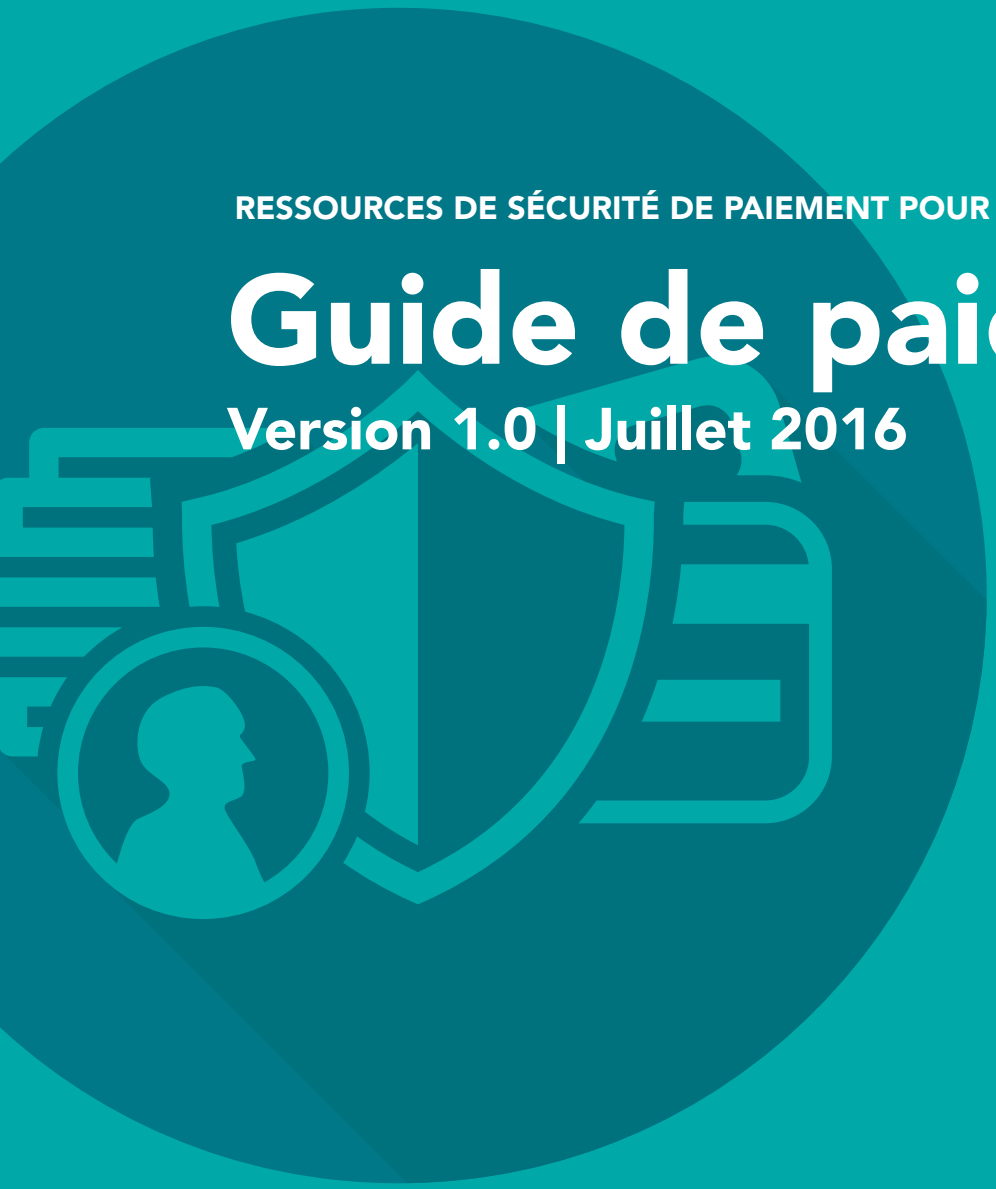
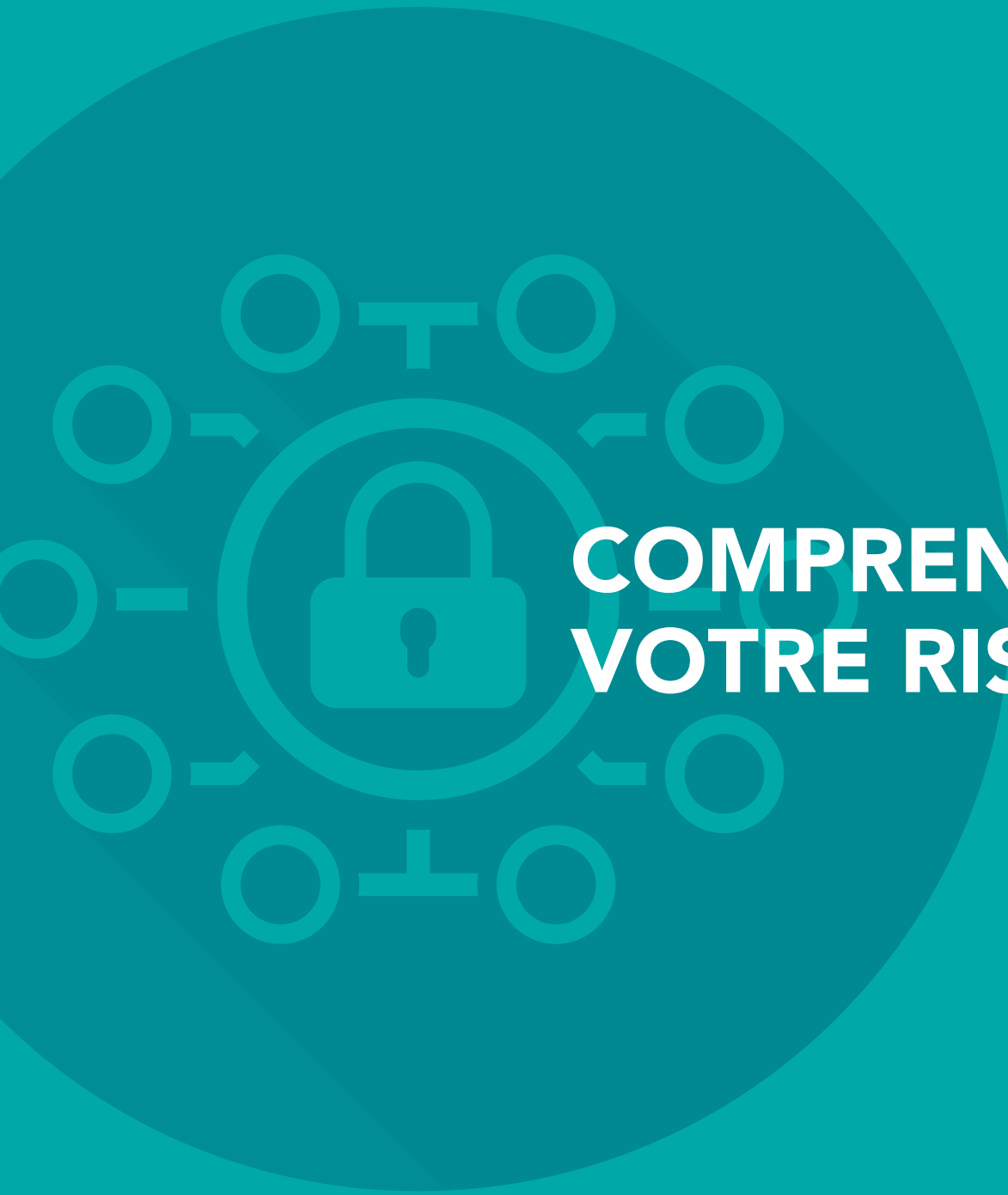


RESSOURCES DE SÉCURITÉ DE PAIEMENT POUR PETITS COMMERÇANTS

Guide de paiement sécurisé

Version 1.0 | Juillet 2016

PCI Security Standards Council®



COMPRENDRE VOTRE RISQUE

Comprendre votre risque

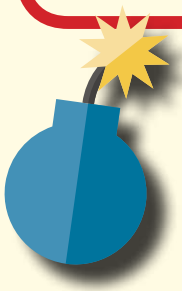
En tant que petite entreprise, vous êtes une cible parfaite pour les voleurs de données.

Lorsque vos données de cartes de paiement font l'objet d'une violation, les conséquences peuvent se montrer rapidement. Vos clients perdent leur confiance en votre capacité à protéger leurs informations personnelles. Ils s'en occupent par eux-mêmes. Cela peut engendrer d'éventuelles pénalités financières et des dommages découlant de procès et votre entreprise risque de perdre sa capacité à accepter les cartes de paiement. Un sondage réalisé 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)*

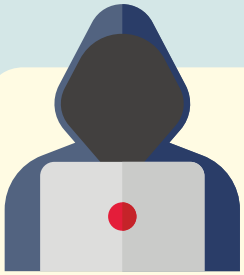
60 %

DES PETITES ENTREPRISES ONT CONNU UNE VIOLATION DE DONNÉES SUR INTERNET.
(HM Government)

20 752 USD



DE COÛT MOYEN POUR UNE PETITE ENTREPRISE DÛ À DU PIRATAGE, S'ÉLEVANT À 8 600 USD EN 2013.
(NSBA)



71 %

DES PIRATES INFORMATIQUES S'EN PRENNENT AUX ENTREPRISES DE MOINS DE 100 EMPLOYÉS
(Verizon 2012)

69 %

DES CONSOMMATEURS AMÉRICAINS ONT PEUR QUE LEURS DONNÉES DE CARTES DE PAIEMENT SOIENT DÉROBÉES.
(Gallup)

PCI Security Standards Council

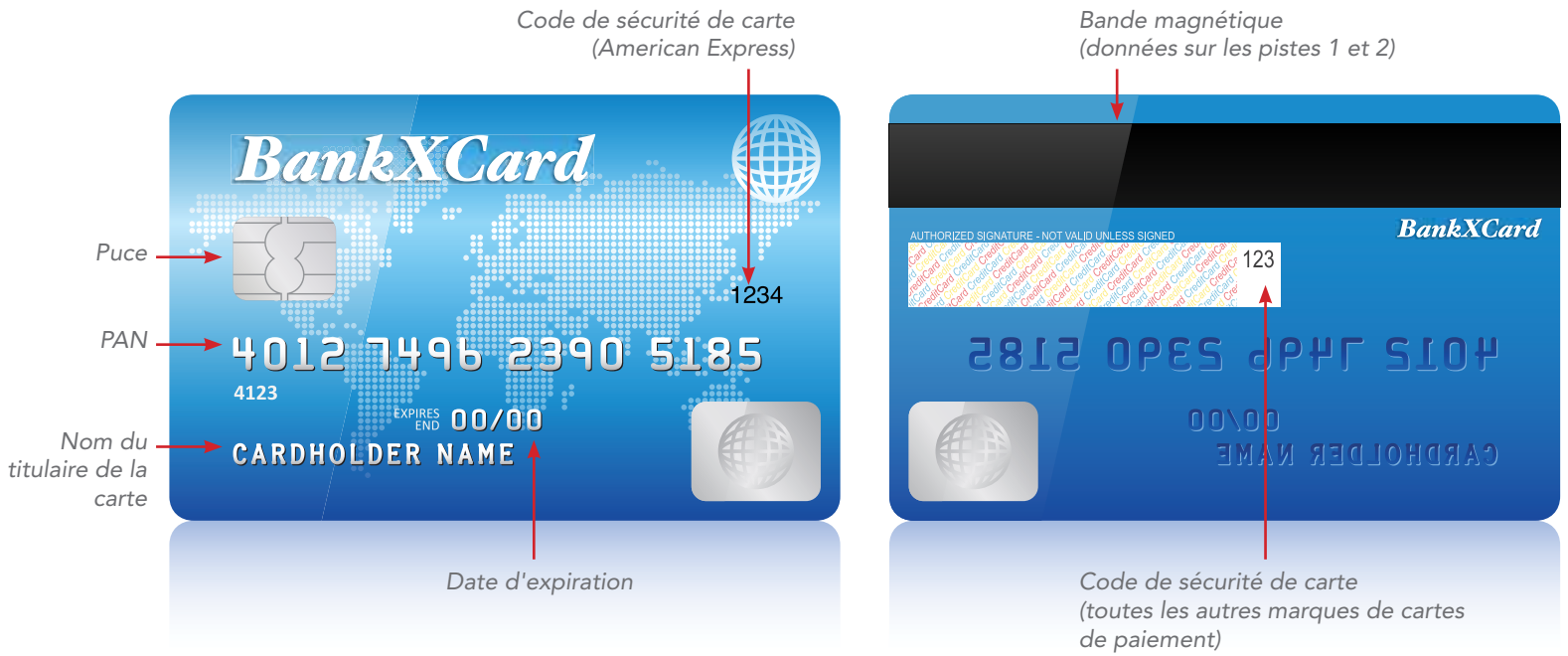
Quels éléments sont concernés par ces risques ?

LES DONNÉES DE CARTE 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.

Des exemples de données de cartes de paiement sont le numéro de compte principal (PAN) et le code de sécurité de carte à trois ou quatre chiffres. Les flèches rouges en dessous des différents types de données requérant 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 d'exigences de sécurité qui peuvent aider les petits commerçants à protéger les données de carte de leurs clients se trouvant sur les cartes de paiement.

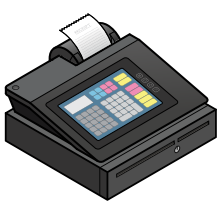
Les petits commerçants peuvent se familiariser avec la validation de leur conformité à la norme PCI DSS via un questionnaire d'auto-évaluation (SAQ).

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

Comprendre votre système de paiement : Termes courants relatifs au paiement

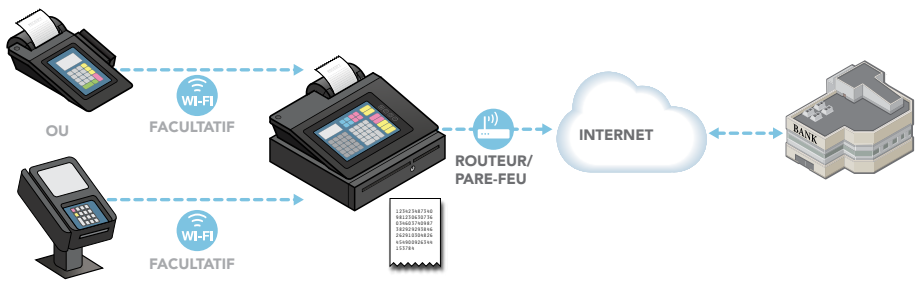
En fonction de là où vous vous trouvez dans le monde, l'équipement utilisé pour accepter les paiements possède des noms différents. Voici les types dont nous parlons dans ce document et comment ils sont communément appelés.

Un **TERMINAL DE PAIEMENT** est l'appareil utilisé pour accepter les paiements par carte client 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.

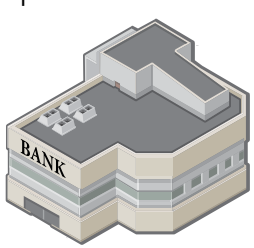


Une **CAISSE ENREGISTREUSE ÉLECTRONIQUE** (ou tiroir-caisse) enregistre et calcule les transactions et peut imprimer des tickets de caisse, mais elle n'accepte pas les paiements par carte client.

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.



Un **SYSTÈME DE PAIEMENT** englobe le processus entier d'acceptation des paiements par carte dans un magasin de vente au détail (notamment les magasins/boutiques et les vitrines virtuelles de commerce en ligne). Il 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), des serveurs avec des éléments de commerce en ligne, tels que des pages de paiement et les connexions sortantes vers la banque marchande.



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

Quel est le risque pour votre entreprise ?

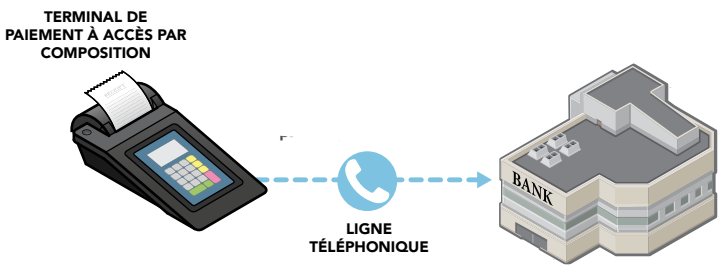
Plus votre système possède de fonctionnalités, plus il est difficile à sécuriser. Ces fonctions complémentaires constituent souvent des moyens faciles pour les criminels à dérober les données de carte de vos clients. Pensez soigneusement à si vous avez vraiment besoin de ces fonctionnalités complémentaires (par exemple, la connexion Wi-Fi ou les caméras) pour votre entreprise.

Comment vendez-vous vos biens et services ? Il existe trois méthodes principales :

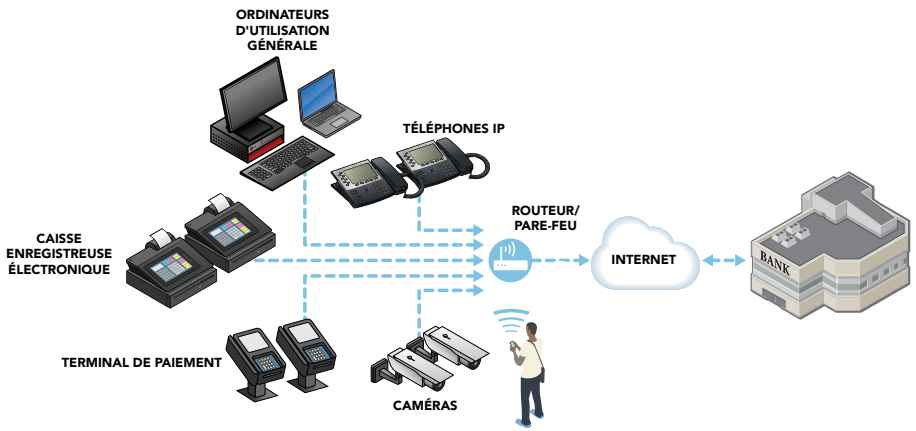
1. *Une personne entre dans votre magasin et fait un achat avec sa carte.*
2. *Une personne consulte votre site Internet et paie en ligne.*
3. *Une personne appelle votre magasin et fournit les détails de sa carte par téléphone ou les envoie par e-mail ou par fax.*

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

Système de commerce en ligne complexe pour les achats de boutiques en ligne, avec le commerçant qui gère son propre site Internet et la page de paiement

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 conversation avec votre banque marchande et vos partenaires fournisseurs.

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 :

	Procédure pour protéger votre entreprise contre les violations de données	Coût	Simplicité	Atténuation des risques
	Utilisez des mots de passe complexes et modifiez les mots de passe par défaut.	1	1	3
	Protégez vos données de carte et conservez uniquement ce dont vous avez besoin.	1	1	2
	Inspectez les terminaux de paiement pour vérifier qu'ils ne sont pas modifiés.	1	1	2
	Installez les correctifs fournis par vos fournisseurs.	1	2	3
	Faites appel à des partenaires commerciaux de confiance et connaissez la méthode de prise de contact avec eux.	1	1	1
	Protégez l'accès en interne à vos données de carte.	1	2	2
	Ne facilitez pas l'accès des hackers à vos systèmes.	2	2	3
	Utilisez des logiciels antivirus.	2	2	2
	Recherchez les vulnérabilités et corrigez les problèmes.	2	2	3
	Utilisez des solutions et des terminaux de paiement sécurisés.	3	2	3
	Protégez votre entreprise contre Internet.	2	3	3
	Pour une protection optimale, rendez vos données inutiles pour les criminels.	3	3	3

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

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

Coût

Simplicité

Atténuation des risques

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 aide à 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.

À propos

80 % **des violations de données impliquent des mots de passe devinés ou volés.**

Verizon PCI 2015

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 définissez-en des nouveaux tous les trois mois.

DEMANDEZ DE L'AIDE. Posez des questions à vos fournisseurs ou prestataires de services concernant les mots de passe par défaut et la procédure à suivre pour les modifier. Puis faites-le !

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 « Steak&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.

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

INFOGRAPHIE
Il est temps de modifier votre mot de passe

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

Les mots de passe par défaut typiques DOIVENT ÊTRE modifiés :

[aucun]

[nom du produit/ fournisseur]

1234 ou 4321

accès

admin

anonyme

basedonnées

invité

gestionnaire

mdp

motdepasse

racine

as

secret

adminsys

utilisateur

PCI Security Standards Council

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

Coût
Simplicité
Atténuation des risques

Il est impossible de protéger les données de carte si vous ne savez pas ce que c'est.

Que pouvez-vous faire ?

La segmentation des données a un objectif similaire à celui du cryptage, mais elle fonctionne différemment. Elle consiste à substituer les données de carte par des données dénuées de sens (un « token ») qui n'a aucune valeur pour un hacker.

DEMANDEZ DE L'AIDE À UN SPÉCIALISTE. Demandez au fournisseur de votre terminal de paiement ou à votre banque marchande où vos systèmes stockent les données 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 22 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 ranger 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 détails 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 cryptage ou de segmentation des données qui rendent les données de carte inutilisables même si elles sont dérobées. (Pour en savoir plus, reportez-vous à la section « » en page 19.)

AMORCE SUR LE CRYPTAGE

La cryptographie utilise une formule mathématique pour rendre le texte brut illisible aux personnes ne disposant pas de connaissances spéciales (formule appelée « clé »). La cryptographie est appliquée sur les données stockées et transférées sur un réseau.

LE CRYPTAGE ***permet de changer le texte brut en texte chiffré.***

LE DÉCRYPTAGE ***permet de changer le texte chiffré en texte brut.***

Par exemple :

Ceci est secret ; ne pas

CLÉ DE CRYPTAGE

5a0 (k$hQ%...

CLÉ DE DÉCRYPTAGE

Ceci est secret ; ne pas

PCI Security Standards Council

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

Coût
Simplicité
Atténuation des risques

Les « dispositifs de copiage de carte » balayent 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 identifier un dispositif de copiage de carte. Vous devez régulièrement vérifier vos terminaux de paiement afin de vous assurer qu'ils n'ont pas été modifiés. Tenez un registre ou un journal des terminaux qui ont été vérifiés, quand, par qui et si quelque chose a été trouvé.

Reportez-vous que PCI Council's guide: Skimming Prevention – Overview of Best Practices for Merchants (Guide de PCI Council : Prévention du copiage de carte – Présentation des meilleures pratiques pour commerçants)

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 cassé sur les caches d'accès ou les vis, un câblage étrange/différent, ou de nouveaux dispositifs ou fonctionnalités que vous ne reconnaissez pas. Le guide de PCI Council (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.

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

Installez les correctifs fournis par vos fournisseurs.

Coût
Simplicité
Atténuation des risques

Souvent, le logiciel contient des défauts ou des erreurs faites par les programmateurs lorsqu'ils écrivent le code (également appelés brèches 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 » remis par le fournisseur visant à corriger les erreurs de codage. Il est essentiel d'installer les correctifs de sécurité en temps opportun !

DEMANDEZ à votre fournisseur ou prestataire de services comment il vous informe 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, systèmes d'exploitation, etc. de sorte qu'ils puissent prendre en charge les derniers correctifs de sécurité. Posez-leur des questions.

COMMERÇANTS DE COMMERCE EN LIGNE. Installer des correctifs dès que possible est très important pour vous aussi. Vérifiez régulièrement auprès de votre prestataire de services de paiement s'il n'y a pas de correctifs disponibles. Demandez à votre fournisseur d'hébergement de commerce en ligne 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 de commerce en ligne et/ou l'application Web, de sorte qu'ils puissent prendre en charge les derniers correctifs.

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

PCI Security Standards Council

Faites appel à des partenaires commerciaux de confiance et connaissez la méthode de prise de contact avec eux.

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. Vous pouvez les appeler services de traitement, fournisseurs, tiers ou prestataires de services. Tous les éléments précités 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. Maintenez que vous savez qui appeler, gardez les noms des entreprises et des contacts, les numéros de téléphone, les adresses des sites Internet et autres coordonnées de contact, 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 commerçants de commerce en ligne, 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 22 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 vous aider à savoir quelles questions poser.

AYEZ CONNAISSANCE DES 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 fournisseurs 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 de commerce en ligne

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)

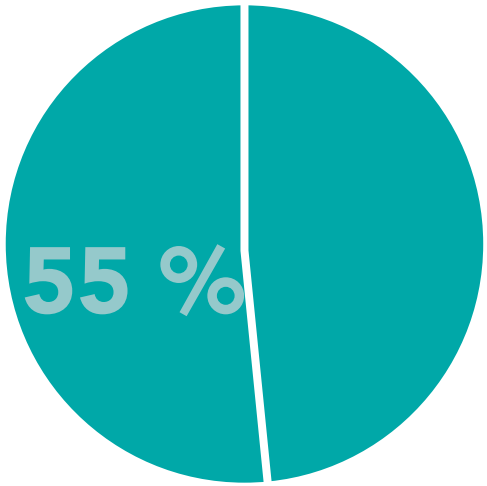
Protégez l'accès en interne à vos données.

Coût
Simplicité
Atténuation des risques

L'abus de privilège signifie 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.

L'ABUS DE PRIVILÈGE EST LA PRINCIPALE ACTION ENGENDRANT DES VIOLATIONS DE DONNÉES : ENVIRON 55 % DE L'ENSEMBLE DES INCIDENTS SIGNALÉS.



Verizon 2015

LE CONTRÔLE D'ACCÈS EST DE LA PLUS GRANDE IMPORTANCE. Configurez votre système de sorte d'autoriser l'accès en se basant uniquement sur le principe « besoin de 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 cryptées 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 en caisse » 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 et partenaires commerciaux de sorte qu'ils sachent ce que l'on attend d'eux.

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 avoir du tout accès.

PCI Security Standards Council

Ne facilitez pas l'accès des hackers à vos systèmes.

Coût
Simplicité
Atténuation des risques

HACKERS = CRIMINELS

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 à plusieurs facteurs utilise un nom d'utilisateur et un mot de passe, plus au moins un autre facteur (comme une carte à puce, une clé électronique* ou un code à usage unique).

**un dispositif pratique qui se connecte à un ordinateur pour autoriser l'accès à des fonctions logicielles sans fil, 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 votre entreprise.

DEMANDEZ COMMENT FAIRE POUR LIMITER L'UTILISATION DE L'ACCÈS À DISTANCE. De nombreux programmes d'accès à distance sont toujours activés par défaut. Réduisez votre risque : demandez à votre fournisseur comment faire pour désactiver l'accès à distance lorsque vous n'en avez pas besoin et comment faire pour l'activer lorsque votre fournisseur ou prestataire de services vous le demande spécifiquement.

DÉSACTIVEZ-LE UNE FOIS QUE VOUS AVEZ TERMINÉ.

UTILISEZ UNE AUTHENTIFICATION FORTE. Si vous devez autoriser l'accès à distance, exigez une authentification à plusieurs facteurs et une cryptographie 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) ou de vous aider à configurer une authentification à plusieurs facteurs. Reportez-vous au document *Questions à poser à vos fournisseurs* pour vous aider à savoir exactement quelles questions leur poser.

Si votre fournisseur offre l'assistance pour ou dépanne votre terminal de paiement depuis ses locaux (et non sur votre site), il utilise Internet et un logiciel d'accès à distance pour le faire.

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

PCI Security Standards Council

Utilisez des logiciels antivirus.

Coût

Simplicité

Atténuation des risques

Les systèmes et logiciels sont extrêmement flexibles et offrent un vaste éventail de fonctions et fonctionnalités. Les hackers écrivent des virus et d'autres codes malveillants pour exploiter ces fonctionnalités et les erreurs de codage, afin de pénétrer dans vos systèmes et dérober les données de carte. Utiliser un logiciel anti-virus (également appelé antiprogramme malveillant) aide à protéger vos systèmes.

INSTALLEZ UN LOGICIEL ANTI-VIRUS 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.

RÉGLEZ LE LOGICIEL SUR « MISE À JOUR AUTOMATIQUE » de sorte que vous bénéficiez toujours 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 par 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.

Recherchez les vulnérabilités et corrigez les problèmes.

Coût
Simplicité
Atténuation des risques

Les nouvelles vulnérabilités, brèches de sécurité et bugs sont détectés quotidiennement. Il est essentiel de faire tester vos systèmes Internet régulièrement pour identifier ces nouveaux risques et les pallier dans les plus brefs délais. Vos systèmes Internet (comme beaucoup de systèmes de paiement) sont les plus vulnérables car ils peuvent facilement être exploités par les criminels, ce qui leur permet de pénétrer dans vos systèmes.

Les prestataires de services d'analyse approuvés par le conseil de PCI (ASV) effectuent l'analyse des vulnérabilités externes et génèrent les rapports associés. Voir la List of PCI-Approved Scanning Vendors (liste des prestataires de services d'analyse agréés par PCI)

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 prestataires peuvent vous aider avec les outils qui analysent automatiquement votre réseau afin de trouver des vulnérabilités. Ils vous fournissent également un rapport si, par exemple, vous devez appliquer un correctif. La liste de PCI Council (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.

VULNÉRABILITÉS DES ADRESSES. Demandez à votre ASV de vous aider à résoudre les problèmes identifiés par l'analyse.

Utilisez des solutions et des terminaux de paiement sécurisés.

Coût
Simplicité
Atténuation des risques

Un moyen sûr de protéger votre société consiste à utiliser des solutions de paiement sécurisé et de faire appel à des professionnels pour vous aider. C'est le meilleur moyen de choisir des produits sécurisés et de s'assurer qu'ils sont configurés de manière sécurisée.

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 *List of PCI Approved PTS Devices (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 *List of PCI Validated Payment Applications. (Liste des applications de paiement validées par PCI.)*

FAITES APPEL À DES PROFESSIONNELS QUALIFIÉS. Assurez-vous que l'installateur de votre application PA-DSS validée l'installe correctement et de façon sécurisée. Choisissez parmi la *List of PCI QIRs (Liste des QIR de PCI)* pour connaître les sociétés qualifiées par le conseil de PCI pour vous aider. Demandez à votre commerçant de vous faire votre sélection.

CONSULTEZ LA LISTE DES QUESTIONS À POSER À VOS FOURNISSEURS. Utilisez le document *Questions à poser à vos fournisseurs* pour vous aider à leur poser les bonnes questions.

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 mes données PIN de vos clients.

Pour les terminaux de paiement et les lecteurs de carte sécurisés de PCI qui cryptent les données de carte, voir la page 19.

PCI Security Standards Council

Protégez votre entreprise contre Internet.

Coût
Simplicité
Atténuation des risques

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 société est sur Internet, tout ce que vous utilisez pour les paiements par carte nécessite une protection complémentaire.

UTILISATION ISOLÉE. N'utilisez pas l'appareil avec lequel vous acceptez les paiements à toute autre fin. Par exemple, ne naviguez pas sur le Web ou les réseaux sociaux ni ne vérifiez vos e-mails à partir de l'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 informations et à vos ordinateurs. 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, connexion à un Wi-Fi public).

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 conserver de façon sécurisée est de les rendre inutiles avant qu'elles ne soient volées en les cachant 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.

DEMANDEZ À VOTRE PRESTATAIRE DE SERVICES OU À VOTRE FOURNISSEUR DE SYSTÈMES DE PAIEMENT si votre terminal de paiement utilise une technologie de cryptage et/ou de segmentation.

UTILISEZ DES DISPOSITIFS PCI QUI CRYPTENT LES DONNÉES DE CARTES. Le conseil PCI approuve les terminaux de paiement qui protègent les données du code PIN (voir  sur la page 17) et les terminaux de paiement ainsi que les « lecteurs de carte sécurisés » qui cryptent davantage les données de carte. Voir la *List of PCI Approved PTS Devices (Liste des dispositifs PTS approuvés par PCI)*.

UTILISEZ DES SOLUTIONS DE CRYPTAGE PCI SÉCURISÉES. Demandez si le cryptage de votre terminal de paiement est effectué via une solution de cryptage point en point et s'il figure sur la *List of PCI P2PE Validated Solutions (Liste des solutions P2PE conformes de PCI)*.

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 cryptage et de segmentation pour dévaluer les données de carte pour les hackers.

FAITES-VOUS PARTIE DES COMMERÇANTS PASSANT DÉSORMAIS AUX TERMINAUX À PUCE EMV ? C'est une grande opportunité pour investir dans un terminal prenant en charge la norme EMV et apportant également la sécurité supplémentaire du cryptage et de la segmentation.

RENSEIGNEZ-VOUS. Voir le document *questions à poser à vos fournisseurs* pour vous aider à leur poser les bonnes questions.

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

PCI Security Standards Council

OÙ TROUVER DE L'AIDE ?

Ressources

Listage du conseil de PCI

Ressource	Lien	URL
List of Validated Payment Applications (Liste d'applications de paiement validées)	PCI Council's Validated Payment Applications (Applications de paiement validées par le conseil de PCI)	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices (Liste des dispositifs PTS approuvés)	PCI Council's Approved PTS Devices (Dispositifs PTS approuvés par le conseil de PCI)	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors (Liste des prestataires d'analyse agréés)	PCI Council's Approved Scanning Vendors (Prestataires d'analyse agréés par le conseil de PCI)	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers (Liste des revendeurs et intégrateurs qualifiés)	PCI Council's Qualified Integrators Resellers (Revendeurs et intégrateurs qualifiés par le conseil de PCI)	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions (Liste des solutions P2PE conformes)	PCI Council's P2PE Validated Solutions (Solutions P2PE validées par le conseil de PCI)	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Listes des marques de paiement

Ressource	Lien	URL
Lists of Compliant Service Providers (Liste des prestataires de services conformes)	MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard)	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa)	http://www.visa.com/splisting/
	Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

Norme PCI DSS et directives associées

Ressource	Lien	URL
More about PCI DSS (En savoir plus sur la norme PCI DSS)	How to Secure with PCI DSS (Comment renforcer la sécurité avec la norme PCI DSS)	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires (Questionnaires d'auto-évaluation PCI DSS)	Self-Assessment Questionnaires (Questionnaires d'auto-évaluation)	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants (Guide : prévention contre le copiage de carte : présentation des meilleures pratiques pour commerçants)	Skimming Prevention: Overview of Best Practices for Merchants (Prévention contre le copiage de carte : présentation des meilleures pratiques pour commerçants)	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Ressources

Infographies et vidéos

Ressource	Lien	URL
Infographie : Il est temps de modifier votre mot de passe	*It's Time to Change Your Password (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	*Fight Cybercrime by Making Stolen Data Worthless to Thieves (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	*Learn Password Security in 2 Minutes (Tout apprendre sur la sécurité des mots de passe en 2 minutes)*	*https://www.youtube.com/watch?v=FsrOXgZKa7U*

Ressources de sécurité de paiement PCI pour petits commerçants

Ressource	Lien	URL
Systèmes de paiement courants	*Systèmes de paiement courants*	*https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf*
Questions de petits commerçants pour les fournisseurs	*Questions de petits commerçants pour les fournisseurs*	*https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf*
Glossaire des petits commerçants	*Glossaire des petits commerçants*	*https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf*

Sources

Gallup – *Gallup Poll (Sondage Gallup)*, octobre 2015

HM Government - *Small Businesses: What You Need to Know about Cyber Security (PME : ce que vous devez savoir sur la cybersécurité)*, Royaume-Uni, 2014

NCSA – *National Cyber Security Alliance survey (Étude de l'Alliance nationale de cybersécurité)*, 2012

NSBA – National Small Business Administration (Administration nationale des petites entreprises), *2014 Year End Economic Report (Rapport économique de fin d'année 2014)*

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report (Rapport d'enquêtes sur les violations de données 2012 Verizon)*

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report (Rapport d'enquêtes sur les violations de données 2015 Verizon)*

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report (Rapport de conformité 2015 Verizon)*