

Hướng dẫn thanh toán an toàn

Version 1.0 | July 2016





HIỂU VỀ RỦI RO

Hiểu về nguy cơ

Doanh nghiệp nhỏ là mục tiêu ưu tiên của tin tặc đánh cắp dữ liệu.

Khi môi trường dữ liệu thẻ thanh toán của bạn bị xâm nhập, doanh nghiệp của bạn sẽ nhanh chóng bị ảnh hưởng. Khách hàng, đối tác mất niềm tin vào năng lực bảo vệ thông tin cá nhân của bạn và chuyển đổi nhà cung cấp. Có rất nhiều án phạt từ các định chế tài chính đang chờ bạn và quan trọng hơn, tài khoản merchant của bạn sẽ bị tạm treo hoặc đóng vĩnh viễn. Một cuộc điều tra với 1.015 doanh nghiệp vừa và nhỏ chỉ ra rằng 60% các doanh nghiệp bị xâm nhập đã đóng cửa trong vòng 6 tháng sau đó. (NCSA)

60%

DOANH NGHIỆP NHỎ BỊ TẤN CÔNG MẠNG.

(HM Government)



71%

TIN TẶC TẤN CÔNG VÀO CÁC DOANH NGHIỆP CÓ ÍT HƠN 100 NHÂN SỰ

(Verizon 2012)

\$20,752



CHI PHÍ TRUNG BÌNH DOANH NGHIỆP NHỎ PHẢI BỎ RA VÌ BỊ TẤN CÔNG MẠNG, CON SỐ NÀY NĂM 2013 LÀ \$8.600 (NSBA)

69%

NGƯỜI TIÊU DÙNG QUAN NGẠI VỀ THẤT THOÁT DỮ LIỆU THẺ THANH TOÁN

(Gallup)



Rủi ro nằm ở đâu?

DỮ LIỆU THẺ CỦA KHÁCH HÀNG LÀ MỎ VÀNG ĐỐI VỚI TỘI PHẠM. ĐỪNG ĐỂ ĐIỀU ĐÓ XẢY RA VỚI BẠN

Tuân thủ theo các hướng dẫn dưới đây để bảo vệ mình khỏi tin tặc đánh cắp dữ liệu.

Ví dụ về dữ liệu thẻ bao gồm số tài khoản, mã an ninh thẻ ba hoặc bốn ký tự. Mũi tên đỏ trong hình bên dưới chỉ ra những dữ liệu cần được bảo mật.

DỮ LIỆU TRÊN THẺ THANH TOÁN



PCI DSS LÀ GÌ?

Tiêu chuẩn an ninh dữ liệu ngành thẻ thanh toán (PCI DSS) là một bộ tiêu chuẩn an ninh giúp các doanh nghiệp nhỏ bảo vệ dữ liệu thẻ khách hàng nằm trên thẻ thanh toán

Các doanh nghiệp nhỏ sẽ thực hiện đánh giá đạt chuẩn PCI DSS thông qua trả lời bộ câu hỏi tự đánh giá (SAQ)

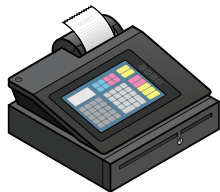
Để tìm hiểu thêm về PCI DSS, tham khảo thêm các tài nguyên được liệt kê phía cuối tài liệu này

Hiểu về hệ thống thanh toán: Các hệ thống thanh toán phổ biến

Tùy thuộc vào nơi bạn sống, các thiết bị thanh toán điện tử có thể được đặt tên khác nhau. Các thuật ngữ sau đây sẽ được sử dụng để mô tả các thiết bị sau.



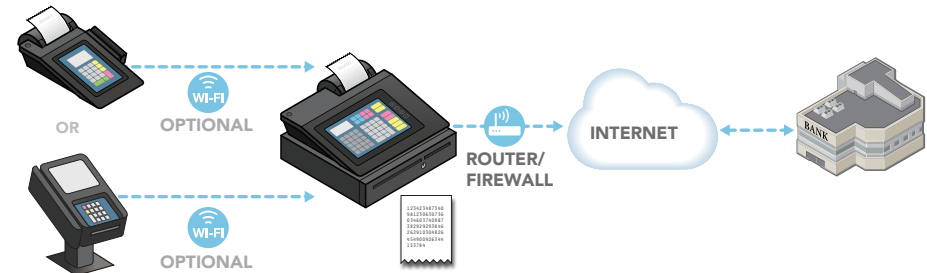
Một **THIẾT BỊ ĐẦU CUỐI THANH TOÁN** là thiết bị được sử dụng để chấp nhận thanh toán qua thẻ bằng cách quẹt, cắm hoặc nhập số thẻ vào thiết bị. POS, máy đọc thẻ tín dụng, thiết bị đầu cuối PDQ, thiết bị đầu cuối cho thẻ chip/ EMV đều được coi là thiết bị đầu cuối thanh toán



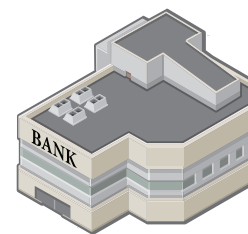
Một **MÁY TÍNH TIỀN ĐIỆN TỬ** có khả năng tính giá trị của giao dịch, in hoá đơn, nhưng không chấp nhận thanh toán thẻ tín dụng



Một **THIẾT BỊ ĐẦU CUỐI THANH TOÁN TÍCH HỢP** là một thiết bị đầu cuối thanh toán kèm máy tính tiền điện tử, với các tính năng tính giá trị giao dịch, in hoá đơn và chấp nhận thanh toán bằng thẻ tín dụng



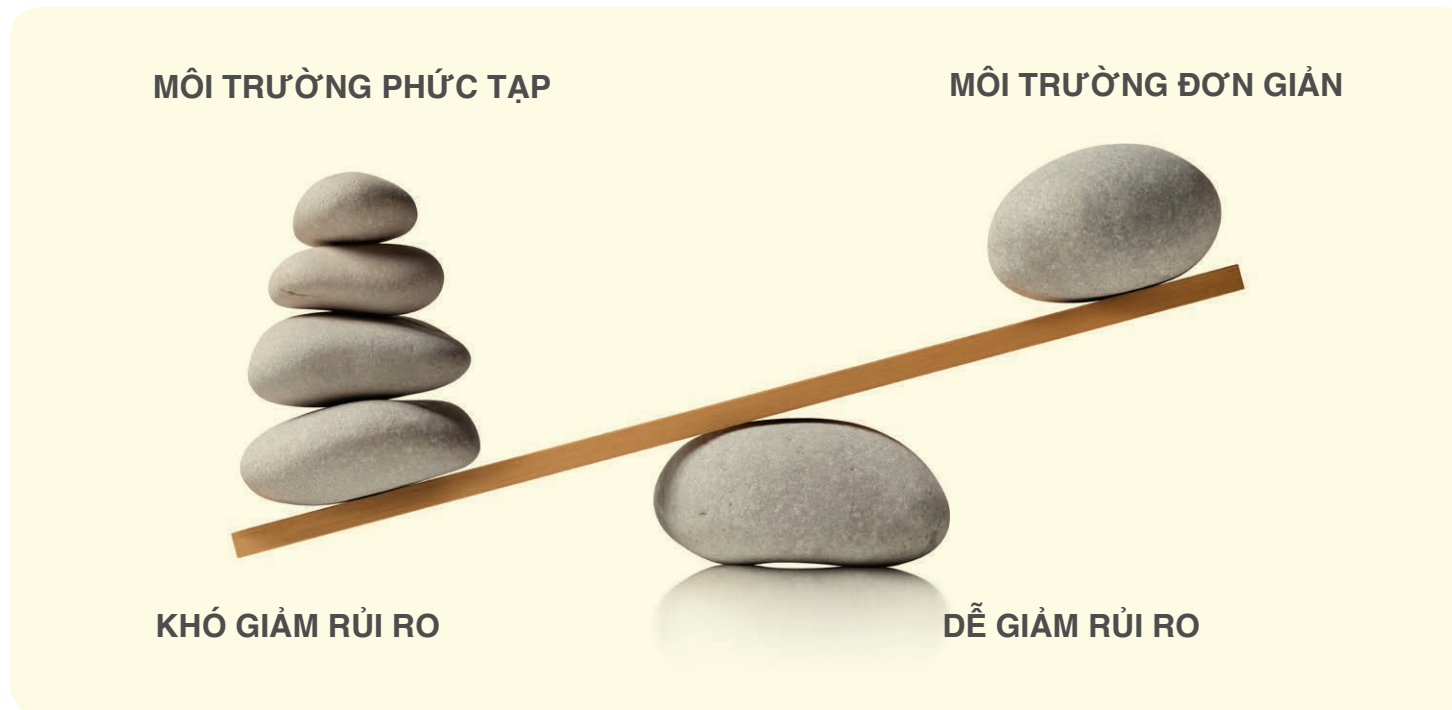
Một **HỆ THỐNG THANH TOÁN** bao gồm toàn bộ quá trình chấp nhận thẻ thanh toán tại một điểm bán lẻ (bao gồm gian hàng, cửa hàng, website TMĐT) và có thể bao gồm thiết bị đầu cuối thanh toán, máy tính tiền điện tử và các thiết bị, hệ thống khác kết nối với thiết bị đầu cuối thanh toán (ví dụ, thiết bị phát WiFi hay một máy tính kiểm soát hàng tồn kho), máy chủ với các thành phần thương mại điện tử như trang thanh toán, đường kết nối đến ngân hàng của merchant.



Một **NGÂN HÀNG CỦA MERCHANT** là ngân hàng/ tổ chức tín dụng xử lý các giao dịch bằng thẻ tín dụng hoặc thẻ ghi nợ thay mặt cho merchant. Các thuật ngữ **Acquirer, acquiring bank, card/ payment processor** cũng có ý nghĩa tương tự

Doanh nghiệp của bạn chịu rủi ro như thế nào?

Hệ thống thanh toán của bạn các nhiều tính năng, yêu cầu đảm bảo an ninh càng phức tạp. Các tính năng bổ sung thường mang lại nhiều cơ hội cho tội phạm đánh cắp dữ liệu thẻ thanh toán của khách hàng hơn. hãy suy tính kỹ càng xem bạn có cần những tính năng bổ sung này không (ví dụ: Wi-Fi hoặc camera) cho doanh nghiệp của mình.

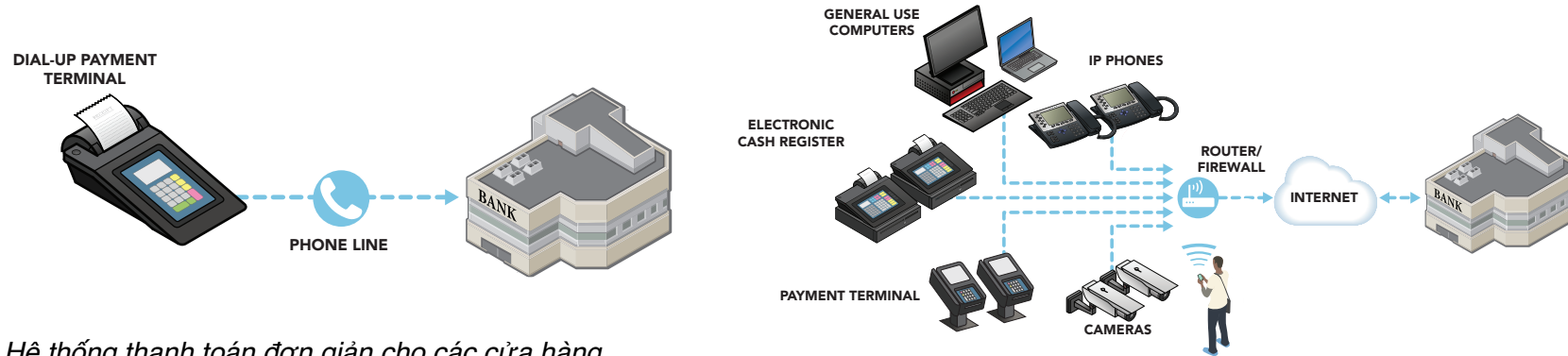


Bạn kinh doanh hàng hoá và dịch vụ như thế nào? Có ba cách cơ bản:

- 1. Một người vào cửa hàng và mua hàng bằng thẻ thanh toán*
- 2. Một người truy cập vào website và thanh toán online*
- 3. Một người gọi cho cửa hàng và cung cấp dữ liệu thẻ qua thoại, email, fax*

Hiểu về rủi ro: các hệ thống thanh toán

Các rủi ro an ninh biến thiên theo mức độ phức tạp của hệ thống thanh toán, trực tiếp hay trực tuyến



Hệ thống thanh toán đơn giản cho các cửa hàng

Hệ thống thanh toán phức tạp cho các cửa hàng, với Wi-Fi, camera, Internet phone, và các thiết bị ngoại vi khác



Hệ thống thanh toán TMĐT phức tạp cho các website trực tuyến, với việc merchant quản lý website và trang thanh toán của mình

**BẢO VỆ DOANH
NGHIỆP VỚI CÁC
PHƯƠNG ÁN AN NINH
CƠ BẢN**

Bạn bảo vệ doanh nghiệp mình theo cách nào?

Bạn có thể bắt đầu bảo vệ doanh nghiệp của mình theo những cách cơ bản như sau

Cách bảo vệ doanh nghiệp tránh bị xâm phạm	Chi phí	Độ khó	Giảm rủi ro
 Sử dụng mật khẩu mạnh và thay đổi mật khẩu mặc định			
 Bảo vệ dữ liệu thẻ và chỉ lưu lại những gì mình thực sự cần			
 Giám sát thiết bị thanh toán chống bị thay đổi			
 Cài đặt bản vá chính hãng			
 Sử dụng các đối tác tin cậy và biết cách liên hệ với họ			
 Bảo vệ truy cập nội bộ đến môi trường thẻ			
 Không cho hacker được dễ dàng xâm nhập hệ thống			
 Sử dụng phần mềm diệt virus			
 Rà soát và fix các lỗ hổng bảo mật			
 Sử dụng các thiết bị và giải pháp thanh toán an toàn, tin cậy			
 Bảo vệ doanh nghiệp trước Internet			
 Làm cho dữ liệu thẻ trở nên vô dụng với tội phạm mạng			

Các kiến thức an ninh cơ bản này được sắp xếp từ đơn giản và rẻ đến phức tạp và tốn kém để triển khai. Khả năng giảm thiểu rủi ro cho hệ thống của mỗi phương án dành cho doanh nghiệp nhỏ được hiểu là “Giảm rủi ro”



Sử dụng mật khẩu mạnh và thay đổi các mật khẩu mặc định

Cost



Ease



Risk Mitigation



Mật khẩu rất quan trọng đối với an toàn cho máy tính và dữ liệu thẻ. Như chìa khoá bảo vệ bất động sản, mật khẩu giúp bảo vệ dữ liệu doanh nghiệp. Cần nhớ rằng các thiết bị và phần mềm thường sử dụng mật khẩu mặc định như “password” hay “admin” và hacker thường tận dụng để tiến hành tấn công dữ liệu

Khoảng

80%

các cuộc tấn công dữ liệu bắt nguồn từ việc suy đoán hoặc đánh cắp mật khẩu

Verizon PCI 2015

ĐỊNH KỲ THAY ĐỔI MẬT KHẨU. Hãy coi mật khẩu như bàn chải đánh răng. Đừng cho ai xài ké và hãy đổi mật khẩu định kỳ 3 tháng/ lần.

YÊU CẦU TRỢ GIÚP. Hỏi hãng hoặc nhà cung cấp dịch vụ bàn giao mật khẩu và cách thay đổi chúng. Và làm ngay!

TẠO MẬT KHẨU KHÓ ĐOÁN. Password thông dụng nhất là “password” và “123456”. Hacker thường thử mật khẩu này vì chúng được sử dụng bởi quá nửa công dân mạng. Một mật khẩu mạnh phải có ít nhất 7 ký tự, có phân biệt viết hoa, bao gồm số và ký tự đặc biệt(!@#\$\$&*). Một cụm từ với các thành phần kể trên cũng được coi là mật khẩu mạnh và dễ nhớ như “B1gMac&frieS.”

KHÔNG CHIA SẺ. Yêu cầu mỗi nhân viên phải tạo một mật khẩu riêng – và không bao giờ chia sẻ!

Các mật khẩu mặc định cần phải thay đổi:

[none]

[name of product/
vendor]

1234 or 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

Tài nguyên bổ sung về vấn đề mật khẩu:

INFOGRAPHIC

It's Time to Change Your
Password



VIDEO

Learn Password
Security in 2 Minutes



Bảo vệ dữ liệu thẻ và chỉ lưu những gì bạn cần

Cost	
Ease	
Risk Mitigation	

Bạn không thể bảo vệ dữ liệu nếu không biết chúng ở đâu.

Bạn có thể làm gì?

Số hoá thẻ (Tokenization) có mục tiêu giống như mã hoá nhưng khác về phương thức thực hiện. Tokenization thay thế dữ liệu thẻ bằng dữ liệu hoàn toàn vô nghĩa (token) và vô giá trị với hacker.

THAM VẤN CHUYÊN GIA. Hãy hỏi bên cung cấp thiết bị đầu cuối hoặc ngân hàng để biết hệ thống của bạn lưu giữ dữ liệu ở đâu, cách xử lý các giao dịch thanh toán. Nhớ hỏi thêm cách thức tiến hành các loại giao dịch cụ thể (ví dụ: giao dịch thanh toán lại) mà không phải lưu mã an ninh thẻ.

OUTSOURCE. Cách tốt nhất để đảm bảo an ninh thẻ là không lưu giữ thông tin thẻ. Hãy outsource dịch vụ xử lý thẻ cho một đơn vị cung cấp đã đạt chuẩn PCI DSS.

NẾU KHÔNG CẦN DỮ LIỆU THẺ THÌ ĐỪNG LƯU. Hãy huỷ dữ liệu thẻ nếu bạn không cần một cách an toàn. Nếu bạn giữ chứng từ có chứa dữ liệu thẻ thì hãy dùng bút đen xóa dữ liệu thẻ và cất giữ chứng từ một cách an toàn.

HẠN CHẾ RỦI RO. Thay vì chấp nhận dữ liệu thẻ qua email, hãy yêu cầu khách hàng của mình điện thoại, fax, gửi thư bưu chính.

SỐ HOÁ HOẶC MÃ HOÁ THẺ. Hãy hỏi ngân hàng xem liệu bạn có thực sự cần lưu dữ liệu thẻ không. Nếu không, hãy hỏi ngân hàng về công nghệ số hoá hay mã hoá thẻ để khiến cho dữ liệu thẻ không còn giá trị nếu bị đánh cắp.

MÃ HOÁ

Mã hoá sử dụng thuật toán để chuyển đổi thông điệp thành mật mã không thể đọc được với phần lớn mọi người. Mã hoá được sử dụng để mã hoá dữ liệu lưu trữ và dữ liệu trên đường truyền.

MÃ HOÁ chuyển đổi thông điệp thành mật mã

GIẢI MÃ chuyển đổi mật mã thành thông điệp

Ví dụ:

Đây là thông tin mật

ENCRYPTION KEY

5a0 (k\$hQ%...

DECRYPTION KEY

Đây là thông tin mật



Giám sát thiết bị thanh toán chống bị thay đổi

Cost



Ease



Risk Mitigation



Thiết bị gián điệp quét nhanh dữ liệu thẻ của khách hàng khi thẻ được đưa vào thiết bị để thực hiện thanh toán. Điều quan trọng là bạn và nhân viên của mình phải có khả năng phát hiện ra thiết bị gián điệp. Bạn cần thường xuyên kiểm tra thiết bị đầu cuối thanh toán để đảm bảo không có những thay đổi ngoài mong muốn. Nên có nhật ký lưu giữ lịch kiểm soát thiết bị kèm thời gian và người thực hiện cùng kết quả

See the [*PCI Council's guide: Skimming Prevention – Overview of Best Practices for Merchants*](#)

Hãy cảnh giác và thực hiện các bước sau:

GIỮ DANH SÁCH tất cả các thiết bị đầu cuối thanh toán và chụp ảnh từng thiết bị (mặt trước, sau và kết nối) để bạn có thể đối chiếu nguyên trạng về sau.

TÌM KIẾM NHỮNG DẤU HIỆU thay đổi, như tem mất nguyên trạng, cáp kết nối không giống ban đầu, thiết bị có thêm những bộ phận lạ.

BẢO VỆ THIẾT BỊ ĐẦU CỐI. Giữ chúng ở ngoài tầm với của khách hàng khi không sử dụng và không cho ai nhìn màn hình của thiết bị. Hãy đảm bảo rằng thiết bị của bạn an toàn mỗi cuối ngày bán hàng, bao gồm cả thiết bị đọc thẻ và nhập mã PIN

KIỂM SOÁT BẢO TRÌ. Bạn và nhân viên của bạn chỉ cho nhân sự chính hãng bảo trì thiết bị nếu như bạn yêu cầu hỗ trợ.

GỌI cho hãng hoặc ngân hàng ngay khi bạn phát hiện dấu hiệu khả nghi!



Cài đặt bản vá chính hãng

Cost



Ease



Risk Mitigation



Thông thường, phần mềm thường có lỗ hổng và lỗi lập trình từ người lập trình, còn gọi là lỗ hổng an ninh. Hacker thường khai thác các lỗ hổng này để bẻ khoá máy tính và đánh cắp dữ liệu tài khoản. Hãy bảo vệ hệ thống bằng cách cài đặt các bản vá chính hãng để xử lý các lỗi phần mềm. Cài đặt bản vá an ninh càng sớm càng tốt.

HỎI hãng hoặc nhà cung cấp cách nhận thông báo về các bản vá bảo mật, và khi nhận được thì hãy nhớ đọc.

AI SẼ GỬI BẢN VÁ CHO BẠN? Bạn có thể nhận bản vá từ hãng cung cấp thiết bị đầu cuối thanh toán, ứng dụng thanh toán, hệ thống thanh toán (máy tính tiền, PC...), hệ điều hành (Android, Windows, iOS), phần mềm ứng dụng, và phần mềm doanh nghiệp.

HÃY ĐẢM BẢO hãng của bạn cập nhật thiết bị đầu cuối thanh toán, hệ điều hành và họ có thể hỗ trợ bạn cập nhật các bản vá an ninh. Hãy hỏi họ.

MERCHANT TMĐT. Cài đặt bản vá càng sớm càng tốt là rất quan trọng. Hãy tìm cả các bản vá từ nhà cung cấp dịch vụ thanh toán. Hãy hỏi nhà cung cấp dịch vụ hosting TMĐT liệu họ có thực hiện cập nhật bản vá không (tần suất như thế nào). Hãy đảm bảo họ cập nhật điều hành, nền tảng TMĐT và ứng dụng web để chúng có thể hỗ trợ các bản vá mới nhất

TUÂN THỦ hướng dẫn từ hãng và nhà cung cấp dịch vụ, đồng thời cài đặt bản vá càng sớm càng tốt.



Sử dụng các đối tác tin cậy và biết cách liên hệ với họ

Cost



Ease



Risk Mitigation



Bạn sử dụng các nhà cung cấp bên ngoài cho các dịch vụ, thiết bị, ứng dụng liên quan đến thanh toán. Bạn có thể có những nhà cung cấp bạn chia sẻ dữ liệu, hỗ trợ hoặc quản lý hệ thống thanh toán, hoặc được bạn trao quyền truy cập dữ liệu thẻ. Bạn có thể gọi họ là cổng thanh toán, hãng, bên thứ ba, nhà cung cấp. Tất cả đối tác này đều có ảnh hưởng đến khả năng bảo vệ dữ liệu thẻ của bạn, vì vậy bạn cần biết rõ về họ và các câu hỏi cần phải hỏi họ.

BIẾT ĐỂ GỌI. Ngân hàng của bạn là ai? Ai hỗ trợ xử lý thanh toán cho bạn? Bạn mua phần mềm/thiết bị thanh toán từ ai và ai cài đặt chúng? Nhà cung cấp dịch vụ của bạn là ai?

LƯU DANH BẠ. Tất cả các đối tượng trên cần được lưu vào danh bạ để bạn gọi được ngay khi cần thiết.

XÁC NHẬN NĂNG LỰC AN NINH VÀ TUÂN THỦ CỦA NHÀ CUNG CẤP Nhà cung cấp của bạn có đáp ứng tuân thủ chưa? Đối với các merchant TMĐT, nhà cung cấp bắt buộc phải đáp ứng tiêu chuẩn DSS

TRUY VẤN. Khi đã biết các thông tin trên, hãy truy vấn nhà cung cấp để hiểu thêm về cách thức họ bảo vệ dữ liệu thẻ.

CÁC LOẠI ĐƠN VỊ CUNG CẤP. Xem phần kế bên

NHÀ CUNG CẤP

Cung cấp thiết bị đầu cuối thanh toán

Cung cấp ứng dụng thanh toán

Tích hợp hệ thống thanh toán

Cung cấp dịch vụ xử lý thanh toán, hosting

Cung cấp dịch vụ đánh giá tuân thủ PCI DSS

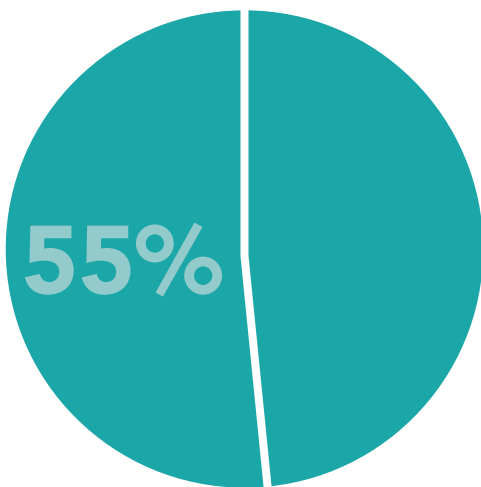
Cung cấp dịch vụ SaaS

Bảo vệ quyền truy cập dữ liệu nội bộ

Lạm dụng quyền truy cập là truy cập trái phép ...

Ai đó truy cập và lạm dụng quyền truy cập của mình vào những môi trường và hệ thống mà người đó không được phép

TRUY CẬP TRÁI PHÉP LÀ HÀNH VI CÓ NGUY CƠ DẪN ĐẾN XÂM PHẠM CAO NHẤT - KHOẢNG 55% CÁC SỰ KIẾN ĐƯỢC CÔNG BỐ.



Verizon 2015

KIỂM SOÁT TRUY CẬP RẤT QUAN TRỌNG. Thiết lập hệ thống với cấu trúc phân quyền truy cập dựa trên nguyên tắc “không phân sự miễn vào”. Là chủ doanh nghiệp, bạn có quyền truy nhập vào mọi môi trường. Nhưng nhân viên chỉ nên có quyền truy cập vào từng vùng dữ liệu, ứng dụng, chức năng.

GIỚI HẠN TRUY CẬP. vào các hệ thống thanh toán và dữ liệu thẻ không được mã hoá với những người có trách nhiệm

LƯU GIỮ LOG. Theo dõi tất cả khách truy cập trong cơ sở dữ liệu logfile, bao gồm tên, lý do truy cập, quyền truy cập. Lưu trữ thông tin trong ít nhất 1 năm

BẢO ĐẢM AN NINH THIẾT BỊ. Hỏi nhà cung cấp cách xoá dữ liệu thẻ trước khi bán hoặc gỡ thiết bị thanh toán (để dữ liệu không thể phục hồi).

CHIA SẺ THÔNG TIN. Chia sẻ thông tin này đến nhân viên, đối tác

Cost



Ease



Risk Mitigation



Xem xét chỉ cho nhân viên quyền truy cập để tiến hành thanh toán nhưng không có quyền hoàn trả, hoặc đặt hàng nhưng không truy cập được vào dữ liệu thẻ của phiên đặt hàng đó. Một số nhân viên không nên có quyền truy cập vào đầu cả.



Đừng để hacker dễ dàng truy cập vào hệ thống

Cost



Ease



Risk Mitigation



HACKERS = TỘI PHẠM

Cách dễ nhất để hacker xâm nhập hệ thống là thông qua người bạn tin cậy. Bạn cần biết được cách thức nhà cung cấp truy cập vào hệ thống của bạn và đảm bảo cách thức đó không tạo kẽ hở cho hacker len vào.

Xác thực đa nhân tố sử dụng username/ password cộng thêm ít nhất một yếu tố khác như smartcard, one-time password.

TÌM HIỂU. Hãy hỏi nhà cung cấp xem họ có sử dụng truy cập từ xa để hỗ trợ hay truy cập vào hệ thống của bạn không.

HỎI CÁCH HẠN CHẾ TRUY CẬP TỪ XA. Có rất nhiều chương trình truy cập từ xa thường xuyên ở chế độ mặc định “bật”. Hãy hạn chế rủi ro bằng cách hỏi nhà cung cấp làm sao để tắt/ bật chế độ khi không cần/ cần

TẮT NGAY KHI HOÀN THÀNH.

SỬ DỤNG BIỆN PHÁP XÁC THỰC MẠNH. Khi phải cho phép truy cập từ xa, hãy yêu cầu biện pháp xác thực đa nhân tố và mã hoá mạnh

ĐẢM BẢO NHÀ CUNG CẤP CHỈ SỬ DỤNG MỘT USERNAME. Mỗi đối tác có một username riêng biệt không dùng chung với bất kỳ ai.

YÊU CẦU TRỢ GIÚP. Yêu cầu nhà cung cấp trợ giúp tắt các chế độ cho phép truy cập và set up cơ chế xác thực hai nhân tố.

Nếu nhà cung cấp hỗ trợ bạn từ văn phòng của họ hoặc không tại chính văn phòng của bạn, có nghĩa là họ đang truy cập từ xa

Nhà cung cấp thường cài VNC & LogMeIn vào thiết bị của bạn để hỗ trợ từ xa.



Dùng phần mềm diệt virus

Cost	
Ease	
Risk Mitigation	

Hệ thống và phần mềm thường rất linh hoạt về chức năng. Hacker có thể tạo virus hoặc mã độc để khai thác các chức năng và lỗi code để giúp chúng xâm nhập hệ thống và đánh cắp dữ liệu thẻ. Sử dụng phần mềm diệt virus, mã độc cập nhật nhất sẽ giải phóng bạn khỏi nguy cơ này.

CÀI PHẦN MỀM DIỆT VIRUS ĐỂ BẢO VỆ HỆ THỐNG THANH TOÁN.

ĐẶT CHẾ ĐỘ TỰ ĐỘNG CẬP NHẬT

LỰA CHỌN PHẦN MỀM DIỆT VIRUS TỐT NHẤT THEO TƯ VẤN CỦA CHUYÊN GIA

ĐỊNH KỲ SCAN



Scan và xử lý lỗ hổng an ninh

Cost



Ease



Risk Mitigation



Lỗ hổng an ninh mới được phát hiện hàng ngày. Do đó, việc hệ thống nằm ngoài Internet của bạn cần được kiểm tra thường xuyên để xác định và xử lý các rủi ro. Các hệ thống nằm ngoài Internet (như hệ thống thanh toán) dễ bị tổn thương nhất vì chúng có thể bị tin tặc khai thác và xâm nhập vào hệ thống

ASV là các đối tác của Hội đồng PCI SSC chuyên cung cấp công cụ rà soát và xử lý lỗ hổng an ninh cho hệ thống nằm ngoài Internet.

LỰA CHỌN ASV VỚI CÔNG NGHỆ VƯỢT TRỘI



Sử dụng giải pháp và thiết bị đầu cuối thanh toán an toàn

Cost



Ease



Risk Mitigation



Sử dụng giải pháp và thiết bị đầu cuối thanh toán an toàn là một cách rất tốt để bảo vệ doanh nghiệp của bạn

SỬ DỤNG THIẾT BỊ NHẬP MÃ PIN VÀ THANH TOÁN AN TOÀN. PCI SSC có danh sách các nhà cung cấp thiết bị thanh toán an toàn có bảo vệ dữ liệu PIN. hãy đảm bảo rằng thiết bị của bạn mua từ các hãng trong danh sách này và có hỗ trợ EMV chip.

SỬ DỤNG PHẦN MỀM AN TOÀN. Phải đảm bảo phần mềm thanh toán của bạn cũng nằm trong danh sách các phần mềm thanh toán được PCI SSC phê chuẩn

SỬ DỤNG NHÂN SỰ CHUYÊN NGHIỆP. Đảm bảo nhân sự đến thực hiện cài đặt phần mềm/ thiết bị cho bạn là nhân viên có trình độ, kinh nghiệm và cấu hình chính xác

Khách hàng cho phép bạn nhập dữ liệu thẻ của họ vào hệ thống thanh toán của bạn. Trách nhiệm của bạn là bảo vệ dữ liệu thẻ của khách hàng

Tham khảo danh sách các đơn vị được PCI SSC phê chuẩn tại trang 19



Bảo vệ doanh nghiệp trước Internet

Cost



Ease



Risk Mitigation



Internet là con đường được tin tặc sử dụng nhằm tấn công và đánh cắp dữ liệu khách hàng của bạn. Vì lý do này, nếu doanh nghiệp của bạn nằm ngoài Internet, bất kỳ điều gì bạn sử dụng để thanh toán thẻ đều cần có biện pháp bảo vệ bổ sung

CÔ LẬP PHẠM VI SỬ DỤNG. Những thiết bị nào được sử dụng để phục vụ quá trình thanh toán thì không sử dụng vào mục đích khác (check mail, duyệt web, lướt mạng xã hội)

BẢO VỆ THIẾT BỊ ẢO. Nếu bạn nhập dữ liệu thẻ của khách hàng qua một thiết bị ảo (webpage được truy cập qua máy tính/ tablet), thì đừng gắn thêm một đầu đọc thẻ vào máy tính.

BẢO VỆ WI-FI. Nếu cửa hàng của bạn cung cấp WiFi miễn phí, cần đảm bảo rằng hệ thống thanh toán của bạn sử dụng một mạng khác (phân mạng), và cần phải cấu hình WiFi đó một cách an toàn.

DÙNG FIREWALL. Nên có firewall để ngăn chặn hacker và các phần mềm mã độc có thể truy cập vào máy tính của bạn.

DÙNG PHẦN MỀM FIREWALL HOẶC THIẾT BỊ TƯƠNG TỰ. Khi hệ thống không có firewall cứng



Đảm bảo dữ liệu của bạn vô dụng với hacker

Cost



Ease



Risk Mitigation



Dữ liệu thẻ dễ bị xâm phạm khi trên đường truyền đến ngân hàng hoặc khi được lưu trữ trong máy tính và thiết bị của bạn. Cách tốt nhất để giữ nó an toàn là làm cho dữ liệu vô dụng kể cả khi hacker đã đánh cắp được nó. Thực hiện điều này cũng khá phức tạp và tốn kém, nhưng trong dài hạn, giải pháp an ninh này sẽ rất hiệu quả và giúp bạn dễ quản lý doanh nghiệp của mình hơn

HỎI NHÀ CUNG CẤP xem liệu thiết bị thanh toán của bạn có sử dụng công nghệ mã hoá thẻ hay mã hoá không?

DÙNG CÁC THIẾT BỊ, GIẢI PHÁP ĐƯỢC PCI SSC PHÊ CHUẨN ĐỂ MÃ HOA DỮ LIỆU THẺ.



DÙNG CÁC GIẢI PHÁP P2PE ĐƯỢC PCI PHÊ CHUẨN

NÂNG CẤP GIẢI PHÁP. Xem xét sử dụng thiết bị thanh toán sử dụng cả hai công nghệ mã hoá và số hoá thẻ để loại bỏ dữ liệu thẻ có thể đọc được.

NẾU BẠN LÀ MERCHANT ĐANG CHUYỂN ĐỔI SANG THIẾT BỊ EMV? Thực sự đây là cơ hội rất tốt để đầu tư vào thiết bị hỗ trợ EMV cung cấp giải pháp an ninh bổ trợ cho mã hoá và số hoá thẻ

PCI approved secure card readers and payment terminals that encrypt card data do it using technology called "Secure Reading and Exchange of Data (SRED)" - ask your vendor if your payment terminal encrypts card data with SRED.

ASK. See [Questions to ask your Vendors](#) for help with questions to ask your vendor or service provider.



NGUỒN TRỢ GIÚP

Tài nguyên

PCI Council Listings

Resource	Link	URL
List of Validated Payment Applications	<i>PCI Council's Validated Payment Applications</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices	<i>PCI Council's Approved PTS Devices</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors	<i>PCI Council's Approved Scanning Vendors</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers	<i>PCI Council's Qualified Integrators Resellers</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions	<i>PCI Council's P2PE Validated Solutions</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Payment Brand Lists

Resource	Link	URL
Lists of Compliant Service Providers	<i>MasterCard's List of Compliant Service Providers</i>	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	<i>Visa's Global Registry of Service Providers</i>	http://www.visa.com/splisting/
	<i>Visa Europe's Registered Member Agents</i>	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS and Related Guidance

Resource	Link	URL
More about PCI DSS	<i>How to Secure with PCI DSS</i>	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires	<i>Self-Assessment Questionnaires</i>	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants	<i>Skimming Prevention: Overview of Best Practices for Merchants</i>	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Tài nguyên

Infographics and Videos

Resource	Link	URL
Infographic: It's Time to Change Your Password	<i>It's Time to Change Your Password</i>	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves	<i>Fight Cybercrime by Making Stolen Data Worthless to Thieves</i>	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Video: Learn Password Security in 2 Minutes	<i>Learn Password Security in 2 Minutes</i>	https://www.youtube.com/watch?v=FsrOXgZKa7U

PCI Payment Protection Resources for Small Merchants

Resource	Link	URL
Common Payment Systems	<i>Common Payment Systems</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Small Merchant Questions for Vendors	<i>Small Merchant Questions for Vendors</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Small Merchant Glossary	<i>Small Merchant Glossary</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Sources

Gallup – *Gallup Poll*, October 2015

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014

NCSA – *National Cyber Security Alliance survey*, 2012

NSBA – National Small Business Administration, *2014 Year End Economic Report*

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report*

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report*

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report*