Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL PUBLISHES MERCHANT GUIDANCE ON SKIMMING PREVENTION

— Resource for retailers and others that handle payment card data updated to address memory scrapers, mobile device weaknesses, EMV chip cards and other new attack scenarios —

ORLANDO, Fla., 10 September 2014 – Today, at its annual North American Community Meeting, the PCI Security Standards Council, an open global forum for the development of payment card security standards, released an update to its guidance for merchants on protecting against card skimming attacks in point-of-sale (POS) environments. *Skimming Prevention: Best Practices for Merchants* educates organizations on how to prevent the unauthorized capture and transfer of payment data to another source for fraudulent purposes, known as skimming. The guidance supports PCI Standards, controls and approved devices for maintaining POS security and a secure terminal environment.

Card skimming continues to be a highly profitable enterprise for criminals, with the United States Secret Service estimating it costs consumers and businesses at least $8 billion annually. While commonly associated with external electronic devices placed on ATMs, skimming can compromise many different payment forms including, POS terminals, wireless networking technologies such as Bluetooth and Wi-Fi and even EMV chip cards. With advancements in payment technology and new skimming techniques, merchants especially continue to be at risk.

In response to this need, the Council formed an industry taskforce to update its guidance on skimming to address a wide range of common targets and new attack vectors, including: data capture from malware and memory scrapers or compromised software; overlay attacks that take advantage of the advances in 3D printers; mobile device weaknesses and attacks against EMV chip cards.

Security best practices outlined in the guidance can help businesses:

- Identify risks relating to skimming - both physical and logical based
- Evaluate and understand vulnerabilities inherent in the use of POS terminals and terminal infrastructures, and those associated with staff that have access to consumer payment devices

- Prevent or deter criminal attacks against POS terminals and terminal infrastructures
- Identify any compromised terminals as soon as possible and notify the appropriate agencies to respond and minimize the impact of a successful attack

Organizations can also reference appendices in the document to assess vulnerability risks, and in their efforts to meet PCI DSS Requirement 9.9 for ensuring proper inspection of POS devices and limiting the attack vector by implementing simple daily routines and training employees.

“Skimming is highly profitable and appeals to a wide range of criminals because it allows them to capture massive amounts of data in a short amount of time, with low risk of detection,” said Troy Leach, chief technology officer, PCI SSC. “Retailers and other organizations can use this guidance document to educate themselves on how to identify and prevent against this type of attack.”

For quick and easy reference, a high-level overview of the guidance is available as a separate document on the PCI Council’s website: https://www.pcisecuritystandards.org/security_standards/documents.php

As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

About the PCI Security Standards Council

The PCI Security Standards Council is an open 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. Founded in 2006 by the major payment card brands American Express, Discover, JCB International, MasterCard and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council

Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###