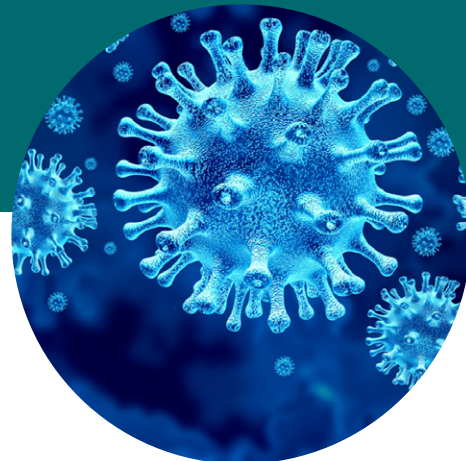


# 8 dicas para ajudar pequenos comerciantes a proteger dados de cartão de pagamento durante o COVID-19

A pandemia do COVID-19 está mudando rapidamente como os pequenos comerciantes aceitam pagamentos. Os comerciantes que anteriormente tinham apenas lojas físicas estão aceitando transações de comércio eletrônico e por telefone. O PCI Security Standards Council compartilha considerações importantes para ajudar pequenos comerciantes a manter seguros os dados de pagamento de seus clientes neste ambiente em rápida mudança.



## COMPREENDENDO O RISCO

Os cibercriminosos estão agindo rapidamente para aproveitar as rápidas mudanças nos ambientes de dados de cartões de pagamento.



**475%** de aumento nos relatórios maliciosos relacionados ao Coronavírus em março.<sup>1</sup>



**41%** das pequenas empresas que sofreram um comprometimento de dados pagaram mais de US\$50.000 para se recuperar.<sup>2</sup>



**29%** dos consumidores pesquisados disseram que nunca mais usariam uma pequena empresa que sofreu uma violação de dados.<sup>3</sup>

1: Fonte: BitDefender

2, 3: Fonte: Bank of America Small Business Payments Spotlight

## DICAS PARA PEQUENOS COMERCIANTES

Esses recursos e muito mais podem ser encontrados na [página de pequenos comerciantes do PCI SSC](#) e no [blog PCI Perspectives](#).



### DICA # 1: REDUZA ONDE OS DADOS DO CARTÃO DE PAGAMENTO PODEM SER ENCONTRADOS

A melhor maneira de se proteger contra comprometimentos de dados é não armazenar os dados do cartão. Muitos pequenos comerciantes estão oferecendo agora a retirada de produtos e estão aceitando pagamentos por telefone em vez das transações presenciais feitas anteriormente. Evite anotar os detalhes do cartão de pagamento e insira-os diretamente no seu terminal seguro.

**Mais informações:** [Documento do grupo de interesse especial do PCI SSC: Aceitando pagamentos telefônicos com segurança](#)



### DICA # 2: USE SENHAS FORTES

O uso de senhas fracas e padrão é uma das principais causas de comprometimentos de dados de pagamento para empresas. Para ser eficaz, as senhas devem ser fortes e atualizadas regularmente. Senhas fracas e padrão do fornecedor são uma fonte frequente de comprometimentos de pequenos comerciantes.

**Mais informações:** [Infográfico de senhas fortes](#)



### DICA # 3: MANTENHA OS SOFTWARES ATUALIZADOS

Os criminosos buscam softwares desatualizados para explorar falhas em sistemas não corrigidos. A instalação oportuna de patches de segurança é crucial para minimizar o risco de comprometimento. Uma maneira de acompanhar todas as alterações necessárias é garantir que as verificações de vulnerabilidades sejam realizadas regularmente para identificar problemas de segurança. Os [fornecedores de verificações de vulnerabilidades aprovados pelo PCI](#) (ASVs) podem ajudá-lo a identificar vulnerabilidades e configurações incorretas em seus sistemas de pagamento voltados para a Internet, site de comércio eletrônico e outros sistemas, fornecendo um relatório de suas vulnerabilidades e como resolvê-las - por exemplo, quais patches aplicar. Certifique-se de agir de acordo com os resultados das verificações de vulnerabilidade ASV e mantenha seu software atualizado.

**Mais informações:** [Infográfico de Patching](#)



#### DICA # 4: USE CRIPTOGRAFIA FORTE

A criptografia torna os dados do cartão de pagamento ilegíveis para as pessoas sem uma chave específica e pode ser usada para proteger os dados armazenados e os dados transmitidos pela rede. Pergunte ao seu fornecedor se a criptografia do terminal de pagamento é feita por meio de uma solução de criptografia ponto a ponto e está na lista de [soluções validadas no PCI P2PE](#) do PCI SSC. Se você estiver configurando um novo site, confirme se o provedor do carrinho de compras está usando criptografia adequada, como TLS v1.2, para proteger os dados de seus clientes.

**Mais informações:** [Suplementos a informações sobre o uso de SSL/TLS antigo](#)



#### DICA # 5: USAR ACESSO REMOTO SEGURO

Para minimizar o risco de comprometimento, é importante que você participe do gerenciamento de como e quando seus fornecedores podem acessar seus sistemas. Os criminosos podem obter acesso aos seus sistemas que armazenam, processam ou transmitem dados de pagamento por meio de controles de acesso remoto fracos. Você deve limitar o uso do acesso remoto e desativá-lo quando não for necessário. Se você precisar permitir o acesso remoto, peça aos seus fornecedores que usem autenticação de múltiplos fatores e credenciais fortes de acesso remoto exclusivas da sua empresa e que não sejam as mesmas usadas para outros clientes.

**Mais informações:** [Infográfico sobre acesso remoto seguro do PCI SSC](#)



#### DICA # 6: ASSEGURAR QUE OS FIREWALLS ESTÃO CONFIGURADOS CORRETAMENTE

Um firewall é um dispositivo ou software que fica entre a sua rede e a Internet. Ele atua como uma barreira para manter o tráfego fora da sua rede e sistemas que você não deseja e não autorizou. As regras do firewall podem parecer complexas, mas configurá-las adequadamente é vital para a segurança. Se você precisar de assistência adicional para configurar corretamente seu firewall, procure ajuda de um profissional de rede.

**Mais informações:** [Recurso para pequenos comerciantes: Noções básicas sobre firewall](#)



#### DICA # 7: PENSE ANTES DE CLICAR

Os hackers usam phishing e outros métodos de engenharia social para atingir organizações com e-mails de aparência legítima e mensagens de mídia social que induzem os usuários a fornecer dados confidenciais, como número do cartão de pagamento, número da conta do comerciante ou senha. Os pequenos comerciantes devem ser extremamente vigilantes e estar atentos a ataques comuns de phishing e engenharia social.

**Mais informações:** [Cuidado com os golpes e ameaças on-line da COVID-19](#)



#### DICA # 8: ESCOLHA PARCEIROS CONFIÁVEIS

É fundamental que você saiba quem são seus provedores de serviços e quais perguntas de segurança devem ser feitas. O seu provedor de serviços está cumprindo os requisitos do PCI DSS? Para comerciantes de comércio eletrônico (e aqueles que recentemente começaram a aceitar pagamentos de comércio eletrônico em vez de pagamentos presenciais), é importante que seus provedores de serviços de pagamento estejam em conformidade com o PCI DSS, incluindo o provedor de serviços que gerencia seu processo de pagamento (seu “provedor de serviços de pagamento” ou PSP).

**Mais informações:** [Perguntas a fazer aos seus fornecedores](#)

### MATERIAIS ADICIONAIS DO PCI SSC



[Práticas recomendadas para proteger o comércio eletrônico](#)



[Protegendo os dados do cartão de pagamento por telefone](#)



[Protegendo pagamentos enquanto trabalha remotamente](#)



[Guia para pagamentos seguros](#)



[Perguntas a fazer aos seus fornecedores](#)



[Sistemas de pagamento comuns](#)

O PCI SSC estabeleceu recursos para atualizações do COVID-19; portanto, verifique regularmente a [página do COVID-19](#) e nosso [blog](#), pois essa é uma situação em constante evolução. Você também pode [se inscrever no nosso blog](#) para receber alertas por e-mail.