

# Como manter sua empresa segura dentro e fora do escritório

Quer você trabalhe em casa ou no escritório, a segurança da sua empresa deve ser priorizada. Apesar de esses dois locais parecerem diferentes, podem-se usar as mesmas precauções independentemente de onde você estiver trabalhando. Vamos analisar algumas regras importantes de segurança cibernética e como elas podem ser usadas em ambos os ambientes de trabalho.

## Use somente dispositivos seguros

- Lembre-se de que a segurança do seu dispositivo depende dos aplicativos executados nele. Nunca instale um aplicativo ou plug-in sem antes consultar o departamento de TI.
- Use seus dispositivos de trabalho somente para tarefas relacionadas ao trabalho. Caso esteja usando seu computador pessoal para trabalhar, recomendamos que você crie uma conta de usuário separada com um nome de usuário e senha exclusivos.
- No escritório, a segurança de rede provavelmente é gerenciada pelo seu departamento de TI. Para ajudar a manter sua conexão de internet segura em casa, use uma senha complexa no roteador. Além disso, se sua empresa oferece acesso a uma Rede Virtual Privada (Virtual Private Network, VPN), conecte-se a ela.

## Proteja seu espaço de trabalho físico

- No escritório, cuidado com piggybacking e tailgating. Um piggybacker é alguém que alega fazer parte de sua empresa e segue você até uma área de segurança sem usar um crachá ou código de entrada. Um tailgater é alguém que espera você entrar ou sair de uma área de segurança para entrar sorrateiramente enquanto a porta ainda estiver aberta. Desconfie de qualquer pessoa que você não reconheça e não hesite em pedir que ela se identifique.
- Em casa, encontre um espaço de trabalho privado e confortável, onde ninguém pode ver sua tela enquanto você trabalha. É essencial manter todas as informações sigilosas fora de alcance de quaisquer pessoas não autorizadas, incluindo seu cônjuge, filhos e amigos.
- Sempre bloqueie seu computador de trabalho ao sair da sua mesa. Ao deixar o computador desbloqueado, qualquer pessoa pode usá-lo para acessar dados sigilosos, roubar suas credenciais de login ou até instalar malware.

## Pense antes de clicar

- Nunca clique em um link ou faça o download de um anexo de um e-mail que você não estava esperando. Mesmo se o remetente parecer ser parte de uma organização legítima, o endereço de e-mail pode ter sido falsificado.
- Quando um e-mail solicitar que você faça login em uma conta ou serviço online, acesse o serviço manualmente em seu navegador. Nunca clique no link contido no e-mail. Ao navegar diretamente até o site, você garante que está fazendo login em um site verdadeiro.
- Quando tiver dúvida, ligue para o remetente do e-mail para confirmar que a solicitação, link ou anexo seja legítimo. Não ligue para o número de telefone contido no e-mail, pois pode ser um número falso.



Equipe de segurança da KnowBe4