

小型商户支付保护资源

安全支付指南

1.0 版 | 2016 年 7 月

了解风险	4
使用安全基本措施保护您的业务	6
可从哪里获取帮助	20



了解风险

了解风险

作为小型企业，您是数据盗用者的主要目标。

当您的支付卡数据外泄时，可能很快就会受到附带结果的冲击。您的客户将对您保护其个人信息的能力失去信任。他们将把业务转移到别处。您可能会遭到金融处罚并蒙受诉讼导致的损失，而您的企业可能会失去接受支付卡的能力。在针对 1,015 个中小型企业开展的一项调查中发现，其中 60% 的企业在近六个月内经历了数据外泄。(NCSA)

60%

的小型企业在经历了网络数据泄露。(英国政府)



71%

遭受黑客攻击的企业员工人数少于 100
(威瑞森 2012)

20,752
美元



小型企业因黑客攻击而付出的平均代价，较 2013 年的 8,600 美元有所上升
(NSBA)

69%

的美国消费者担心支付卡数据被盗
(盖洛普)



高风险领域

您的客户卡数据正是不法分子的财源。千万不要让数据被盗这种事情发生在您的身上！
请按照本指南中的措施防止数据被盗。

支付卡数据示例包括主帐户 (PAN) 和三位或四位数卡安全代码。下方红色箭头指向需要保护的数据类型。

存储在支付卡上的数据类型



什么是 PCI DSS?

支付卡行业数据安全标准 (PCI DSS) 是有助于小型商户保护支付卡上存储的客户卡数据的一套安全要求。

小型商户可能对通过自我评估调查问卷 (SAQ) 验证其 PCI DSS 遵从性已经非常熟悉。

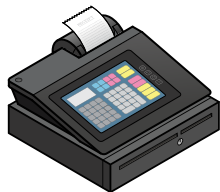
有关 PCI DSS 的更多信息，请参阅本指南末尾的“资源”部分。

了解您的支付系统：常用支付术语

支付设备的名称因地而异。此处列出了本文档提及的类型以及它们的常见名称。



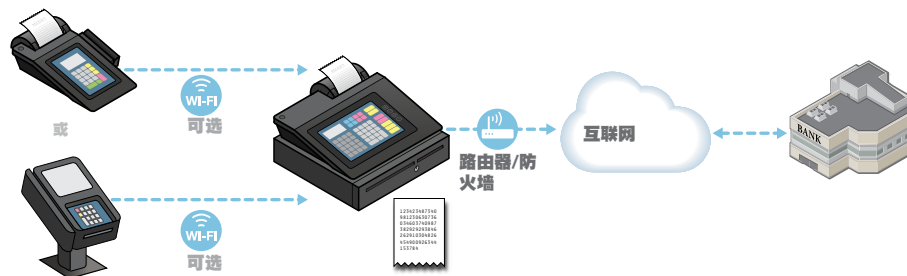
支付终端是一种用于通过刷卡、读卡、插卡、触卡，或手动输入卡号完成客户卡支付的设备。销售点（或 POS）终端、刷卡机、PDQ 终端或符合 EMV 标准/可读取芯片卡的终端也是用于描述这些设备的名称。



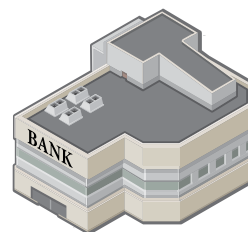
电子现金出纳机（收银机）可以登记和计算交易并打印收据，但不接受客户卡支付。



集成支付终端是一种将支付终端和电子现金出纳机合二为一的设备，这意味着它可以接受卡支付、登记并计算交易，以及打印收据。



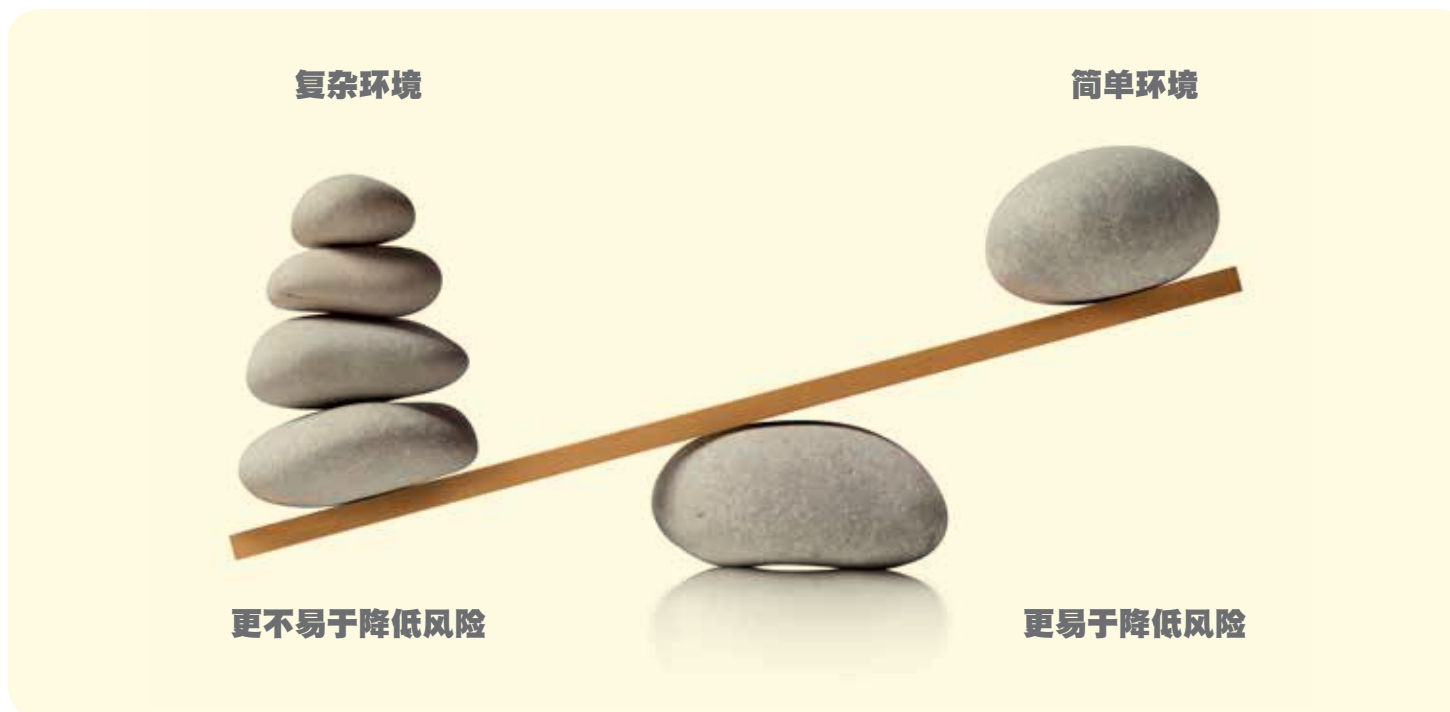
一种**支付系统**，包含在零售地点（包括商店/商铺和电商店面）接受卡支付的整个过程，并且可能包括支付终端、电子现金出纳机、连接支付终端的其他设备或系统（例如，用于实现互连的 Wi-Fi，或用于盘点的 PC）、带电子商务组件的服务器（例如支付页面），以及外连至商业银行的连接。



商业银行是代表商户处理信用卡和/或借记卡支付的银行或金融机构。此类实体又称为收单机构、收单银行、卡片处理商或支付处理商。

您的业务是如何处于危险之中的？

支付系统的功能越多，保护支付系统的复杂度就越高。这些附加功能通常为不法分子窃取客户卡数据提供了便利。请仔细考虑您的业务是否真的需要这些附加功能（例如 Wi-Fi 或摄像头）。



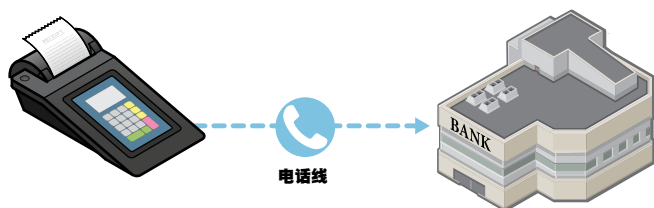
您如何销售商品或服务？主要通过以下三种方式：

1. 顾客走进商店，用卡购买。
2. 顾客访问网站，并在线支付。
3. 顾客打电话给商店，并通过电话提供卡片详细信息，或通过邮件或传真发送详细信息。

了解风险： 支付系统类型

无论是面对面交易还是在线交易，安全风险在很大程度上取决于支付系统的复杂度。

拨号支付终端



适用于店内购买的简单支付系统



适用于店内购买的复杂支付系统（配备 Wi-Fi、摄像头、互联网电话和其他互连系统）

商户电子商务网站



适用于网上商店购买的复杂电子商务支付系统（商户可以自主管理其网站和支付页面）

使用 常见支付系统 帮助您识别您使用的支付系统类型、您的风险，以及建议安全提示，以作为您与商业银行和供应商合作伙伴展开对话的出发点。

**使用安全基本措施
保护您的业务**



如何保护您的业务？

好消息是，从即日起您可以使用以下安全基本措施保护您的业务：

如何防止业务数据外泄	成本	简易度	风险降低
 使用强效密码，并更改默认密码			
 保护卡数据，仅存储需要的卡数据			
 检查支付终端是否遭到篡改			
 安装供应商提供的补丁			
 雇用值得信赖的业务合作伙伴，并掌握其联系方式			
 保护卡数据的内部访问			
 不要让黑客轻易能够访问您的系统			
 使用杀毒软件			
 扫描漏洞并修复问题			
 使用安全的支付终端和解决方案			
 禁止企业连接互联网			
 为实现最佳保护，请让您的数据成为对不法分子无用的数据			

这些安全基本措施按照从实施难度和成本最低到实施复杂度和成本较高的顺序排列。“风险降低”列还指示了各项基本措施帮助小型商户降低的风险量。



使用强效密码，并更改默认密码

成本



简易度



风险降低



密码对计算机和卡数据安全至关重要。就像门锁可以保护实物财产一样，密码有助于保护您的商业数据。另外还要注意，开箱即用的计算机设备和软件（包括支付终端）通常设有默认（预设）密码，例如“password”或“admin”，这类密码通常为黑客所知，并且是小型商户数据外泄的常见源头。

大约

80%

的数据泄露与密码被猜中或被
盗有关

威瑞森 PCI 2015

定期更改密码。像处理牙刷一样处理密码。不要让任何其他人员使用该密码，并且每隔三个月更换一次密码。

寻求帮助。询问供应商或服务提供商默认密码的相关事宜，以及更改默认密码的方法。然后予以实施！

设置难以被猜中的密码。“password”和“123456”是最常用的密码。黑客会尝试输入很容易猜到的密码，因为半数的用户会使用此类密码。强效密码拥有七个或更多字符，并且使用大小写字母、数字和符号组合（例如 !@#\$%*）。短语也可作为强效密码（而且更易于记忆），例如“B1gMac&frieS”。

不要与他人共享密码。督促每名员工均拥有个人登录 ID 和密码 — 切勿与他人共享！

须更改的典型默认密码：

[无]

[产品/供应商的名称]

1234 或 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

有关密码安全的详情，请参阅 PCI 委员会网站上的资源：

信息图

是时候更改您的密码了

视频

了解密码安全
(2 分钟)



保护卡数据，仅存储需要的卡数据

成本



简易度



风险降低



如果您连卡数据存储在哪都不知道的话，要想保护卡数据是不可能的。

您可以做些什么？

令牌化的目的和加密类似，但工作原理有所不同。它会将卡数据替换为对黑客而言毫无价值的无意义数据（“令牌”）。


请教专家。 询问支付终端供应商或商业银行系统存储数据的位置，以及能否简化处理支付的方式。另外，请询问他们如何在不存储卡安全代码的情况下进行具体的交易（例如，定期支付）。

外包。 不存储卡数据是防止数据外泄的最佳方法。可以考虑将您的卡处理外包给符合 PCI DSS 的服务提供商。参阅第 22 页上的“资源”部分，查看合规服务提供商列表。

如果不需要卡数据，就不要存储。

安全地损毁/粉碎不需要的卡数据。如果需要保存含有敏感卡数据的文档，请用较粗的黑色马克笔标记数据，直到数据不可读，然后将文档放入带锁的抽屉或保险箱里保管，并且仅允许少数人查看。

限制风险。 请让客户通过电话、传真或常规邮件提供支付详情，而非通过电子邮件提供。

令牌化或加密。 询问商业银行，了解您是否真的需要存储这些卡数据。如果确实需要，请咨询商业银行或服务提供商能否提供即使在卡数据被盗的情况下也可令卡数据失效的加密或令牌化技术。（有关详情，请参阅第 19 页上的“”部分）。

加密入门指南

加密法使用数学公式将纯文本设置为对不具备专门知识（称为密钥）的人不可读。加密法适用于已存储的数据，以及通过网络传输的数据。

加密可将纯文本更改为密文。

解密可将密文恢复为纯文本。

例如：

此为机密信息，请勿

加密密钥

5a0 (k\$hQ%...

解密密钥

此为机密信息，请勿



检查支付终端是否遭到篡改

成本



简易度



风险降低



客户卡数据进入支付终端时，“盗用设备”会将其全部扫描一遍。您和您的员工知道如何识别盗用设备至关重要。您需要定期检查支付终端，以确保其未遭篡改。记录检查了哪些终端、检查日期、检查人员，以及是否发现任何情况。

参阅 [PCI Council's guide: Skimming Prevention: Overview of Best Practices for Merchants \(PCI 委员会指南：防止盗用-商户最优方法概述\)](#)

请保持警惕，并根据下列步骤操作：

保存所有支付终端的清单，并拍照（正面、背面、电线和接头），了解其外观应该是什么样的。

寻找明显的篡改迹象，例如检修盖板或螺丝钉密封件损坏、奇怪/有所不同的布线，或者您不认识的新设备或功能。委员会指南（参见下文）可以提供帮助。

保护终端。不使用时，请将终端置于客户触碰不到的位置，并且避免公众看到其屏幕。在当天商店关门时确保支付终端（包括任何可读取客户支付卡或接受个人识别码 (PIN) 的设备）的安全。

控制维修。仅允许授权维修工作人员在您需要的情况下维修支付终端。也请告知您的员工。

如果有任何可疑状况，请立即致电您的支付终端供应商或商业银行！



安装供应商提供的补丁

成本



简易度



风险降低



通常，在程序员编写代码时可能会为软件引入缺陷或错误，又称为安全漏洞、bug 或漏洞。黑客会利用这些错误侵入您的计算机并盗取帐户数据。可以使用供应商提供的用于修复编码错误的“补丁”来保护系统。及时安装安全补丁至关重要！

询问您的供应商或服务提供商将如何通知您有新的安全补丁，并确保您能接收并读取这些通知。

哪一个供应商将向您发送补丁？ 您可以从支付终端、支付应用程序、其他支付系统（收银机、现金出纳机、PC 等）、操作系统（Android、Windows、iOS 等）、应用程序软件（包括 Web 浏览器）和商业软件供应商处获取补丁。

确保您的供应商更新支付终端、操作系统等，以便能够支持最新的安全补丁。尽管要求他们这么做。

电子商务商户。 尽快安装补丁对您而言也非常重要。同样可以设法从支付服务提供商处获取补丁。询问电子商务托管服务提供商是否修补您的系统（以及多久进行一次）。确保他们更新操作系统、电子商务平台和/或网络应用程序，以便支持最新的补丁。

请按照供应商/服务提供商的说明操作，并尽快安装这些补丁。



雇用值得信赖的业务合作伙伴，并掌握其联系方式

成本



简易度



风险降低



您可以雇用外部供应商提供与支付相关的服务、设备和应用程序。您还可以雇用与您共享卡数据的、支持或管理您的支付系统的、或获得卡数据访问权限的服务提供商。您可以称之为处理商、供应商、第三方，或服务提供商。他们会影响您保护卡数据的能力，因此了解他们的身份以及可以向其请教的安全问题至关重要。

知道可以打电话给谁。您的商业银行是哪家？还有谁能帮您处理支付？您从什么人手中购买了支付设备/软件，以及谁帮您进行了安装？您的服务提供商是谁？

保存清单。既然您已经知道可以打电话给谁，请将公司名和联系人姓名、电话号码、网站地址及其他联系方式保存在您可以在紧急情况下轻松找到的地方。

确认服务提供商的安全性。您的服务提供商是否符合 PCI DSS 要求？对电子商务商户而言，支付服务提供商符合 PCI DSS 也非常重要！参阅第 22 页上的“资源”部分，查看合规服务提供商列表。

提问。知道外部提供商的身份及其为您提供的服务后，可以与他们进行交流，以了解其保护卡数据的方式。利用[要请教供应商的若干问题](#)帮助您了解要问的问题。

了解一般供应商。向右浏览侧边栏，了解与您共事的常见供应商/服务提供商类型。

一般供应商

有关一般供应商的更多详情，请参阅[要请教供应商的若干问题](#)中的表格：

支付终端供应商

支付应用程序供应商

支付系统安装商（又称为集成商/经销商）

执行支付处理，或电子商务托管或处理的服务提供商

帮助您满足 PCI DSS 要求（例如，提供防火墙或杀毒服务）的服务提供商

软件即服务提供商



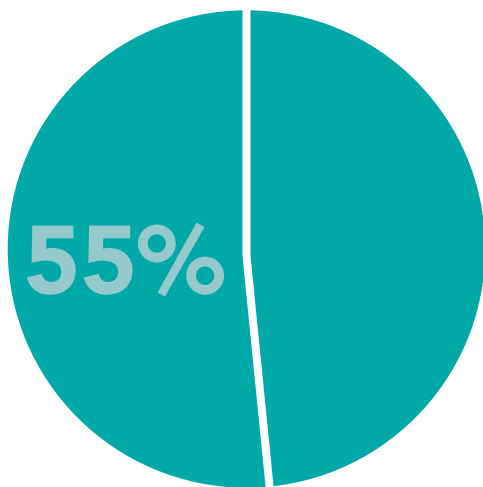
保护内部访问数据

成本	
简易度	
风险降低	

权限滥用表示个人使用...

他人的访问权限和权限访问未被授权访问的系统或数据。

权限滥用是导致数据泄露的首要原因 — 占有所有报告事件的 55%。



威瑞森 2015

访问控制非常重要。将系统设置为仅根据“业务知情需要”授予访问权限。作为所有者，您可以访问所有数据。而大部分员工在开展工作时仅可访问数据、应用程序和功能的子集。

支付系统和未加密卡数据的访问权限仅限于需要访问权限的员工，并且仅限于开展工作所需的数据、应用程序和功能。

做记录。跟踪公司的后台访客。包括姓名、访问原因，以及授予访客访问权限的员工的姓名。至少连续记录一年。

安全地处理设备。询问支付系统供应商或服务提供商如何在销售或处理支付设备前安全地移除卡数据（使数据不可恢复）。

分享这些信息。将本指南提供给您员工和业务合作伙伴，让他们了解业务期望。

考虑授予员工收取支付款项的权限，但不得处理退款，或者授予其处理新预订/订单的权限，但不得访问与现有预订/订单有关的支付卡数据。一些员工根本不应拥有访问权限。



不要让黑客轻易能够访问您的系统

成本



简易度



风险降低



黑客 = 不法分子

利用您信任的人是黑客侵入系统最便利的方式之一。您需要了解供应商访问系统的方式，以确保未暴露任何漏洞让黑客有机可乘。

多因素验证使用用户名和密码，外加至少一个其他因素（例如智能卡、加密狗*，或一次性密码）。

*一种连接至计算机以允许访问无线、软件功能等等的便携设备

弄清楚、查明白。询问您的支付系统供应商或服务提供商是否使用远程访问支持或访问您的业务。

询问限制使用远程访问的方法。许多远程访问程序在默认情况下始终处于启用状态。降低风险 — 询问供应商如何在不需要时禁用远程访问，以及如何在供应商或服务提供商特别请求时启用。

完成后请禁用该功能。

使用强效验证。如果必须允许远程访问，需要使用多因素验证和强效加密法。

确保服务提供商使用独一无二的凭证。每个服务提供商均须使用专用于您的企业的远程访问凭证，而且这些远程访问凭证不得与用于其他客户的相同。

寻求帮助。向您的供应商或服务提供商寻求帮助以禁用远程访问，或（如果供应商或服务提供商需要远程访问的话）寻求帮助以设置多因素验证。参阅[要请教供应商的若干问题](#)，助您确切地了解要问的问题。

如果供应商要从其办公室（而非您所在的位置）支持或故障排除您的支付终端，则需使用互联网和远程访问软件。

供应商可能在您的终端上安装并用于提供远程支持的产品示例包括 VNC 和 LogMeIn。



使用杀毒软件

成本	
简易度	
风险降低	

系统和软件极为灵活，并且提供各种各样的功能和特性。黑客编写病毒和其他恶意代码来利用这些功能和编码错误，以便侵入您的系统并盗取卡数据。使用最新的杀毒（又称为反恶意软件）软件，以帮助保护您的系统。

安装杀毒软件以保护您的支付系统。 安装过程十分简单，并且可以从您当地的办公用品商店或 IT 零售商处获取。

将软件设置为“自动更新”， 以便您始终能够获取最新的可用保护。

获取建议。 从您的 IT 零售商处了解其推荐的杀毒/反恶意软件保护产品。

运行定期扫描。 定期运行全系统扫描，因为您的系统可能已经被在杀毒软件能够检测到前已经发布的全新恶意软件感染。



扫描漏洞并修复问题

成本



简易度



风险降低



每天都会发现新的漏洞、安全漏洞和漏洞。让面向互联网的系统定期接受测试，以识别并尽快解决这些风险至关重要。面向互联网的系统（例如许多支付系统）通常最易受到攻击，因为不法分子可以轻松利用这些系统，以便他们偷偷侵入您的系统。

PCI 委员会的授权扫描服务商 (ASV) 执行外部漏洞扫描和报告。参见 PCI 的 [List of PCI-Approved Scanning Vendors](#) (PCI 授权扫描服务商列表)

获取建议。 询问商业银行是否与任何 PCI 授权扫描服务商 (ASV) 之间存在合作关系。另请询问您的供应商和服务提供商。

与 PCI ASV 进行对话。 这些供应商可以借助能够自动搜索网络以找到漏洞并提供相关报告（例如，如果您需要应用补丁的话）的工具为您提供帮助。PCI 委员会列表（参见下文）可以帮助您查找扫描服务商。

选择一个扫描仪。 联系若干 PCI ASV，找到一款配备适用于小型企业的程序的扫描仪。

解决漏洞。 向您的 ASV 寻求帮助，以修正通过扫描发现的问题。



使用安全的支付终端和解决方案

成本



简易度



风险降低



使用安全的支付解决方案和训练有素的专业人员来帮助您是一个能够更好地保护您的企业的可靠方法。如何选择安全的产品并确保安全设置这些产品如下所示。

使用安全支付终端和 PIN 输入设备。 PCI 委员会认可能够保护 PIN 数据的支付终端。确保您的支付终端或设备列于针对提供最佳安全并支持“EMV 芯片”的设备的 [List of PCI Approved PTS Devices \(PCI 认可的 PTS 设备列表\)](#) 上。

使用安全的软件。 确保您的支付软件列于 [List of PCI Validated Payment Applications \(经 PCI 认证的支付应用程序列表\)](#) 上

使用合格的专业人员。 确保经 PA-DSS 认证的应用程序的安装人员正确安全地进行安装。从 [List of PCI QIRs \(PCI QIR 列表\)](#) 中选择通过 PCI 委员会资格认证的公司为您提供帮助。让商业银行帮助您做选择。

参考此供应商问题列表。 利用[要请教供应商的若干问题](#)帮助您了解要询问供应商和服务提供商哪些问题。

您的客户将他们的支付卡个人识别码 (PIN) 输入到您的支付终端或 PIN 输入设备中。使用安全的设备保护客户的 PIN 数据非常重要。

有关加密卡数据的 PCI 支付终端和安全读卡器，请参阅第 19 页上的 .



禁止企业连接互联网

成本	
简易度	
风险降低	

互联网是数据盗用者攻击并窃取客户卡数据所利用的主要捷径。因此，如果您的业务在互联网上进行，则需额外保护用于完成卡支付的任何操作。

单独使用。请勿将用于支付的设备同时用于任何其他用途。例如，请勿通过用于支付交易的同一个设备或计算机进行网上冲浪或查看电子邮件或社交媒体。有业务需要时（例如更新企业的社交媒体网页），请使用另一台计算机而非支付设备完成这些更新。

保护您的“虚拟终端”。如果通过虚拟终端（通过计算机或平板电脑访问的网页）输入客户支付款项，请将风险最小化——请勿连接外部读卡器。

保护 Wi-Fi。如果您的商店为客户提供免费 Wi-Fi，请确保为支付系统选用另一个网络（这叫做“网络分段”）。让您的网络安装商帮助您安全配置 Wi-Fi。

使用防火墙。防火墙若谷可以起到缓冲区的作用，从而防止黑客和恶意软件访问您的计算机和信息。与您的支付终端供应商或服务提供商商议，确保您安装有一个防火墙，或请求他们帮您正确配置。

使用个人防火墙软件或等效产品（当支付系统不受企业防火墙保护时，例如，连接公共 Wi-Fi）。



为实现最佳保护，请让您的数据成为对不法分子无用的数据

成本



简易度




风险降低



将数据传输到商业银行时，以及将其保存或存储在您的计算机和设备上时，数据易受到攻击。保护数据的最佳方法就是在不需要时通过隐藏和全部删除数据使其失效（即使在被盗用的情况下）。虽然要将其落实到位可能会更加复杂，但从长远的角度来看，这样将更便于管理安全。

询问您的支付系统供应商或服务提供商您的支付系统是否使用了加密技术和/或令牌化技术。

使用加密卡数据的 PCI 设备。PCI 委员会认可保护 PIN 数据的支付终端（参见第 17 页上的 ），以及能够另外加密卡数据的支付终端和“安全读卡器”。参见 [List of PCI Approved PTS Devices \(PCI 认可的 PTS 设备列表\)](#)。

使用安全的 PCI 加密解决方案。询问您的支付终端加密是否通过点到点加密解决方案完成，以及该解决方案是否列于 PCI 委员会的 [List of PCI P2PE Validated Solutions \(PCI P2PE 认证解决方案列表\)](#) 上

升级解决方案。降低风险 — 考虑获取利用加密和令牌化技术使卡数据对黑客失去价值的全新支付终端。

您是否是现在正在向 EMV 芯片终端迁移的商户？这是投资支持 EMV 并且进一步提高加密和令牌化安全性的终端的绝佳机会。

提问。参见 [要请教供应商的若干问题](#)，获取要询问供应商或服务提供商的问题方面的帮助。

PCI 认可了通过一项名为“安全读取并交换数据 (SRED)”的技术加密卡数据的安全读卡器和支付终端 — 询问您的供应商您的支付终端是否通过 SRED 加密卡数据。

The image features a teal background with a large, lighter teal circle on the left side. Inside this circle, three stylized human figures in business suits are standing on a circular platform. The figures are rendered in a simple, flat style with no facial features. The central figure is slightly taller than the two flanking figures. The text '可从哪里获取帮助' is overlaid on the right side of the image, in a bold, white, sans-serif font.

可从哪里获取帮助

PCI 委员会列表

资源	链接	网址
List of Validated Payment Applications (认证支付应用程序列表)	PCI Council's Validated Payment Applications (PCI 委员会的认证支付应用程序)	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices (认可的 PTS 设备列表)	PCI Council's Approved PTS Devices (PCI 委员会认可的 PTS 设备)	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors (授权扫描服务商列表)	PCI Council's Approved Scanning Vendors (PCI 委员会的授权扫描服务商)	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers (合格集成商/经销商列表)	PCI Council's Qualified Integrators Resellers (PCI 委员会的合格集成商经销商)	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions (P2PE 认证解决方案列表)	PCI Council's P2PE Validated Solutions (PCI 委员会的 P2PE 认证解决方案)	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

支付品牌列表

资源	链接	网址
Lists of Compliant Service Providers (合规服务提供商列表)	MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表)	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿)	http://www.visa.com/splisting/
	Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS 和相关指南

资源	链接	网址
More about PCI DSS (详细了解 PCI DSS)	How to Secure with PCI DSS (如何利用 PCI DSS 实施保护)	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires (PCI DSS 自我评估调查问卷)	Self-Assessment Questionnaires (自我评估调查问卷)	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants (指南：防止盗用：商户最优方法概述)	Skimming Prevention: Overview of Best Practices for Merchants (防止盗用：商户最优方法概述)	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

信息图和视频

资源	链接	网址
Infographic: It's Time to Change Your Password (信息图: 是时候更改您的密码了)	It's Time to Change Your Password (是时候更改您的密码了)	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves (信息图: 通过让被盗数据对盗用者失去价值来抵抗网络犯罪)	Fight Cybercrime by Making Stolen Data Worthless to Thieves (通过让被盗数据对盗用者失去价值来抵抗网络犯罪)	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Video: Learn Password Security in 2 Minutes (视频: 了解密码安全 (2 分钟))	Learn Password Security in 2 Minutes (了解密码安全 (2 分钟))	https://www.youtube.com/watch?v=FsrOXgZKa7U

小型商户 PCI 支付保护资源

资源	链接	网址
常见支付系统	常见支付系统	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
小型商户要请教供应商的若干问题	小型商户要请教供应商的若干问题	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
小型商户词汇表	小型商户词汇表	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

来源

Gallup – Gallup Poll, October 2015 (盖洛普 – 盖洛普民意测验, 2015 年 10 月)

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014 (英国政府 - 小型企业: 网络安全须知, 英国 2014 年)

NCSA – *National Cyber Security Alliance survey*, 2012 (NCSA – 国家网络安全联盟调查, 2012 年)

NSBA – *National Small Business Administration, 2014 Year End Economic Report* (NSBA – 国家小型企业管理, 2014 年底经济报告)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (威瑞森 2012 – 威瑞森 2012 数据泄露调查报告)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (威瑞森 2015 – 威瑞森 2015 数据泄露调查报告)

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report* (威瑞森 PCI 2015 – 威瑞森 2015 PCI 遵从性报告)