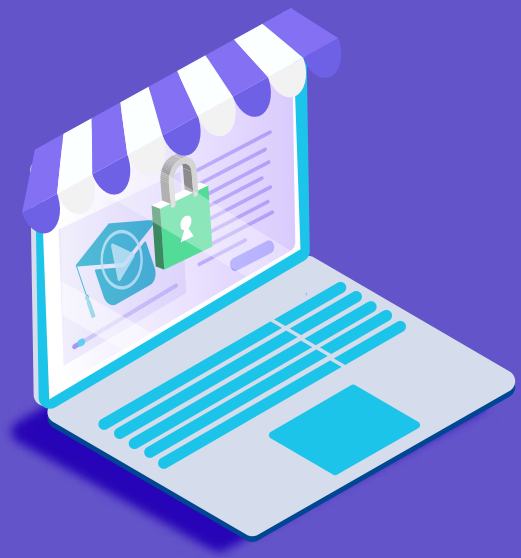
Como proteger seu negócio online de ameaças cibernéticas

Boas práticas de segurança de dados para sua página de vendas



Obtenha um checkout seguro

É no checkout que o cliente preencherá suas informações pessoais e de pagamento.

Utilize o protocolo HTTPs

O HTTPs possui criptografia e protege a troca de informações entre o cliente e o servidor.

Escolha um processador de pagamentos seguro e confiável

Processador de pagamentos que siga as normas do PCI-DSS, utilize criptografia SSL/TLS para proteger dados sensíveis e que esteja registrado no Banco Central.

Contrate um provedor de hospedagem confiável

Criptografia SSL/ TLS, backups frequentes, firewalls, gerenciamento de atividades suspeitas e proteção a ataques de DDoS.

Boas práticas de segurança de dados no backoffice

Tenha um bom controle de usuários

Garanta que cada colaborador tenha seu próprio usuário no sistema e sua respectiva senha de acesso guardada de forma sigilosa.

Determine as funções e permissões de cada usuário

Crie funções para cada grupo de usuários determinando o que cada um pode ver e fazer dentro do sistema. Isso garante que apenas pessoas autorizadas tenham acesso a informações sensíveis da empresa.

Exija a autenticação de 2 fatores

Incentive os usuários a ativarem a autenticação 2 fatores que exige um código aleatório a cada login. Dessa forma, você adiciona mais uma camada de segurança no login dos usuários.