RESSOURCES DE SÉCURITÉ DE PAIEMENT POUR PETITS COMMERÇANTS

Glossaire des termes de paiement et de sécurité des informations

VERSION 1.0 | JUILLET 2016

PCI Security Standards Council®

Introduction

Ce *Glossaire des termes de paiement et de sécurité des informations* vient en complément du *Guide de paiement sécurisé*, faisant partie du document Ressources de sécurité de paiement pour petits commerçants. Il vise à expliquer les termes pertinents de l'industrie des cartes de paiement (PCI) et de la sécurité des informations dans un langage compréhensible.

Les définitions des termes portant une astérisque (*) sont fondées sur/dérivent des définitions du document *Industrie des cartes de paiement (PCI), norme de sécurité des données (DSS)* et *norme de sécurité des données d'application de paiement (PA-DSS) : Glossaire des termes, abréviations et acronymes*, Version 3.2, avril 2016.

Veuillez vous reporter au *Guide de paiement sécurisé* et aux autres Ressources de sécurité de paiement pour petits commerçants, aux endroits suivants :

RESSOURCE	URL
Guide de paiement sécurisé	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Systèmes de paiement courants	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Questions à poser à vos fournisseurs	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

Remarque :
La dernière version de *Industrie des cartes de paiement (PCI), norme de sécurité des données (DSS) et norme de sécurité des données d'application de paiement (PA-DSS) : Glossaire de termes, abréviations et acronymes* est considérée comme la source faisant autorité et doit être consultée pour obtenir les définitions actuelles et complètes de PCI DSS et PA-DSS.

Glossaire

TERME	DÉFINITION
Acquéreur *	Voir *banque marchande* et *service de traitement de paiement*.
Logiciel antivirus *	Programme informatique qui détecte, supprime, retire et assure une protection contre les logiciels malveillants (également appelés « maliciels »), notamment les virus, vers, chevaux de Troie, spywares ou logiciels espions, adware ou publiciel et outils de dissimulation d'activité. Également appelés « logiciel anti logiciel malveillant ou anti malware. »
Application *	Programme informatique ou groupe de programmes fonctionnant sur ordinateur, tablette, serveur interne ou serveur Web.
Prestataire de services d'analyse agréé (ASV) *	Société agréée par le PCI SSC offrant des services d'analyse dans le but d'identifier des faiblesses dans la configuration du système. Voir également *ASV*.
ASV *	Acronyme d'« Approved Scanning Vendor », prestataire de services d'analyse agréé.
Authentification *	Processus de vérification de l'identité d'une personne, d'un dispositif ou d'un processus. L'authentification se fait généralement par l'utilisation d'un ou plusieurs facteurs d'authentification, tels que : • Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; • Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; • Quelque chose que vous détenez, comme une mesure biométrique.
Autorisation *	Lors d'une transaction par carte de paiement, l'autorisation est donnée lorsque le commerçant reçoit l'approbation de la transaction une fois que l'acquéreur a validé la transaction avec l'émetteur/le processeur.
Numéro d'identification bancaire (BIN)	Les six premiers chiffres (ou plus) d'un numéro de carte de paiement identifiant l'établissement financier qui émet la carte de paiement pour le titulaire de carte.
Besoin de connaître	Accès à des systèmes ou à des données accordé selon le principe du « besoin de connaître » d'un utilisateur (uniquement ce qui est nécessaire par rapport aux fonctions professionnelles d'un utilisateur).
Données de carte/Données de carte client *	Les données de carte désignent au minimum le numéro de compte primaire (PAN) et peuvent inclure également le nom du titulaire de carte et la date d'expiration. Le PAN est visible au recto de la carte et est encodé dans la bande magnétique et/ou la puce intégrée de la carte. Également appelé « données du titulaire ». Voir également *Données d'authentification sensibles* pour plus d'informations sur les autres éléments pouvant être transmis ou traités (mais non stockés) dans le cadre d'une transaction de paiement.
Puce	Également appelé « puce EMV ». Microprocesseur (ou « puce ») d'une carte de paiement utilisé lors du traitement de transactions selon les spécifications internationales relatives aux transactions EMV.

Glossaire

TERME	DÉFINITION
Puce et PIN	Processus de vérification durant lequel un consommateur saisit son code PIN sur un terminal de paiement à puce EMV lors d'un achat de biens ou de services.
Puce et signature	Processus de vérification durant lequel un consommateur utilise sa signature sur un terminal de paiement à puce EMV lors d'un achat de biens ou de services.
Justificatif d'authentification	Informations utilisées pour identifier et authentifier un utilisateur afin qu'il puisse accéder à un système. Le nom d'utilisateur et le mot de passe sont des justificatifs d'authentification répandus. L'empreinte digitale, la lecture rétinienne ou un code à utilisation unique généré par un « générateur de jeton » portable sont d'autres formes de justificatifs d'authentification. La sécurité est plus élevée lorsque plusieurs justificatifs d'authentification sont demandés pour obtenir un accès.
Cyberattaque	Tout type de tentative offensive ayant pour but de s'introduire par effraction dans un ordinateur ou un système. Installer un spyware sur un ordinateur, s'introduire par effraction dans un système de paiement pour dérober des données de carte ou tenter de couper l'alimentation d'une infrastructure critique telle qu'un réseau électrique sont des exemples de cyberattaques.
Violation de données	Incident durant lequel des données sensibles peuvent être potentiellement visualisées, dérobées ou utilisées par une partie non autorisée. Les violations de données peuvent concerner des données de carte, des informations personnelles relatives à la santé (PHI), des informations permettant une identification personnelle (PII), des secrets industriels ou la propriété intellectuelle, etc.
Mot de passe par défaut	Mot de passe simple attribué avec un nouveau logiciel ou un nouvel équipement informatique. Les mots de passe par défaut (comme « admin » ou « motdepasse » ou « 123456 ») sont facilement identifiables et sont généralement disponibles via une recherche en ligne. Ils ne visent qu'à remplacer le mot de passe de façon temporaire et n'offrent aucune véritable sécurité. Ils doivent être remplacés par un mot de passe plus sécurisé, une fois que l'installation du nouveau logiciel ou du nouvel équipement informatique est terminée.
Caisse enregistreuse électronique (ECR)	Dispositif qui enregistre et calcule les transactions et peut imprimer des tickets de caisse, mais qui n'accepte pas les paiements par carte client. Également appelée « tiroir-caisse ».
Cryptage	Processus utilisant la cryptographie pour convertir des informations de façon mathématique en une forme inutilisable, sauf pour les détenteurs d'une clé numérique spécifique. L'utilisation du cryptage protège les informations en les dévaluant pour les criminels. Voir également *cryptographie*.
Pare-feu *	Matériel et/ou logiciel protégeant les ressources réseau contre les accès non autorisés. Un pare-feu autorise ou bloque la communication circulant entre des ordinateurs ou des réseaux de différents niveaux de sécurité, selon un ensemble de règles et d'autres critères.
Enquêteur judiciaire	Les enquêteurs judiciaires PCI (PFI) sont des sociétés agréées par le conseil de PCI qui aident à déterminer quand et comment une violation de données de carte peut se produire. Ils mènent des enquêtes au sein du secteur financier à l'aide d'outils et de méthodologies d'investigation éprouvés. Ils travaillent également avec les forces de l'ordre pour apporter un soutien aux parties prenantes lors de toute enquête criminelle.

Glossaire

TERME	DÉFINITION
Hacker (pirate)	Personne ou organisation qui tente de contourner les mesures de sécurité de systèmes informatiques pour s'emparer de leur accès ou de leur contrôle. Le but étant habituellement de dérober des données de carte.
Fournisseur d'hébergement *	Offre des services divers à des commerçants et autres prestataires de services. Les données de leurs clients sont « hébergées » ou résidentes sur les serveurs du fournisseur. Les services comprennent généralement un espace partagé par plusieurs commerçant sur un serveur, la fourniture d'un serveur pour un seul commerçant ou encore des applications Web telles qu'un site Internet disposant d'un « panier d'achat ».
Terminal de paiement intégré	Appareil combinant un terminal de paiement à une caisse enregistreuse électronique qui accepte les paiements, enregistre et calcule les transactions et imprime des tickets de caisse.
Intégrateur/revendeur	Société qui installe/configure (et/ou propose une assistance) des terminaux de paiement, systèmes de paiement et/ou applications de paiement pour commerçants. Ces sociétés peuvent également vendre les dispositifs ou applications de paiement dans le cadre de leurs services. Voir également *revendeur ou intégrateur qualifié (QIR)*.
Journal *	Fichier créé automatiquement lorsque certains événements prédéfinis (souvent liés à la sécurité) se produisent au sein d'un système ou réseau informatique. Les données de journal incluent l'horodatage, la description et les informations uniques relatives à cet événement. Ces fichiers sont utiles pour résoudre les problèmes techniques ou pour les enquêtes sur des violations de données. Également appelé « journal d'audit » ou « vérification à rebours ».
Logiciel malveillant *	Logiciel malveillant conçu pour s'infiltrer dans un système informatique dans le but de dérober des données ou d'endommager des applications ou le système d'exploitation. Ce type de logiciel s'introduit généralement dans un réseau au cours d'activités approuvées par l'entreprise, par exemple par le biais d'e-mails ou en parcourant des sites Web. Les virus, les vers, les chevaux de Troie, les logiciels spyware et adware et les outils de dissimulation d'activité sont des exemples de logiciels malveillants.
Banque marchande *	Établissement bancaire ou financier qui traite les paiements par carte de crédit et/ou débit pour le compte de commerçants. Également appelée « acquéreur », « banque acquéreuse », « service de traitement de carte » ou « service de traitement de paiement ». Voir également *service de traitement de paiement*.
Appareil mobile	Terme générique désignant une catégorie d'appareils électroniques détenus par les consommateurs, de petite taille, portables et qui peuvent se connecter à des réseaux informatiques sans fil, tels que des smartphones et des tablettes.
Validation des paiements mobiles	Utilisation d'un appareil mobile pour valider et traiter des transactions de paiement. L'appareil mobile est généralement jumelé avec un lecteur de carte disponible à la vente.
Authentification à plusieurs facteurs *	Méthode d'authentification d'un utilisateur par la vérification de deux ou plusieurs facteurs. Ces facteurs sont constitués d'un élément que possède l'utilisateur (comme une carte à puce ou une clé de sécurité), d'un élément que l'utilisateur connaît (comme un mot de passe, une locution de passage ou un code PIN), ou d'un élément qui identifie ou que fait l'utilisateur effectue (comme une empreinte digitale ou autre forme de mesure biométrique, etc.).
Réseau *	Deux ou plusieurs ordinateurs connectés les uns aux autres par des moyens physiques ou sans fil.

Glossaire

TERME	DÉFINITION
Système d'exploitation *	Logiciel d'un système informatique, responsable de la gestion et de la coordination de toutes les activités et du partage des ressources informatiques. Microsoft Windows, Apple OSX, iOS, Android, Linux et Unix sont des exemples de systèmes d'exploitation.
P2PE	Acronyme désignant la norme de cryptage point en point du conseil de PCI. Pour plus détails, consulter le site *www.pcisecuritystandards.org*.
PA-DSS *	Acronyme de « Payment Application Data Security Standard », norme de sécurité des données des applications de paiement du conseil de PCI. Pour plus détails, consulter le site *www.pcisecuritystandards.org*.
Mot de passe *	Mot, expression ou chaîne de caractères utilisé(e) pour authentifier un utilisateur. Combiné avec le nom d'utilisateur, le mot de passe vise à confirmer l'identité de l'utilisateur afin qu'il puisse accéder aux ressources informatiques.
Correctif *	Mise à jour du logiciel existant pour ajouter des fonctionnalités ou corriger un défaut (ou un « bug »).
Application de paiement *	Associée à la norme PA-DSS, application logicielle qui stocke, traite ou transmet des données de titulaires de cartes dans le cadre de l'autorisation ou du règlement de transactions de paiement.
Fournisseur d'applications de paiement *	Entité qui vend, distribue ou octroie des licences d'une application de paiement à des intégrateurs/revendeurs POS à intégrer dans les systèmes de paiement de commerçants ou directement installables et utilisables par les commerçants.
Logiciel médiateur de paiement	Terme générique désignant un logiciel qui connecte deux ou plusieurs applications de paiement avec ou sans lien. Par exemple, il peut transmettre des données de carte entre une application sur un terminal de paiement et d'autres systèmes marchands qui envoient les données de carte vers un service de traitement.
Service de traitement de paiement *	Entité engagée par un commerçant pour gérer les transactions par carte de paiement en son nom. Bien qu'ils fournissent généralement des services d'acquisition, les services de traitement de paiement ne sont pas considérés comme des acquéreurs (banques marchandes), à moins qu'ils ne soient définis comme tels par la marque de carte de paiement. Également appelé « passerelle de paiement » ou « prestataire de services de paiement (PSP) ». Voir également *banque marchande.*
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 une banque marchande.
Fournisseur de systèmes de paiement	Entité qui vend, octroie des licences ou distribue une solution complète de paiement à un commerçant. La solution englobe le matériel informatique et les logiciels nécessaires pour gérer les paiement au sein du magasin et permet de se connecter à un service de traitement de paiement.
Terminal de paiement	Appareil utilisé pour accepter les paiements par carte client via insertion latérale, verticale ou horizontale ou lecture par contact. Également appelé « terminal de paiement électronique (POS) », « lecteur de carte de crédit » ou « terminal PDQ ».

Glossaire

TERME	DÉFINITION
PCI *	Acronyme de « Payment Card Industry », secteur des cartes de paiement.
PCI DSS *	Acronyme de « Payment Card Industry Data Security Standard », norme de sécurité des données de l'industrie des cartes de paiement du conseil de PCI. Pour plus détails, consulter le site *www.pcisecuritystandards.org*.
Conforme à la norme PCI DSS	Satisfait toutes les exigences applicables de la norme PCI DSS actuellement en vigueur, de façon continue via une approche tendancielle. Cette conformité est évaluée et validée de façon ponctuelle. Toutefois, il incombe à chaque commerçant de respecter de façon continue les exigences associées afin de garantir une sécurité robuste. Les banques marchandes et/ou les marques de paiement peuvent disposer d'exigences relatives à la validation annuelle de la conformité à la norme PCI DSS.
Certifié conforme à la norme PCI DSS	Atteste de façon ponctuelle que toutes les exigences de la norme PCI DSS applicables sont respectées. Selon les exigences spécifiques à la marque de paiement et/ou à la banque marchande, cette validation peut être obtenue par le biais du questionnaire d'auto-évaluation PCI DSS applicable ou d'un rapport de conformité issu d'une évaluation sur site.
Application de paiement validée par PCI	Application logicielle validée par la norme de sécurité des données d'applications de paiement (PA-DSS) de PCI, listée le sur site Web du conseil de PCI.
Terminal de paiement approuvé par PCI	Terminal de paiement approuvé par la norme de sécurité des transactions PIN (PTS) de PCI, listé sur le sur site Web du conseil de PCI.
Solution de cryptage point en point listée par PCI	Solution de cryptage validée par la norme de cryptage point en point de PCI (P2PE), listée sur le site Web du conseil de PCI.
PED *	Acronyme de « PIN entry device », dispositif de saisie du code PIN. Clavier ou pavé numérique au moyen duquel le client saisit son code PIN. Également appelé « clavier PIN ».
PIN *	Acronyme de « personal identification number », numéro d'identification personnel. Numéro unique, connu uniquement de l'utilisateur et du système, afin d'authentifier l'utilisateur. Les codes PIN sont utilisés pour les distributeurs automatiques lors de transactions de retrait d'espèces ou pour les cartes à puce EMV en remplacement de la signature du titulaire de carte. Les codes PIN aident à déterminer si le titulaire de carte est autorisé à utiliser la carte et à empêcher que la carte ne soit utilisée en cas de vol.
Numéro de compte primaire (PAN) *	Numéro unique de cartes de paiement et de débit identifiant le compte du titulaire de carte.
Abus de privilège	Utilisation des privilèges d'accès à un système informatique de façon abusive. Par exemple : un administrateur système accédant à des données de carte à des fins malveillantes ou une personne dérobant et utilisant les privilèges d'accès élevé d'un administrateur à des fins malveillantes.
PTS *	Acronyme de « PIN Transaction Security Standard », norme de sécurité des transactions PIN du conseil de PCI. La norme PTS est un ensemble de critères d'évaluation modulaire pour l'acceptation du code PIN par les terminaux de point d'interaction (POI). Pour plus détails, consulter le site www.pcisecuritystandards.org.
QIR *	Acronyme de « qualified integrator or reseller », intégrateur ou revendeur qualifié. Pour plus détails, consulter le site *www.pcisecuritystandards.org*.

Glossaire

TERME	DÉFINITION
Évaluateur de sécurité qualifié (QSA) *	Société agréée par le conseil des normes de sécurité de PCI pour valider l'adhésion d'une entité aux exigences PCI DSS.
Paiement échelonné	Mode de facturation par lequel des commerçants facturent leurs clients de façon répétée dans le temps, sous forme de souscriptions ou d'adhésions mensuelles par exemple. Moyen sécurisé de le faire par l'acquéreur/processeur pour segmenter les données de carte, assurant sa protection et délestant le commerçant de cette responsabilité.
Accès à distance *	Accès à un réseau informatique depuis un emplacement situé en dehors de ce réseau. Les connexions d'accès à distance peuvent provenir soit de l'intérieur du propre réseau de la société soit d'un emplacement distant. Le VPN (réseau privé virtuel) est un exemple de technologie d'accès à distance. L'accès à distance peut être soit interne (par exemple, assistance IT) ou externe (par exemple, prestataire de services, agents tiers, intégrateurs/revendeurs).
Revendeur/intégrateur *	Entité qui vend et/ou intègre des applications de paiement, mais ne les développe pas.
Routeur *	Matériel ou logiciel qui connecte deux ou plusieurs réseaux informatiques internes ou externes pour « faire transiter » ou guider des données dans un réseau et assurer des flux de données appropriés entre ces réseaux. Le routeur peut également créer davantage de sécurité en permettant uniquement au trafic autorisé de transiter et en bloquant le trafic non autorisé.
Lecteur de carte sécurisé (SCR)	Dispositif approuvé PTS qui s'utilise avec un téléphone mobile ou une tablette pour accepter de façon sécurisée les cartes de paiement. Les lecteurs de carte SCR approuvés PCI PTS protègent et cryptent les données de carte via SRED. Voir également *SRED*.
Code de sécurité *	Numéro à trois ou à quatre chiffres figurant au recto ou au verso de la carte de paiement. Ce code est associé de façon unique avec une carte individuelle et sert de vérification complémentaire pour assurer que la carte est en possession du titulaire de carte légitime, généralement lors d'une transaction avec carte absente. Également désigné comme code de sécurité de carte.
Questionnaire d'auto-évaluation (SAQ) *	Outil de validation PCI DSS utilisé pour documenter les résultats de l'auto-évaluation de l'évaluation PCI DSS d'une entité.
Données d'identification sensibles *	Informations relatives à la sécurité utilisées pour authentifier les titulaires de carte et/ou pour autoriser les transactions par carte de paiement, stockées dans la bande magnétique ou la puce de la carte.
Prestataire de services *	Entité commerciale proposant des services divers à des commerçants. Ces entités proposent généralement le stockage, le traitement ou la transmission des données de carte pour le compte d'une autre entité (telle qu'un commerçant) ou sont des prestataires de services gérés proposant des pare-feu gérés, la détection d'intrusion, l'hébergement et d'autres services liés aux technologies de l'information. Également appelé « fournisseur ».
Copiage de carte	Vol de données de carte directement via la carte de paiement du consommateur ou via l'infrastructure de paiement sur un emplacement marchand, tel qu'un lecteur de carte de poche trafiqué ou des modifications effectuées sur le terminal de paiement du commerçant. Le copiage de carte est une menace sérieuse et une fraude. Il peut également endommager l'environnement du commerçant.

Glossaire

TERME	DÉFINITION
Dispositif de copiage de carte	Un appareil physique, souvent fixé à un appareil de lecture de carte légitime, conçu pour capturer illégalement et/ou stocker les informations d'une carte de paiement. Également appelé « copieur de carte ».
Petit commerçant	Société disposant généralement d'un local unique ou parfois de plusieurs locaux, d'un budget technologies de l'information (TI) limité voire inexistant et d'un effectif inexistant consacré aux TI.
SRED	Acronyme de « reading and exchange of data », lecture et échange de données. Ensemble d'exigences PCI PTS conçues pour protéger et crypter les données de cartes dans les terminaux de paiement. Une solution de cryptage point en point (P2PE) listée par le conseil de PCI doit utiliser un terminal de paiement listé et approuvé PTS avec SRED effectuant activement le cryptage des données de carte.
Terminal autonome	Terminal de paiement qui ne dépend pas de la connexion à un autre appareil au sein de l'environnement du commerçant et qui n'a pas d'autres fonctions. Le terminal autonome doit disposer d'une connexion au processeur via une connexion internet ou une ligne téléphonique pour fonctionner. Si le terminal nécessite une connexion à une caisse enregistreuse électronique informatisée ou est multifonction (comme un appareil mobile), il ne s'agit pas d'un terminal autonome.
Authentification forte	Utilisée pour vérifier l'identité d'un utilisateur ou d'un appareil pour garantir la sécurité du système protégé. Authentification forte est souvent synonyme d'authentification à plusieurs facteurs (MFA).
Tiroir-caisse	Voir *caisse enregistreuse électronique*.
Segmentation	Processus par lequel le numéro de compte primaire (PAN) est remplacé par une valeur de substitution appelée « token » (jeton d'authentification). Les tokens peuvent être utilisés à la place du PAN original pour accomplir des fonctions en l'absence de cartes comme pour les vides, remboursement ou facturation récurrente. Les tokens apportent également davantage de sécurité s'ils sont volés car ils sont inutilisables et n'ont donc aucune valeur pour un criminel.
Données non cryptées	Toute donnée lisible sans qu'aucun cryptage préalable ne soit nécessaire. Également appelées « texte en clair » ou « message en clair ».
Fournisseur	Entité commerciale fournissant à un commerçant un produit ou un service nécessaire à son activité. Lorsque des services sont proposés, le fournisseur peut être considéré comme un prestataire de services et peut avoir besoin d'accéder à des emplacements physiques ou à des systèmes informatiques au sein de l'environnement du commerçant pouvant affecter la sécurité des données de carte. Voir également *prestataire de services*.
Terminal de paiement virtuel *	Accès par navigateur Web au site Web d'un acquéreur, d'un processeur ou d'un prestataire de services tiers pour autoriser les transactions par carte de paiement. Contrairement aux terminaux physiques, les terminaux de paiement virtuels ne lisent pas les données directement sur la carte de paiement. Le commerçant saisit manuellement les données de carte de paiement par le biais de son navigateur Web connecté de façon sécurisée. Les transactions par carte de paiement étant saisies manuellement, les terminaux virtuels sont généralement utilisés plutôt que des terminaux physiques dans l'environnement des commerçants dont le volume de transactions est faible.
Réseau privé virtuel (VPN) *	Circuits virtuels au sein d'un réseau plus important, comme Internet, remplaçant les connexions directes par des câbles physiques. Les extrémités du VPN forment un « tunnel » à travers le réseau de plus grande dimension, ce qui a pour effet de créer une connexion privée sécurisée.

Glossaire

Virus	Logiciel malveillant qui se duplique dans d'autres fichiers de données ou logiciels sur un ordinateur infecté. Lorsqu'il se duplique, le virus peut exécuter une tâche de manipulation malveillante, comme la suppression de toutes les données de l'ordinateur. Un virus peut rester en sommeil et exécuter sa tâche de manipulation ultérieurement ou bien ne jamais déclencher d'action malveillante. Un virus qui se duplique en se renvoyant lui-même par le biais de pièces jointes d'e-mails ou d'un message réseau s'appelle un « vers ».
Vulnérabilité *	Défaut ou faiblesse qui, s'il est exploité, peuvent compromettre un système, intentionnellement ou non.
Analyse de vulnérabilité	Outil logiciel qui détecte et classifie les faiblesses potentielles (vulnérabilités) d'un réseau ou d'un ordinateur. Une analyse de vulnérabilité peut être effectuée par le service TI d'une organisation ou par un prestataire de services de sécurité (comme un prestataire de service d'analyses agréé). Voir également *prestataire de services d'analyse agréé (ASV)*.
Wi-Fi *	Réseau sans fil qui connecte des ordinateurs sans connexion physique par câbles.
Terminal de paiement sans fil	Terminal de paiement connecté à Internet à l'aide d'une technologie sans fil.