

RISORSE PER LA PROTEZIONE DEI PAGAMENTI PER PICCOLI ESERCENTI

# Guida ai pagamenti sicuri

Versione 1.0 | Luglio 2016



INFORMAZIONI SUI VOSTRI RISCHI .....	4
PROTEGGETE I DATI DELLE CARTE E LA VOSTRA AZIENDA CON I PRINCIPI DI BASE DELLA SICUREZZA .....	6
DOVE POTETE TROVARE ASSISTENZA .....	20



# **INFORMAZIONI SUI VOSTRI RISCHI**

# Informazioni sui vostri rischi

**Come piccola azienda, siete gli obiettivi principali dei ladri di dati.**

Quando vengono violati i vostri dati delle carte di pagamento, le conseguenze possono verificarsi rapidamente. I vostri clienti perdono fiducia nella vostra capacità di proteggere le loro informazioni personali. Si rivolgono altrove per svolgere i loro affari. Vi sono potenziali pene finanziarie e danni da cause giudiziarie e la vostra azienda potrebbe perdere la possibilità di accettare carte di pagamento. Un sondaggio effettuato su 1.015 piccole e medie aziende ha rilevato che il 60% è stato violato nel giro di sei mesi. (NCSA)

**Il 60%**

DI PICCOLE AZIENDE  
SONO STATE VITTIME DI  
VIOLAZIONI CIBERNETICHE.  
(Governo HM)



**Il 71%**

DI HACKER ATTACCA  
AZIENDE CON MENO DI 100  
IMPIEGATI  
(Verizon 2012)

**\$20.752**



COSTO MEDIO PER  
UNA PICCOLA AZIENDA  
DOVUTO AD ATTACCHI,  
PARTE DA \$8.600 NEL  
2013  
(NSBA)

**Il 69%**



DEI CONSUMATORI  
AMERICANI TEME IL FURTO  
DEI DATI DELLE LORO CARTE  
DI PAGAMENTO  
(Gallup)



# Cos'è un rischio?

**I DATI DELLE CARTE DI PAGAMENTO DEI VOSTRI CLIENTI SONO UNA MINIERA D'ORO PER I CRIMINALI. NON PERMETTETE CHE QUESTO ACCADA ANCHE A VOI!**

**Seguite le operazioni contenute in questa guida per proteggervi da furti di dati.**

**Esempi di dati di carte di pagamento sono il PAN (numero di conto primario) e un codice di sicurezza a tre o quattro cifre della carta. La seguente freccia rossa indica i tipi di dati che richiedono protezione.**

## TIPI DI DATI SU UNA CARTA DI PAGAMENTO



## COS'È PCI DSS?

Il PCI DSS (Payment Card Industry Data Security Standard) è una serie di requisiti di sicurezza che aiutano i piccoli esercenti a proteggere i dati delle carte bancarie dei clienti che si trovano nelle carte di pagamento.

I piccoli esercenti possono avere familiarità con la convalida della loro conformità a PCI DSS mediante un SAQ (Self-Assessment Questionnaire).

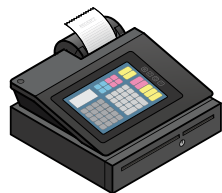
Per ulteriori informazioni sul PCI DSS, consultare le Risorse alla fine di questa guida.

# Informazioni sul vostro sistema di pagamento: Termini comuni di pagamento

In base a quale parte del mondo vi trovate, l'apparecchiatura utilizzata per ricevere i pagamenti viene denominata in modi diversi. Questi sono i tipi a cui facciamo riferimento in questa documentazione e i modi con cui vengono comunemente chiamati.



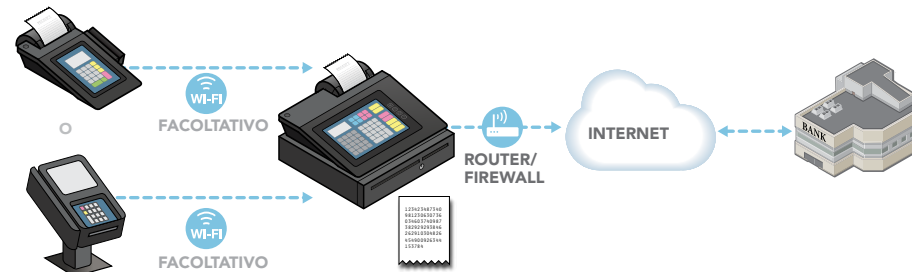
Un **TERMINALE DI PAGAMENTO** è il dispositivo utilizzato per ricevere i pagamenti con carta del cliente mediante strisciata, dip, a inserimento, appoggio o inserimento manuale del numero della carta. Anche terminale POS (Point-of-sale), dispositivo automatico a carte bancarie, terminale PDQ o terminale EMV/abilitato con chip sono nomi utilizzati per descrivere tali dispositivi.



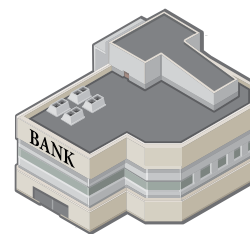
Un **REGISTRATORE DI CASSA ELETTRONICO** (o cassa) registra e calcola le transazioni e può stampare le ricevute, ma non accetta pagamenti mediante carta di credito.



Un **TERMINALE DI PAGAMENTO INTEGRATO** è contemporaneamente un terminale di pagamento e un registratore di cassa, vale a dire che è in grado di ricevere pagamenti, registrare e calcolare transazioni e stampare ricevute.



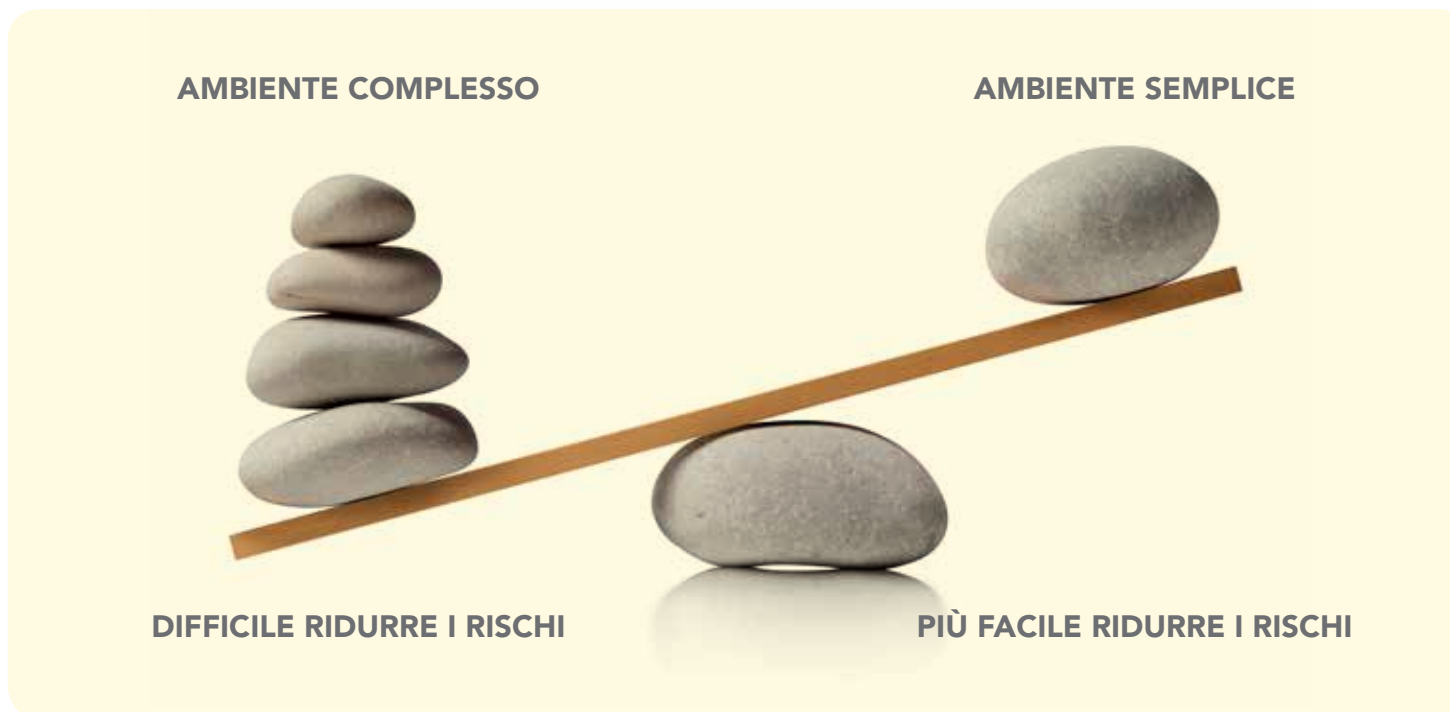
Un **SISTEMA DI PAGAMENTO** include l'intero processo di accettazione di pagamenti mediante carte bancarie in un punto vendita (inclusi negozi e vetrine e-commerce) e potrebbe includere un terminale di pagamento, un registratore di cassa elettronico, altri dispositivi o sistemi collegati a un terminale di pagamento (ad esempio, Wi-Fi per la connettività o un PC utilizzato per l'inventario), server con componenti e-commerce quali pagine di pagamento e le connessioni alla banca d'affari.



Una **BANCA D'AFFARI** è una banca o istituto finanziario che elabora pagamenti con carte di credito o di debito per conto degli esercenti. Anche acquirente, banca acquirente e elaboratore pagamenti o carte sono termini utilizzati per questa entità.

# Quali sono i rischi per la vostra azienda?

**Quante più funzioni il vostro sistema di pagamento dispone, tanto più complesso sarà proteggerlo. Queste funzioni aggiuntive spesso facilitano i criminali nell'appropriazione dei dati delle carte di pagamento dei clienti. Riflettete attentamente sulla reale necessità di tali funzioni aggiuntive (ad esempio, Wi-Fi o telecamere) per la vostra azienda.**

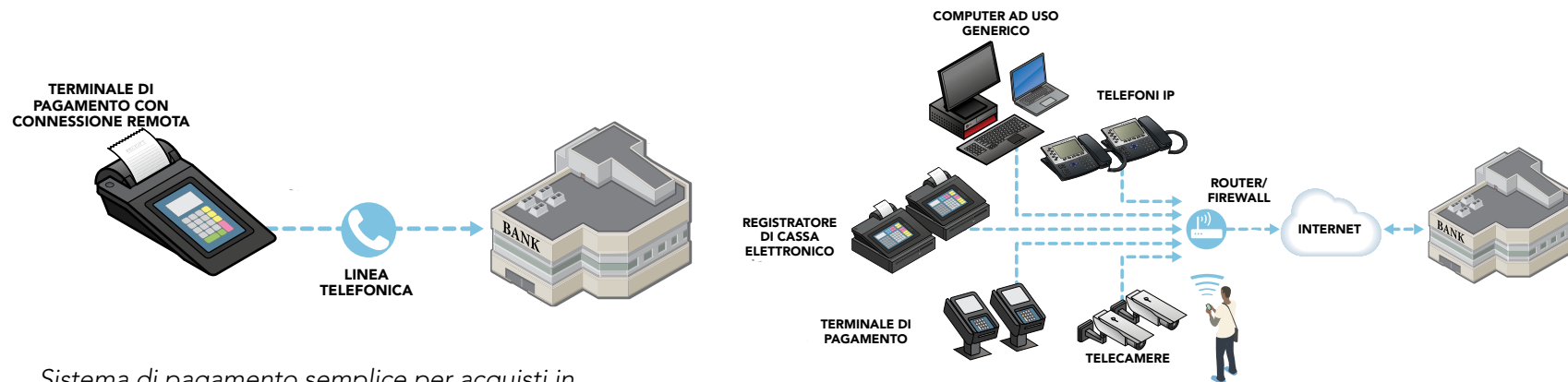


*Come vendete merci o servizi? Vi sono tre modi principali:*

- 1. Una persona entra nel vostro negozio ed effettua un acquisto utilizzando la propria carta di pagamento.*
- 2. Una persona visita il vostro sito Web e paga online.*
- 3. Una persona chiama il vostro negozio e fornisce i dettagli della carta di pagamento al telefono, tramite email o fax.*

# Informazioni sui vostri rischi: Tipi di sistemi di pagamento

I rischi per la vostra sicurezza variano enormemente a seconda della complessità del vostro sistema di pagamento, di persona o online.




*Sistema di pagamento semplice per acquisti in negozio*

*Sistema di pagamento complesso per acquisti in negozio, con Wi-Fi, telecamere, telefoni IP e altri sistemi collegati*



*Sistema di pagamento e-commerce complesso per acquisti online, con l'esercente che gestisce il proprio sito Web e la propria pagina di pagamento*





















































































Utilizzate i Sistemi comuni di pagamento che faciliteranno l'identificazione del tipo di sistema di pagamento da utilizzare, i vostri rischi e i consigli di sicurezza suggeriti come punto di partenza delle conversazioni con la vostra banca d'affari e i vostri fornitori.



**PROTEGGETE I DATI  
DELLE CARTE E LA  
VOSTRA AZIENDA CON  
I PRINCIPI DI BASE  
DELLA SICUREZZA**

# Come potete proteggere la vostra azienda?

La buona notizia è che potete iniziare a proteggerla oggi stesso con questi principi di base della sicurezza:

Come salvaguardare la vostra azienda da violazioni	Costo	Facilità	Riduzione dei rischi
 Utilizzate password difficili e modificate quelle predefinite			  
 Proteggete i vostri dati delle carte di pagamento e memorizzate solo ciò di cui avete bisogno			 
 Verificate che non vi siano alterazioni ai terminali di pagamento			 
 Installate le patch dei vostri fornitori		 	  
 Utilizzate partner aziendali fidati e informatevi su come contattarli			
 Proteggete l'accesso in-house ai vostri dati delle carte di pagamento		 	 
 Non fornite agli hacker un facile accesso ai vostri sistemi	 	 	  
 Utilizzate un software antivirus	 	 	 
 Eseguite la scansione per le vulnerabilità e risolvete i problemi	 	 	  
 Utilizzate terminali e soluzioni di pagamento sicuri	  	 	  
 Proteggete la vostra azienda da Internet	 	  	  
 Per la migliore protezione, rendete i vostri dati inutili ai criminali	  	  	  

Questi principi di base della sicurezza sono organizzati a partire dal più semplice e più economico da implementare, fino a quelli più complessi e più costosi da implementare. La quantità di riduzione dei rischi che ognuno apporta ai piccoli esercenti viene indicata anche nella colonna "Riduzione dei rischi".



# Utilizzate password difficili e modificate quelle predefinite

Costo



Facilità



Riduzione dei rischi



Le vostre password sono fondamentali per la sicurezza dei computer e dei dati delle carte di pagamento. Proprio come un lucchetto sulla vostra porta protegge la proprietà fisica, una password facilita la protezione dei vostri dati aziendali. Inoltre, è bene che sappiate che computer e software standard (incluso il vostro terminale di pagamento) spesso vengono forniti con password predefinite, quali "password" o "admin", che sono solitamente note agli hacker e sono di frequente una fonte di violazioni dei piccoli esercenti.

Circa

l'80%

delle violazioni dei dati includono password indovinate o rubate

Verizon PCI 2015

## MODIFICATE REGOLARMENTE LE VOSTRE

**PASSWORD.** Trattate le vostre password come se fossero spazzolini da denti. Non consentite a nessun altro di utilizzarle e cambiatele ogni tre mesi.

**FATEVI AIUTARE.** Chiedete ai vostri fornitori o provider di servizi informazioni sulle password predefinite e su come modificarle. Poi modificatele!

## RENDETELE DIFFICILI DA INDOVINARE.

Le password più comuni sono "password" e "123456". Gli hacker provano le password facili da indovinare poiché vengono utilizzate dalla metà delle persone. Una password difficile presenta sette o più caratteri e una combinazione di lettere maiuscole e minuscole, numeri e simboli (quali !@#\$%&\*). Anche una frase può essere una password difficile (e potrebbe essere più facile da ricordare), come "B1gMac&frieS".

**NON RENDETELE NOTE A NESSUNO.** Insistete perché ogni impiegato abbia i propri ID e password di login. Mai condividere!

Password predefinite tipiche che DEVONO ESSERE modificate:

[nessuna]

[nome del prodotto/  
fornitore]

1234 o 4321

accesso

admin

anonimo

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

Per ulteriori informazioni relative alla sicurezza delle password, consultate queste risorse sul sito Web dell'Ente PCI:

### INFOGRAFICA

È ora di modificare la vostra password



### VIDEO

Due minuti di informazioni sulla sicurezza della password







# Proteggete i dati delle carte di pagamento e memorizzate solo ciò di cui avete bisogno

Costo



Facilità



Riduzione dei rischi



**È impossibile proteggere i dati delle carte di pagamento se non sapete dove si trovano.**

**Cosa potete fare?**

*La tokenizzazione ha un obiettivo simile alla cifratura, ma funziona in maniera diversa. Sostituisce i dati delle carte di pagamento con dati insignificanti (un "token") che non hanno alcun valore per un hacker.*


**CHIEDETE A UN ESPERTO.** Chiedete al fornitore del vostro terminale di pagamento o alla banca d'affari dove i vostri sistemi memorizzano i dati e se potete semplificare l'elaborazione dei pagamenti. Chiedete anche come eseguire specifiche transazioni (ad esempio, per pagamenti ricorrenti) senza salvare il codice di sicurezza della carta.

**AVVALETEVI DI TERZE PARTI.** Il modo migliore per proteggervi da violazioni di dati è quello di non memorizzare affatto i dati delle carte di pagamento. Prendete in considerazione l'affido dell'elaborazione delle carte di pagamento a un provider di servizi conforme al PCI DSS. Consultate le Risorse alla pagina 22 per gli elenchi di provider di servizi conformi.

## **SE NON AVETE BISOGNO DEI DATI DELLE CARTE DI PAGAMENTO, NON CONSERVATELI!**

Distruggete/sminuzzate i dati delle carte di pagamento di cui non avete bisogno. Se dovete conservare materiale cartaceo con dati sensibili delle carte di pagamento, ricoprite i dati con un pennarello nero e spesso, fino a quando non sono più leggibili, e conservate il materiale cartaceo in un cassetto chiuso a chiave o in una cassaforte a cui solo poche persone possono accedere.

**LIMITATE I RISCHI.** Piuttosto che accettare dettagli di pagamento tramite email, chiedete ai clienti di fornirli tramite telefono, fax o posta.

**UTILIZZATE TOKEN O LA CIFRATURA.** Chiedete alla vostra banca d'affari se DAVVERO avete bisogno di memorizzare tali dati delle carte di pagamento. Se sì, chiedete alla vostra banca d'affari o al provider di servizi informazioni sulle tecnologie di cifratura o di tokenizzazione che rendono i dati delle carte di pagamento inutili anche se rubati. (Consultate "  alla pagina 19 per ulteriori informazioni).

## **MANUALE INTRODUTTIVO SULLA CIFRATURA**

*La cifratura utilizza una formula matematica per rendere illeggibile un testo non formattato alle persone senza conoscenza speciale (denominata chiave). La cifratura viene applicata ai dati memorizzati e ai dati trasmessi su una rete.*

**LA CIFRATURA**  
*modifica il testo non formattato in testo cifrato.*

**LA DECODIFICA**  
*modifica il testo cifrato in testo non formattato.*

*Ad esempio:*

Questo è materiale segreto, non

**CHIAVE DI CIFRATURA**

5a0 (k\$hQ%...

**CHIAVE DI DECODIFICA**

Questo è materiale segreto, non





# Verificate che non vi siano alterazioni ai terminali di pagamento

Costo



Facilità



Riduzione dei rischi



**“Dispositivi di skimming” raccolgono i dati delle carte di pagamento dei vostri clienti quando vengono inseriti in un terminale di pagamento. È fondamentale che voi e il vostro personale sappiate come individuare un dispositivo di skimming. Dovete controllare regolarmente i vostri terminali di pagamento per assicurarvi che non siano stati alterati. Conservate un registro dei terminali controllati, di quando sono stati controllati, chi li ha controllati e se è stato rilevato qualcosa.**

*Consultate la PCI Council's guide: Skimming Prevention: Overview of Best Practices for Merchants (Guida dell'Ente PCI: Prevenzione dello skimming: Panoramica delle migliori pratiche per gli esercenti)*

## Siate attenti e seguite questi passi:

**CONSERVATE UN ELENCO** di tutti i terminali di pagamento e fate foto (davanti, dietro, cavi e collegamenti) così che sappiate il modo in cui devono apparire.

**CERCATE SEGNI EVIDENTI** di alterazione, quali sigilli danneggiati sulle placche o viti degli sportelli, un cablaggio strano/ diverso o nuovi dispositivi o funzioni che non riconoscete. La guida dell'Ente (a cui viene fatto riferimento di seguito) può esservi di aiuto.

**PROTEGGETE I TERMINALI.** Teneteli lontani dalla portata dei clienti quando non in uso e nascondetene gli schermi dalla vista del pubblico. Assicuratevi che i terminali di pagamento siano al sicuro prima di chiudere il vostro negozio alla fine della giornata, inclusi tutti i dispositivi che leggono le carte di pagamento dei vostri clienti o accettano i loro PIN (personal identification number).

**CONTROLLATE LE RIPARAZIONI.** Consentite le riparazioni ai terminali di pagamento solo a un personale autorizzato e solo se previste. Informate anche il vostro personale.

**CHIAMATE** il fornitore del terminale di pagamento o la banca d'affari immediatamente se avete il minimo sospetto!



# Installate le patch dei vostri fornitori

Costo



Facilità



Riduzione dei rischi



**Spesso, il software presenta dei difetti o errori fatti dai programmatori al momento della scrittura del codice, noti anche come falle della sicurezza, bug o vulnerabilità. Gli hacker traggono vantaggio da tali errori per intrufolarsi nel vostro computer e appropriarsi dei dati di account. Proteggete i vostri sistemi mediante l'applicazione delle "patch" del fornitore che risolvono gli errori di codifica. L'installazione tempestiva della sicurezza è fondamentale!**

**CHIEDETE** al vostro fornitore o al provider di servizi il modo in cui vi informa delle nuove patch di sicurezza e assicuratevi di ricevere e leggere tali notifiche.

**QUALI FORNITORI VI INVIANO PATCH?** Potete ricevere patch dai fornitori dei terminali di pagamento, applicazioni di pagamento, altri sistemi di pagamento (casche, registratori di cassa, PC, ecc.), sistemi operativi (Android, Windows, iOS, ecc.), software di applicazioni (incluso il vostro browser) e software aziendale.

**ASSICURATEVI** che i vostri fornitori aggiornino i vostri terminali di pagamento, sistemi operativi, ecc. così che possano supportare le ultime patch di sicurezza. Chiedeteglielo.

**ESERCENTI E-COMMERCE.** L'installazione delle patch quanto prima possibile è molto importante anche per voi. Inoltre, fate attenzione alla patch del vostro provider di servizi di pagamento. Chiedete al vostro provider di hosting e-commerce se installano patch sul vostro sistema (e con quale frequenza). Assicuratevi che aggiornino il sistema operativo, la piattaforma e-commerce e/o l'applicazione Web in modo che supportino le ultime patch.

**SEGUITE** le istruzioni del vostro fornitore/provider di servizi e installate tali patch quanto prima possibile.



# Utilizzate partner aziendali fidati e informatevi su come contattarli

Costo



Facilità



Riduzione dei rischi



**Utilizzate provider esterni per servizi, dispositivi e applicazioni relativi al pagamento. Potete avere anche provider di servizi con cui condividete i dati delle carte di pagamento, che supportano o gestiscono i vostri sistemi di pagamento o a cui consentite l'accesso agli stessi dati. Li potete chiamare elaboratori, fornitori, terze parti o provider di servizi. Tutti loro hanno un impatto sulla vostra capacità di proteggere i dati delle carte di pagamento. Quindi è fondamentale che sappiate chi sono e le domande relative alla sicurezza che dovete porre loro.**

**SAPPIATE CHI CHIAMARE.** Qual'è la vostra banca d'affari? Chi vi aiuta nell'elaborazione dei pagamenti? Da chi avete acquistato il vostro dispositivo/software di pagamento e chi lo ha installato per voi? Chi sono i vostri provider di servizi?

**FATE UN ELENCO.** Ora che sapete chi chiamare, conservate i nomi delle società e dei contatti, i numeri di telefono, gli indirizzi dei siti Web e altri dettagli di contatto lì dove potete trovarli facilmente in caso di emergenza.

**CONFERMATE LA SICUREZZA DEI VOSTRI PROVIDER DI SERVIZI.** Il vostro provider di servizi è conforme ai requisiti di PCI DSS? Per gli esercenti e-commerce, è importante che anche il vostro provider di servizi di pagamento sia conforme a PCI DSS! Consultate le Risorse alla pagina 22 per gli elenchi di provider di servizi conformi.

**PONETE DOMANDE.** Una volta che sapete chi sono i vostri provider esterni e i servizi che vi forniscono, conversate con loro per informarvi sulle modalità con cui proteggono i dati delle carte di pagamento. Utilizzate [Domande da chiedere ai vostri fornitori](#) per le informazioni sulle domande da porre.

**INFORMAZIONI SUI FORNITORI COMUNI.** Prendete visione della barra laterale a destra per le informazioni sui tipi comuni di fornitori o provider di servizi con cui potreste collaborare.

## FORNITORI COMUNI

*Fate riferimento alla tabella in [Domande da chiedere ai vostri fornitori](#) per ulteriori dettagli su questi fornitori comuni:*

*Fornitori di terminali di pagamento*

*Fornitori di applicazioni di pagamento*

*Installatori di sistemi di pagamento (chiamati Integratori/Rivenditori)*

*Provider di servizi che eseguono l'elaborazione dei pagamenti o l'hosting o l'elaborazione dell'e-commerce*

*Provider di servizi che vi assistono nella conformazione ai requisiti del PCI DSS (ad esempio, fornendo servizi di firewall o antivirus)*

*Provider di software come servizio*



# Proteggete l'accesso in-house ai vostri dati

Costo



Facilità



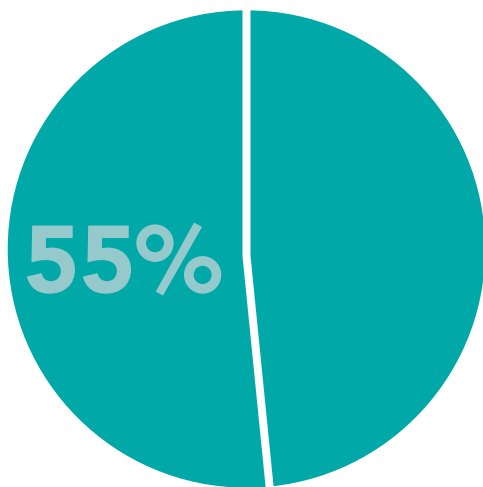
Riduzione dei rischi



**Abuso di privilegio indica una persona che usa...**

**L'accesso e i privilegi di terzi per poter accedere ai sistemi o ai dati pur non essendone autorizzati.**

**L'ABUSO DI PRIVILEGIO È L'AZIONE PRINCIPALE CHE CONDUCE A VIOLAZIONI: CIRCA IL 55% DI TUTTI GLI EPISODI DENUNCIATI.**



Verizon 2015

## **IL CONTROLLO DELL'ACCESSO È MOLTO IMPORTANTE.**

Configurate il vostro sistema in modo che consenta l'accesso solo in base al principio "bisogno di conoscere". Come proprietari, avete l'accesso a tutto. Ma la maggior parte degli impiegati possono svolgere il loro lavoro solo con l'accesso a una sotto serie di dati, applicazioni e funzioni.

**LIMITATE L'ACCESSO** ai sistemi di pagamento e ai dati non cifrati delle carte di pagamento solo a quegli impiegati che ne hanno bisogno e solo ai dati, alle applicazioni e alle funzioni di cui hanno bisogno per svolgere il loro lavoro.

**CONSERVATE UN LOG.** Tenete traccia di tutti i visitatori "dietro il banco" nella vostra azienda. Includete nome, motivo della visita e nome dell'impiegato che ha autorizzato l'accesso del visitatore. Conservate il log per almeno un anno.

**GETTATE IN MANIERA SICURA I DISPOSITIVI.** Chiedete al vostro fornitore del sistema di pagamento o provider di servizi come rimuovere in sicurezza i dati delle carte di pagamento prima di vendere o gettare i dispositivi di pagamento (così che i dati non vengano recuperati).

**CONDIVIDETE QUESTE INFORMAZIONI.** Fornite questa guida ai vostri impiegati e partner aziendali, così che sappiano cosa aspettarsi.

*Prendete in considerazione di concedere ai vostri impiegati l'accesso alla ricezione dei pagamenti ma non all'elaborazione dei rimborsi o alla ricezione di nuovi ordini/prenotazioni ma non ai dati delle carte di pagamento relativi a ordini/prenotazioni esistenti. Alcuni impiegati non devono avere alcun accesso.*



# Non fornite agli hacker un facile accesso ai vostri sistemi

Costo



Facilità



Riduzione dei rischi



## HACKER = CRIMINALI

Uno dei modi più semplici per gli hacker di entrare nel vostro sistema è tramite persone di vostra fiducia. Dovete essere a conoscenza del modo in cui i fornitori accedono al vostro sistema per assicurarvi che non apra falle che gli hacker possono sfruttare.

*L'autenticazione a più fattori utilizza un nome utente e una password, più almeno un altro fattore (come una smart card, un dongle\* o un codice usa e getta).*

\*un utile dispositivo che si collega a un computer per consentire l'accesso al wireless, a funzioni software, ecc.

**INFORMATEVI.** Chiedete al vostro fornitore del sistema di pagamento o provider di servizi se utilizzano l'accesso remoto per supportare o accedere al vostro business.

**CHIEDETE COME LIMITARE L'USO DELL'ACCESSO REMOTO.** Molti programmi di accesso remoto sono sempre attivi per impostazione predefinita. Riducete i vostri rischi: chiedete al vostro fornitore come disabilitare l'accesso remoto quando non è necessario e come abilitarlo quando il vostro fornitore o provider di servizi lo richiede appositamente.

### DISABILITATELO UNA VOLTA FINITO.

**UTILIZZATE UN'AUTENTICAZIONE SOLIDA.** Se dovete consentire l'accesso remoto, richiedete un'autenticazione a più fattori e una crittografia avanzata.

**ASSICURATEVI CHE I PROVIDER DI SERVIZI UTILIZZINO CREDENZIALI ESCLUSIVE.** Ognuno deve utilizzare credenziali di accesso remoto che siano esclusive per la vostra azienda e che non siano le stesse utilizzate per altri clienti.

**CHIEDETE ASSISTENZA.** Chiedete al vostro fornitore o provider di servizi di aiutarvi nella disabilitazione dell'accesso remoto o (se il fornitore o il provider di servizi ha bisogno dell'accesso remoto) di aiutarvi nella configurazione dell'autenticazione a più fattori. Consultate [Domande da chiedere ai vostri fornitori](#) per le informazioni sulle domande da porre.

*Se il vostro fornitore supporta o risolve i problemi del vostro terminale di pagamento dal proprio ufficio (e non dalla vostra sede), vuol dire che utilizza Internet e un software di accesso remoto.*

*Esempi di prodotti che il vostro fornitore potrebbe installare sul vostro terminale e utilizzarli per assistervi in remoto, includono VNC e LogMeIn.*



# Utilizzate un software antivirus

Costo



Facilità



Riduzione dei rischi



I sistemi e il software sono estremamente flessibili e offrono un'ampia gamma di funzioni e caratteristiche. Gli hacker scrivono virus e altri codici dannosi per trarre vantaggio di tali funzioni ed errori di codice, così da poter violare i vostri sistemi e appropriarsi dei dati delle carte di pagamento. L'utilizzo di un software antivirus aggiornato (chiamato anche anti-malware) vi assiste nella protezione dei vostri sistemi.

## **INSTALLATE DEL SOFTWARE ANTIVIRUS PER PROTEGGERE IL VOSTRO SISTEMA DI PAGAMENTO.**

È facile da installare e potrete acquistarlo presso il vostro negozio di articoli d'ufficio o un rivenditore IT della zona.

**IMPOSTATE IL SOFTWARE SU "AGGIORNA AUTOMATICAMENTE"** così che riceviate sempre la protezione disponibile più recente.

**FATEVI CONSIGLIARE.** Chiedete al vostro rivenditore IT informazioni su prodotti consigliati per l'antivirus o per la protezione anti-malware.

**ESEGUITE SCANSIONI PERIODICHE.** Eseguite regolarmente scansioni dell'intero sistema, dato che i vostri sistemi potrebbero essere stati infettati da nuovo malware rilasciato prima che il vostro software antivirus sia stato in grado di rilevarlo.



# Eseguite la scansione per le vulnerabilità e risolvete i problemi

Costo



Facilità



Riduzione dei rischi



Ogni giorno vengono scoperte nuove vulnerabilità, falle della sicurezza e nuovi bug. È fondamentale far verificare regolarmente i vostri sistemi con interfaccia Internet al fine di identificare nuovi rischi e risolverli quanto prima possibile. I vostri sistemi con interfaccia Internet (come numerosi sistemi di pagamento) sono i più vulnerabili, poiché i criminali possono facilmente trarne vantaggio allo scopo di introdursi nei vostri sistemi.

*I fornitori ASV approvati dall'Ente PCI eseguono una scansione delle vulnerabilità esterne e creano un rapporto. Consultate [List of PCI-Approved Scanning Vendors \(Elenco del PCI dei Fornitori di scansione approvati dal PCI.\)](#)*

**FATEVI CONSIGLIARE.** Chiedete alla vostra banca d'affari se è partner con un qualsiasi fornitore di scansione approvato (ASV) dal PCI. Chiedete anche ai vostri fornitori e provider di servizi.

**CONTATTATE UN FORNITORE ASV PCI.** Tali fornitori possono assistervi con strumenti che cercano vulnerabilità nella vostra rete e forniscono un rapporto se, ad esempio, occorre applicare una patch. L'elenco dell'Ente PCI (a cui si fa riferimento di seguito) può aiutarvi a trovare un fornitore per la scansione.

**SCEGLIETE UN FORNITORE DI SCANSIONE.** Contattate diversi fornitori ASV PCI per trovarne uno con un programma idoneo per la vostra piccola azienda.

**RISOLVETE LE VULNERABILITÀ.** Chiedete al vostro fornitore ASV di aiutarvi nella risoluzione dei problemi trovati dalla scansione.





# Utilizzate terminali e soluzioni di pagamento sicuri

Costo




Facilità



Riduzione dei rischi



Una modalità sicura che vi aiuterà a proteggere meglio la vostra azienda è quella di utilizzare soluzioni di pagamento sicure e professionisti qualificati che vi assistano. Ecco come scegliere prodotti sicuri e accertarvi che siano configurati per la sicurezza.

Per i terminali di pagamento PCI e i lettori sicuri di carte di pagamento che cifrano i dati delle carte, consultate  alla pagina 19.

**UTILIZZATE TERMINALI DI PAGAMENTO SICURI E PIN ENTRY DEVICE.** Il PCI Council approva terminali di pagamento che proteggono i dati dei PIN. Assicuratevi che il vostro terminale o dispositivo di pagamento si trovi [List of PCI Approved PTS Devices \(Elenco dei Dispositivi PTS approvati dal PCI\)](#) per l'apparecchiatura che fornisce la sicurezza migliore e supporta il "chip EMV".

**UTILIZZATE UN SOFTWARE SICURO.** Assicuratevi che il vostro software di pagamento si trovi nell'[Elenco delle List of PCI Validated Payment Applications \(Applicazioni convalidate dal PCI\)](#).

**UTILIZZATE PROFESSIONISTI QUALIFICATI.** Assicuratevi che la persona che installa la vostra applicazione convalidata da PA-DSS lo faccia correttamente e in sicurezza. Scegliete [List of PCI QIRs \(Elenco dei QIR del PCI\)](#) le società approvate dall'Ente PCI perché vi assistano. Chiedete alla vostra banca d'affari perché vi aiuti nella scelta.

**FATE RIFERIMENTO A QUESTO ELENCO DI DOMANDE PER I FORNITORI.** Utilizzate [Domande da chiedere ai vostri fornitori](#) per le informazioni sulle domande da porre ai vostri fornitori e provider di servizi.

*I vostri clienti inseriscono il loro PIN (personal identification number) delle loro carte di pagamento nel vostro terminale di pagamento o nel PIN entry device. È importante che utilizzate dispositivi sicuri per la protezione dei dati del PIN dei vostri clienti.*





# Proteggete la vostra azienda da Internet

Costo



Facilità



Riduzione dei rischi



**Internet è il mezzo principale utilizzato dai ladri di dati per attaccare e appropriarsi dei dati delle carte di pagamento dei clienti. Per questo motivo, se la vostra azienda si trova su Internet, qualsiasi sistema utilizzate per i pagamenti con carta, ha bisogno di maggiore protezione.**

**UTILIZZO ISOLATO.** Non utilizzate per altri motivi il dispositivo con cui ricevete i pagamenti. Ad esempio, non navigate sul Web, controllate email o andate sui social media dallo stesso dispositivo o computer che utilizzate per le transazioni dei pagamenti. Quando è necessario per motivi aziendali (ad esempio aggiornare la pagina della vostra azienda sul social media), utilizzate un altro computer e non il dispositivo di pagamento per effettuare tali aggiornamenti.

**PROTEGGETE IL VOSTRO "TERMINALE VIRTUALE".** Se inserite i pagamenti dei clienti mediante un terminale virtuale (una pagina Web a cui accedete mediante un computer o un tablet), riducete i rischi: non collegatevi un lettore carte di pagamento esterno.

**PROTEGGETE IL WI-FI.** Se il vostro negozio offre il Wi-Fi gratuito ai clienti, assicuratevi di utilizzare un'altra rete per il vostro sistema di pagamento (operazione chiamata "segmentazione di rete"). Chiedete al vostro tecnico di installazione della rete di assistervi nella configurazione sicura del Wi-Fi.

**UTILIZZATE UN FIREWALL.** Un firewall correttamente configurato funziona come buffer che impedisce agli hacker e ai software dannosi di accedere ai vostri computer e informazioni. Verificate con il vostro fornitore del terminale di pagamento o il provider di servizi che ne disponete di uno e chiedetegli di assistervi nella sua corretta configurazione.

**UTILIZZATE UN FIREWALL PERSONALE O UN EQUIVALENTE** quando i sistemi di pagamento non sono protetti dal vostro firewall aziendale (ad esempio, quando collegati a una connessione Wi-Fi pubblica).



# Per la migliore protezione, rendete i vostri dati inutili ai criminali

Costo



Facilità




Riduzione dei rischi



I vostri dati sono vulnerabili quando vengono trasferiti alla vostra banca d'affari e quando vengono conservati o memorizzati sui vostri computer e dispositivi. Il modo migliore di tenerli al sicuro è di renderli inutili anche se rubati, nascondendoli ed eliminandoli completamente se non necessari. Sebbene questa operazione potrebbe essere più complessa da eseguire, alla lunga, può rendere la sicurezza più facile da gestire.

**CHIEDETE AL FORNITORE DI SISTEMI DI PAGAMENTO O AL PROVIDER DI SERVIZI** se il vostro terminale di pagamento utilizza una tecnologia di cifratura e/o di tokenizzazione.

**UTILIZZATE DISPOSITIVI PCI CHE CODIFICANO I DATI DELLE CARTE DI PAGAMENTO.** L'Ente PCI approva i terminali di pagamento che proteggono i dati dei PIN (consultate  alla pagina 17) e i terminali di pagamento e i "lettori sicuri di carte" che cifrano ulteriormente i dati delle carte di pagamento. Consultate [List of PCI Approved PTS Devices](#). (*Elenco di dispositivi PTS approvati dal PCI*).

**UTILIZZATE SOLUZIONI DI CIFRATURA PCI.** Informatevi se la cifratura del vostro terminale di pagamento è stata eseguita mediante una soluzione di cifratura P2PE (Point-to-Point Encryption) e se si trova [List of PCI P2PE Validated Solutions](#) (*Elenco di soluzioni convalidate P2PE dal PCI*) dell'Ente PCI.

**AGGIORNATE LA VOSTRA SOLUZIONE.** Riducete i vostri rischi: prendete in considerazione l'acquisizione di un nuovo terminale di pagamento che utilizza entrambe le tecnologie di cifratura e tokenizzazione perché i dati della carte di pagamento non siano più utili agli hacker.

**SIETE DEGLI ESERCENTI IN FASE DI TRANSIZIONE VERSO TERMINALI CON CHIP EMV?** Questa è una grande opportunità di fare un investimento in un terminale che supporti EMV e che fornisca anche la sicurezza aggiuntiva della cifratura e della tokenizzazione.

**CHIEDETE.** Consultate [Domande da chiedere ai vostri fornitori](#) per le domande da porre al vostro fornitore o provider di servizi.

*Il PCI ha approvato lettori di carte di pagamento e terminali di pagamento sicuri che cifrano i dati delle carte mediante la tecnologia chiamata SRED ("Secure Reading and Exchange of Data"). Chiedete al vostro fornitore se il vostro terminale di pagamento cifra i dati delle carte di pagamento con SRED.*

Three stylized human figures in business suits are standing on a circular platform. The figures are rendered in a light teal color against a darker teal circular background. The central figure is slightly taller than the two flanking figures. The platform has a subtle shadow beneath it. The overall design is minimalist and modern.

**DOVE POTETE TROVARE  
ASSISTENZA**

## Elenchi dell'Ente PCI

Risorsa	Collegamento	URL
List of Validated Payment Applications (Elenco di Applicazioni di pagamento convalidate)	<a href="#"><i>PCI Council's Validated Payment Applications (Applicazioni di pagamento convalidate dall'Ente PCI)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement">https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement</a>
List of Approved PTS Devices (Elenco di dispositivi PTS approvati)	<a href="#"><i>PCI Council's Approved PTS Devices (Dispositivi PTS approvati dal PCI Council)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices">https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices</a>
List of Approved Scanning Vendors (Elenco di fornitori di scansioni approvati (ASV))	<a href="#"><i>PCI Council's Approved Scanning Vendors (Fornitori di scansioni approvati dell'Ente PCI)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors">https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors</a>
List of Qualified Integrators / Resellers (Elenco di responsabili dell'integrazione e rivenditori qualificati)	<a href="#"><i>PCI Council's Qualified Integrators Resellers (Responsabili dell'integrazione e rivenditori qualificati dell'Ente PCI)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers">https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers</a>
List of P2PE Validated Solutions (Elenco di soluzioni convalidate P2PE)	<a href="#"><i>PCI Council's P2PE Validated Solutions (Soluzioni convalidate P2PE dell'Ente PCI)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions">https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions</a>

## Elenco di marchi di pagamento

Risorsa	Collegamento	URL
Lists of Compliant Service Providers (Elenchi di provider di servizi conformi)	<a href="#"><i>MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard)</i></a>	<a href="https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html">https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html</a>
	<a href="#"><i>Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa)</i></a>	<a href="http://www.visa.com/splisting/">http://www.visa.com/splisting/</a>
	<a href="#"><i>Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe)</i></a>	<a href="https://www.visaeurope.com/receiving-payments/security/downloads-and-resources">https://www.visaeurope.com/receiving-payments/security/downloads-and-resources</a>

## PCI DSS e guida correlata

Risorsa	Collegamento	URL
More about PCI DSS (Ulteriori informazioni su PCI DSS)	<a href="#"><i>How to Secure with PCI DSS (Come garantire la sicurezza con PCI DSS)</i></a>	<a href="https://www.pcisecuritystandards.org/pci_security/how">https://www.pcisecuritystandards.org/pci_security/how</a>
PCI DSS Self-Assessment Questionnaires (Questionari di autovalutazione di PCI DSS)	<a href="#"><i>Self-Assessment Questionnaires (Questionari di autovalutazione)</i></a>	<a href="https://www.pcisecuritystandards.org/pci_security/completing_self_assessment">https://www.pcisecuritystandards.org/pci_security/completing_self_assessment</a>
Guide: Skimming Prevention: Overview of Best Practices for Merchants (Guida: Prevenzione dello skimming: Panoramica delle migliori pratiche per gli esercenti)	<a href="#"><i>Skimming Prevention: Overview of Best Practices for Merchants" Prevenzione dello skimming: Panoramica delle migliori pratiche per gli esercenti)</i></a>	<a href="https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf">https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf</a>

## Infografica e video

Risorsa	Collegamento	URL
Infographic: It's Time to Change Your Password (Infografica: È ora di modificare la vostra password)	<a href="#"><i>It's Time to Change Your Password (È ora di modificare la vostra password)</i></a>	<a href="https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf">https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf</a>
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves (Infografica: Combattete i crimini cibernetici rendendo i dati rubati inutili ai ladri.)	<a href="#"><i>Fight Cybercrime by Making Stolen Data Worthless to Thieves (Combattete i crimini cibernetici rendendo i dati rubati inutili ai ladri)</i></a>	<a href="https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf">https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf</a>
Video: Learn Password Security in 2 Minutes (Video: Due minuti di informazioni sulla sicurezza della password)	<a href="#"><i>Learn Password Security in 2 Minutes (Due minuti di informazioni sulla sicurezza della password)</i></a>	<a href="https://www.youtube.com/watch?v=FsrOXgZKa7U">https://www.youtube.com/watch?v=FsrOXgZKa7U</a>

## Risorse per la protezione dei pagamenti per piccoli esercenti del PCI

Risorsa	Collegamento	URL
Sistemi di pagamento comuni	<a href="#"><i>Sistemi di pagamento comuni</i></a>	<a href="https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf">https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf</a>
Domande dei piccoli esercenti ai fornitori	<a href="#"><i>Domande dei piccoli esercenti ai fornitori</i></a>	<a href="https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf">https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf</a>
Glossario per piccoli esercenti	<a href="#"><i>Glossario per piccoli esercenti</i></a>	<a href="https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf">https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf</a>

# Origini

Gallup – *Gallup Poll*, October 2015 (Gallup – *Sondaggio Gallup*, Ottobre 2015)

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014  
(Governo HM – *Piccole imprese: cosa sapere sulla sicurezza informatica*, Regno Unito 2014)

NCSA – *National Cyber Security Alliance survey*, 2012 (NCSA – *Sondaggio National Cyber Security Alliance*, 2012)

NSBA – *National Small Business Administration, 2014 Year End Economic Report* (NSBA, *Rapporto economico di fine anno 2014*)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (Verizon 2012 – *Rapporto sulle analisi delle violazioni dei dati Verizon 2012*)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (Verizon 2015 – *Rapporto sulle analisi delle violazioni dei dati Verizon 2015*)

Verizon PCI 2015 – *Report sulla conformità agli standard PCI 2015* (Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report*)