

Plataforma Zoom

Como reagir a ataques às sessões

Tipo de Documento: Alerta/Recomendação #006/2020

Identificação: Plataforma Zoom / Como reagir a ataques às sessões

Nível de Acesso: Público

Versão: 1.0

Data: 20/04/2020

Revisão: 22/04/2020

UNIVERSIDADE DE AVEIRO
GABINETE DE CIBERSEGURANÇA

ZOOM – COMO REAGIR A ATAQUES A SESSÕES

MOTIVAÇÃO

A utilização eficiente e produtiva do Zoom depende de um conjunto de medidas preventivas e outras reativas que garantam o correto controlo de cada sessão. Por vezes, os utilizadores são confrontados com situações inadvertidas ou propositadas na forma de ataque à sessão que perturbam o seu funcionamento. Os pontos seguintes tentam enquadrar respostas preventivas e reativas a estes ataques, começando com uma infografia de dicas de segurança disponibilizada pela FCT-FCCN¹.

10 DICAS
PARA MELHORAR A
SEGURANÇA NAS SUAS
SESSÕES DE COLIBRI

01 Utilize um ID exclusivo
Escolha "Gerar ID Aleatório" de forma a evitar que "invadam" a sua sessão.

02 Exija uma Password
Partilhe só com os seus participantes, por um outro meio de comunicação. Assim, não existirá partilha indevida da mesma.

03 Crie uma "Sala de Espera"
Verifique os nomes na sala de espera. Não reconhece algum dos nomes? Não os deixe entrar!

04 Ative a partilha de ecrã apenas para o Anfitrião
Ative esta configuração antes da sessão. Não há problema se esquecer, pode ativar durante a reunião.

05 Crie sessões com inscrição obrigatória
Proteja a sua sessão permitindo apenas utilizadores com convite e cujos endereços de email constam na sua lista.

06 Bloqueie a sua sessão
Selecione "Gerir Participantes", escolha "Mais" e depois "Bloquear Reunião"


07 Modere a sua sessão
Remova os participantes indesejados. Passe o rato sobre o nome da pessoa e escolha "Remove".

08 Desative o áudio dos participantes
Selecione "Participantes", clique no ícone de "silenciar todos". Ative o microfone apenas quando necessário.

09 Destaque o orador principal
Sob a imagem do orador clique em "mais opções" e selecione "Fixar Vídeo".

10 Grave a sua sessão
Grave a sua sessão no seu computador ou na cloud. No final transfira as suas gravações para o Educast

www.fccn.pt
www.colibri.fccn.pt

 **Colibri**

E-mail: colibri@fccn.pt
Telefone: +351 21 844 01 00

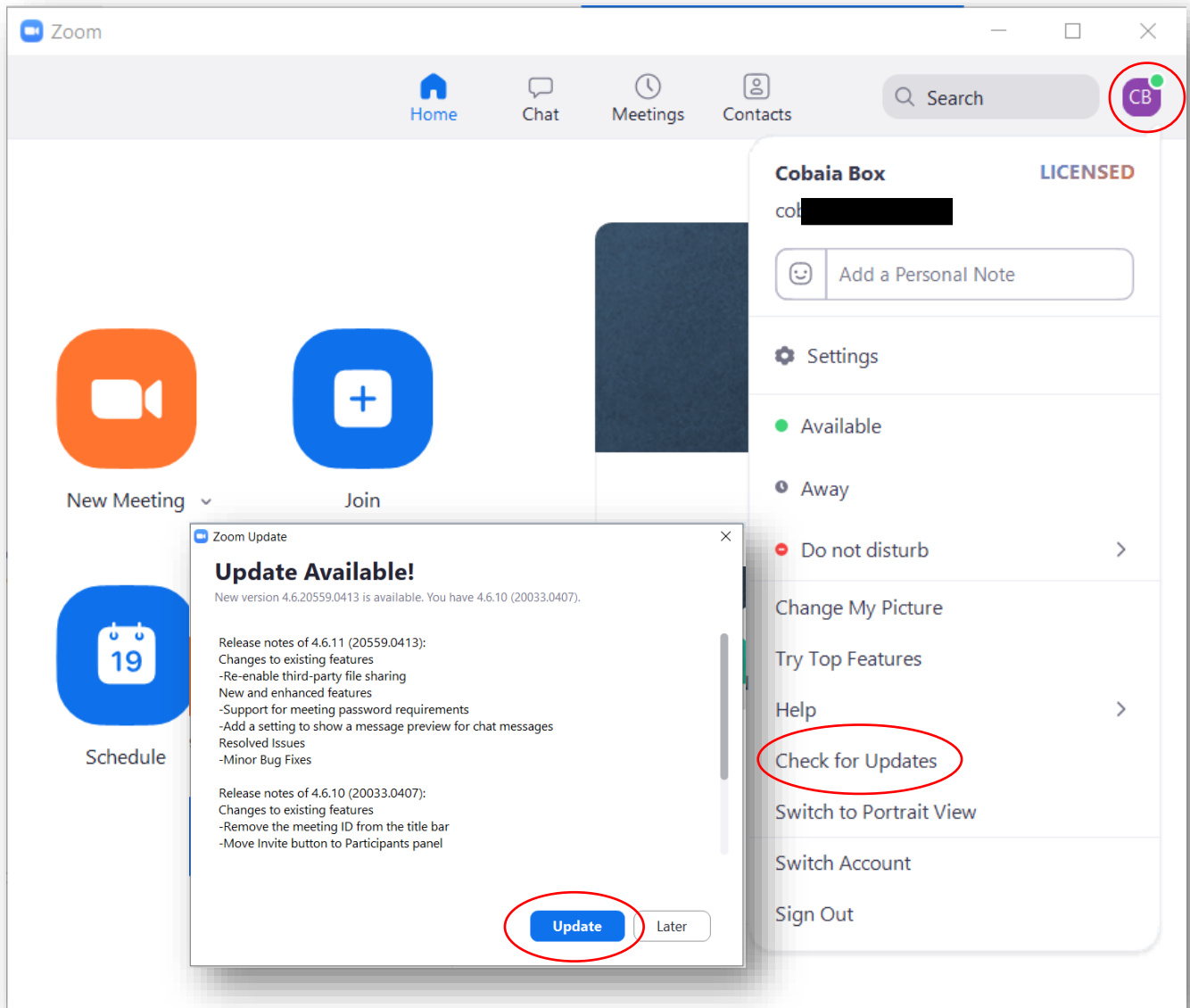
¹ <https://www.fccn.pt/colibri-colaboracao-com-seguranca-reforcada/>, de 22 de abril

MEDIDAS PREVENTIVAS

Todos os screenshots foram recolhidos na versão 4.6.10 para Windows.

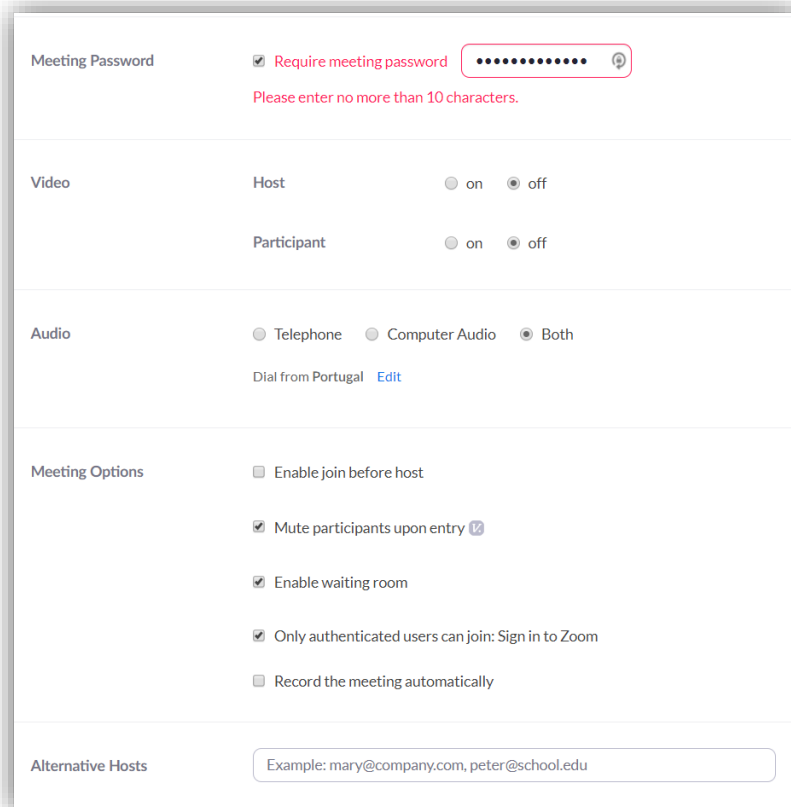
ATUALIZAÇÃO DA APLICAÇÃO

1. Verifique se tem a sua aplicação Zoom atualizada

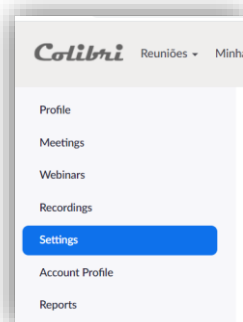


CRIAÇÃO DA SESSÃO

1. Criar a sessão (através do site <https://videoconf-colibri.zoom.us/>) com:
 - a. Password/PIN
 - b. Sala de espera
 - c. Autenticação de utilizadores
 - d. Áudio e vídeo desligados
 - e. Não ativar a reunião antes de o anfitrião entrar



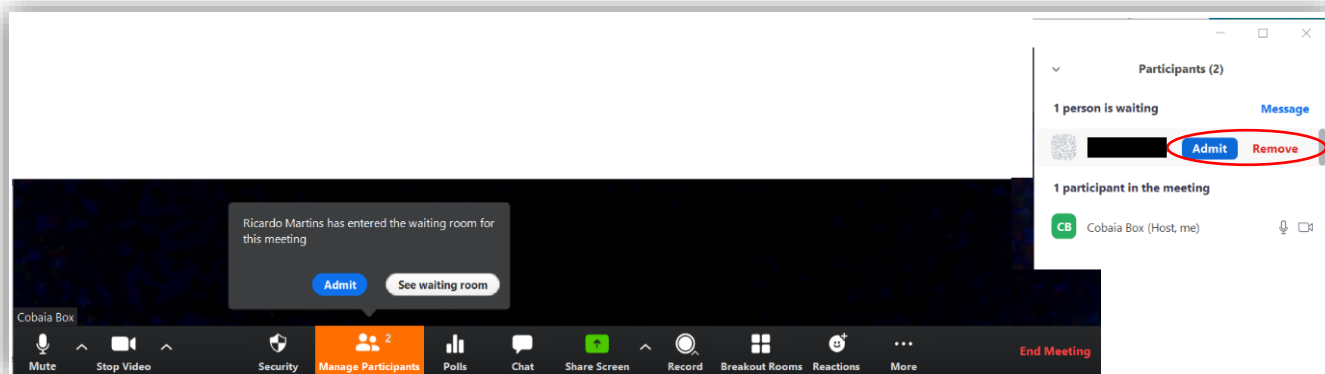
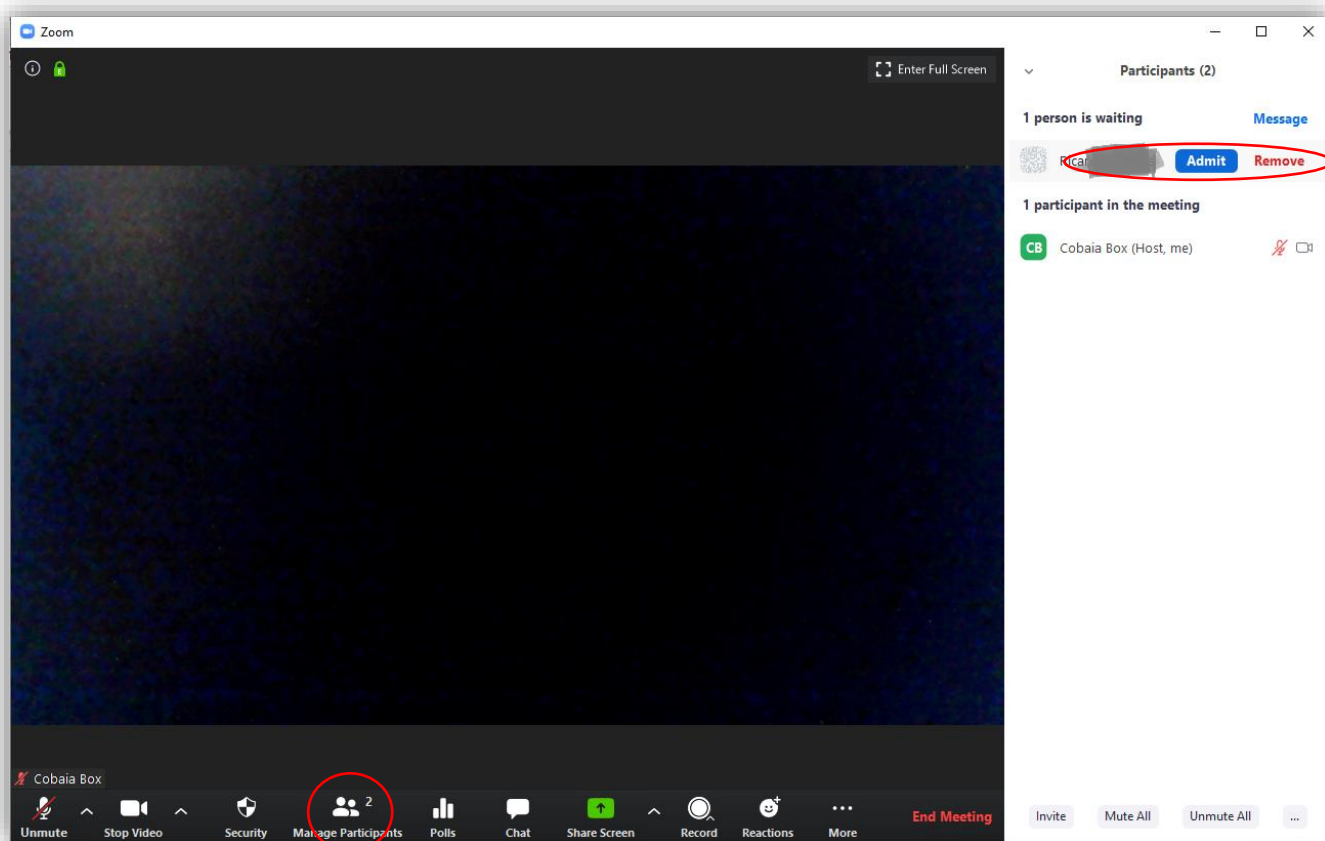
The screenshot shows the Zoom meeting creation settings page. It includes sections for Meeting Password, Video, Audio, Meeting Options, and Alternative Hosts. The Meeting Password section has a checkbox for 'Require meeting password' which is checked, and a password field with 10 dots. The Video section has radio buttons for Host and Participant, both set to 'off'. The Audio section has radio buttons for Telephone, Computer Audio, and Both, with 'Both' selected. The Meeting Options section has checkboxes for 'Enable join before host', 'Mute participants upon entry', 'Enable waiting room', 'Only authenticated users can join: Sign in to Zoom', and 'Record the meeting automatically'. The Alternative Hosts section has a text field with the example 'mary@company.com, peter@school.edu'.



2. Outras opções de segurança disponíveis em “Configurações/Settings”, dependem dos requisitos que a sessão vai ter em termos de funcionamento

ARRANQUE DA SESSÃO:

1. Verificar e autorizar a entrada a partir da sala de espera



(a admissão pode ser feita, um-a-um ou todos de uma só vez)

2. Eventualmente, pode bloquear a sessão e não permitir mais entradas na sala de espera.

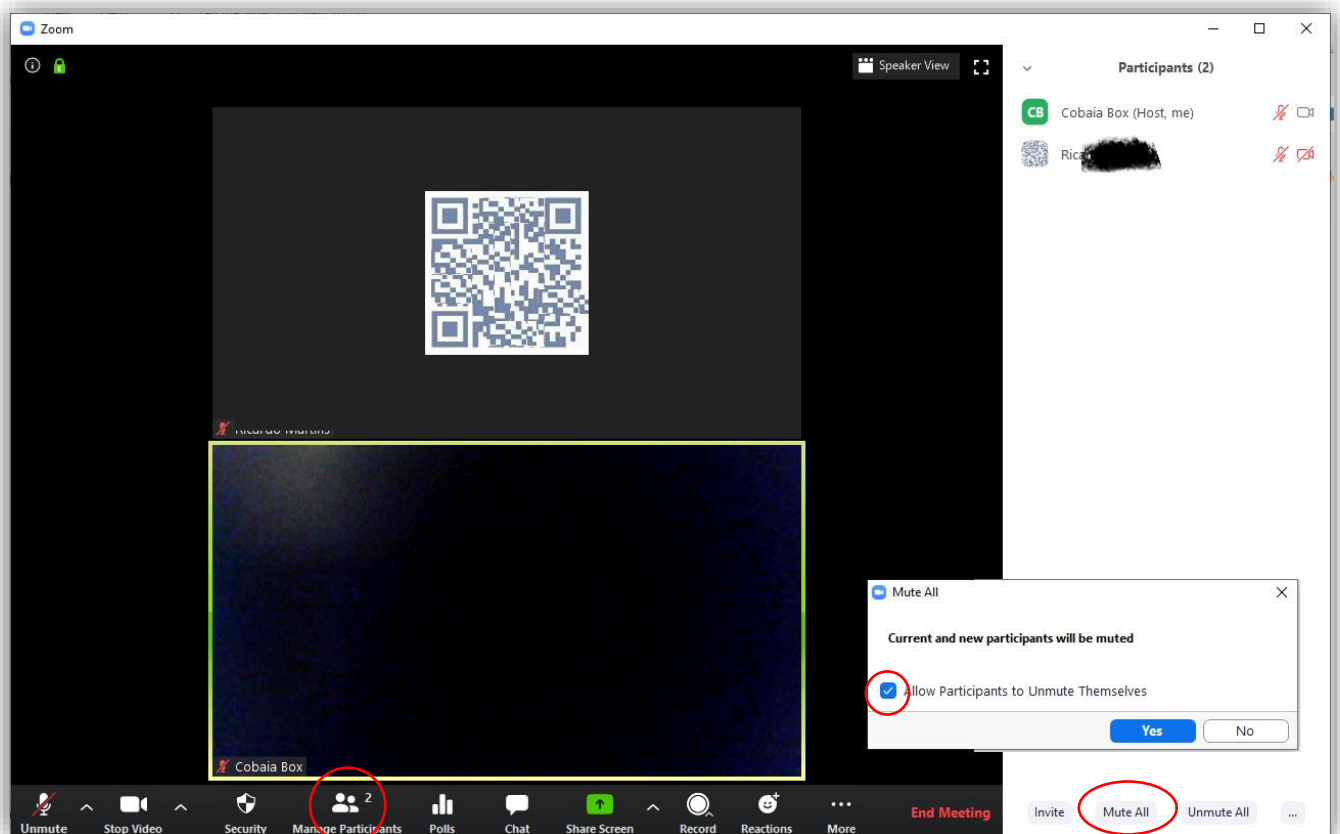
MEDIDAS REATIVAS

ALGUÉM INVADIU A SUA SESSÃO. O QUE FAZER?

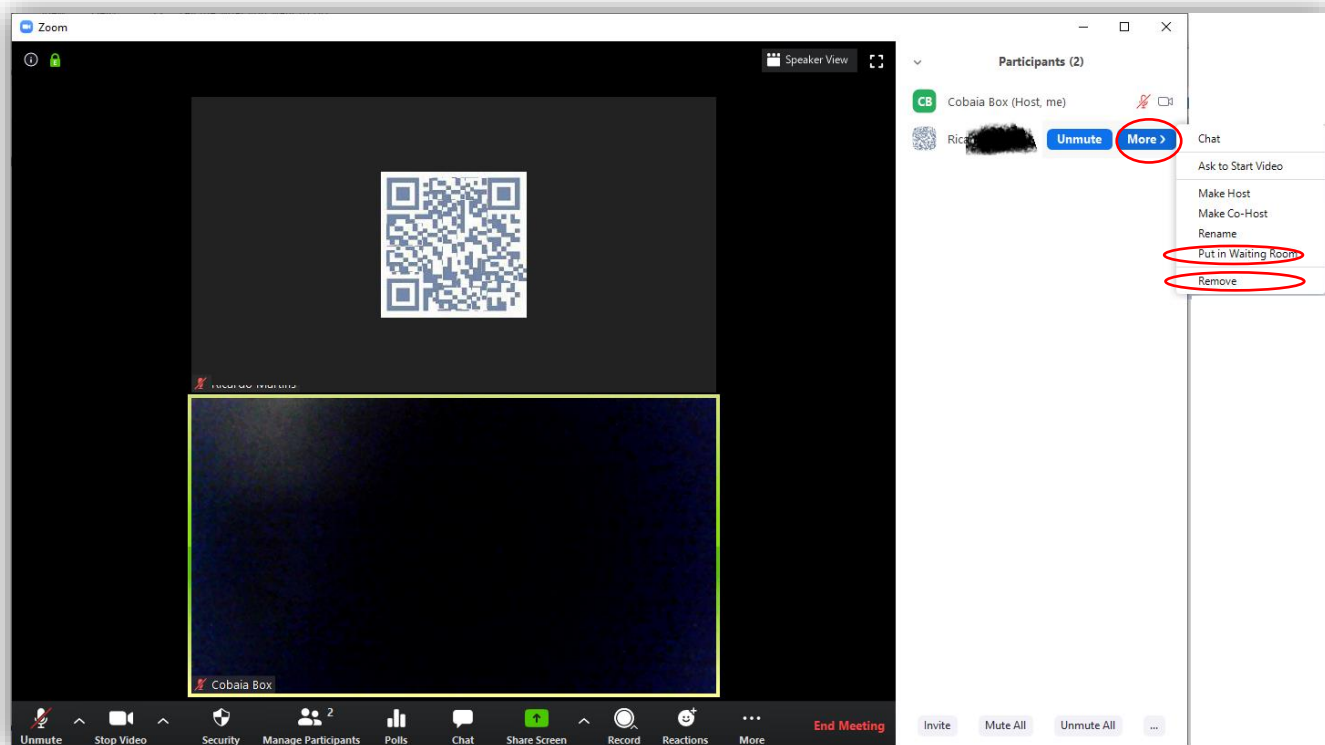
1. Bloquear a sessão (a barra pode aparecer em baixo ou cima, se estiver a partilhar conteúdos).



2. Silenciar o microfone de todos os participantes, impedindo-os de reativar o microfone

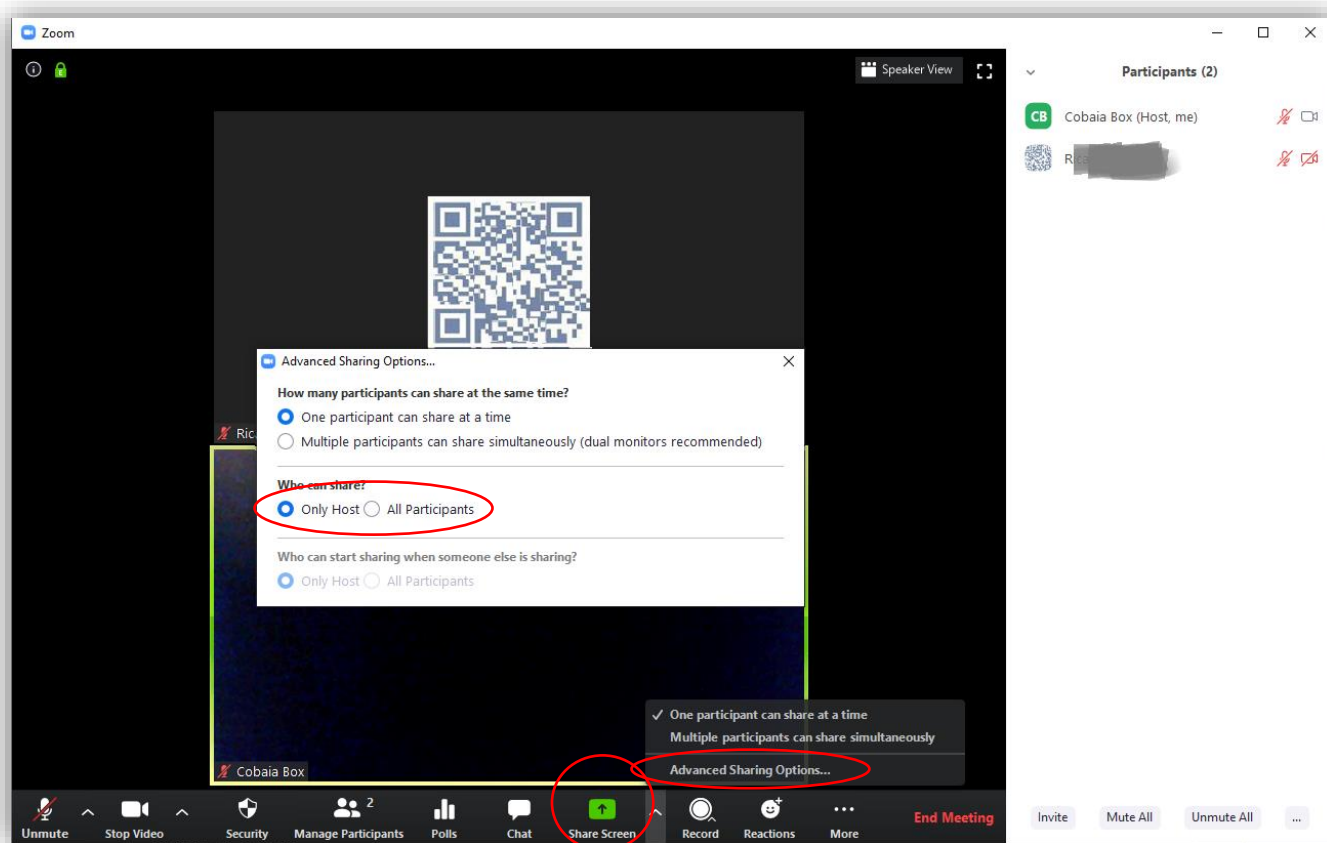


3. Optar por:
 - a. Colocar o utilizador na sala de espera (pode-o readmitir mais tarde)
 - b. Remover o utilizador da reunião (não pode voltar a entrar na reunião)



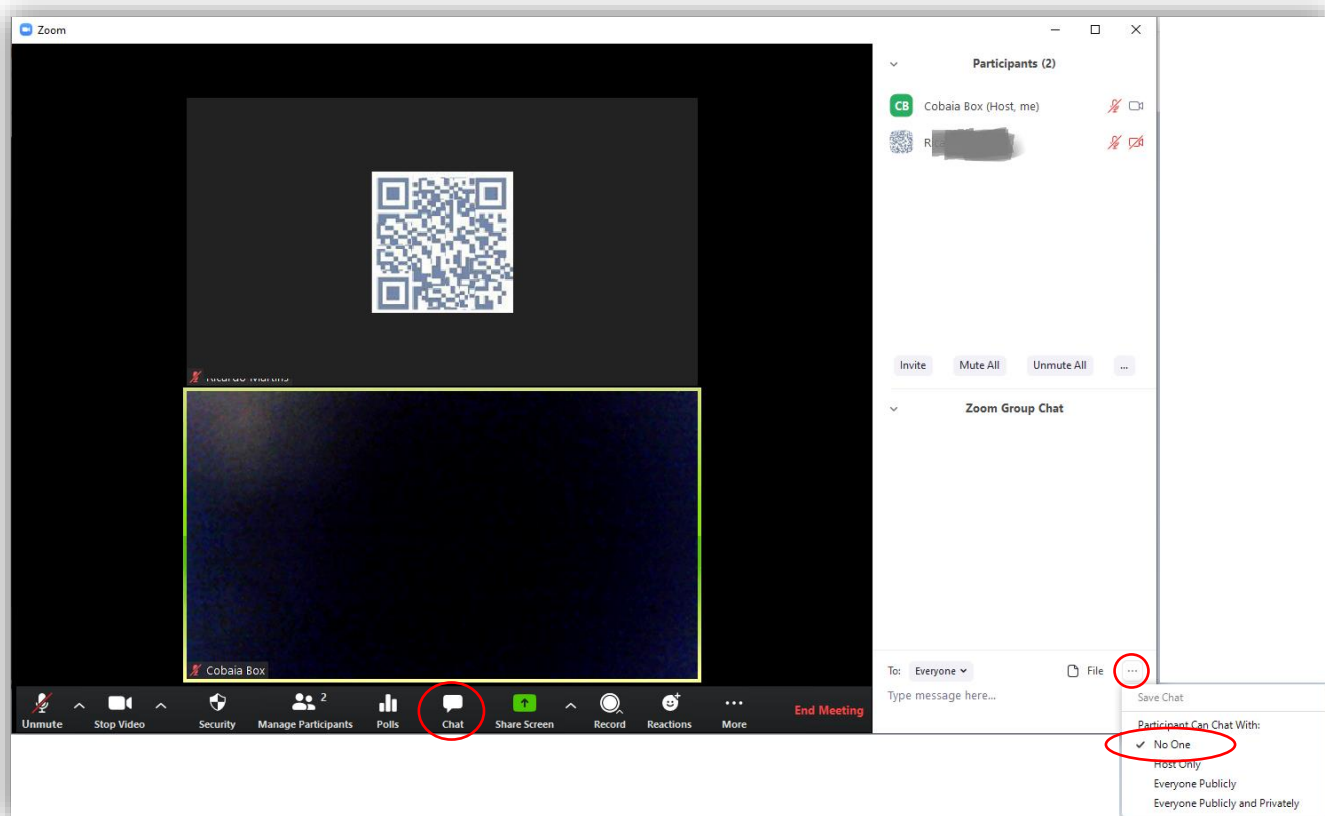
ALGUÉM ENTROU NA SESSÃO E ESTÁ A PARTILHAR CONTEÚDOS INDEVIDAMENTE. O QUE FAZER?

1. Bloquear a sessão
2. Colocar em Sala de Espera ou remover o responsável
3. Permitir apenas a partilha pelo anfitrião da sessão



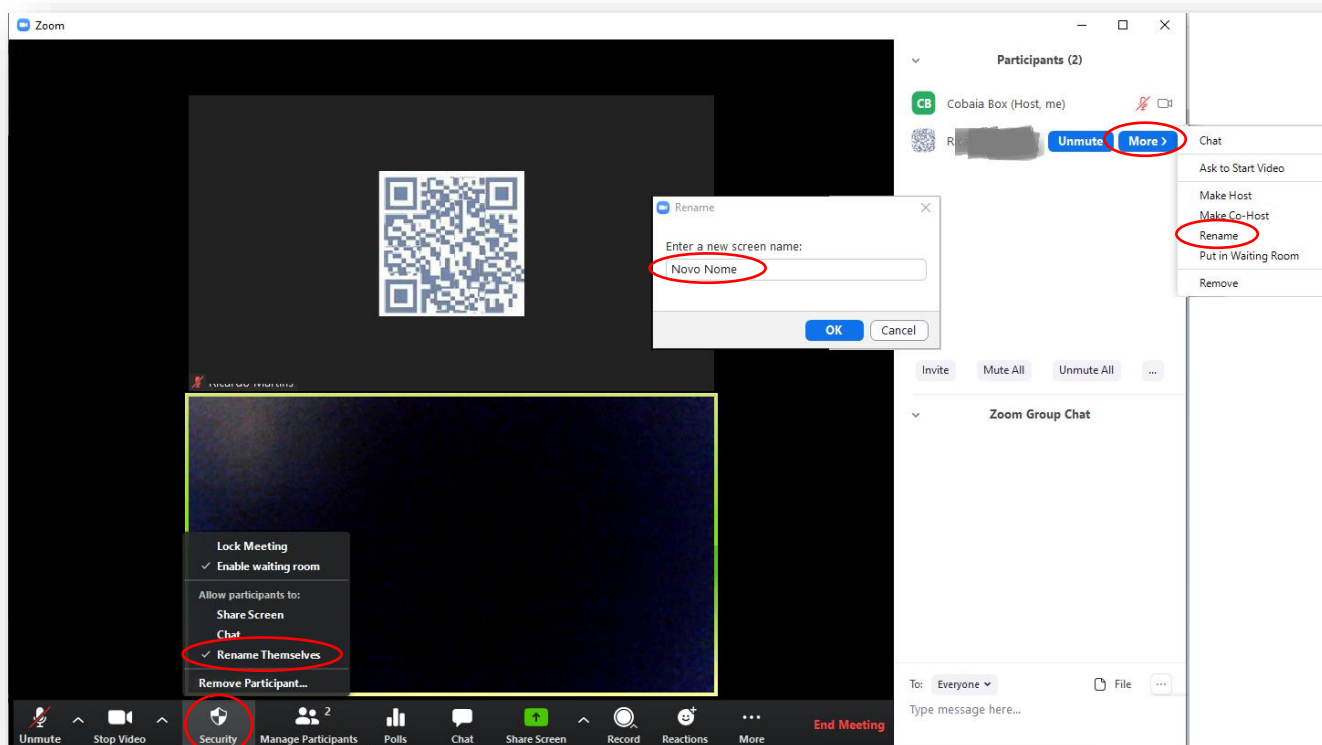
O CHAT ESTÁ A SER USADO PARA CRIAR DISTÚRBO NA SESSÃO. O QUE FAZER?

1. Bloquear o Chat, permitindo apenas o anfitrião



OS NOMES DOS PARTICIPANTES ESTÃO A SER ALTERADOS. O QUE FAZER?

1. Impedir os participantes de se renomearem
2. Renomear (um-a-um) os participantes



A SUA SESSÃO FOI PERTURBADA E QUER APRESENTAR QUEIXA. O QUE FAZER?

1. Recolha a informação sobre:
 - a. Data/hora
 - b. ID da Sessão
 - c. Participante(s) que perturbaram
 - d. Screenshots das ocorrências
 - e. Lista de participantes
2. Contacte o Gabinete de Cibersegurança

REFERÊNCIAS VÁRIAS

<https://www.ua.pt/stic/page/14597>

<https://www.ua.pt/pt/apoio-ensino>

<https://www.fccn.pt/colibri-colaboracao-com-seguranca-reforcada/>

<https://videoconf-colibri.fccn.pt/doc/secure>

<https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/>

<https://www.cncs.gov.pt/recursos/noticias/orientacoes-para-utilizacao-das-tecnologias-para-o-ensino-a-distancia/>