PCI DSS

Payment Card Industry Data Security Standard

Le PCI DSS est un ensemble de règles assurant la sécurité des paiements par cartes bancaires.

L'avènement du e-commerce

71

millions de cartes bancaires en France

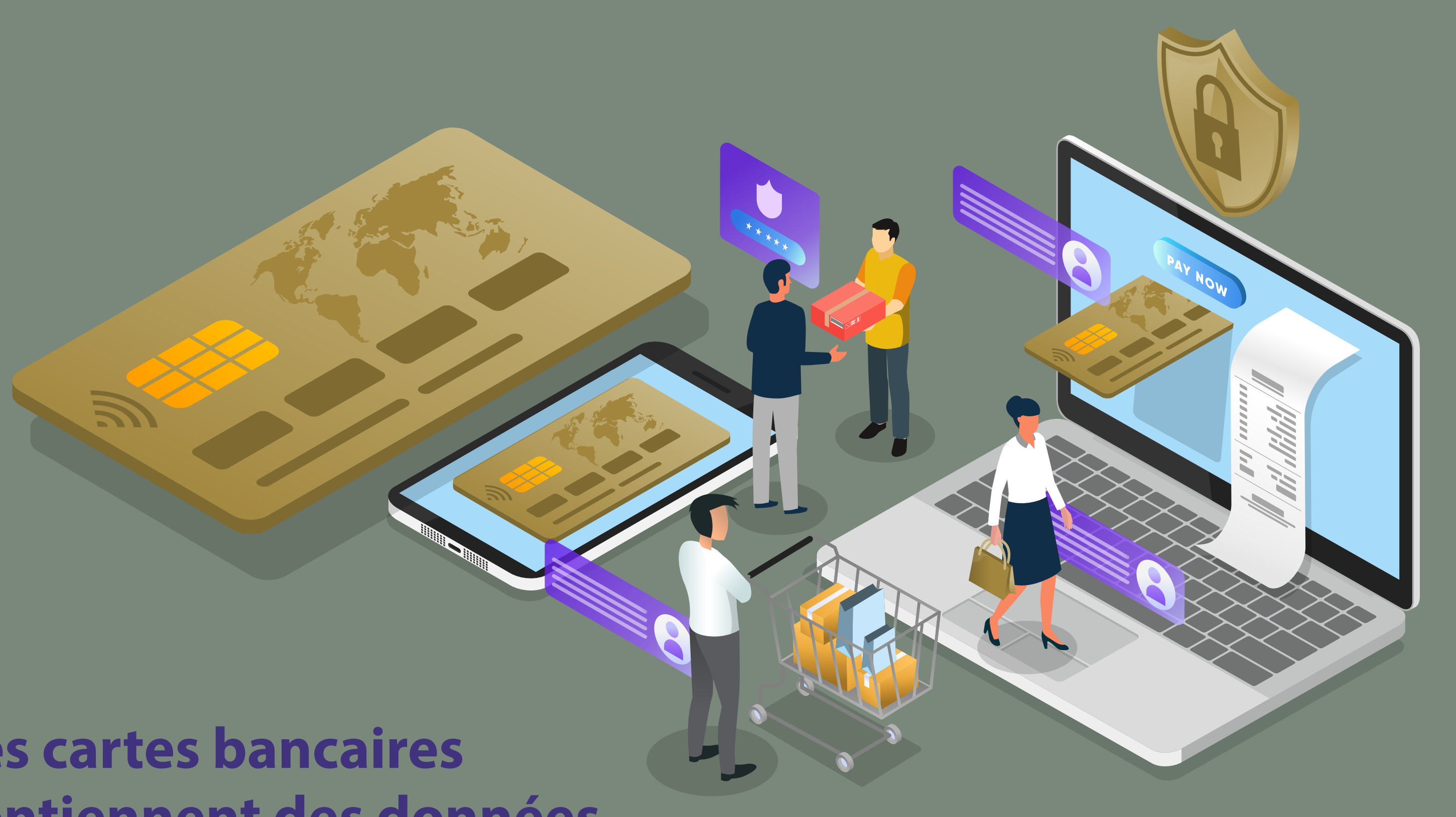
500

milliards d'euros de transactions par carte bancaire en france

Source : Observatoire CB en france en 2019

1

Quelles sont les données des cartes bancaires ?



Les cartes bancaires contiennent des données personnelles :

- ✓ Le nom du porteur
- ✓ Le numéro d'identification unique de la carte
- ✓ Le code PIN
- ✓ La date d'expiration
- ✓ La signature du porteur
- ✓ Le cryptogramme

Il faut être vigilant avec les données des cartes bancaires !

Les marchands (ex. e-commerçants) et les fournisseurs de services (ex. call centers) doivent ne pas conserver ou limiter au maximum le stockage des données des titulaires de cartes bancaires.

2

Les données de cartes bancaires peuvent être récupérées, par des personnes malveillantes, de différentes manières si elles ne sont pas bien sécurisées (ex. absence de chiffrement) :

Via un TPE (terminal de paiement électronique)

Via une base de données du système de paiement

Via les réseaux filaires ou sans fil

Via des dossiers au format papier ou autres type de documents

3

RGPD & PCI DSS

- ✓ La réglementation **RGPD** et le référentiel **PCI DSS** ont pour objectif commun **la protection des données**.
- ✓ Ils impliquent des principes et des règles techniques ou organisationnels de **la sécurité de l'information**.
- ✓ **Il est impératif d'être conforme à ces deux standards**, la certification de l'un facilitant la conformité de l'autre.

4

Le coût des données usurpées ou perdues

80%

des cartes bancaires piratées ont un solde positif

Source : PrivacyAffairs.com

ENTRE

10€ ET 20€

pour les données d'une carte bancaire avec un solde positif

Source : PrivacyAffairs.com

Les données de cartes bancaires sont un marché très lucratif pour les cyber-attaquants

Source : PrivacyAffairs.com

entre **10** et **30 €**

Le prix d'une carte bancaire clonée avec code PIN varie en fonction **des banques et de la marque de la carte**.

entre **100** et **250 €**

Le tarif d'un compte de type Paypal associé à une carte bancaire varie selon **les liquidités disponibles.**

Laissez-vous guider dans votre **auto-évaluation PCI DSS**

evidence

by XMCO

L'application française qui simplifie votre mise en conformité **PCI DSS**

- ✓ Une **application** SaaS développée par les QSA XMCO
- ✓ Des conseils d'**experts** et un accompagnement à chaque étape jusqu'à votre **auto-évaluation**
- ✓ Un parcours de questions, simple et didactique, **adapté à votre contexte métier**
- ✓ Un SAQ **pré-rempli** détaillant toutes les exigences sur le PCI DSS
- ✓ Des **modules de formations** pédagogiques pour sensibiliser vos équipes

© plusdebleu.com - ©AdobeStock.com

evidence.xmco.fr