Cat6, Cat7, etc) but are not normally necessary for short runs of cable

Follow-up Questions?

Would you benefit from additional support during the Covid-19 crisis:

- 1:1 support setting up for e-Therapy
- Trial-run sessions
- Ongoing support

Contact us

John.kavanagh@bluePANGOLIN.co.uk



John Kavanagh

bluePANGOLIN



Embrace • Connect • Energise

info@bluePANGOLIN.CO.UK

www.bluePANGOLIN.co.uk
