Zoom Meetings:
8 dicas e boas práticas de segurança

09 de abril de 2020

O Zoom, ferramenta robusta e consolidada de videoconferência empresarial, apresentou falhas de segurança da informação recentemente admitidas pelo CEO da empresa. Lançada em 2011, ela apresentou um crescimento vertiginoso de quase 2.000% de seu uso durante a pandemia do novo coronavírus (o covid-19). Segundo a empresa, o número de participantes diários passou de cerca de 10 milhões (no fim de 2019) para 200 milhões (em março de 2020).

O que isso significa na prática?

Essa crescente popularidade do aplicativo atraiu *trolls* e *hackers* que exploraram algumas das falhas de segurança encontradas para praticar diversos ataques cibernéticos, entre eles o *Zoombombing* ou "invadindo o Zoom", em tradução livre (uma prática criminosa de assédio virtual, conhecida pela interrupção de reuniões públicas com intuito de exibir conteúdos impróprios).

Por padrão, as reuniões do Zoom são públicas e permitem o compartilhamento de tela por qualquer um dos participantes. Dessa forma, os criminosos se aproveitam dessas configurações permissivas para invadir reuniões e compartilhar pornografias e imagens violentas, além de insultos raciais, discursos de ódio, entre outras ofensas.

Outras vulnerabilidades já identificadas possibilitam que *hackers* mais sofisticados possam ouvir as conferências, controlar as câmeras dos participantes e acessar as mensagens do bate-papo.

Qual a relação das vulnerabilidades do Zoom com as normativas de Proteção de Dados?

Dentre as vulnerabilidades identificadas verificou-se algumas que ferem os direitos fundamentais de liberdade e de privacidade do usuário.

Um dos recursos do aplicativo, já descontinuado desde o início de abril, possibilitava o cruzamento e a transferência dos dados cadastrados no aplicativo para as redes sociais LinkedIn e Facebook. Dessa forma, por meio da integração era possível obter alguns outros dados do usuário como o seu nome real, cargo, localidade, modelo do smartphone, entre outros. Portanto, tanto a coleta como o tratamento de alguns desses dados, realizados sem o consentimento prévio, estão em desacordo com as legislações vigentes de Privacidade e Proteção de Dados.

Após relatos de sequestros em massa de videoconferência, o escritório do FBI notificou o Zoom sobre suas medidas de privacidade e segurança da informação. Também foi divulgado um canal para que qualquer pessoa, dos Estados Unidos, que tenha sido prejudicada entre em contato com o Centro de Reclamações de Crimes pela Internet.

No Brasil, o Ministério da Justiça e Segurança Pública também solicitou esclarecimentos sobre o compartilhamento de dados e a política de privacidade de forma a embasar e concluir um parecer sobre a potencial violação de direitos dos consumidores, com base na legislação brasileira. Caso a solicitação não seja atendida no prazo de até 10 dias, será instaurado processo administrativo, que eventualmente poderá resultar na imposição de multa.

Vale ressaltar que a legislação brasileira que entrará em vigor em breve, a LGPD – Lei Geral de Proteção de Dados Pessoais, em seu capítulo dedicado a Segurança e Boas Práticas, aborda a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado dos dados.

Comprovada a infração e a não adoção das medidas adequadas as empresas ficarão sujeitas às sanções administrativas da LGPD que vão desde a advertência até a multa simples, de até 2% (dois por cento) do faturamento, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

O Zoom é seguro? Qual o impacto para os usuários que continuam utilizando?

Para o público em geral o Zoom não apresentou muitas medidas significativas imediatas, além da adoção de senhas codificadas para todas as reuniões e bloqueio de alguns recursos. A sua política de privacidade foi atualizada recentemente, como uma tentativa de demonstrar a transparência de suas ações, mas ainda deixa muito a desejar em relação a conformidade com às normativas vigentes de Privacidade e Proteção de Dados. Segundo a empresa, o plano para finalizar as correções é de 90 dias.

O zoom foi projetado para ambientes corporativos com suporte completo de Tecnologia da Informação e não para discussões públicas abertas, eventos sociais como os encontros casuais com amigos. Portanto, é importante explicitar que a criticidade de se utilizar o aplicativo está relacionada aos riscos de segurança da informação que assumimos com essa escolha (o compartilhamento de informações confidenciais e restritas por meio de recursos – PC, Notebook, Tablet, Navegador de Internet – que não possuem os requisitos mínimos de segurança da informação e/ou não estão configurados adequadamente).

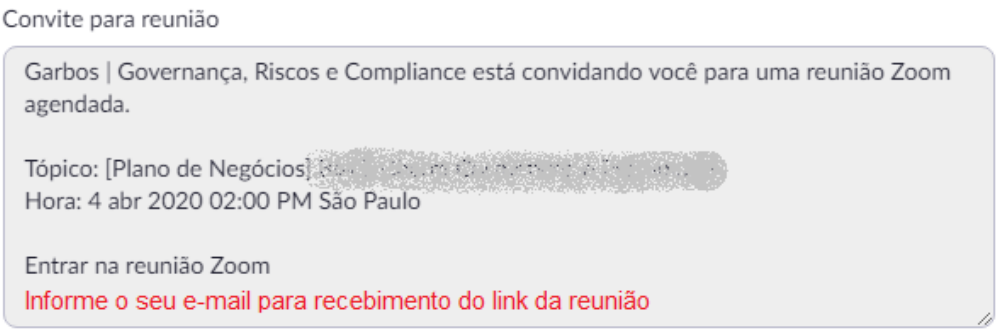
Sem as atualizações e correções de segurança necessárias, os usuários domésticos ficarão mais vulneráveis e desprotegidos e, portanto, é aconselhável que adotem algumas práticas de segurança para atenuar as ameaças e prevenir dos ataques cibernéticos.

Dicas e boas práticas para utilização do Zoom com segurança

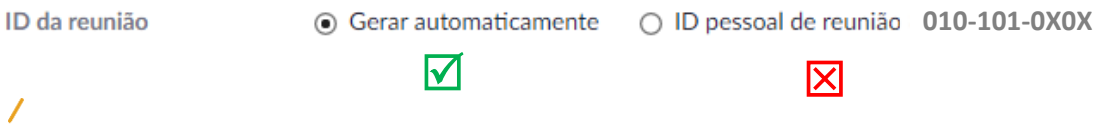
O Zoom possui vários recursos que poderão ser configurados (aba Configurações) para maior segurança e proteção de suas reuniões.

Atualmente podemos encontrar muitos links de reunião compartilhados nas redes sociais ou em outros fóruns públicos, ato que torna o evento público e, portanto, qualquer outra pessoa mal-intencionada que consiga o link poderá participar da reunião. Para evitar esse e outros tipos de problemas, seguem algumas dicas.

O **CONVITE PARA A REUNIÃO** deve ser enviado, preferencialmente, por e-mail ou outra forma de mensagem privada. Opcionalmente você também poderá configurar suas chamadas para exigir um RSVP (responda, por favor). Nesse caso, as pessoas convidadas precisam enviar o seu e-mail para confirmação e recebimento do link da reunião.



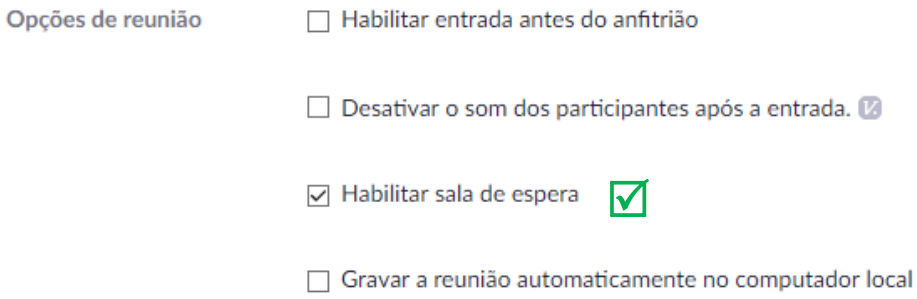
Evite usar seu **ID DE REUNIÃO** pessoal para organizar eventos públicos, pois ele poderá ficar suscetível a utilização futura por criminosos. O uso do ID de reunião aleatório, gerado automaticamente, é uma boa prática a ser adotada.



O **USO DE SENHAS** é indispensável. Essa é a melhor forma de evitar que reuniões sejam invadidas ou monitoradas com esse método de rastreamento (*Zoombombing*).

4

O recurso **SALA DE ESPERA** é indispensável para que o administrador da reunião possa controlar quem poderá ingressar na sala de reunião (todos os participantes ou somente os participantes autorizados). Você pode autorizar um a um ou então todos de uma só vez.



5

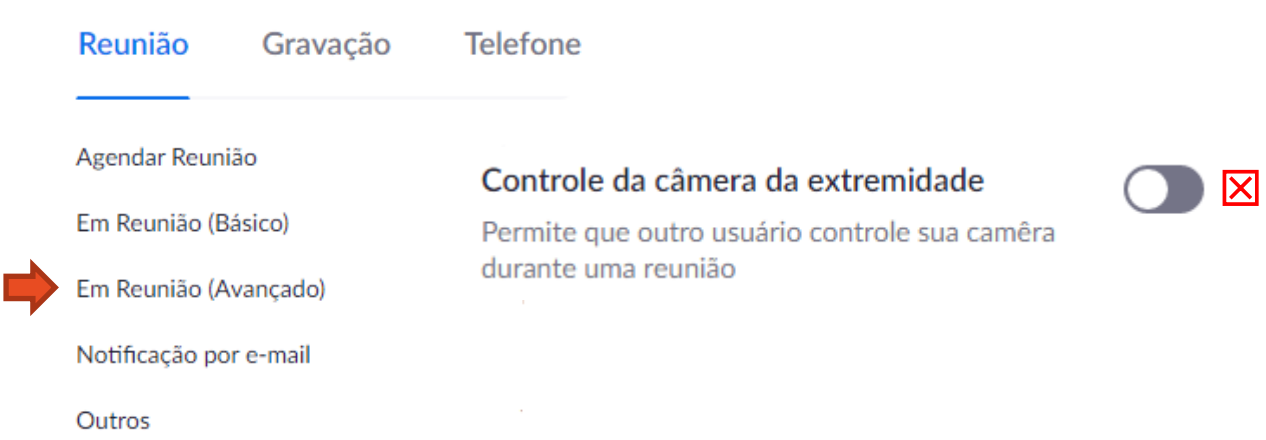
É recomendável que o administrador da reunião restrinja o recurso de **COMPARTILHAMENTO DA TELA** para que ele seja o único responsável e assim reduza as chances de compartilhamento de conteúdo indesejado com os participantes.

6

Desabilitar a opção de **BATE-PAPO PRIVADO** reduz as chances de envio de spam e a transferência de arquivos impróprios por meio de um invasor que se faz passar por outra pessoa na tentativa de entrar em contato com um dos participantes da reunião.

É permitido utilizar qualquer imagem como **PLANO DE FUNDO** durante as chamadas no Zoom. A partir desse momento, toda chamada que você realizar com o Zoom adotará por padrão esta imagem ou vídeo como plano de fundo. Esse recurso evita a exibição acidental ou ilícita dos participantes.

Desabilitar a opção de **CONTROLE DE CÂMERA** reduz as chances de um invasor se passar por um dos participantes e desbloquear a sua câmera, evitando assim uma exibição ilícita e embaraçosa.



Como a Garbos irá auxiliar a sua empresa?

A Garbos oferece uma variedade de serviços de gestão e governança para auxiliar sua empresa, de forma rápida e eficiente, como a consultoria em Segurança da Informação para elaboração dos documentos normativos: políticas, normas, procedimentos e manuais. Entre em contato e agende uma visita, sem compromisso, com nossos consultores: contato@garbos8.com.br

GARBOS

GOVERNANÇA, RISCOS E COMPLIANCE

www.garbos8.com.br

contato@garbos8.com.br

garbos8

/company/garbos8

garbos8

garbos8