P&B COMPLIANCE | PAGLIA & BREUNIG

Guia de boas práticas para reuniões on-line.

Participar de reuniões on-line já era uma prática comum no dia a dia de muitos trabalhadores, entretanto, após o surgimento da pandemia causada pelo novo coronavírus (COVID-19), e consequentemente pelo isolamento social recomendado pelas autoridades de saúde, a realização de reuniões por meio da internet se tornou uma prática diária e indispensável para o funcionamento de escritórios, empresas, organizações e até mesmo reuniões de amigos.

Desta forma, a P&B Compliance elaborou o presente "Guia de boas práticas para reuniões on-line", que busca minimizar exposições pessoais, riscos relacionados à segurança da informação e o vazamento de dados pessoais.

1 - Minimização de exposições pessoais:

1.1. A escolha do ambiente ideal:

É importante estar atento ao ambiente físico dentro de sua casa em que você participará da reunião. Escolha um local que não tenha grande circulação e, se possível, feche a porta. Durante a atual pandemia diversos vídeos viralizaram pela internet com participações inusitadas em videoconferências, como animais de estimação e crianças interrompendo as reuniões.

1.2. Comporte-se:

A reunião pode estar acontecendo por videoconferência e você pode estar dentro da sua casa, entretanto é importante que se mantenha a etiqueta e o comportamento exatamente como se você estivesse no escritório. Assim, vista-se de acordo com o esperado, arrume os cabelos, lave o rosto, tenha um bloco de anotações à mão e, se possível, indique que gostaria de participar, sem interromper os outros participantes. A pontualidade também é um fator fundamental para o sucesso da sua reunião.

1.3. O uso de câmeras e microfones:

Caso não haja necessidade, deixe sua câmera e seu microfone desligados. Desta forma, haverá menos interrupções durante a reunião. Utilize fones de ouvido com microfone, estes equipamentos são melhores do que o uso do microfone interno do notebook, que pode causar ecos ou distorções. Ainda, prefira áudio ao vídeo, pois se a qualidade de uma conexão for baixa a experiência da reunião não será tão boa quanto poderia.

2 – Segurança da Informação:

2.1. Utilize ferramentas confiáveis e, se possível, criptografadas:

Há diversas ferramentas que possibilitam uma reunião online. Pesquisa todas as ferramentas disponíveis e veja a que melhor se adeque às necessidades de sua reunião e de sua empresa. Opte para que toda a empresa utilize a mesma ferramenta, para que o uso seja uniforme e todos saibam utilizá-la adequadamente. Prefira ferramentas que tenham recursos como sala de bate papo, essencial para a anotação de dúvidas e observações sobre a matéria, e se há modos de indicar quando um participante quiser participar, como a ferramenta de "levantar a mão".

2.2. Políticas e normas de segurança da informação:

O vazamento de informações é algo que vem preocupando cada dia mais as empresas e durante o home office as empresas têm dificuldade de monitorar se os seus funcionários estão seguindo todas as diretrizes relacionadas à segurança da informação. Assim, é importante que a empresa mantenha treinamentos frequentes relacionados à segurança da informação para os seus funcionários, explique detalhadamente cada norma e cada política, bem como a importância de evitar incidentes.

2.3. Proíba que funcionários gravem as reuniões:

Seguindo a linha da segurança da informação, é essencial que os funcionários sejam avisados se é permitida ou não a gravação das reuniões. Durante as videoconferências podem ser expostas informações valiosas sobre a empresa, sobre funcionários, segredos de negócios e mais ativos de informação essenciais para a vida

da empresa. Desta maneira é essencial que a empresa explique aos funcionários sobre as complicações que podem ser geradas por conta de uma informação disponibilizada a terceiros de maneira ilegal. Ainda, se possível, utilize aplicativos que não permitam gravações de tela, nem o famoso print screen.

2.4. Desative a VPN:

Talvez a empresa em que você trabalha tenha lhe fornecido um serviço de VPN (Virtual Private Network), que permite que você use a rede da empresa quanto trabalha remotamente. Muitas vezes a VPN limita a largura de banda larga disponível. Nesse caso, você pode fazer as reuniões por videoconferência fora da VPN para ter uma experiência de melhor qualidade.

2.5. Cada usuário deve utilizar um login:

Forneça um e-mail e uma senha para cada usuário acessar a reunião. Normalmente são utilizados o e-mail profissional e a senha deste e-mail para a participação em videoconferências, porém, é sempre importante frisar que cada funcionário deve utilizar o seu próprio login e que logins não devem ser compartilhados entre colegas. Esta é uma medida fundamental que garante que só acessarão a reunião e as informações disponibilizadas os funcionários que precisem de tais informações.

2.6. Faça um disclaimer no convite para a videoconferência:

Envie um pequeno manual de como as pessoas devem se comportar durante a videoconferência, quais as principais regras, quais dados pessoais poderão ser tratados e porque serão tratados durante a videoconferência, bem como o assunto que será tratado.

3 - Vazamento de Dados Pessoais

3.1. Fique atento às permissões concedidas aos aplicativos:
É essencial que a empresa escolha um aplicativo confiável para as videoconferências, conforme destacado acima, entretanto, os funcionários devem prestar muita atenção às permissões que concedem aos aplicativos, principalmente quando baixados no celular. Suspeite de permissões invasivas e confira os dados aos quais o aplicativo requer acesso para funcionar, que devem ser relacionados apenas ao funcionamento da câmera e do microfone do aparelho celular

3.2. Desative notificações em pop-up ao compartilhar a tela:
Ao compartilhar a tela do computador ou do celular durante chamadas de vídeo é importante desativas notificações em pop-up de e-mails, redes sociais e aplicativos de mensagem. As mensagens podem tratar de assuntos privados desnecessários à reunião.

3.3. Envie o convite da chamada apenas para e-mails confiáveis:
Não compartilhe links de convites de chamadas de vídeo pelas redes sociais, prefira encaminhá-los de forma privada utilizando o endereço de e-mail dos participantes da reunião. Compartilhar a URL dos convites pode atrair desconhecidos e cibercriminosos para a chamada de vídeo, comprometendo informações dos participantes.

3.4. Evite o phishing:

Phishing é um tipo de crime virtual. Trata-se da prática de coletar informações e dados secretos dos usuários através de informações falsas ou dados não reais, porém muito atrativos. Atualmente muitos cibercriminosos utilizam sites semelhantes aos sites dos aplicativos de conferência para "roubar" as informações de logins e senhas de e-mails de pessoas e fazer mau uso de tais informações. Portanto, é importante estar atento aos sites e aplicativos que você fornece suas informações de acesso.

3.5. Atualize o antivírus:

O antivírus é um programa de segurança básico e essencial para ter em seu computador. Além de proteger a máquina e os sistemas contra vírus e malwares, ele ainda pode evitar travamentos e a lentidão do computador.

3.6. Habilite a autenticação de dois fatores em suas contas de e-mail e redes sociais:

Recentemente muitos usuários do aplicativo de mensagens instantâneas WhatsApp foram surpreendidos ao caírem em um golpe que "roubava" sua conta do aplicativo. Como medida de segurança foi indicado que todos os usuários do aplicativo instalassem a autenticação em dois fatores para o uso do mesmo. É essencial que esta medida seja adotada para todos os aplicativos possíveis, como contas de e-mail e redes sociais. Assim, você precisará inserir uma senha sempre que abrir o aplicativo em seu celular.

P&B COMPLIANCE | PAGLIA & BREUNIG

Rua Funchal, n. 263, 1° andar
Vila Olímpia - São Paulo/SP - 04551-060
contato@compliancepb.com.br