Monthly Cyber Security Tips

NEWSLETTER

April 2009 Volume 4, Issue 4

Security of Credit Card Transactions

From the Desk of Darrell Davis

The use of credit cards to pay for goods and services is a common practice around the world. It enables business to be transacted in a convenient and cost effective manner. However, more than 100 million personally-identifiable, customer records have been breached in the US over the past two years[1]. Many of these breaches involved credit card information. Continued use of credits cards requires confidence by consumers that their transaction and credit card information are secure. The following provides information as to how the credit card industry has responded to security issues and steps you can take to protect your information.

Who regulates the security of credit card transactions?

The Payment Card Industry (PCI) Security Standards Council developed standards and policies that must be met by all vendors which accept credit card transactions. The Council's members include American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International. The Council created an industry-wide, global framework that details how companies handle credit card data – specifically, banks, merchants and payment processors. The result was the Payment Card Industry (PCI) Data Security Standard (DSS)[2], a set of best practice requirements for protecting credit card data throughout the information lifecycle.

The PCI compliance security standards outline technical and operational requirements created to help organizations prevent credit card fraud, hacking and various other security vulnerabilities and threats.

The PCI DSS requirements are applicable if a credit card number is stored, processed, or transmitted. The major credit card companies require compliance with PCI DSS rules via contracts with merchants and their vendors that accept and process credit cards. Banks, merchants and payment processors must approach PCI DSS compliance as an ongoing effort.

---

[1] Source: www.privacyrights.org
[2] Source: www.pcisecuritystandards.org

Compliance must be validated annually, and companies must be prepared to address new aspects of the standard as it evolves based on emerging technologies and threats.

How is my credit card information protected?

The PCI standards detail what protective measures are required regarding the string and transmission of credit card information. For electronic Point of Sale (POS) transactions, the information is encrypted and transmitted directly to the credit card processor. For an online transaction, the merchant is required to have a secure server and an encrypted connection to the customer. Access to credit card information is restricted based on a business need-to-know. The standards include guidelines for developing and maintaining secure systems and applications. Recent focus includes heightened security requirements for wireless networks due to the jump in the use of wireless POS terminals.

What if a merchant does not follow the standards?

If a member, merchant, or service provider does not comply with the security requirements or fails to rectify a security issue, they may face fines up to $500,000 per incident or restrictions imposed by the credit card companies, including denying their ability to accept or process credit card transactions.

What can I do to secure my credit card information?

You can help secure your credit card information by adhering to the following guidelines:

- ***Don't respond to email or pop-up messages.*** If you get an email or pop-up message while you're browsing, don't reply or click on the link in the message or any attachments, especially if personal or financial information is requested. Legitimate organizations don't ask for this information in these ways.
- ***Guard the security of your transaction.*** When purchasing online, look for the "lock" icon on the browser's status bar and be sure "https" or "s-http" appears in the website's address bar. The "s" stands for "secure."
- ***Use temporary account authorizations when available.*** Some credit card companies offer virtual or temporary credit card authorization numbers. This kind of service gives you use of a secure and unique account number for each online transaction. These numbers are often issued for a short period of time and cannot be used after that period. Contact your credit card company to see if they offer this service.
- ***Limit your online shopping to merchants you know and trust.*** If you have questions about a merchant, verify it with the Better Business Bureau or the Federal Trade Commission.

For more monthly cyber security newsletter tips visit:

www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:	

MS-ISAC

www.msisac.org