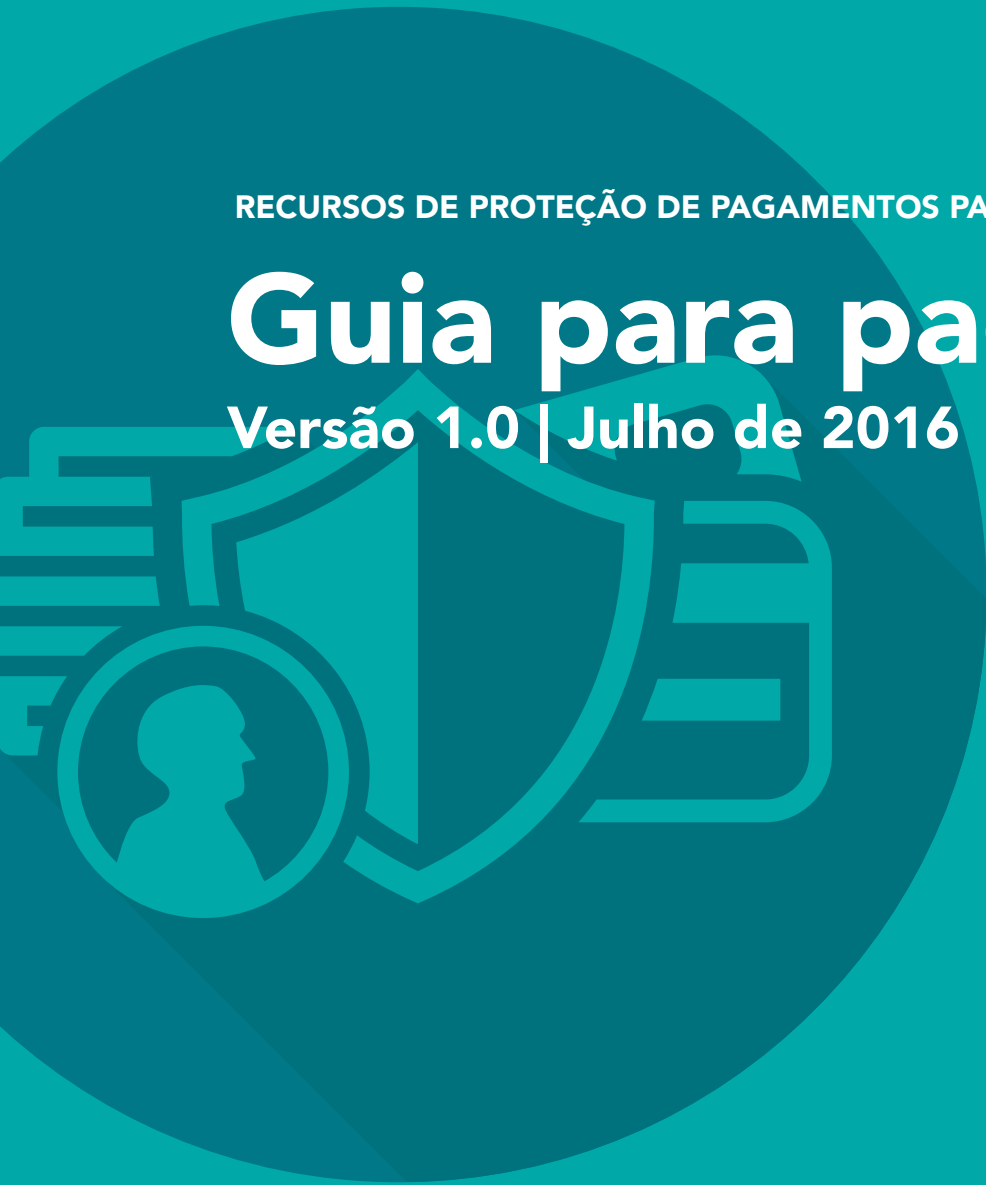


RECURSOS DE PROTEÇÃO DE PAGAMENTOS PARA PEQUENOS COMERCIANTES

Guia para pagamentos seguros

Versão 1.0 | Julho de 2016



ENTENDENDO SEU RISCO	4
PROTEJA SEU NEGÓCIO COM ESSES PRINCÍPIOS BÁSICOS DE SEGURANÇA.....	7
ONDE OBTER AJUDA.....	20



ENTENDENDO SEU RISCO

Entendendo seu risco

Por ser uma pequena empresa, você é alvo de ladrões de dados.

Se seus dados de cartões de pagamento forem violados, as consequências podem aparecer rapidamente. Em situações como essa, seus clientes deixariam de confiar em sua capacidade de proteger informações pessoais. E levariam seus negócios para outros lugares. Poderiam ocorrer sanções financeiras e danos resultantes de ações judiciais, e sua empresa poderia perder a capacidade de aceitar cartões de pagamento. Uma pesquisa com 1.015 pequenas e médias empresas detectou que 60% das empresas que sobrem violações fecham em seis meses. (NCSA)

60%



DAS PEQUENAS EMPRESAS JÁ SOFRERAM UMA VIOLAÇÃO CIBERNÉTICA. (Commonwealth)



71%

DOS HACKERS ATACAM EMPRESAS COM MENOS DE 100 FUNCIONÁRIOS (Verizon 2012)

US\$ 20.752



É O CUSTO MÉDIO PARA UMA PEQUENA EMPRESA QUE SOFRE UM ATAQUE HACKER (CONTRA OS US\$ 8.600 EM 2013) (NSBA)

69%



DOS CONSUMIDORES AMERICANOS SE PREOCUPAM COM O ROUBO DOS DADOS DE SEU CARTÃO DE PAGAMENTO (Gallup)

O que está em risco?

OS DADOS DO CARTÃO DE SEUS CLIENTES É UMA MINA DE OURO PARA OS CRIMINOSOS. NÃO DEIXE QUE ISSO ACONTEÇA COM VOCÊ!

Siga as ações contidas neste guia para se proteger contra o roubo de dados.

O número da conta principal (PAN) e o código de segurança do cartão de três ou quatro dígitos são exemplos de dados de cartão de pagamento. As setas vermelhas abaixo apontam para os tipos de dados que requerem proteção.

TIPOS DE DADOS EM UM CARTÃO DE PAGAMENTO



O QUE É O PCI DSS?

O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) é um conjunto de requisitos de segurança que podem ajudar os pequenos comerciantes a protegerem os dados de cartões de clientes localizados em cartões de pagamento.

Os pequenos comerciantes podem estar familiarizados com a validação de sua conformidade com o PCI DSS por meio de um Questionário de autoavaliação (SAQ).

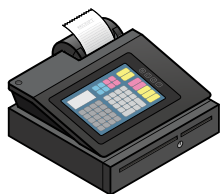
Para obter mais informações sobre o PCI DSS, consulte Recursos no final deste guia.

Entendendo seu sistema de pagamento: Condições comuns de pagamento

Dependendo do país onde você está, o equipamento usado para receber pagamentos é chamado por diferentes nomes. Veja abaixo os tipos que mencionamos neste documento e como são geralmente chamados.



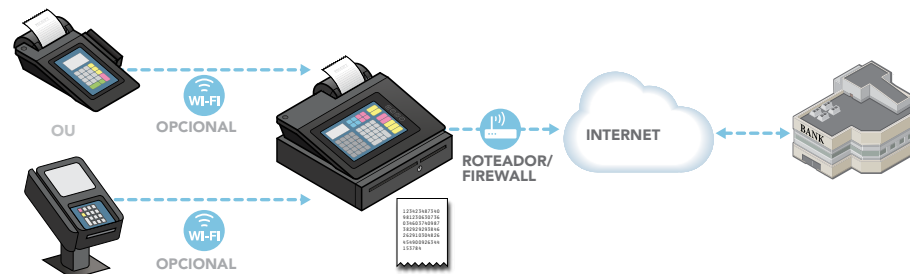
Um **TERMINAL DE PAGAMENTO** é o dispositivo usado para receber pagamentos com cartão do cliente ao passar, inserir, tocar ou introduzir manualmente o número do cartão. Terminal de ponto de venda (POS), máquina de cartão de crédito, terminal PDQ ou terminal EMV/habilitado para chip também são nomes usados para descrever esses dispositivos.



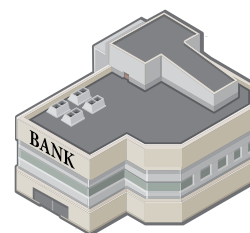
Uma **CAIXA REGISTRADORA ELETRÔNICA** (ou gaveta) registra e calcula transações e pode imprimir recibos, mas não aceita pagamentos com cartão do cliente.



Um **TERMINAL DE PAGAMENTO INTEGRADO** é um terminal de pagamento e uma caixa registradora eletrônica ao mesmo tempo, o que significa que recebe pagamentos com cartão, registra e calcula transações e imprime recibos.



Um **SISTEMA DE PAGAMENTO** engloba todo o processo de aceitação de pagamentos com cartão em um local de varejo (inclusive lojas e lojas de e-commerce) e pode incluir um terminal de pagamento, uma caixa registradora eletrônica, outros dispositivos ou sistemas conectados a um terminal de pagamento (por exemplo, Wi-Fi para conectividade ou um PC usado para inventário), servidores com componentes de e-commerce, como páginas de pagamento, e as conexões para o banco comercial.



Um **BANCO COMERCIAL** é um banco ou uma instituição financeira que processa pagamentos com cartão de crédito e/ou débito em nome de comerciantes. Adquirente, banco adquirente e cartão ou processador de pagamento também são termos para esta entidade.

Como sua empresa está em risco?

Quanto mais recursos seu sistema de pagamento tiver, mais complexo será para protegê-lo. Esses recursos extras geralmente fornecem maneiras fáceis para os criminosos roubarem dados de cartões de clientes. Pense bem se sua empresa realmente precisa desses recursos extras, como Wi-Fi e câmeras.

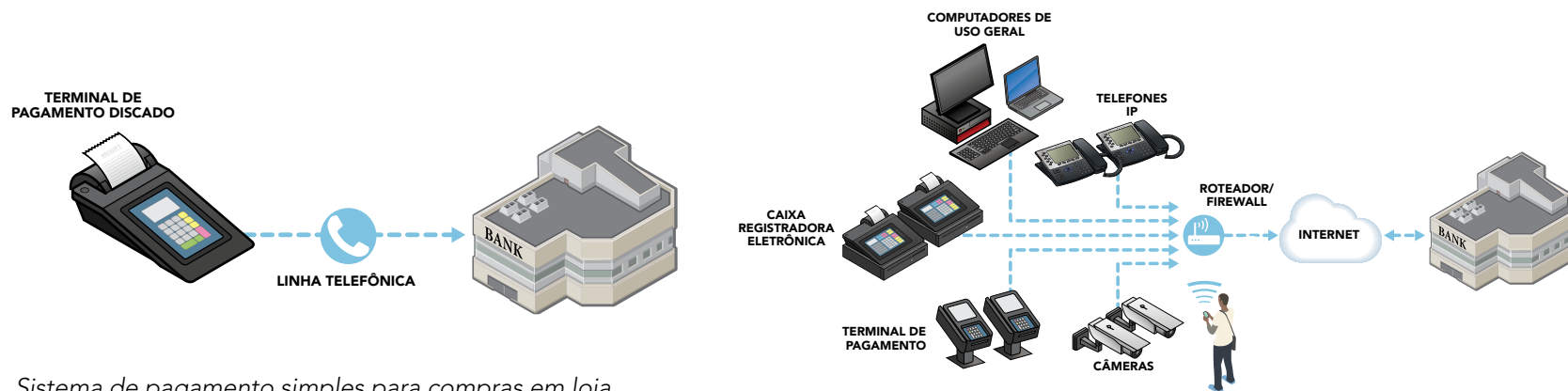


Como você vende suas mercadorias ou serviços? Há três maneiras principais:

1. Uma pessoa entra em sua loja e faz uma compra usando um cartão.
2. Uma pessoa acessa seu site e paga online.
3. Uma pessoa liga para sua loja e fornece detalhes do cartão por telefone, ou envia os detalhes por e-mail ou fax.

Entendendo seu risco: Tipos de sistema de pagamento

Os riscos de segurança variam muito dependendo da complexidade do sistema de pagamento, seja presencial ou online.



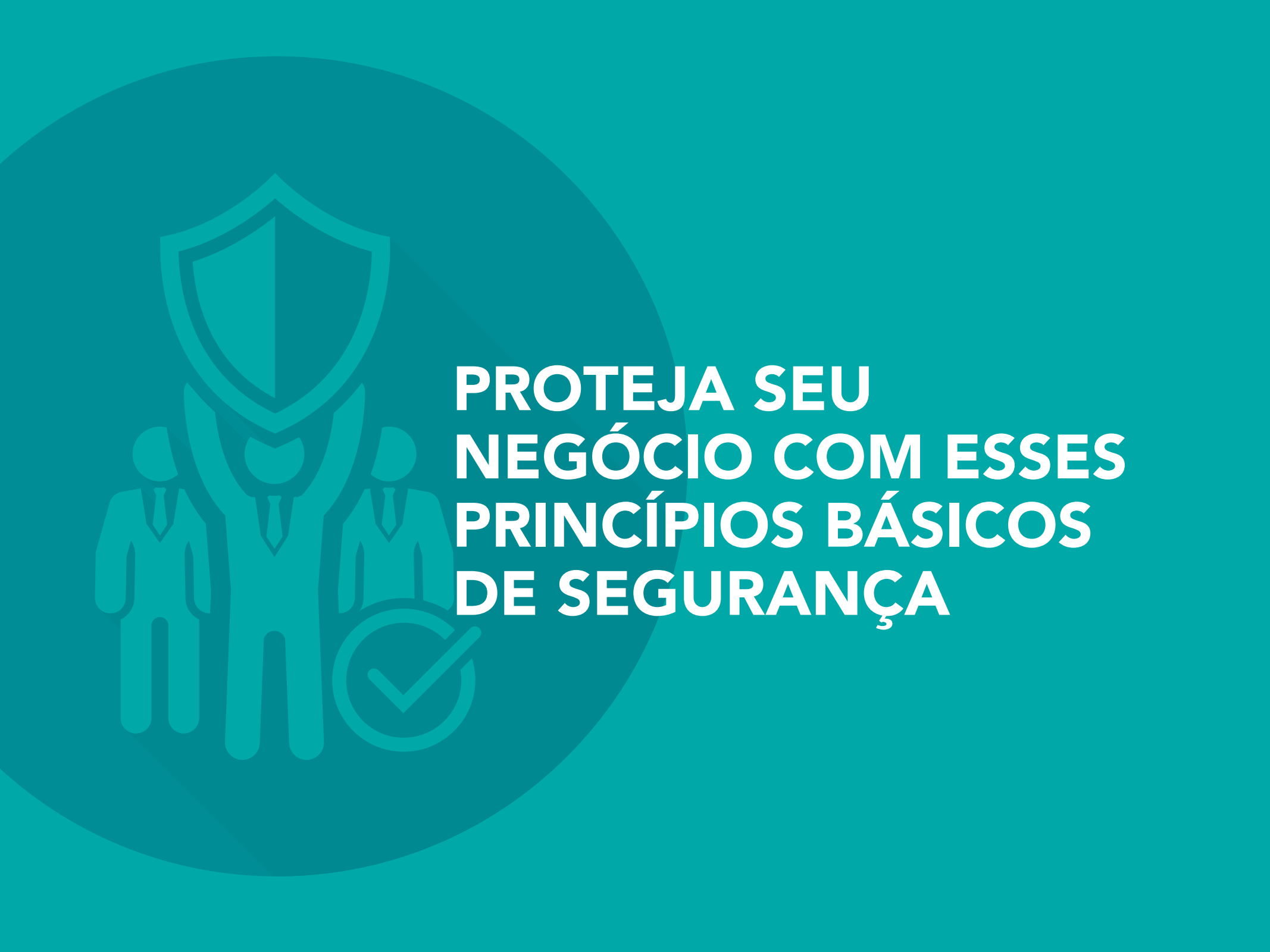
Sistema de pagamento simples para compras em loja

Sistema de pagamento complexo para compras em loja, com Wi-Fi, câmeras, telefones pela Internet e outros sistemas conectados



Sistema de pagamento de e-commerce complexo para compras em loja online, no qual o comerciante gerencia seu próprio site e página de pagamento

















































Use os Sistemas comuns de pagamento para ajudar na identificar do tipo de sistema de pagamento que você usa, seu risco e as dicas de segurança recomendadas como ponto de partida para conversas com seu banco comercial e parceiros fornecedores.



**PROTEJA SEU
NEGÓCIO COM ESSES
PRINCÍPIOS BÁSICOS
DE SEGURANÇA**

Como você protege sua empresa?

A boa notícia é que você pode começar a proteger sua empresa hoje com esses princípios básicos de segurança.

Como proteger sua empresa contra violações	Custo	Facilidade	Mitigação de riscos
 Use senhas fortes e altere as senhas-padrão			
 Proteja os dados do seu cartão e armazene apenas o que você precisa			
 Inspecione se os terminais de pagamento foram adulterados			
 Instale os patches de seus fornecedores			
 Use parceiros de negócios confiáveis e saiba como contatá-los			
 Proteja o acesso interno aos dados de cartão			
 Não permita que os hackers tenham acesso fácil aos seus sistemas			
 Use software antivírus			
 Verifique se há vulnerabilidades e corrija os problemas			
 Use terminais e soluções de pagamento seguros			
 Proteja sua empresa contra vulnerabilidades da Internet			
 Para ter o máximo de proteção, torne seus dados inúteis para criminosos			

Esses princípios básicos de segurança são organizados em ordem, desde os mais fáceis e com implementação menos onerosa, até os mais complexos e com implementação mais cara. A quantidade de redução de risco que cada um oferece aos pequenos comerciantes também é indicada na coluna "Mitigação de riscos".



Use senhas fortes e altere as senhas-padrão

Custo



Facilidade



Mitigação de riscos



Suas senhas são essenciais para a segurança dos dados do computador e dos cartões. Assim como uma trava em sua porta protege a propriedade física, uma senha ajuda a proteger seus dados empresariais. Esteja ciente de que equipamentos de computador e software prontos para uso (inclusive seu terminal de pagamento) geralmente vêm com senhas-padrão (senhas predefinidas) como "senha" ou "admin". Elas geralmente são conhecidas por hackers, por isso são uma fonte frequente de violações de pequenos comerciantes.

Cerca de

80%

das violações de dados envolvem senhas adivinhadas ou roubadas

Verizon PCI 2015

MUDE SUAS SENHAS REGULARMENTE. Trate suas senhas como uma escova de dentes. Não deixe que mais ninguém a use; além disso, altere-a a cada três meses.

PROCURE AJUDA. Pergunte aos fornecedores ou prestadores de serviços sobre senhas-padrão e como alterá-las. E então altere-as!

DIFICULTE A ADIVINHAÇÃO. As senhas mais comuns são "senha" e "123456." A primeira tentativa dos hackers sempre são senhas fáceis de adivinhar, pois elas são usadas por quase todas as pessoas. Uma senha forte tem sete ou mais caracteres e uma combinação de letras maiúsculas e minúsculas, números e símbolos (como !@#\$&*). Uma frase também pode ser uma senha forte (e pode ser mais fácil de lembrar), como "B1gMac&frieS".

NÃO COMPARTILHE. Insista para que cada funcionário tenha sua própria ID de login e senha, as quais nunca devem compartilhar!

Senhas-padrão comuns que DEVEM SER alteradas:

[nenhuma]

[nome do produto ou fornecedor]

1234 or 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

Para obter mais informações sobre a segurança de senhas, consulte estes recursos no site do PCI Council:

INFOGRÁFICO



It's Time to Change Your Password (É hora de alterar sua senha)



VÍDEO

Learn Password Security in 2 Minutes (Aprenda sobre segurança da senha em 2 minutos)



Proteja os dados de cartões e armazene apenas o que você precisa

Custo



Facilidade



Mitigação
de riscos



É impossível proteger os dados do cartão se você não souber onde eles estão.

O que você pode fazer?

A tokenização tem um objetivo semelhante à criptografia, mas funciona de maneira diferente. Ela substitui os dados do cartão por dados sem significado (um "token"), que não têm valor para um hacker.

PERGUNTE A UM ESPECIALISTA. Pergunte ao seu fornecedor de terminal de pagamento ou banco comercial onde seus sistemas armazenam dados e se você pode simplificar o processamento de pagamentos. Pergunte também como conduzir transações específicas (por exemplo, para pagamentos recorrentes) sem armazenar o código de segurança do cartão.

TERCEIRIZE. A melhor maneira de se proteger contra violações de dados é não armazenar dados de cartões de nenhuma forma. Considere terceirizar o processamento do seu cartão para um prestador de serviços em conformidade com o PCI DSS. Consulte Recursos na página 22 para ver listas de prestadores de serviços compatíveis.

SE VOCÊ NÃO PRECISA DOS DADOS DO CARTÃO, NÃO OS ARMAZENE.

Destrua/rasgue os dados do cartão dos quais você não precisa. Se você precisar manter documentos em papel que contenham dados confidenciais de cartões, passe um marcador preto e espesso sobre esses dados até que fiquem ilegíveis e guarde o documento em uma gaveta trancada com trava ou em um cofre ao qual apenas algumas pessoas tenham acesso.

LIMITE O RISCO. Em vez de aceitar os detalhes do pagamento por e-mail, peça que os clientes os forneçam por telefone, fax ou correio normal.

TOKENIZE OU CRIPTOGRAFE. Pergunte ao seu banco comercial se você REALMENTE precisa armazenar os dados do cartão. Em caso afirmativo, pergunte ao seu banco comercial ou prestador de serviços sobre tecnologias de criptografia ou de tokenização que tornam os dados do cartão inúteis, mesmo se forem roubados. (Consulte "🔒" na página 19 para obter mais informações).

GUIA SOBRE CRIPTOGRAFIA

A criptografia usa uma fórmula matemática para fazer com que textos não criptografados se tornem ilegíveis a pessoas sem uma chave. A criptografia é aplicada aos dados armazenados, bem como aos dados transmitidos por uma rede.

A CRIPTOGRAFIA transforma o texto não criptografado em texto cifrado.

A DESCRIPTOGRAFIA parte do texto cifrado e transforma-o novamente em texto não criptografado.

Por exemplo:

Isso é segredo, não

CHAVE DE CRIPTOGRAFIA

5a0 (k\$hQ%...

CHAVE DE DESCRIPTOGRAFIA

Isso é segredo, não



Inspecione se os terminais de pagamento foram adulterados

Custo



Facilidade



Mitigação de riscos



“Dispositivos de clonagem” varrem os dados do cartão quando o cliente o insere em um terminal de pagamento. É essencial que você e sua equipe saibam como identificar um dispositivo de clonagem. Você precisa verificar regularmente seus terminais de pagamento para se certificar de que não tenham sido adulterados. Mantenha um registro ou log de quais terminais foram verificados, quando foram verificados, quem fez a verificação e se alguma coisa foi encontrada.

Consulte o [PCI Council's guide: Skimming Prevention: Overview of Best Practices for Merchants](#) (guia do PCI Council: Prevenção contra clonagem – Visão geral das melhores práticas para comerciantes)

Esteja atento e siga as recomendações abaixo.

FAÇA UMA LISTA de todos os terminais de pagamento e tire fotos (parte frontal e posterior, cabos e conexões) para que saiba futuramente como eles devem estar sempre.

PROCURE SINAIS ÓBVIOS de adulteração, como vedações quebradas em portas ou parafusos de acesso, cabeamento estranho/diferente e dispositivos ou recursos novos que você não reconhece. O guia do PCI Council (mencionado abaixo) pode ajudar.

PROTEJA OS TERMINAIS. Mantenha-os fora do alcance dos clientes quando não estiverem em uso e obscureça suas telas para que não sejam vistas pelo público. Certifique-se de que seus terminais de pagamento estejam seguros antes de fechar a loja ao final do dia, inclusive quaisquer dispositivos que leiam cartões de pagamento de seus clientes ou aceitem seus números de identificação pessoal (PINs).

CONTROLE OS REPAROS. Permita reparos de terminais de pagamento somente por pessoal de reparo autorizado e com agendamento. Diga a sua equipe para fazerem o mesmo.

LIGUE imediatamente para o fornecedor de seu terminal de pagamento ou para o banco comercial se suspeitar de alguma coisa!



Instale os patches de seus fornecedores

Custo



Facilidade



Mitigação de
riscos



Muitas vezes, os softwares apresentam falhas ou erros cometidos por programadores ao escreverem o código, que também são chamados de brechas de segurança, bugs ou vulnerabilidades. Os hackers exploram esses erros a fim de invadir o seu computador e roubar os dados de sua conta. Proteja seus sistemas aplicando patches disponibilizados pelo fornecedor para corrigir erros de codificação. A instalação oportuna de patches de segurança é essencial!

PERGUNTE ao seu fornecedor ou prestador de serviços como ele o notifica sobre novos patches de segurança. Sempre leia essas notificações.

QUAIS FORNECEDORES ENVIAM PATCHES? Você pode obter patches de fornecedores de seu terminal de pagamento, aplicativos de pagamento, outros sistemas de pagamento (gavetas, caixas registradoras, PCs, etc.), sistemas operacionais (Android, Windows, iOS, etc.), software aplicativo (inclusive navegador da Web) e software de negócios.

CERTIFIQUE-SE de que seus fornecedores atualizam os seus terminais de pagamento, sistemas operacionais, etc., para que possam suportar os patches de segurança mais recentes. Pergunte a eles.

COMERCIANTE DE E-COMMERCE. Instalar patches o mais rápido possível é muito importante para você também. Também fique atento a patches do seu prestador de serviços de pagamento. Pergunte ao seu provedor de hospedagem de e-commerce se eles corrigem o seu sistema (e com que frequência). Certifique-se de que eles atualizam o sistema operacional, a plataforma de e-commerce e/ou o aplicativo da Web para que possam suportar os patches mais recentes.

SIGA as instruções do seu fornecedor ou prestador de serviços e instale esses patches assim que possível.



Use parceiros de negócios confiáveis e saiba como contatá-los

Custo



Facilidade



Mitigação de riscos



Use provedores externos para serviços, dispositivos e aplicativos relacionados a pagamentos. Você também pode ter prestadores de serviços com os quais compartilha dados de cartão, que suportam ou gerenciam seus sistemas de pagamento ou que dão acesso aos dados do cartão. Você pode chamá-los de processadores, fornecedores, terceiros ou prestadores de serviços. Eles afetam sua capacidade de proteger seus dados de cartão, portanto é fundamental que você saiba quem eles são e quais perguntas de segurança deve fazer a eles.

SAIBA PARA QUEM LIGAR. Quem é o seu banco comercial? Quem mais o ajuda a processar pagamentos? De quem você comprou seu dispositivo ou software de pagamento e quem o instalou para você? Quem são seus prestadores de serviços?

MANTENHA UMA LISTA. Agora que você sabe para quem ligar, guarde os nomes das empresas e dos contatos, números de telefone, endereços de sites e outros detalhes de contato pelos quais você possa encontrá-los facilmente no caso de uma emergência.

CONFIRME QUE SEUS PRESTADORES DE SERVIÇOS SÃO SEGUROS. Seu prestador de serviços está cumprindo os requisitos do PCI DSS? Para comerciantes de e-commerce, é importante que seu prestador de serviços de pagamento seja compatível com o PCI DSS também! Consulte Recursos na página 22 para ver listas de prestadores de serviços compatíveis.

FAÇA PERGUNTAS. Quando você souber quem são seus provedores externos e o que eles fazem por você, converse com eles para entender como protegem os dados de cartões. Use o documento [Perguntas que você deve fazer aos seus fornecedores](#) para saber o que perguntar.

CONHEÇA OS TIPOS COMUNS DE FORNECEDORES. Revise a barra lateral à direita para entender os tipos comuns de fornecedores ou prestadores de serviços com os quais você pode trabalhar.

FORNECEDORES COMUNS

Consulte a tabela no documento [Perguntas que você deve fazer aos seus fornecedores para obter mais detalhes sobre estes fornecedores comuns](#):

Fornecedores de terminal de pagamento

Fornecedores de aplicativo de pagamento

Instaladores de sistema de pagamento (chamados de Integradores/ Revendedores)

Prestadores de serviços que realizam processamento de pagamentos ou hospedagem ou processamento de e-commerce

Prestadores de serviços que ajudam você a atender ao(s) requisito(s) do PCI DSS (por exemplo, fornecendo serviços de firewall ou antivírus)

Prestadores de software como um serviço



Proteja o acesso interno aos seus dados

Custo



Facilidade



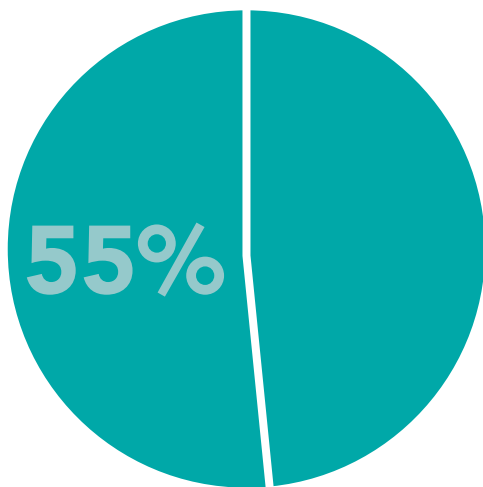
Mitigação de
riscos



Abuso de privilégio significa uma pessoa usando...

Acesso e privilégios de outra pessoa para acessar sistemas ou dados aos quais essa pessoa não tem acesso autorizado.

ABUSO DE PRIVILÉGIO É A PRINCIPAL AÇÃO QUE LEVA A VIOLAÇÕES – CERCA DE 55% DE TODOS OS INCIDENTES RELATADOS.



Verizon 2015

O CONTROLE DE ACESSO É MUITO IMPORTANTE.

Configure seu sistema para conceder acesso somente com base na necessidade empresarial de conhecer a informação. Como proprietário, você tem acesso a tudo. Mas a maioria dos funcionários consegue trabalhar com acesso apenas a um subconjunto de dados, aplicativos e funções.

LIMITE O ACESSO a sistemas de pagamento, dados não criptografados de cartões, aplicativos e funções apenas aos funcionários que precisam de acesso e apenas o suficiente para fazerem seu trabalho.

MANTENHA UM REGISTRO. Acompanhe todos os visitantes que entrarem em contato com os processos internos de seu estabelecimento. Inclua nome, motivo da visita e nome do funcionário que autorizou o acesso do visitante. Guarde o registro por pelo menos um ano.

DESCARTE DISPOSITIVOS COM SEGURANÇA.

Pergunte ao fornecedor do seu sistema de pagamento ou prestador de serviços sobre a maneira ideal de remover os dados de cartões com segurança antes de vender ou descartar dispositivos de pagamento (para que os dados não possam ser recuperados).

COMPARTILHE ESSAS INFORMAÇÕES. Disponibilize este guia aos seus funcionários e parceiros de negócios para que eles saibam o que é esperado deles.

Considere dar acesso aos funcionários para que recebam pagamentos, mas não para que processem reembolsos, ou para que recebam novas reservas e pedidos, mas não para que acessem dados de cartões de pagamento relacionados a reservas e pedidos existentes. Alguns funcionários não devem ter nenhum acesso.



Não permita que os hackers tenham acesso fácil aos seus sistemas

Custo



Facilidade



Mitigação de riscos



HACKERS = CRIMINOSOS

Uma das maneiras mais fáceis que os hackers usam para entrar em um sistema é usando pessoas em quem o dono confia. Você precisa saber como seus fornecedores estão acessando seu sistema para se certificar de que eles não estejam deixando brechas para os hackers.

A autenticação de múltiplos fatores usa um nome de usuário e uma senha além de pelo menos um outro fator (como um cartão inteligente, um dongle* ou um código de acesso único).

*Um dispositivo útil que se conecta a um computador para permitir acesso a recursos de software sem fio, etc.

DESCUBRA. Pergunte ao fornecedor do sistema de pagamento ou ao prestador de serviços se ele usa acesso remoto para oferecer suporte ou acessar seu negócio.

PERGUNTE COMO LIMITAR O USO DO ACESSO REMOTO. Muitos programas de acesso remoto permanecem sempre ativados por padrão. Reduza seu risco: pergunte ao fornecedor como desabilitar o acesso remoto quando seu uso não for necessário e como habilitá-lo quando o fornecedor ou prestador de serviços solicitar.

DESATIVE-O QUANDO A ATIVIDADE DESEJADA FOR FINALIZADA.

USE AUTENTICAÇÃO FORTE. Se você precisar permitir o acesso remoto, solicite autenticação de múltiplos fatores e criptografia forte.

CERTIFIQUE-SE DE QUE OS PRESTADORES DE SERVIÇOS USAM CREDENCIAIS EXCLUSIVAS. Cada um deve usar credenciais de acesso remoto que sejam exclusivas para sua empresa e que não sejam as mesmas usadas para outros clientes.

PEÇA AJUDA. Peça ajuda ao fornecedor ou prestador de serviços para desativar o acesso remoto ou, se o fornecedor ou prestador de serviços precisar de acesso remoto, peça ajuda na configuração da autenticação de múltiplos fatores. Consulte [Perguntas que você deve fazer aos seus fornecedores](#) para saber exatamente o que perguntar.

Se o fornecedor suportar ou solucionar problemas no seu terminal de pagamento trabalhando no escritório dele (e não no seu estabelecimento), quer dizer que ele estará usando a Internet e um software de acesso remoto para fazer isso.

VNC e LogMeIn são alguns exemplos de produtos que o fornecedor pode instalar no seu terminal e usar para suporte remotamente.



Use software antivírus

Custo



Facilidade



Mitigação de
riscos



Sistemas e softwares são extremamente flexíveis e oferecem uma ampla gama de funções e recursos. Os hackers criam vírus e outros códigos mal-intencionados para explorar esses recursos e erros de codificação, para que possam entrar em seus sistemas e roubar dados do cartão. O uso de software antivírus atualizado (também chamado de antimalware) ajuda a proteger seus sistemas.

INSTALE SOFTWARE ANTIVÍRUS PARA PROTEGER SEU SISTEMA DE PAGAMENTO. É fácil de instalar e pode ser obtido em sua loja de suprimentos de escritório local ou varejista de TI.

DEFINA A CONFIGURAÇÃO DE “ATUALIZAÇÃO AUTOMÁTICA” DO SOFTWARE para que você sempre tenha a proteção mais recente disponível.

OBTENHA ACONSELHAMENTO. Pergunte ao seu varejista de TI sobre os produtos que eles recomendam para proteção antivírus/antimalware.

FAÇA VERIFICAÇÕES PERIÓDICAS. Execute regularmente verificações completas do sistema, pois seus sistemas podem ter sido infectados por um novo malware que foi lançado antes que seu software antivírus pudesse detectá-lo.



Verifique se há vulnerabilidades e corrija os problemas

Custo	
Facilidade	
Mitigação de riscos	

Novas vulnerabilidades, brechas de segurança e bugs são descobertos todos os dias. É muito importante fazer com que seus sistemas que usam a Internet sejam testados regularmente a fim de identificar esses novos riscos e tratá-los assim que possível. Seus sistemas que usam a Internet (como muitos sistemas de pagamento) são os mais vulneráveis porque podem ser facilmente explorados por criminosos, permitindo que se infiltrem em seus sistemas.

Os fornecedores de verificação aprovados pelo PCI Council executam verificações de vulnerabilidade e relatórios externos. Consulte a [List of PCI-Approved Scanning Vendors](#) (Lista de fornecedores de verificação aprovados pelo PCI)

OBTENHA ACONSELHAMENTO. Pergunte ao seu banco comercial se ele possui parcerias com fornecedores de verificação aprovados pelo PCI, ou ASV (Fornecedor de Varredura Aprovado). Faça a mesma pergunta aos seus fornecedores e prestadores de serviços.

CONVERSE COM UM ASV DO PCI. Esses fornecedores podem ajudá-lo com ferramentas que pesquisam a rede automaticamente para encontrar vulnerabilidades e fornecer um relatório se, por exemplo, você precisar aplicar um patch. A lista do PCI Council (referenciada abaixo) pode ajudá-lo a encontrar um fornecedor de verificação.

SELECIONE UM SCANNER. Entre em contato com vários ASVs do PCI para encontrar um fornecedor que use um programa adequado para sua pequena empresa.

TRATE AS VULNERABILIDADES. Peça ao seu ASV ajuda para corrigir os problemas encontrados pela verificação.



Use terminais e soluções de pagamento seguros

Custo




Facilidade



Mitigação de riscos



Uma maneira segura de proteger melhor sua empresa é usar soluções de pagamento seguras e profissionais treinados para ajudá-lo. Veja como escolher produtos seguros e certificar-se de que estejam configurados com segurança.

Para os terminais de pagamento do PCI e leitores de cartões seguros que criptografam os dados de cartões, consulte  na página 19.

USE TERMINAIS DE PAGAMENTO E DISPOSITIVOS DE DIGITAÇÃO DE PIN QUE SEJAM SEGUROS.

O PCI Council aprova os terminais de pagamento que protegem dados de PIN. Certifique-se de que o terminal ou dispositivo de pagamento esteja na [List of PCI Approved PTS Devices \(Lista de dispositivos PTS aprovados pelo PCI\)](#) para equipamentos que oferecem a melhor segurança e suportam "chip EMV".

USE SOFTWARE SEGURO. Certifique-se de que o software de pagamento esteja na [List of PCI Validated Payment Applications \(Lista de aplicativos de pagamento validados pelo PCI\)](#).

USE PROFISSIONAIS QUALIFICADOS. Certifique-se de que a pessoa que está instalando o aplicativo validado pelo PA-DSS o faz de forma correta e segura. Escolha na [List of PCI QIRs \(Lista de QIRs do PCI\)](#) as empresas qualificadas pelo PCI Council para ajudá-lo. Peça ao seu banco comercial para ajudá-lo a fazer a seleção.

CONSULTE ESTA LISTA DE PERGUNTAS DO FORNECEDOR. Use [Perguntas que você deve fazer aos seus fornecedores](#) para saber o que perguntar aos seus fornecedores e prestadores de serviços.

Seus clientes digitam os números de identificação pessoal (PINs) para seus cartões de pagamento em seu terminal de pagamento ou dispositivo de digitação de PIN. É importante usar dispositivos seguros para proteger os dados de PIN dos seus clientes.



Proteja sua empresa contra vulnerabilidades da Internet

Custo	
Facilidade	
Mitigação de riscos	

A Internet é a principal via utilizada pelos ladrões de dados para atacar e roubar os dados dos seus clientes. Por isso, se a sua empresa está na Internet, qualquer coisa que você usa para pagamentos com cartão precisa de proteção extra.

ISOLE O USO. Não use o dispositivo com o qual você recebe pagamentos para nenhuma outra finalidade. Por exemplo, não navegue na Web nem acesse e-mails ou mídia social no mesmo dispositivo ou computador que você usa para transações de pagamento. Quando for necessário usar a Internet para negócios (por exemplo, atualizar a página na mídia social da sua empresa), use outro computador, e não seu dispositivo de pagamento.

PROTEJA SEU "TERMINAL VIRTUAL". Se você inserir pagamentos de clientes por meio de um terminal virtual (uma página da Web que você acessa com um computador ou tablet), não conecte um leitor de cartão externo; isso minimiza seu risco.

PROTEJA O WI-FI. Se sua loja oferecer Wi-Fi gratuito para seus clientes, use outra rede para seu sistema de pagamento (isso é chamado de "segmentação de rede"). Peça que o instalador de rede ajude com a configuração segura do Wi-Fi.

USE UM FIREWALL. Um firewall configurado corretamente atua como um buffer para impedir que hackers e softwares mal-intencionados obtenham acesso a seus computadores e informações. Verifique com seu fornecedor de terminal de pagamento ou prestador de serviços se você tem um firewall e solicite ajuda para configurá-lo corretamente.

USE SOFTWARE FIREWALL PESSOAL OU EQUIVALENTE quando os sistemas de pagamento não estiverem protegidos por seu firewall corporativo (por exemplo, quando conectado a Wi-Fi público).



Para ter o máximo de proteção, torne seus dados inúteis para criminosos

Custo



Facilidade




Mitigação de riscos



Seus dados ficam vulneráveis quando se deslocam para seu banco comercial e quando são mantidos ou armazenados em seus computadores e dispositivos. A melhor maneira de mantê-los seguros é torná-los inúteis mesmo para o caso de serem roubados e removê-los totalmente quando não forem mais necessários. Embora isso possa ser mais complexo de ser implementado, em longo prazo, pode facilitar muito o gerenciamento da segurança.

PERGUNTE AO SEU FORNECEDOR DE SISTEMAS DE PAGAMENTO OU PRESTADOR DE SERVIÇOS se seu terminal de pagamento está usando tecnologia de criptografia e/ou de tokenização.

USE DISPOSITIVOS PCI QUE CRIPTOGRAFEM OS DADOS DE CARTÕES. O PCI Council aprova terminais de pagamento que protegem os dados de PIN (consulte  na página 17) e terminais de pagamento e “leitores de cartões seguros” que também criptografam os dados de cartões. Consulte a [List of PCI Approved PTS Devices \(Lista de dispositivos PTS aprovados pelo PCI\)](#).

USE SOLUÇÕES DE CRIPTOGRAFIA SEGURAS DO PCI. Pergunte se a criptografia do seu terminal de pagamento é feita por uma solução de criptografia de ponto a ponto que está na [List of PCI P2PE Validated Solutions \(Lista de soluções validadas pelo PCI P2PE\)](#) do PCI Council.

ATUALIZE SUA SOLUÇÃO. Reduza seu risco: considere obter um novo terminal de pagamento que use tecnologia de criptografia e de tokenização para remover o valor dos dados do cartão para hackers.

VOCÊ É UM COMERCIANTE QUE ESTÁ MUDANDO AGORA PARA TERMINAIS COM CHIP EMV? É uma ótima oportunidade para fazer um investimento em um terminal que suporte EMV e também ofereça a segurança adicional de criptografia e tokenização.

PERGUNTE. Consulte [Perguntas que você deve fazer aos seus fornecedores](#) para obter ajuda em relação a perguntas que você deve fazer a seu fornecedor ou prestador de serviços.

Leitores de cartões e terminais de pagamento seguros aprovados pelo PCI que criptografam os dados de cartões fazem isso usando a tecnologia chamada “Leitura segura e intercâmbio de dados (SRED)”. Pergunte ao fornecedor se seu terminal de pagamento criptografa os dados de cartões com SRED.



ONDE OBTER AJUDA

Recursos

Listagens do PCI Council

Recurso	Link	URL
List of Validated Payment Applications (Lista de aplicativos de pagamento validados)	<u>PCI Council's Validated Payment Applications (Aplicativos de pagamento validados pelo PCI Council)</u>	<u>https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement</u>
List of Approved PTS Devices (Lista de dispositivos PTS aprovados)	<u>PCI Council's Approved PTS Devices (Dispositivos PTS aprovados pelo PCI Council)</u>	<u>https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices</u>
List of Approved Scanning Vendors (Lista de fornecedores de verificação aprovados)	<u>PCI Council's Approved Scanning Vendors (Fornecedores de verificação aprovados pelo PCI Council)</u>	<u>https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors</u>
List of Qualified Integrators / Resellers (Lista de integradores/ revendedores qualificados)	<u>PCI Council's Qualified Integrators Resellers (Integradores e revendedores qualificados do PCI Council)</u>	<u>https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers</u>
List of P2PE Validated Solutions (Lista de soluções validadas P2PE)	<u>PCI Council's P2PE Validated Solutions (Soluções validadas P2PE pelo PCI Council)</u>	<u>https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions</u>

Listas de bandeiras de pagamento

Recurso	Link	URL
Lists of Compliant Service Providers (Listas de prestadores de serviços em conformidade)	<u>MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade)</u>	<u>https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html</u>
	<u>Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa)</u>	<u>http://www.visa.com/splisting/</u>
	<u>Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)</u>	<u>https://www.visaeurope.com/receiving-payments/security/downloads-and-resources</u>

PCI DSS e orientação relacionada

Recurso	Link	URL
More about PCI DSS (Mais informações sobre o PCI DSS)	<u>How to Secure with PCI DSS (Como se proteger com o PCI DSS)</u>	<u>https://www.pcisecuritystandards.org/pci_security/how</u>
PCI DSS Self-Assessment Questionnaires (Questionários de autoavaliação do PCI DSS)	<u>Self-Assessment Questionnaires (Questionários de autoavaliação)</u>	<u>https://www.pcisecuritystandards.org/pci_security/completing_self_assessment</u>
Guide: Skimming Prevention: Overview of Best Practices for Merchants (Guia: Prevenção contra clonagem: Visão geral das melhores práticas para comerciantes)	<u>Skimming Prevention: Overview of Best Practices for Merchants (Prevenção contra clonagem: Visão geral das melhores práticas para comerciantes)</u>	<u>https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf</u>

Recursos

Infográficos e vídeos

Recurso	Link	URL
Infographic: It's Time to Change Your Password (Infográfico: É hora de alterar sua senha)	<i>It's Time to Change Your Password (É hora de alterar sua senha)</i>	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves (Infográfico: Combater o crime cibernético, deixando os dados roubados sem valor para os ladrões)	<i>Fight Cybercrime by Making Stolen Data Worthless to Thieves (Combater o crime cibernético, deixando os dados roubados sem valor para os ladrões)</i>	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Vídeo: Learn Password Security in 2 Minutes (Vídeo: Aprenda sobre segurança da senha em 2 minutos)	<i>Learn Password Security in 2 Minutes (Aprenda sobre segurança da senha em 2 minutos)</i>	https://www.youtube.com/watch?v=FsrOXgZKa7U

Recursos de proteção de pagamentos do PCI para pequenos comerciantes

Recurso	Link	URL
Sistemas comuns de pagamento	<i>Sistemas comuns de pagamento</i>	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Pequenos comerciantes - Perguntas para fornecedores	<i>Pequenos comerciantes - Perguntas para fornecedores</i>	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Glossário para pequenos comerciantes	<i>Glossário para pequenos comerciantes</i>	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Fontes

Gallup – *Gallup Poll*, October 2015 (Gallup – *Pesquisa Gallup*, outubro de 2015)

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014 (Governo do Reino Unido – *Pequenas empresas: o que você precisa saber sobre cibersegurança*, Reino Unido 2014)

NCSA – *National Cyber Security Alliance survey*, 2012 (NCSA – *Pesquisa da Aliança Nacional de Cibersegurança dos EUA*, 2012)

NSBA – *National Small Business Administration, 2014 Year End Economic Report* (NSBA – *Administração Nacional de Pequenas Empresas do EUA, Relatório econômico de final de ano de 2014*)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (Verizon 2012 – *Relatório de investigações de violação de dados da Verizon 2012*)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (Verizon 2015 – *Relatório de investigações de violação de dados da Verizon 2015*)

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report* (Verizon PCI 2015 – *Relatório de conformidade com o PCI da Verizon 2015*)