



Ecommerce Melee

26 nov 2009, Sécurité des paiements

Mr Pinguet, Crédit Agricole
Mr Granja,
Mr Piotrowski, ITrust



La Fraude sur Internet

Problématique et risques

- Commerçants :
 - Perte de marge : impayés
 - Perte de temps : contrôles

- Consommateurs
 - Contestation : mécontentement et image négative

État des lieux 2008 (taux de fraude)

- Montant: 2,69%
- Nombre : 2,07%
- Panier Moyen : 435€ (activité...)

Source Fia_Net sur 2,6 Md € analysés



La Fraude sur Internet

2 grands types de fraudes :

1/ Attaque à la fausse carte (Ecarding)

2/ Attaque sur les sites afin d'initier des transactions frauduleuses (panier à 1 Euro, attaques Paypal)

Risques et responsabilités

	Risques	Responsabilités
Consommateurs	Keylogger, Phising...	Sécurisation de l'ordinateur
E-Commerçants	Attaque Web, Spoofing...	Sécurisation du site et des données
Banques	Carding...	Sécurisation des opérations et des données CB

Les solutions de paiement en ligne

- **Les solutions bancaires** (Atos, Paybox, Solutions propriétaires)
 - Affiliation Carte Bancaire en Vente à Distance (CB VAD Internet)
 - Page de paiement sécurisée (SSL)
 - Sécurisation des échanges entre le site et la banque ?
- **Les solution mixtes** (Paybox, Ogone, Bluepaid...)
 - Affiliation CB VAD Internet auprès de sa banque
 - Page de paiement sécurisé (SSL)
 - Sécurisation des échanges en le site et le prestataire ?
- **Les solutions "VAD incluse"** (Paypal, Bluepaid, EuroWebpayment...)
 - Affiliation CB hors banque + page de paiement sécurisée
- **Les solutions "maison"**
 - Page de saisie en ligne (SSL ?)
 - Re-saisie de données CB sur une solution VAD classique

Sécuriser son site de E-Commerce

Pourquoi :

- Eviter la perte de données confidentielles (fichier client)
- Respecter les réglementations liées à la vie privée (données client)
- Sécuriser son panier (éviter les paniers falsifiés)
- Eviter le defacing

Comment :

- Auditer son site régulièrement
- Programmer sécurisé
- Travailler avec un hébergeur de qualité

Sécuriser la transaction avec le centre de paiement

- HTTPS
- La transaction vers la banque est elle chiffrée
- Traçabilité, conservation des données

Risques :

- The man in the middle
- Preuve

Moyens de paiement et authentification

- La Carte Bancaire
 - CB, Visa, Mastercard...Amex, JCB, Dinners...
- Les tokens (usb, cartes, etc ...)
- La E-Card Visa ou Mastercard
 - Génération de n° à utilisation unique
- La E-Monnaie
 - Échange de compte à compte (Paypal...)
- Authentification : 3D Secure : Mot de passe de confirmation
 - Sécurité pour l'acheteur ?
 - Garantie de paiement pour le E-Commerçant
 - Information internautes ?



Les alertes à la fraude 1/2

- Les ventes "miracles"
- Les commandes incohérentes
- Les adresses à risque
- Les "Multinationaux" (Carte – IP – Livraison)

Les contrôles possibles

- L'appel téléphonique...
- Les documents justificatifs...
- Le paiement de substitution

Les alertes à la fraude 2/2

- Attaques de masse
- Ecarding
- Attaques de sites
- Spoofing d'identité



Les normes et meilleures pratiques

- Normes internationales : 27001,X
- Normes propriétaires : PCI DSS
- Labels : Fianet, hackersafe, Verisign

Les 8 conseils

- Sécuriser son code, son système
- Auditer son site et son application
- Tracer les transactions
- Consolider sa comptabilité
- Vérifier l'HTTPS pour le paiement client
- Un serveur dédié (si possible)
- Sécuriser l'administration de son site
- Utiliser les bons outils afin de monitorer l'activité de son magasin