SEGURANÇA ESSENCIAL DOS DADOS DE PAGAMENTO

Senhas fortes

QUAL É O RISCO?

81%

de violações relacionadas com hackers devido a senhas roubadas e/ou fracas

(Relatório de Investigação de Violação de Dados Verizon 2017)

O uso de senhas fracas e senhas padrão é uma das principais causas de violações de dados nas empresas.

As senhas são essenciais para a segurança do computador e dos dados de pagamentos. Mas para serem eficazes, elas devem ser fortes e atualizadas regularmente.

Os equipamentos de computação e software prontos para uso (incluindo terminais de pagamento) geralmente vêm com senhas padrão do fornecedor ou predefinidas, como "password" ou "admin", que são comumente conhecidas e facilmente exploradas por criminosos.

Senhas padrão típicas que DEVEM ser alteradas:

[nenhuma]	guest
[nome do produto/ fornecedor]	manager
1234 ou 4321	pass
access	password
admin	root
anonymous	sa
database	secret
	sysadmin
	user

PRÁTICAS RECOMENDADAS PARA SENHAS

Para minimizar o risco de violação, as empresas devem alterar as senhas padrão do fornecedor com senhas mais fortes e nunca as compartilhar. Cada funcionário deve ter sua própria ID de acesso e senha.

Troque suas senhas regularmente

Trate suas senhas como escovas de dentes. Não deixe que mais ninguém as use e troque-as a cada três meses.

Não compartilhe senhas

Insista em que cada funcionário tenha sua próprio ID de acesso e senha, nunca compartilhe!

Faça senhas difíceis de adivinhar

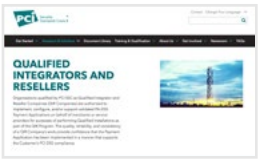
As senhas mais comuns são "senha", "senha1" e "123456". Os hackers tentam senhas fáceis de adivinhar porque são usadas por metade das pessoas. Uma senha forte tem sete ou mais caracteres e uma combinação de letras maiúsculas e minúsculas, números e símbolos (como !@#$&*). Uma frase contendo números e símbolos também pode ser uma senha forte, o importante é escolher uma frase com um significado específico para você, para que seja fácil de lembrar, como um hobby favorito, por exemplo (como @doroPe$c@rTrut@$!).

RECURSOS

Acesse ***pcissc.org/Merchants*** para mais recursos

Os fornecedores e provedores de serviços podem ajudar as empresas na identificação de senhas padrão e na alteração dessas senhas.

O Guia para Pagamentos Seguros fornece às empresas segurança básica para se protegerem contra roubo de dados de pagamento.



A lista PCI Qualified Integrators e Resellers (QIR) é um recurso que as empresas podem utilizar para encontrar instaladores de sistemas de pagamento, treinados pelo PCI Security Standards Council em senhas fortes e outros itens essenciais de segurança de dados de pagamento.

Assista a esta breve animação para saber como as empresas podem minimizar as chances de serem violadas, trocando as senhas padrão dos fornecedores por senhas mais fortes e nunca compartilhando as senhas.

PCI Security Standards Council