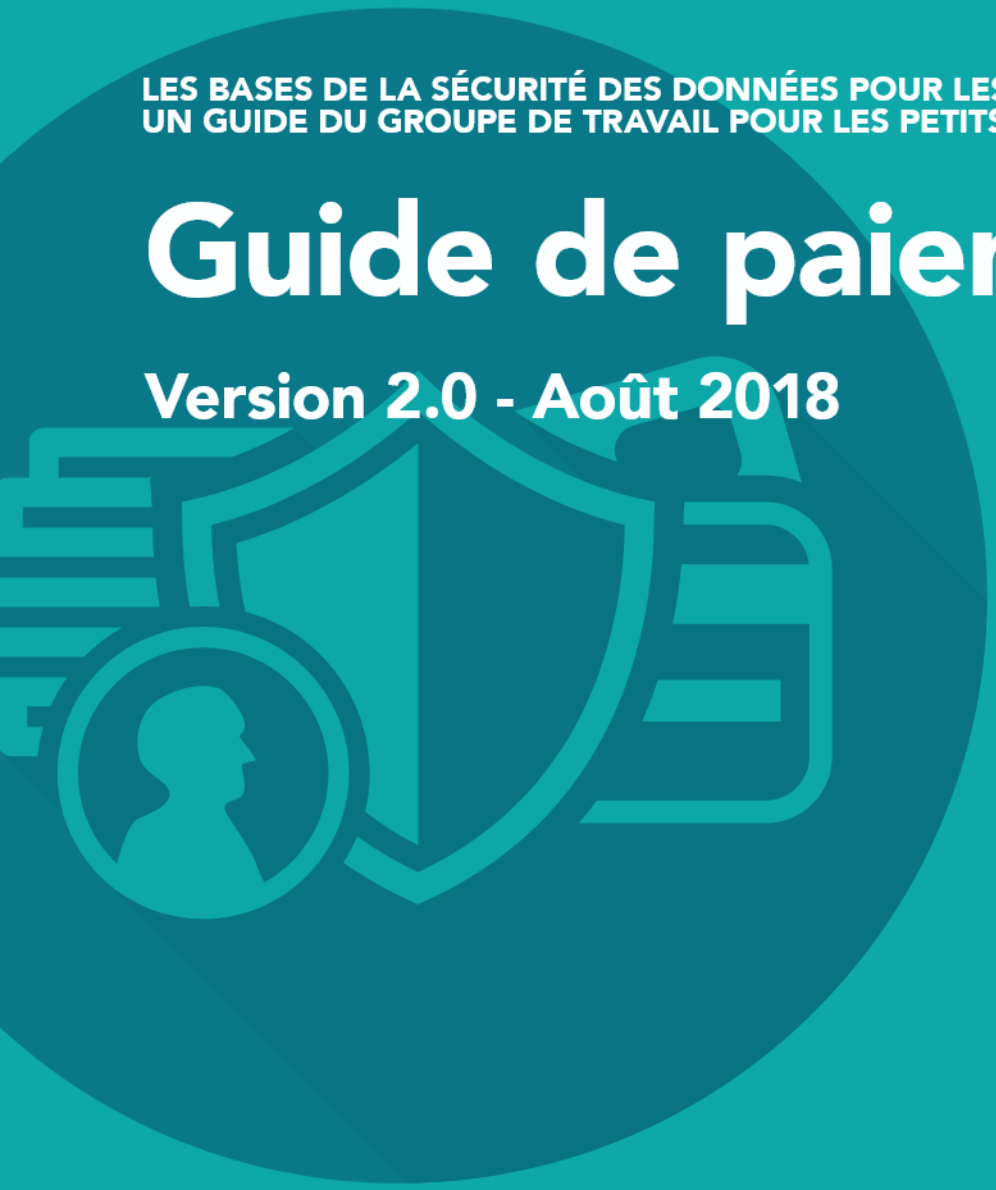
LES BASES DE LA SÉCURITÉ DES DONNÉES POUR LES PETITS COMMERÇANTS
UN GUIDE DU GROUPE DE TRAVAIL POUR LES PETITS COMMERÇANTS DE PCI

Guide de paiement sécurisé

Version 2.0 - Août 2018



PCI Security Standards Council

**Les bases de la sécurité des données pour les petits commerçants :
Guide de paiement sécurisé Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.**

Ce guide de paiement sécurisé est fourni par le Conseil des normes de sécurité PCI (PCI SSC) pour informer et sensibiliser les commerçants et autres entités impliquées dans le traitement des cartes de paiement. Pour plus d'informations sur le PCI SSC et les normes que nous gérons, rendez-vous sur le site *www.pcisecuritystandards.org*

Ce document a pour but de fournir des informations complémentaires, qui ne remplacent pas ou n'annulent pas les normes PCI ou leurs documents d'appui.

COMPRENDRE VOTRE RISQUE

Comprendre votre risque

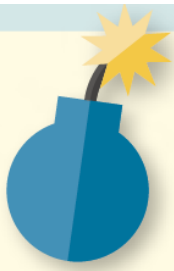
En tant que petite entreprise, vous êtes une cible parfaite pour les voleurs de données.

Lorsque vos données de cartes de paiement font l'objet d'une violation, les conséquences peuvent se faire ressentir rapidement. Vos clients perdent leur con iance en votre capacité à protéger leurs informations personnelles, ce qui les incite à aller voir vos concurrents.

Cela peut engendrer d'éventuelles pénalités inancières et dommages-intérêts pour votre entreprise, qui risque également de perdre sa capacité à accepter les cartes de paiement. Une enquête réalisée auprès de 1 015 petites et moyennes entreprises a révélé que 60 % de celles ayant connu une violation de données ont fermé en six mois. (NCSA)

DES PETITES ENTREPRISES ONT SUBI DES VIOLATIONS AU COURS DES 12 DERNIERS MOIS.

(Ponemon Institute)



30 milliards de £

COÛT POUR LES ENTREPRISES BRITANNIQUES LIÉ AUX VIOLATIONS DE SÉCURITÉ INFORMATIQUE EN 2016

(Beaming UK)

DES VIOLATIONS ONT TOUCHÉ LES PETITES ENTREPRISES L'ANNÉE DERNIÈRE, CONTRE 53 % L'ANNÉE PRÉCÉDENTE

(Verizon 2017)

DES PETITES ENTREPRISES ONT DES POLITIQUES PRÉCISES COUVRANT LES RISQUES DE CYBERSÉCURITÉ EN 2017

(Département britannique de la culture, des médias et des sports)

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

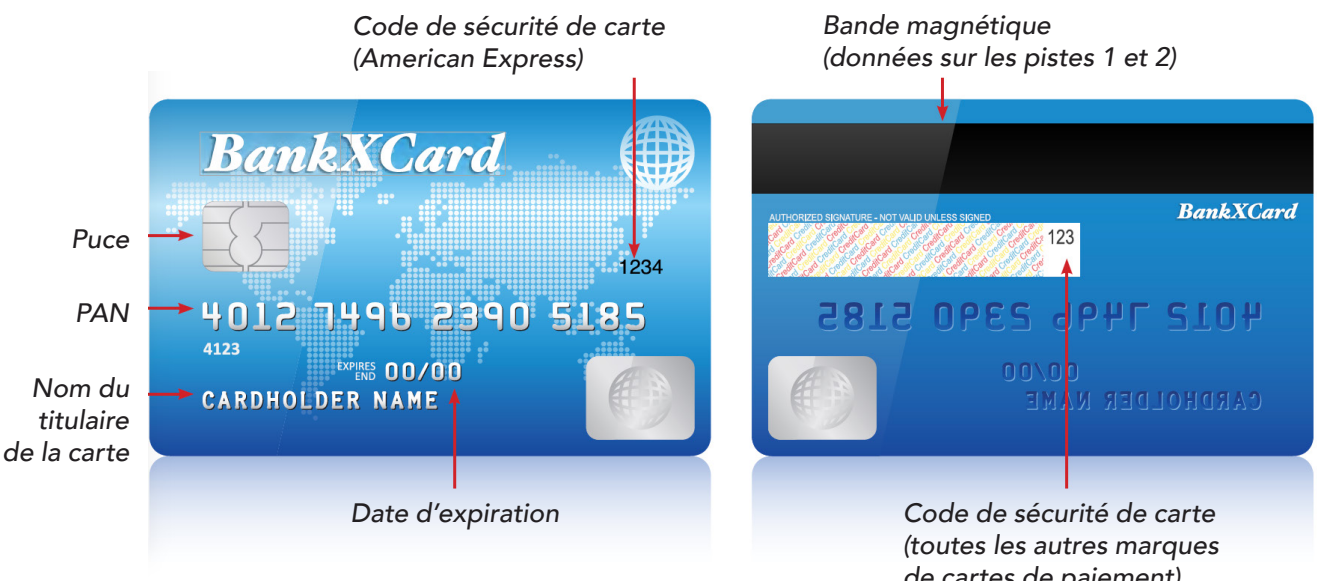
Quels éléments sont concernés parces risques ?

LES DONNÉES DES CARTES DE VOS CLIENTS SONT UNE MINE D'OR POUR LES FRAUDEURS. NE LAISSEZ PAS CELA VOUS ARRIVER !

Prenez les mesures proposées dans ce guide pour vous protéger contre le vol de données.

Le numéro de compte primaire (PAN) et le code de sécurité à trois ou quatre chiffres de la carte de paiement sont des exemples de données de carte de paiement. Les flèches rouges ci-dessous indiquent différents types de données nécessitant une protection.

TYPES DE DONNÉES SUR UNE CARTE DE PAIEMENT



QU'EST-CE QUE PCI DSS ?

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un ensemble de règles de sécurité qui peuvent aider les petits commerçants à protéger les données des cartes de paiement de leurs clients.

Les petits commerçants peuvent procéder à la validation de leur conformité à la norme PCI DSS via un questionnaire d'auto-évaluation (SAQ).

Pour en savoir plus sur la norme PCI DSS, reportez-vous aux ressources mentionnées à la fin de ce guide.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Comprendre votre système de paiement : Termes courants relatifs au paiement

L'acceptation des paiements par carte en face à face pour vos clients nécessite un équipement spécial. En fonction de là où vous vous trouvez dans le monde, l'équipement utilisé pour accepter les paiements possède des noms différents. Voici les types dont nous parlons dans ce document et comment ils sont communément appelés.

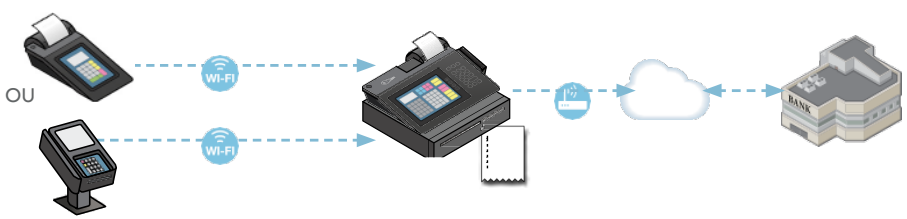
Un **TERMINAL DE PAIEMENT** est l'appareil utilisé pour accepter les paiements par carte des clients via insertion latérale, verticale ou horizontale, via lecture par contact ou via la saisie manuelle du numéro de carte. Terminal de paiement électronique (ou POS), lecteur de carte de crédit, terminal PDQ ou terminal EMV/à puce sont également des noms employés pour décrire ces appareils.

Une **CAISSE ENREGISTREUSE ÉLECTRONIQUE** (ou tiroir-caisse) enregistre et calcule les transactions et peut imprimer des tickets de caisse, mais elle n'accepte pas les paiements par carte des clients.

Un **TERMINAL DE PAIEMENT INTÉGRÉ** est un terminal de paiement combiné à une caisse enregistreuse électronique, ce qui signifie que cet appareil accepte les paiements par carte, enregistre et calcule les transactions et imprime des tickets de caisse.

Une **BANQUE MARCHANDE** est une banque ou un établissement financier qui traite les paiements par carte de crédit et/ou débit pour le compte des commerçants. Acquéreur, banque acquéreuse, processeur de paiement et service de traitement de paiement ou de cartes sont également des termes employés pour désigner cette entité.

Le **CHIFFREMENT** (ou cryptographie) rend les données de la carte illisibles pour les personnes ne disposant pas d'informations spéciales (par ex., une clé). La cryptographie peut être utilisée sur les données stockées et les données transmises sur un réseau. Les terminaux de paiement qui font partie d'une solution P2PE agréée par PCI offrent aux commerçants la meilleure assurance quant à la qualité du chiffrement. Avec une solution P2PE agréée par PCI, les données de carte sont toujours saisies directement dans un terminal de paiement approuvé par PCI à l'aide d'une fonction de lecture et d'échange sécurisés des données (SRED). Cette approche minimise le risque pour les données de carte en clair et protège les commerçants contre les attaques des terminaux de paiement, notamment via des logiciels malveillants d'extraction de données en mémoire. Tout chiffrement qui n'est pas effectué à l'aide d'une solution P2PE agréée par PCI doit être examiné avec votre fournisseur.



Un **SYSTÈME DE PAIEMENT** englobe le processus entier d'acceptation des paiements par carte. Également appelé « environnement de données des titulaires de carte (CDE) », votre système de paiement peut inclure un terminal de paiement, une caisse enregistreuse électronique, d'autres appareils ou systèmes connectés à un terminal de paiement (par exemple, au réseau Wi-Fi pour la connectivité ou à un ordinateur utilisé pour l'inventaire), et les connexions vers une banque marchande. Il est important de n'utiliser que des terminaux et des solutions de paiement sécurisés pour gérer votre système de paiement. Rendezvous sur la *page 21* pour de plus amples informations.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Comprendre votre système de paiement d'e-commerce

Lorsque vous vendez des produits ou des services en ligne, vous êtes classé comme un e-commerçant. Voici quelques termes courants que vous risquez de rencontrer et ce qu'ils signifient.

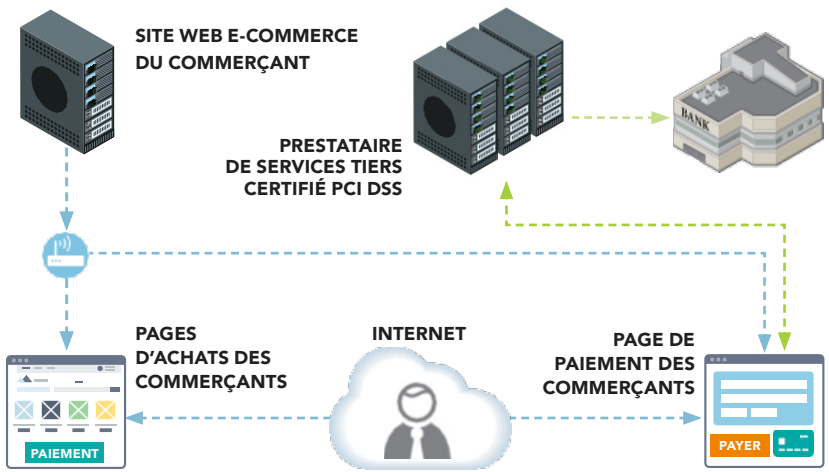
Un **SITE WEB E-COMMERCE** héberge et présente le site Web de votre entreprise et les pages d'achat à vos clients. Le site Web peut être hébergé et géré par vous-même ou par un fournisseur d'hébergement tiers.

Vos **PAGES D'ACHAT** sont les pages Web qui présentent votre produit ou service à vos clients, leur permettant ainsi d'accéder à vos produits et de les sélectionner. Ces pages vous permettent de recueillir leurs coordonnées personnelles et informations de livraison. Aucune donnée relative aux cartes de paiement n'est demandée ou saisie sur ces pages.

Votre **PAGE DE PAIEMENT** est la page Web ou le formulaire utilisé pour collecter les données de la carte de paiement de votre client après qu'il a décidé d'acheter votre produit ou vos services.

Le traitement des données de la carte peut être

1) géré exclusivement par le commerçant à l'aide d'un panier d'achat ou d'une application de paiement ;
2) partiellement géré par le commerçant avec l'aide d'un tiers en utilisant diverses méthodes ; ou
3) entièrement sous-traité à un tiers. La plupart du temps, le recours à une tierce partie entièrement externalisée est l'option la plus sûre. Et il est important de s'assurer qu'il s'agit d'une tierce partie certifiée PCI DSS.



Un **SYSTÈME DE PAIEMENT E-COMMERCE** englobe l'ensemble du processus permettant à un client de choisir des produits ou des services, et au commerçant en ligne d'accepter les paiements par carte. Il peut inclure un site Web comportant des pages d'achat et une page ou un formulaire de paiement, d'autres périphériques ou systèmes connectés (par exemple, une connexion Wi-Fi ou un PC utilisé pour l'inventaire), et des connexions à la banque marchande (également appelée prestataire de services de paiement ou passerelle de paiement). Selon le scénario de paiement en ligne du commerçant, un système de paiement e-commerce est soit entièrement externalisé à un tiers, soit partiellement géré par le commerçant avec l'aide d'un tiers, soit géré exclusivement par le commerçant.

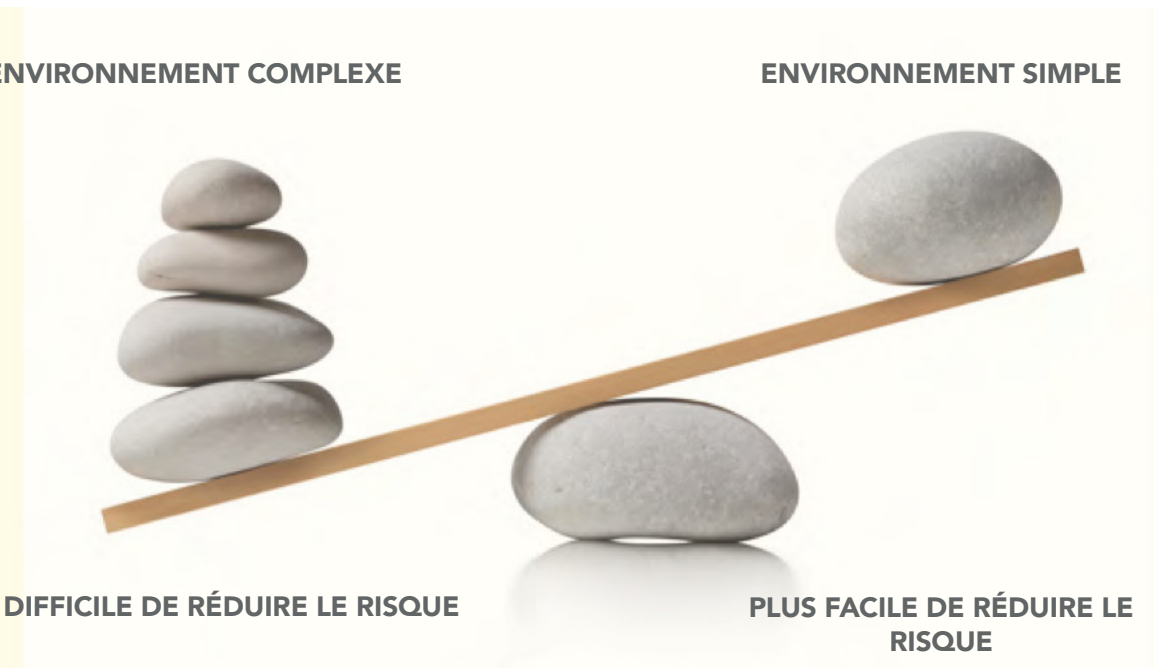
Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Quel est le risque pour votre entreprise ?

Plus votre système possède de fonctionnalités, plus il est difficile à sécuriser.

Réfléchissez bien pour savoir si vous avez vraiment besoin de onctionnalités supplémentaires telles que le Wi-Fi, un logiciel d'accès à distance, des caméras connectées à Internet ou des systèmes d'enregistrement d'appels pour votre entreprise. Si elles ne sont pas correctement configurées et gérées, chacune de ces onctionnalités peut permettre aux criminels d'accéder facilement aux données des cartes de paiement de vos clients.

Si vous êtes un e-commerçant, il est très important de comprendre comment ou si les données de paiement sont saisies sur votre site Web. Dans la plupart des cas, le recours à une tierce partie entièrement externalisée pour saisir et traiter les paiements est l'option la plus sûre.



Comment vendezvous vos biens et services ?

Il existe trois méthodes principales :

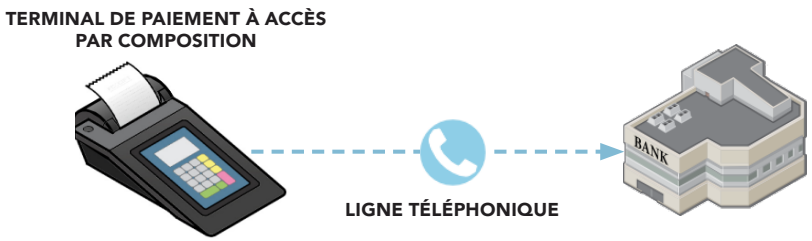
1. Une personne entre dans votre magasin et fait un achat avec sa carte.
2. Une personne consulte votre site Web et paie en ligne.
3. Une personne appelle votre magasin et fournit les détails de sa carte par téléphone ou les envoie par e-mail ou par fax.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

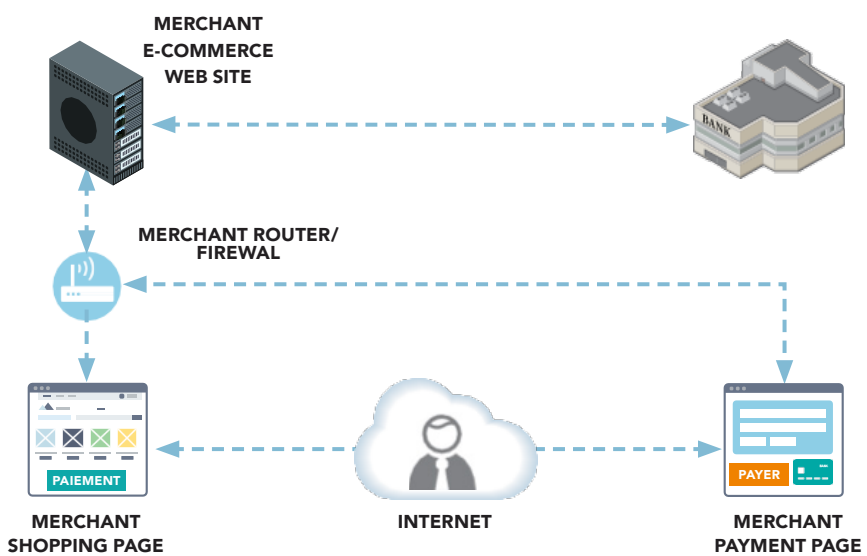
Comprendre votre risque : Types de systèmes de paiement

Vos risques de sécurité varient considérablement en fonction de la complexité de votre système de paiement, que ce soit en face à face ou en ligne.

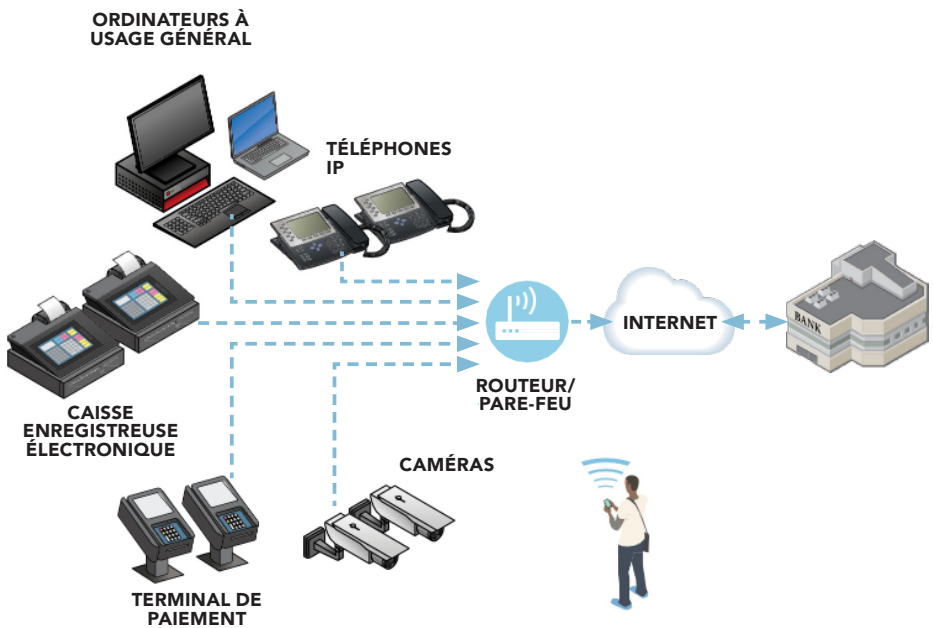
Système de paiement simple pour les achats en magasin



Système de paiement e-commerce complexe pour les achats en ligne, le commerçant gérant son propre site Web et sa propre page de paiement



Système de paiement complexe pour les achats en magasin, avec connexion Wi-Fi, caméras, téléphones Internet et autres systèmes associés



Utilisez le document ***Systèmes de paiement*** courants pour vous aider à identifier le type de système de paiement que vous utilisez, votre risque et les mesures de sécurité recommandées, comme point de départ pour les conversations avec votre banque marchande et vos partenaires fournisseurs.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

PROTÉGEZ VOTRE ENTREPRISE AVEC CES ÉLÉMENTS DE SÉCURITÉ DE BASE

Comment protégez-vous votre entreprise ?

La bonne nouvelle est que vous pouvez commencer à protéger votre entreprise dès aujourd'hui avec ces éléments de sécurité de base :

Utilisez des mots de passe complexes et modifiez les mots de passe par défaut

Coût	1
Simplicité	1
Atténuation des risques	3

Protégez vos données de carte et conservez uniquement ce dont vous avez besoin

Coût	1
Simplicité	1
Atténuation des risques	2

Inspectez les terminaux de paiement pour vérifier qu'ils ne sont pas modifiés

Coût	1
Simplicité	1
Atténuation des risques	2

Faites appel à des partenaires de confiance et sachez comment les contacter

Coût	1
Simplicité	1
Atténuation des risques	1

Installez les correctifs fournis par vos fournisseurs

Coût	1
Simplicité	2
Atténuation des risques	3

Sécurisez l'accès en interne à vos données de carte.

Coût	1
Simplicité	2
Atténuation des risques	2

Ne facilitez pas l'accès des hackers à vos systèmes

Coût	2
Simplicité	2
Atténuation des risques	3

Utilisez des logiciels antivirus

Coût	2
Simplicité	2
Atténuation des risques	2

Recherchez les vulnérabilités et corrigez les problèmes

Coût	2
Simplicité	2
Atténuation des risques	3

Utilisez des solutions et des terminaux de paiement sécurisés

Coût	3
Simplicité	2
Atténuation des risques	3

Protégez votre entreprise contre Internet

Coût	2
Simplicité	3
Atténuation des risques	3

Pour une protection optimale, rendez vos données inutiles pour les criminels

Coût	3
Simplicité	3
Atténuation des risques	3

Ces éléments de sécurité de base sont organisés du plus facile et moins coûteux à mettre en place aux plus complexes et coûteux. La valeur de réduction des risques que chacun offre aux petits commerçants est également indiquée dans la colonne « Atténuation des risques ».

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Utilisez des mots de passe complexes et modifiez les mots de passe par défaut

Coût	
Simplicité	
Atténuation des risq	

Vos mots de passe sont essentiels pour garantir la sécurité des ordinateurs et des données de carte. Tout comme une serrure sur votre porte protège vos biens physiques, un mot de passe permet de protéger vos données professionnelles. Veuillez également noter que l'équipement informatique et les logiciels prêts à l'emploi (notamment votre terminal de paiement) sont souvent accompagnés de mots de passe par défaut (prédéfinis), tels que « motdepasse » ou « admin », qui sont souvent connus par les hackers et représentent une source fréquente de violations de données chez les petits commerçants.

MODIFIEZ RÉGULIÈREMENT VOS MOTS DE PASSE.
Traitez vos mots de passe comme une brosse à dents. Ne laissez personne d'autre que vous les utiliser et changez-les tous les trois mois.

PARLEZ À VOS PRESTATAIRES DE SERVICES.
Demandez à vos fournisseurs ou prestataires de services quels sont les mots de passe par défaut et comment les modifier. Puis faites-le ! De plus, si votre prestataire de services gère les mots de passe de vos systèmes, demandez-lui s'il a modifié les mots de passe par défaut.

FAITES EN SORTE QU'ILS SOIENT DIFFICILES À DEVINER.
Les mots de passe les plus courants sont « motdepasse » et « 123456 ». Les hackers essaient les mots de passe faciles à deviner, car ils sont utilisés par la moitié des gens. Un mot de passe complexe possède sept caractères ou plus et une combinaison de majuscules et minuscules, de chiffres et de symboles (comme !@#$&*). Une expression peut également être un mot de passe complexe (et peut-être plus facile à retenir), comme « St3ak&friteS ».

NE LES COMMUNIQUEZ PAS.
Insistez sur le fait que chaque employé doit avoir son propre identifiant de connexion et son propre mot de passe et qu'ils ne doivent jamais les communiquer.

LES MOTS DE PASSE PAR DÉFAUT TYPIQUES QUI DOIVENT ÊTRE MODIFIÉS :

[aucun]

[nom du produit/fournisseur]

1234 ou 4321

accès admin

anonyme

nomdesociété

base de données

invité

gestionnaire

mdp

motdepasse

racine

as secret

adminsys

utilisateur

65%

des PME qui ont une politique en matière de mots de passe ne l'appliquent pas strictement

Ponemon Institute

Pour en savoir plus sur la sécurité des mots de passe, reportez vous aux ressources suivantes sur le site Internet du Conseil PCI :

INFOGRAPHIE
Il est temps de modifier votre mot de passe

VIDÉO
Tout apprendre sur la sécurité des mots de passe en 2 minutes

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Protégez vos données de carte et conservez uniquement ce dont vous avez besoin

Coût	
Simplicité	
Atténuation des risq	

Il est impossible de protéger les données de carte si vous ne savez pas où elles se trouvent.

Que pouvez-vous faire ?

Vous pouvez également déterminer si vous stockez des données de paiement dans des e-mails. Si vous recevez les détails d'une carte par e-mail, vous pouvez toujours traiter la transaction, mais supprimez immédiatement l'e-mail et indiquez à l'expéditeur quelle méthode privilégier pour l'envoi de ses informations de paiement (en lui précisant que l'e-mail n'est pas la meilleure façon de procéder). Ne vous contentez pas de répondre en utilisant l'e-mail d'origine de votre client. Supprimez plutôt les détails de la carte dans le courrier de réponse, sinon vous exposez davantage les données de la carte en stockant l'e-mail d'origine, l'e-mail envoyé, etc.

L'objectif de la tokenisation est similaire à celui du chiffrement, mais leur fonctionnement est différent. La tokenisation consiste à substituer les données de carte par des données dénuées de sens (un « token » ou « jeton ») qui n'ont aucune valeur pour un hacker. Les commerçants peuvent utiliser des jetons pour soumettre des transactions ultérieures ou encore traiter un remboursement sans avoir besoin de stocker les informations réelles de la carte de paiement. Le jeton est utilisé par votre service de traitement de paiement pour rechercher les détails de la carte, qu'il stocke à votre place.

DEMANDEZ DE L'AIDE À UN SPÉCIALISTE. Demandez au fournisseur de votre terminal de paiement, à votre prestataire de services ou à votre banque marchande où vos systèmes stockent les données, le cas échant, et si vous pouvez simplifier la manière dont vous traitez les paiements. Demandez également comment effectuer des transactions spécifiques (par exemple, pour les paiements récurrents) sans devoir conserver le code de sécurité de la carte.

SOUS-TRAITEZ. Le meilleur moyen pour vous protéger contre les violations de données est de ne pas du tout conserver les données de carte. Pensez à sous-traiter votre processus de traitement de cartes à un prestataire de services conforme à la norme PCI DSS. Reportez-vous aux ressources mentionnées en *page 25* pour obtenir une liste des prestataires de services conformes.

SI VOUS N'AVEZ PAS BESOIN DES DONNÉES DE CARTE, ALORS NE LES STOCKEZ PAS. Détruisez de manière sécurisée les données de carte dont vous n'avez pas besoin. Si vous devez conserver des documents papier contenant des données de carte sensibles, rayez les données avec un marqueur noir épais jusqu'à ce qu'elles soient illisibles, puis rangez les documents papier dans un tiroir verrouillé ou un coffre-fort auquel seules quelques personnes ont accès.

LIMITEZ LES RISQUES. Plutôt que d'accepter des informations de paiement par e-mail, demandez aux clients de les fournir par téléphone, fax ou courrier standard.

SEGMENTEZ OU CRYPTEZ LES DONNÉES. Demandez à votre banque marchande si vous devez VRAIMENT conserver ces données de carte. Si oui, posez des questions à votre banque marchande ou à votre prestataire de services concernant les technologies de chiffrement ou de tokenisation des données qui rendent les données de carte inutilisables même si elles sont dérobées

VOIR PAGE 23

AMORCE DU CHIFFREMENT

Le chiffrement utilise une formule mathématique pour rendre le texte brut illisible aux personnes ne disposant pas de connaissances spéciales (ce que l'on appelle une « clé »). Le chiffrement est appliqué sur les données stockées et transférées sur un réseau.

Le **CHIFFREMENT** permet de changer le texte brut en texte chiffré.

LE DÉCHIFFREMENT permet de changer le texte chiffré en texte brut.

Par exemple :

This is secret stuff

CLÉ DE CHIFFREMENT

5a0 (k$hQ%...)

This is secret stuff

CLAVE DE DESCIFRADO

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Inspectez les terminaux de paiement pour vérifier qu'ils ne sont pas modifiés

Coût	
Simplicité	
Atténuation des risques	

Les « dispositifs de clonage de carte » analysent les données de carte de vos clients lorsqu'elles entrent dans un terminal de paiement. Il est essentiel que vous et votre personnel sachiez comment repérer un dispositif de clonage, à quoi doivent ressembler vos terminaux de paiement et combien vous en avez. Vous devez régulièrement vérifier vos terminaux de paiement afin de vous assurer qu'ils n'ont pas été modifiés. Si vous soupçonnez qu'un terminal a été trafiqué, NE L'UTILISEZ PAS et signalez-le immédiatement à votre banque marchande et/ou au fournisseur du terminal.

Soyez vigilant et suivez ces étapes :

TENEZ UNE LISTE de tous les terminaux de paiement et prenez des photos (devant, derrière, cordons et raccordements), de sorte que vous sachiez à quoi ils sont censés ressembler.

RECHERCHEZ DES SIGNES ÉVIDENTS de modification, tels que des joints cassés sur les caches d'accès ou les vis, un câblage étrange/différent, ou de nouveaux périphériques ou fonctionnalités que vous ne reconnaissez pas. Le guide du Conseil PCI (référencé ci-dessous) peut vous aider.

PROTÉGEZ VOS TERMINAUX. Tenez-les hors de la portée des clients lorsqu'ils ne sont pas utilisés et cachez leurs écrans de la vue des clients. Assurez-vous que vos terminaux de paiement sont sécurisés avant de fermer votre magasin pour la journée, notamment tous les dispositifs qui lisent les cartes de paiements de vos clients ou qui acceptent leurs numéros d'identification personnels (codes PIN).

CONTRÔLEZ LES DISPOSITIFS APRÈS UNE RÉPARATION. Autorisez uniquement les réparations de terminaux de paiement réalisées par un personnel de réparation autorisé et uniquement si vous les aviez prévues. Informez également vos employés. Surveillez les tiers ayant un accès physique à vos terminaux de paiement, même s'ils sont là pour une autre raison, afin de vous assurer qu'ils ne modifient pas vos terminaux.

APPELEZ IMMÉDIATEMENT le fournisseur de votre terminal de paiement ou votre banque marchande si vous suspectez quoi que ce soit !

Reportez-vous au *Guide du Conseil PCI : Prévention du clonage de carte – Présentation des meilleures pratiques pour* commerçants

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Faites appel à des partenaires les contacter de confiance et sachez comment

Coût
Simplicité
Atténuation des risques

Vous utilisez des prestataires externes pour les services, dispositifs et applications de paiement. Vous pouvez également avoir des prestataires de services avec lesquels vous partagez les données de carte, qui assurent l'assistance et la gestion de vos systèmes de paiement, ou auxquels vous donnez accès aux données de carte. Il peut s'agir de processeurs de paiements, fournisseurs, tiers ou prestataires de services. Tous les éléments ci-dessus impactent votre capacité à protéger vos données de carte. Il est donc essentiel que vous sachiez qui ils sont et quelles questions leur poser concernant la sécurité.

SACHEZ QUI APPELER.
Qui est votre banque marchande ? Qui d'autre vous aide à traiter les paiements ? Auprès de qui avez-vous acheté votre logiciel/dispositif de paiement et qui l'a installé pour vous ? Qui sont vos prestataires de services ?

TENEZ UNE LISTE.
Maintenant que vous savez qui appeler, gardez les noms des entreprises et des contacts, les numéros de téléphone, les adresses des sites Web et autres coordonnées, grâce auxquels vous pouvez facilement les trouver en cas d'urgence.

VÉRIFIEZ LA SÉCURITÉ DE VOS PRESTATAIRES DE SERVICES.
Votre prestataire de services satisfait-il les exigences de la norme PCI DSS ? Pour les e-commerçants, il est important que votre prestataire de services de paiement soit lui aussi conforme à la norme PCI DSS ! Reportez-vous aux ressources mentionnées en *page 25* pour obtenir une liste des prestataires de services conformes.

POSEZ DES QUESTIONS.
Une fois que vous savez qui sont vos prestataires externes et ce qu'ils font pour vous, parlez avec eux pour comprendre comment ils protègent les données de carte. Utilisez le document *Questions à poser à vos fournisseurs* pour savoir quoi leur demander.

COMPRENEZ QUI SONT LES FOURNISSEURS COURANTS.
Examinez l'encadré à droite pour connaître les types courants de fournisseurs et de prestataires de services avec lesquels vous êtes susceptible de travailler.

FOURNISSEURS COURANTS

Reportez-vous au tableau du document *Questions à poser à vos f*ournisseurs *pour en savoir plus sur ces* fournisseurs courants :

- Fournisseurs de terminaux de paiement
- Fournisseurs d'applications de paiement
- Installateurs de systèmes de paiement (appelés intégrateurs / revendeurs)
- Prestataires de services qui s'occupent du traitement des paiements ou de l'hébergement/traitement du e-commerce
- Prestataires de service qui vous aident à respecter les exigences de la norme PCI DSS (par exemple en fournissant des services de pare-feu ou d'antivirus)
- Fournisseurs de logiciels en tant que service (SaaS)

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Installez les correctifs fournis par vos fournisseurs

Coût	
Simplicité	
Atténuation des risques	

Les logiciels peuvent avoir des défauts qui sont découverts après leur publication et causés par des erreurs commises par les programmeurs lorsqu'ils écrivent le code. Ces défauts sont également appelés failles de sécurité, bugs ou vulnérabilités. Les hackers exploitent ces erreurs pour pénétrer dans votre ordinateur et dérober les données de compte. Protégez vos systèmes en appliquant les « correctifs » fournis par le fournisseur visant à corriger les erreurs de codage. Il est essentiel d'installer les correctifs de sécurité rapidement !

Il est important que vous sachiez comment votre logiciel est régulièrement mis à jour avec des correctifs et qui en est responsable, car cette responsabilité peut vous revenir. De plus, certains correctifs s'installent automatiquement lorsqu'ils sont disponibles. Si vous n'êtes pas sûr de la manière dont les correctifs sont ajoutés ou de la personne responsable, n'hésitez pas à demander à votre fournisseur.

DEMANDEZ à votre fournisseur ou prestataire de services comment il est censé vous informer en cas de disponibilité de nouveaux correctifs de sécurité et comment il s'assure que vous ayez bien reçu et lu ces notifications.

QUELS FOURNISSEURS VOUS ENVOIENT DES CORRECTIFS ?
Vous pouvez obtenir des correctifs auprès des fournisseurs de votre terminal de paiement, d'applications de paiement, d'autres systèmes de paiement (tiroirs-caisses, caisses enregistreuses, ordinateurs, etc.), de systèmes d'exploitation (Android, Windows, iOS, etc.), de logiciels d'application (notamment votre navigateur Internet) et de logiciels professionnels.

ASSUREZ-VOUS que vos fournisseurs mettent à jour vos terminaux de paiement ou systèmes d'exploitation, de sorte qu'ils puissent prendre en charge les derniers correctifs de sécurité. Posez-leur des questions.

E-COMMERÇANTS.
Installer des correctifs dès que possible est très important pour vous aussi. Vérifiez régulièrement auprès de votre prestataire de services de paiement si des correctifs sont disponibles. Demandez à votre fournisseur d'hébergement e-commerce s'il fournit des correctifs pour votre système (et à quelle fréquence). Assurez-vous qu'ils mettent à jour le système d'exploitation, la plateforme d'e-commerce et/ou l'application Web, de sorte que ceux-ci puissent prendre en charge les derniers correctifs.

SUIVEZ les instructions de votre fournisseur/prestataire de services et installez ces correctifs dès que possible.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

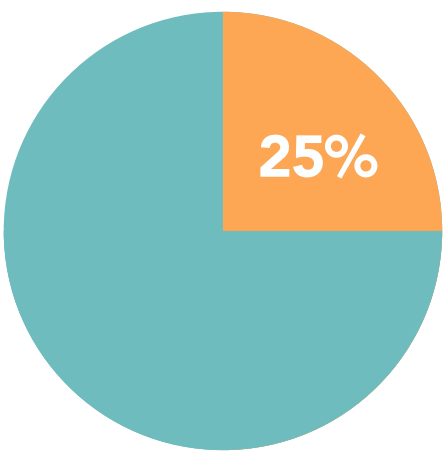
Sécurisez l'accès en interne à vos données

Coût	
Simplicité	
Atténuation des risques	

L'abus de privilège signi ie qu'une personne utilise...

Les droits d'accès et privilèges d'une autre personne pour obtenir l'accès aux systèmes ou aux données auxquels cette personne n'est pas autorisée à accéder.

25% DES VIOLATIONS CONCERNENT DES ACTEURS INTERNES.



Verizon 2017

LE CONTRÔLE D'ACCÈS EST DE LA PLUS GRANDE IMPORTANCE.
Configurez votre système pour n'accorder l'accès qu'en fonction du « besoin d'en connaître ». En tant que propriétaire, vous avez accès à tout. Mais la plupart des employés peuvent faire leur travail en n'ayant accès qu'à un sous-ensemble de données, d'applications et de fonctions.

LIMITEZ L'ACCÈS aux systèmes de paiement et aux données de carte non chiffrées aux seuls employés qui ont besoin d'y accéder et uniquement pour les données, les applications et les fonctions dont ils ont besoin pour leur travail.

TENEZ UN JOURNAL.
Faites le suivi de l'ensemble des visiteurs « passant derrière le comptoir » au sein de votre établissement. Les informations à noter incluent le nom, la raison de la visite et le nom de l'employé qui a autorisé l'accès du visiteur. Tenez le journal pendant au moins une année.

METTEZ VOS DISPOSITIFS AU REBUT DE MANIÈRE SÉCURISÉE.
Demandez au fournisseur de votre terminal de paiement ou à votre prestataire de services comment faire pour supprimer de manière sécurisée les données de carte avant de vendre ou de mettre au rebut des dispositifs de paiement (de sorte que les données ne puissent pas être récupérées).

PARTAGEZ LES INFORMATIONS.
Remettez ce guide à vos employés, partenaires et prestataires de services tiers (tels que les fournisseurs d'hébergement e-commerce) de sorte qu'ils sachent ce que l'on attend d'eux.

CRÉEZ DES IDENTIFIANTS UTILISATEURS UNIQUES pour chaque personne ayant accès à votre système de paiement, dans la mesure du possible. Vous pourrez ainsi savoir qui se connecte et quand, ainsi que les modifications qu'ils apportent.

Envisagez de donner l'accès aux employés pour accepter des paiements, mais pas pour effectuer des remboursements, ou pour prendre de nouvelles réservations/commandes mais pas pour accéder aux données de cartes de paiements relatives aux réservations/commandes existantes. Certains employés ne doivent pas du tout avoir accès.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Ne facilitez pas l'accès des hackers à vos systèmes

Coût	
Simplicité	
Atténuation de risques	

HACKERS = MENACES

L'un des moyens les plus faciles pour les hackers de pénétrer dans votre système est de passer par les personnes en qui vous avez confiance. Vous devez savoir comment vos fournisseurs accèdent à votre système, afin de vous assurer que leur processus n'ouvre pas de brèches pour les hackers.

L'authentification multifacteur utilise un nom d'utilisateur et un mot de passe, ainsi qu'au moins un autre facteur (comme une carte à puce, un dongle* ou un code d'accès unique).

**appareil pratique qui se connecte à un ordinateur pour permettre l'accès à la connexion sans fil, aux fonctionnalités logicielles, etc.*

CHERCHEZ À SAVOIR. Demandez au fournisseur de votre système de paiement ou à votre prestataire de services s'il utilise un accès à distance pour assurer l'assistance et accéder à vos systèmes internes.

DEMANDEZ COMMENT FAIRE POUR LIMITER L'UTILISATION DE L'ACCÈS À DISTANCE. De nombreux programmes d'accès à distance sont toujours activés, ou toujours disponibles par défaut, ce qui signifie que le fournisseur peut accéder à vos systèmes à distance en permanence (cela signifie que les hackers peuvent aussi accéder à vos systèmes puisque de nombreux fournisseurs utilisent des mots de passe connus pour l'accès à distance). Réduisez les risques : demandez à votre fournisseur comment désactiver l'accès à distance lorsqu'il n'est pas nécessaire et comment l'activer lorsque votre fournisseur ou votre fournisseur de services le demande spécifiquement.

DÉSACTIVEZ-LE UNE FOIS QUE VOUS AVEZ TERMINÉ. Pour protéger votre entreprise, il est important que vous sachiez exactement comment et quand vos fournisseurs peuvent accéder à vos systèmes.

UTILISEZ UNE AUTHENTIFICATION FORTE. Si vous devez autoriser l'accès à distance, exigez une authentification multifacteur et un chiffrement robuste.

ASSUREZ-VOUS QUE LES PRESTATAIRES DE SERVICES UTILISENT DES IDENTIFIANTS DE CONNEXION UNIQUES. Chacun d'entre eux doit utiliser des identifiants de connexion à l'accès à distance qui sont réservés à votre entreprise (uniques) et qui ne sont pas identiques à ceux utilisés pour d'autres clients.

DEMANDEZ DE L'AIDE. Demandez à votre fournisseur ou prestataire de services de vous aider à désactiver l'accès à distance ou (si votre fournisseur ou prestataire de services a besoin de l'accès à distance) de vous aider à configurer une authentification multifacteur. Reportez-vous au document *Questions à poser à vos fournisseurs* pour savoir exactement quoi leur demander.

Si votre fournisseur prend en charge ou dépanne votre système de paiement depuis ses locaux (et non sur votre site), il utilise pour ce faire Internet et un logiciel d'accès à distance.

Les exemples de produits que votre fournisseur peut installer sur votre terminal et utiliser pour vous aider à distance incluent VNC et LogMeIn.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Utilisez des logiciels antivirus

Coût	
Simplicité	
Atténuation de risques	

Les hackers écrivent des virus et d'autres codes malveillants pour exploiter les fonctionnalités logicielles et les erreurs de codage, afin qu'ils puissent pénétrer dans vos systèmes et voler des données de carte. L'utilisation d'un logiciel antivirus (également appelé anti-malware) à jour permet de protéger vos systèmes.

INSTALLEZ UN LOGICIEL ANTIVIRUS POUR PROTÉGER VOTRE SYSTÈME DE PAIEMENT.
Il est facile à installer et peut être obtenu auprès de votre magasin de fournitures de bureau ou de votre revendeur informatique.

CONFIGUREZ LE LOGICIEL SUR « MISE À JOUR AUTOMATIQUE » de sorte à toujours bénéficiez de la protection la plus récente disponible.

DEMANDEZ DES CONSEILS.
Posez des questions à votre revendeur informatique concernant les produits qu'il recommande pour la protection antivirus/ antiprogramme malveillant.

EFFECTUEZ DES ANALYSES PÉRIODIQUES.
Effectuez régulièrement des analyses complètes du système, puisque vos systèmes peuvent avoir été infectés par de nouveaux programmes malveillants qui se sont mis en place avant que votre logiciel antivirus ait pu les détecter.

E-COMMERÇANTS.
L'installation d'un logiciel antivirus est également très importante pour vous. Demandez à votre ou vos prestataires de services s'ils ont installé un logiciel antivirus sur votre système (et à quelle fréquence il est mis à jour). Assurez-vous qu'ils maintiennent le logiciel antivirus à jour et qu'ils analysent régulièrement votre système à la recherche de logiciels malveillants.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Recherchez les vulnérabilités et corrigez les problèmes

Coût	
Simplicité	
Atténuation de risques	

De nouvelles vulnérabilités, des failles de sécurité et des bugs sont découverts chaque jour. Il est essentiel de faire tester vos systèmes Internet régulièrement pour identifier ces nouveaux risques et y remédier le plus rapidement possible. Vos systèmes en ligne (comme de nombreux systèmes de paiement) sont les plus vulnérables, car ils peuvent être facilement exploités par des criminels, qui peuvent ainsi s'introduire dans vos systèmes

DEMANDEZ DES CONSEILS.
Demandez à votre banque marchande si elle dispose de partenariats avec certains des prestataires de services d'analyse agréés par PCI (ASV). Posez aussi des questions à vos fournisseurs et prestataires de services.

PARLEZ À UN ASV DE PCI.
Ces fournisseurs peuvent vous aider grâce à des outils qui identifient automatiquement les vulnérabilités et les mauvaises configurations de vos systèmes de paiement, de votre site de e-commerce et/ou de vos réseaux et vous fournissent un rapport si, par exemple, vous devez appliquer un correctif. La liste du Conseil PCI (référencée ci-dessous) peut vous aider à trouver un prestataire de services d'analyse.

CHOISISSEZ UN PRESTATAIRE DE SERVICES D'ANALYSE.
Contactez plusieurs ASV PCI pour en trouver un qui dispose d'un programme adapté à votre petite entreprise.

ATTAQUEZ-VOUS AUX VULNÉRABILITÉS.
Demandez à votre ASV, votre fournisseur ou prestataire de services du système de paiement ou à votre banque marchande de vous aider à résoudre les problèmes identifiés par l'analyse.

Les prestataires de services d'analyse approuvés par le Conseil PCI (ASV) effectuent l'analyse des vulnérabilités externes et génèrent les rapports associés. Voir la *Liste des prestataires de services d'analyse agréés par PCI*

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Utilisez des solutions et des terminaux de paiement sécurisés

Coût	
Simplicité	
Atténuation des risques	

Pour mieux protéger votre entreprise, vous devez utiliser des solutions de paiement sécurisées et des professionnels qualifiés pour vous aider. Voici quelques conseils pour choisir des produits sûrs et s'assurer qu'ils sont installés en toute sécurité.

UTILISEZ DES TERMINAUX DE PAIEMENT SÉCURISÉS ET DES DISPOSITIFS DE SAISIE DE CODE PIN.
Le Conseil PCI approuve les terminaux de paiement qui protègent vos données PIN. Assurez-vous que votre appareil ou terminal de paiement figure sur la *Liste des appareils PTS approuvés par PCI* pour connaître les équipements fournissant la meilleure sécurité et prenant en charge la « puce EMV ».

UTILISEZ UN LOGICIEL SÉCURISÉ.
Assurez-vous que votre logiciel de paiement figure sur la *Liste des applications de paiement validées par PCI*.

FAITES APPEL À DES PROFESSIONNELS QUALIFIÉS.
Assurez-vous que la personne qui installe votre système de paiement le fait correctement et en toute sécurité. Choisissez parmi la *Liste des QIR de PCI* pour connaître les sociétés qualifiées pour vous aider. Demandez à votre banque marchande de vous aider à faire votre choix.

UTILISEZ DES PRESTATAIRES DE SERVICES DE PAIEMENT ÉLECTRONIQUE SÉCURISÉS.
Si ce n'est pas déjà fait, envisagez de faire appel à un prestataire de services conforme à la norme PCI DSS pour vous aider à traiter en toute sécurité vos transactions de paiement électronique et/ou à gérer votre site Web d'e-commerce.

RECHERCHEZ DES PRESTATAIRES DE SERVICES CONFORMES À LA NORME PCI DSS.
Assurez-vous que votre prestataire de services de paiement est conforme à la norme PCI DSS. Consultez les listes de Mastercard et de Visa pour vous assurer que vos prestataires y figurent :

- *Liste des prestataires de services conformes de MasterCard*
- *Registre mondial des prestataires de services de Visa*
- *Agents certifiés par Visa Europe*

CONSULTEZ CETTE LISTE DE QUESTIONS POUR LES FOURNISSEURS.
Consultez le document *Questions à poser à vos fournisseurs* pour savoir quoi demander à vos fournisseurs et prestataires de services.

Vos clients saisissent leur numéro d'identification personnel (PIN) associé à leur carte de paiement dans le terminal de paiement ou le dispositif de saisie du code PIN. Il est important d'utiliser des dispositifs sécurisés pour protéger les données PIN de vos clients.

Pour les terminaux de paiement et les lecteurs de carte sécurisés de PCI qui chiffrent les données de carte, voir la *page 23*.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Protégez votre entreprise contre Internet

Internet est « l'autoroute principale » utilisée par les voleurs de données pour attaquer et dérober les données de carte des clients. Par conséquent, si votre activité se passe sur Internet, tout ce que vous utilisez pour les paiements par carte nécessite une protection complémentaire.

Un pare-feu est un équipement ou un logiciel qui se situe entre votre système de paiement et Internet. Il agit comme une barrière pour maintenir le trafic que vous ne voulez pas et que vous n'avez pas autorisé hors de votre réseau et de vos systèmes. Les pare-feux sont configurés (au niveau du matériel, des logiciels ou des deux) selon des critères spécifiques pour bloquer ou empêcher l'accès non autorisé à un réseau. Les pare-feux sont souvent inclus avec le routeur fourni par votre fournisseur d'accès à Internet.

UTILISATION ISOLÉE.
N'utilisez pas l'appareil ou le système avec lequel vous acceptez des paiements. Par exemple, ne surfez pas sur le Web ou ne consultez pas vos e-mails ou vos réseaux sociaux depuis le même appareil ou ordinateur que vous utilisez pour les transactions de paiement. Lorsque cela est nécessaire pour votre activité (par exemple pour mettre à jour la page de votre entreprise sur un réseau social), utilisez un autre ordinateur et non pas votre dispositif de paiement pour effectuer ces mises à jour.

PROTÉGEZ VOTRE « TERMINAL VIRTUEL ».
Si vous avez effectué des paiements clients via un terminal virtuel (page Web à laquelle vous accédez avec un ordinateur ou une tablette), réduisez les risques : n'y insérez pas de lecteur de carte externe.

PROTÉGEZ VOTRE CONNEXION WI-FI.
Si vous proposez une connexion Wi-Fi gratuite à vos clients dans votre magasin, assurez-vous d'utiliser un autre réseau pour votre système de paiement (selon le principe de « segmentation réseau »). Demandez à l'installateur de votre réseau de vous aider à configurer votre connexion Wi-Fi de façon sécurisée.

UTILISEZ UN PARE-FEU.
Un pare-feu correctement configuré sert de tampon qui empêche les hackers et les logiciels malveillants d'accéder à vos systèmes de paiement, à votre site de e-commerce et/ou à vos données de carte. Vérifiez auprès de votre prestataire de services ou de votre fournisseur de terminal de paiement pour vous assurer que vous disposez d'un pare-feu et demandez-leur de vous aider à le configurer correctement.

UTILISEZ UN LOGICIEL DE PARE-FEU PERSONNEL OU ÉQUIVALENT lorsque les systèmes de paiement ne sont pas protégés par le pare-feu de votre société (par exemple, en cas de connexion à un Wi-Fi public).

Pour des conseils simples sur la configuration de votre pare-feu, consultez le document Principes de base des pare-feux

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Pour une protection optimale, rendez vos données inutiles pour les criminels.

Coût	
Simplicité	
Atténuation des risques	

Vos données sont vulnérables lorsqu'elles transitent par votre banque marchande et lorsqu'elles sont conservées ou stockées sur vos ordinateurs et appareils. Le meilleur moyen de les protéger est de les rendre inutiles avant qu'elles ne soient volées en les chiffrant lors de leur stockage ou de leur envoi et en les supprimant lorsqu'elles ne sont pas indispensables. Bien que cela puisse être plus complexe à mettre en place, la sécurité sera beaucoup plus facile à gérer sur le long terme.

Qu'est-ce que la tokenisation ? Voir la *page 13* pour obtenir une explication.

COLLABOREZ AVEC VOTRE PRESTATAIRE DE SERVICES OU VOTRE FOURNISSEUR DE SYSTÈMES DE PAIEMENT.
Vous devez chiffrer toutes les données de carte que vous stockez ou envoyez. Assurez-vous que votre système de paiement utilise une technologie de chiffrement et/ou de tokenisation. Si vous n'êtes pas sûr, demandez-leur.

UTILISEZ DES DISPOSITIFS PCI QUI CHIFFRENT LES DONNÉES DE CARTE.
Le Conseil PCI approuve les terminaux de paiement qui protègent les données PIN, les terminaux de paiement et les « lecteurs de cartes sécurisés » qui ajoute un niveau de chiffrement aux données de carte. Voir la *Liste des dispositifs PTS approuvés par PCI.*

CONSULTATE PAGINA 21

UTILISEZ DES SOLUTIONS DE CHIFFREMENT PCI SÉCURISÉES.
Demandez si le chiffrement de votre terminal de paiement est effectué via une solution de chiffrement point à point et si elle figure sur la *Liste des solutions P2PE validées par le Conseil PCI*.

ÊTES-VOUS UN COMMERÇANT QUI PASSE MAINTENANT AUX TERMINAUX À PUCE EMV ?
C'est une excellente occasion d'investir dans un terminal qui prend en charge les cartes EMV et offre également un niveau de sécurité supplémentaire grâce au chiffrement et à la tokenisation.

METTEZ À NIVEAU VOTRE SOLUTION.
Réduisez les risques en envisageant l'achat d'un nouveau terminal de paiement utilisant à la fois une technologie de chiffrement et de tokenisation pour dévaluer les données de carte pour les hackers.

RENSEIGNEZ-VOUS.
Consultez le document *Questions à poser à vos fournisseurs* pour savoir quoi demander à vos fournisseurs et prestataires de services.

Les terminaux de paiement et les lecteurs de carte sécurisés approuvés par PCI qui chiffrent les données de carte le font en utilisant la technologie SRED (lecture et échange sécurisés des données). Demandez à votre fournisseur si votre terminal de paiement chiffre les données de carte avec la technologie SRED.

Les sites de e-commerce doivent chiffrer les données de carte qui sont envoyées sur Internet, par exemple, en utilisant le protocole TLS (Transport Layer Security). Demandez à votre prestataire de services comment il chiffre les données de carte.

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

OÙ TROUVER DE L'AIDE ?

Ressources

LISTE DU CONSEIL PCI	
Ressource	**URL**
Liste d'applications de paiement validées	*https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement*
Liste des dispositifs PTS approuvés	*https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices*
Liste des prestataires d'analyse agréés	*https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors*
Liste des revendeurs et intégrateurs qualifiés	*https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers*
Liste des solutions P2PE conformes	*https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions*

LISTES DES MARQUES DE PAIEMENT		
Ressource		**URL**
Liste des prestataires de services conformes	Liste des prestataires de services conformes de MasterCard	*https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html recommendations/merchants-need-to-know.html*
	Registre mondial des prestataires de services de Visa	*http://www.visa.com/splisting/*
	Opérateurs certifiés par Visa Europe	*https://www.visaeurope.com/receiving-payments/security/downloads-and-resources resources*

NORME PCI DSS ET CONSIGNES ASSOCIÉES	
Ressource	**URL**
En savoir plus sur la norme PCI DSS	*https://www.pcisecuritystandards.org/pci_security/how*
Questionnaires d'auto-évaluation PCI DSS	*https://www.pcisecuritystandards.org/pci_security/completing_self_assessment*
Guide : Prévention du clonage de carte : présentation des meilleures pratiques pour commerçants	*https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf*

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Ressources

INFOGRAPHIES ET VIDÉOS	
Ressource	**URL**
Infographie : Il est temps de modifier votre mot de passe	*https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf*
Infographie : Lutter contre la cybercriminalité en dévaluant les données volées	*https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf*
Vidéo : Tout apprendre sur la sécurité des mots de passe en 2 minutes	*https://www.youtube.com/watch?v=FsrOXgZKa7U*
Vidéo : Mots de passe	*https://www.youtube.com/watch?v=dNVQk65KL8g*
Infographie : Mots de passe	*https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf*
Vidéo : Application de correctifs	*https://www.youtube.com/watch?v=0NGz1mGO3Jg*
Infographie : Application de correctifs	*https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf*
Vidéo : Accès à distance	*https://www.youtube.com/watch?v=MxgSNFgvAVc*
Infographique : Accès à distance	*https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.pdf*
PRINCIPES ESSENTIELS DE SÉCURITÉ DES DONNÉES PCI POUR PETITS COMMERÇANTS ET DIRECTIVES CONNEXES	
Ressource	**URL**
Systèmes de paiement courants	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf*
Questions à poser aux fournisseurs pour les petits commerçants	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf*
Glossaire des petits commerçants	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*
Infographie : Principes de base des pare-feux	*https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf*
Outil d'évaluation : Aperçu des acquéreurs	*https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf*
Outil d'évaluation : Aperçu des petits commerçants	*https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf*

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

Sources et références utiles

Département britannique de la culture, des médias et des sports – *Enquête 2017 sur les atteintes à la cybersécurité*

Institut Ponemon – *État en 2016 de la cybersécurité dans les petites et moyennes entreprises (PME) (Sponsorisé par Keeper Security), juin 2016*

National Cyber Security Centre du Royaume-Uni – *Guide de la cybersécurité pour les petites entreprises, 2017*

Beaming UK – *Les violations de sécurité informatique ont coûté aux entreprises britanniques près de 30 milliards de livres sterling en 2016, mars 2017*

Verizon 2017 – *Rapport d'enquête sur la violation de données de Verizon*

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.

À propos du Conseil des normes de sécurité PCI

Le *Conseil des normes de sécurité PCI* est un forum international permettant au secteur de se réunir pour développer, améliorer, diffuser et aider à la compréhension des normes de sécurité pour la protection des comptes de paiement. Pour en savoir plus sur l'initiative d'engagement pour la sécurité mondiale des paiements de PCI SSC, consultez le document à l'adresse *www.pcisecuritystandards.org/pdfs/PCI_SSC_Partnering_for_ Global_Payment_Security.pdf*

Le Conseil gère, fait évoluer et promeut les normes de sécurité du secteur des cartes de paiement. Il fournit également les outils essentiels nécessaires à la mise en œuvre des normes, tels que l'évaluation et l'analyse des qualifications, les questionnaires d'auto-évaluation, la formation et la sensibilisation, et les programmes de certification des produits.

Les membres fondateurs du Conseil, American Express, Discover Financial Services, JCB International, MasterCard et Visa Inc. ont convenu d'intégrer la norme de sécurité des données PCI (PCI DSS) dans les exigences techniques de chacun de leurs programmes de conformité en matière de sécurité des données. Chaque membre fondateur reconnaît également les évaluateurs de sécurité qualifiés et les prestataires de services d'analyse agréés, qualifiés par le Conseil des normes de sécurité PCI.

Les cinq marques de paiement, ainsi que les membres stratégiques, partagent de manière égale la gouvernance du Conseil, ont une contribution égale au Conseil des normes de sécurité PCI et partagent la responsabilité de mener à bien le travail de l'organisation. Les autres parties prenantes du secteur sont encouragées à rejoindre le Conseil en tant que membres stratégiques ou affiliés et organisations
participantes pour examiner les ajouts ou modifications proposés aux normes. Les organisations participantes peuvent être des commerçants, des banques, des processeurs de paiement, des développeurs de matériel et de logiciels, et des fournisseurs de points de vente.

Ce guide fournit des informations supplémentaires qui ne remplacent pas ou n'annulent pas les normes de sécurité PCI SSC ou leurs documents d'appui.

FONDATEURS DE PCI SSC

ORGANISATIONS PARTICIPANTES

Commerçants, banques, processeurs de paiement, développeur de matériel et de logiciels et fournisseurs de points de vente

Copyright 2018 PCI Security Standards Council, LLC. Tous droits réservés.