Media Contacts

Lindsay Goodspeed
PCI Security Standards Council
+1-781-258-5843
press@pcisecuritystandards.org
Twitter @PCISSC

Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL ISSUES BEST PRACTICES FOR SECURING E-COMMERCE

— E-commerce Security More Important Than Ever For Merchants—

WAKEFIELD, Mass., 31 January 2017 — Exponential online sales growth paired with the EMV chip migration in the US makes e-commerce payment security for merchants more important than ever before. As EMV chip technology continues to reduce face-to-face credit card fraud, the shift to e-commerce security becomes increasingly important to businesses large and small. To help merchants shore up their e-commerce platforms, today the PCI Security Standards Council released *Best Practices for Securing E-commerce*. The information supplement will educate merchants on accepting payments securely online and is an update to existing guidance previously published in 2013.

Securing the e-commerce environment continues to be critically important- a recent survey found that 66% of consumers claim they won't purchase from an organization that has been breached.[1] The *Best Practices for Securing E-commerce* information supplement includes practical recommendations and case studies to help merchants identify the best solution for their specific cardholder data environment. In addition to educating merchants, this latest resource from the Council also provides guidance for third party e-commerce service providers and assessors that support the ongoing security of e-commerce environments.

Following industry recommendations, in December 2015 the Council announced that all organizations that accept payment cards must use TLS 1.1 encryption or higher by June 2018. SSL/TLS encrypts a channel between two endpoints (for example, between a web browser and web server) to provide privacy and reliability of data transmitted over the communications channel. To underline the importance of using an encrypted channel, Google announced that beginning in January 2017, the Chrome browser will warn users when a website doesn't use HTTPS. As there is still confusion in the industry regarding encryption and certificate selection, a large portion of the e-commerce supplement is dedicated to explaining SSL/TLS, with guidance on how to select a certificate authority, an outline of the different types of certificates and a list of potentials questions merchants can ask service providers regarding digital certificates and encryption.

The *Best Practices for Securing E-commerce* information supplement is a result of a Council-led Special Interest Group (SIG). SIGs bring together smart, experienced payment security professionals from a wide-ranging group of PCI stakeholders- including merchants, financial institutions, service providers, assessors and industry associations to address important security challenges related to PCI Security Standards.

"Our community of members boasts a wealth of payment security knowledge to protect e-commerce transactions all over the world," said Troy Leach, Chief Technology Officer for the Council. "This information supplement is a testament to their collaboration and willingness to share their experience with others and provides easy to understand examples of e-commerce scenarios along with best practices to secure cardholder data and meet PCI DSS requirements. Their engagement on Council efforts like this paper, the Small Merchant Task Force, and other resource guides help educate merchants on how to make better business decisions to secure cardholder data. Our aim is to make cardholder data more secure in the most sensible way possible." Additional comments from Troy on this supplement can be found in a Q&A on the PCI Perspectives blog.

Visit the Special Interest Group page to learn how your organization can provide expertise and develop practical payment security resources for the industry. Best Practices of Securing E-commerce is available on the PCI SSC website.

[1] Gemalto, Data Breaches and Customer Loyalty Report

About the PCI Security Standards Council
The PCI Security Standards Council is a global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

###