BIZCOMMUNITY

Security rules for online retailers increase

By Peter Harvey

22 Jan 2014

Security rules for online credit card payments are being tightened, with global associations, Visa and MasterCard being trendsetters in this space, fulfilling their first priority of protecting their own customers, the credit card holders, from any financial loss if their card data is stolen or hacked.

If a cardholder disputes a transaction, they can get a refund and the merchant who passed the transaction is the one who pays. However, the card associations cannot rely only on chargebacks because if it becomes too risky for merchants to accept credit cards, cardholders will forgo the convenience of online shopping.

Therefore, the card associations have developed a set of security standards to benefit everyone in the industry, by protecting card data properly so it cannot be used fraudulently.

PCI-DSS sets practices, processes

The Payment Card Industry Data Security Standard (PCI-DSS) specifies a broad range of business practices and processes that should be in place at any organisation that processes, stores or transmits credit card data. The data that is protected includes the credit card number, the cardholder's name, the card expiry data and the CVV number or security code on the back of the card.

If any of this data falls into the wrong hands through a security leak, the responsible organisations face hefty fines and the risk that their banks might stop them from processing any more transactions, which could sink an online business overnight.

Achieving full compliance with the PCI standards is an onerous and expensive process, but online merchants have a way out. The best thing they can do is not to process or store any card data at all. The easiest way to do that is to have a hosted payment page with a payment services provider that is itself fully PCI-compliant. That means none of the customer's card

data ever touches their systems - it is all handled by the gateway and the compliance problem is its.

Utilise tokenisation

If merchants must store card data themselves, they should use tokenisation. This replaces card numbers with secure tokens that are validated at every transaction. This reduces the number of places any person's card details are stored, which makes it easier to secure.

In addition, merchants should use fraud-monitoring services to help identify suspicious transactions before they are processed.

Maintaining card data security in compliance with the PCI standards is increasingly going to be a condition of doing business online. Merchants should approach their payment gateways to find out exactly how they are affected and what steps they should take to protect their business.

ABOUT PETER HARVEY

Peter Harvey is the MD of PayGate. Leading through integrity, with more than 26 years in IT and payment processing, Peter is a master when it comes to creating solutions to clients' exact requirements. He is a truly integral member of the PayGate team and works tirelessly to ensure its continuing culture of integrity and quality.

- Security rules for online retailers increase - 22 Jan 2014
- Different approaches needed for African e-commerce - 25 Oct 2013

View my profile and articles...