FIQUE MAIS SEGURO

Recomendações de segurança para a utilização da plataforma Zoom (versão 1.1.1)

O Zoom é a plataforma de videoconferência adotada pela PUC-Rio para a realização de reuniões remotas, aulas on-line, e para gravação de aulas.

A fornecedora da ferramenta foi questionada, formalmente, pela Coordenação Central de Educação a Distância – CCEAD, acerca da segurança da plataforma, e ofereceu uma série de recomendações e cuidados, listados abaixo.

1. Caso estejam disponíveis atualizações oferecidas pela ferramenta, recomenda-se aplicar.

   Isto garante que você esteja sempre em linha com as práticas mais seguras, correção de bugs e atualizações periódicas. Se o seu Zoom já foi atualizado, algumas das recomendações abaixo serão selecionadas como padrão.

2. Não compartilhe arquivos ou links no chat; se alguém compartilhar, não os utilize, a menos que tenha certeza da origem.

   Lembre-se de que a Internet não é um ambiente totalmente seguro. Neste sentido, é importante que você tenha cuidado ao navegar em links desconhecidos ou ao acessar arquivos que tenham origem duvidosa.

3. Gravação e disponibilização de videoaulas.

   O Zoom notifica os participantes quando um anfitrião grava uma reunião, e oferece uma forma segura para que guarde a gravação. As reuniões do Zoom são gravadas apenas a pedido do anfitrião e somente devem ser gravadas localmente na máquina do anfitrião. A disponibilização destes vídeos deve ser feita em uma plataforma de streaming de vídeo proprietária e com acesso limitado. A CCEAD tem disponível um serviço de publicação de vídeos no Vimeo, que atende a esse quesito.

4. Nível de segurança das informações compartilhadas.

   O conteúdo é transmitido de forma criptografada entre um "Zoom endpoint" e outro "Zoom endpoint", que é a forma como a empresa se refere aos seus servidores. A companhia também informa que o conteúdo não é decifrado enquanto trafega pela sua nuvem.

5. Atenção e cuidado com o compartilhamento de tela dos convidados.

   Ao restringir o compartilhamento de tela ao anfitrião da chamada, você pode impedir que outras pessoas exibam o que está nas suas na áreas de trabalho. Isso não impedirá ninguém de participar da reunião, mas, pelo menos, impedirá que um hacker assuma o controle e compartilhe material inapropriado.

6. Exija que o anfitrião (professor) esteja presente.

   O Zoom fornece a opção para a sua reunião iniciar já quando a primeira pessoa ingressa, mesmo que não seja o anfitrião. Isto pode ser conveniente se você estiver organizando uma reunião e se encontrar alguns minutos atrasado. Entretanto, para uma melhor proteção, verifique se a configuração "Habilitar ingressar antes do anfitrião" está desativada (geralmente está, por padrão) no 'menu avançado', quando for agendar uma reunião.

7. Mantenha seu ID da reunião pessoal privado.

Não compartilhe seu ID Pessoal de Reunião (personal ID, ou PMI). Se o fizer, será relativamente fácil para qualquer pessoa o encontrar e participar de qualquer reunião que você esteja organizando. Em vez disso, use uma identificação de reunião exclusiva para cada reunião. Ao agendar uma reunião, o Zoom pode fazer isso por padrão. Apenas certifique-se de que a opção de configuração de agendamento **ID da Reunião** tenha a opção "**Gerar automaticamente**" selecionada.

8. **Use uma senha.**

   Você poderá ativar o recurso no Zoom que protege as reuniões com uma senha, e compartilhá-la apenas com as pessoas que você deseja na sua reunião. A senha pode ser incorporada pelo próprio Zoom na URL, e recomenda-se que ela seja sempre usada.

9. **Use a sala de espera.**

   Outra opção é ativar o recurso de sala de espera (waiting room), que coloca todos os convidados em uma sala de espera virtual antes do início da reunião. Quando estiver pronto, você precisará autorizar manualmente seus convidados a entrar. Essa opção também se encontra no 'menu avançado', quando você agenda uma reunião. Uma recomendação para o anfitrião é verificar se os alunos listados como participantes de fato fazem parte da turma. Solicite sempre que eles se identifiquem com seus dados reais.

Ao consultar formalmente a Zoom, a PUC-Rio recebeu um conjunto de recomendações e posicionamentos que a mantém confiante de que esta é uma ótima plataforma para uso em atividades on-line, no momento. Para oferecer mais transparência, seguem os links fornecidos:

- https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/
- https://zoom.us/security
- https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/
- https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/
- https://zoom.us/privacy
- https://zoom.us/docs/en-us/covid19.html

A CCEAD sempre atualizará estas recomendações em suas páginas e, neste momento, orienta a leitura dos seguintes documentos:

CONDUTA, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS
FAQ DIREITOS AUTORAIS E CUIDADOS COM O VIMEO
https://www.educacaodigital.ccead.puc-rio.br/ na seção FIQUE LEGAL

10 DICAS PARA BONS ENCONTROS ONLINE
https://www.educacaodigital.ccead.puc-rio.br/ na seção TUTORIAIS/FOLHETOS

Atenciosamente,
Coordenação Central de Educação a Distância