付款資料安全要項

強式密碼

風險何在？

81%

的駭入相關資料外洩是利用竊得及/或安全性弱的密碼

(2017 年 Verizon 資料外洩調查報告)

使用安全性弱和預設的密碼，是企業資料外洩的一大成因。

密碼是電腦和付款資料安全的要項。不過為了能夠有效，必須為強式，並且定期更新。

隨即可用的電腦設備與軟體（包括付款終端機）經常附有廠商出廠或預設密碼，例如 “password” 或 “admin”，為一般已知，能輕易受罪犯利用。

必須變更的典型預設密碼：

[無]
[產品/廠商名稱] 1234 或 4321
通過存取密碼
匿名
私密的
a 資料庫
sysadmin
訪客管理員
使用者

密碼最佳實務

為使資料外洩的風險降至最低，企業應將廠商的預設密碼變更為強式密碼，並且絕不共用 – 每位員工應有自己的登入 ID 和密碼。

請定期變更您的密碼

請將密碼如同牙刷般看待。別讓任何人使用，並且每三個月更換。

勿共用密碼

堅持讓每位員工有自己的登入 ID 和密碼 – 切勿共用！

使密碼很難猜到

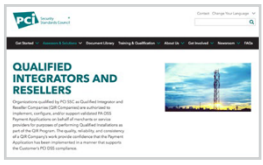
最常見的密碼有 “password”、“password1” 和 “123456”。因為半數的人使用容易猜出的密碼，所以駭客會加以嘗試。強式密碼有至少七個字元，並且混合大小寫字母、數字和符號（例如!@#$&*）。數字和符號並用的片語也是一種強式密碼 – 關鍵是選擇對您有特殊意義的片語以便幫助記憶，例如喜愛的嗜好（像是 ILove2Fish4Trout!）。

資源

請瀏覽 pcissc.org/Merchants 取得更多資源

廠商和服務供應商能協助企業識別預設密碼，並加以變更。

安全付款指南可為企業提供防範付款資料遭竊的安全基本知識。



PCI Qualified Integrators and Resellers (QIR) 清單是企業能用以尋找付款系統安裝者的資源，其受過支付卡產業安全標準委員會 (PCI Security Standards Council) 就強式密碼和其他付款資料安全要項所提供的培訓。

請看這段動畫短片，了解企業如何能藉由將廠商的預設密碼變更為強式密碼，並且絕不共用密碼，使得資料外洩的可能性降至最低。

© 2020 PCI Security Standards Council LLC.
www.pcisecuritystandards.org

PCI Security Standards Council