

Protect Your Business: PCI Resources for Securing Payment Data

Presenter:

Elizabeth Terry

Community Engagement Manager

PCI Security Standards Council

Agenda

- Housekeeping
- Presenters
- About Conexus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: info@conexxus.org

Presenters

Conexxus Host

Allie Russell

Conexxus

arussell@conexxus.org

Jenny Bullard

Conexxus

jbullard@conexxus.org

Moderator

Kara Gunderson

Chair, Data Security Committee

POS Manager, CITGO Petroleum

kgunder@citgo.com

Speaker

Elizabeth Terry

PCI Security Standards Council

Community Engagement Manager

About Conexus

- **We are an independent, non-profit, member driven technology organization**
- **We set standards...**
 - Data exchange
 - Security
 - Mobile commerce
- **We provide vision**
 - Identify emerging tech/trends
- **We advocate for our industry**
 - Technology is policy



2019 Conexus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 24, 2019	Managed Detection and Response	Tom Callahan Mark Carl	ControlScan
February 28, 2019	PCI DSS for Petro Merchants	Elizabeth Terry	PCI SSC
March 2019	Protecting Your Stores and Main Office from Data Security & Ransomware Attacks	Dirk Heinen	Acumera
April 2019	Don't get Phished! Train Your Employees to Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
May 2019	Firewall compliance! The basics, the benefits, and the security	Simon Gamble	Mako Networks
June 2019	TBD	David Ezell Ian Jacobs	Conexus W3C

2019 Conexus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
July 2019	Skimming	TBD	TBD
August 2019	TBD	TBD	TBD
September 2019	Updated Data Science Presentation	Ashwin Swamy Thomas Duncan	Omega ATC Omega ATC
November 2019	Outdoor EMV	Brian Russell Linda Toth	Verifone Conexus
December 2019	TBD	TBD	TBD



Conexxus thanks our 2018 Annual Diamond Sponsors!



Protect Your Business: PCI Resources for Securing Payment Data

Presenter:

Elizabeth Terry

Community Engagement Manager

PCI SSC

PCI Security Standards Council

**We Help
Secure
Payment
Data**

Global, cross-industry effort to increase payment security

Industry-driven, flexible and effective standards and programs

Helping businesses detect, mitigate and prevent criminal attacks and breaches

PCI Security Standards and Programs

Standards, Training and Certification Programs, Educational Resources



Payment **Equipment**



Payment **Software**



Merchant & Payment Service Provider
Environments

Certification – Equipment, Service Providers, Assessors, Investigators

Training – Assessors, Investigators

Small Merchant Resources

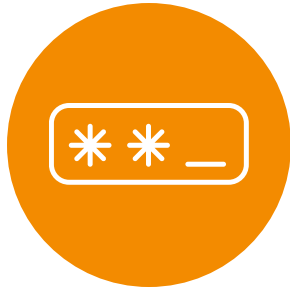
Organized Crime is a Business

A man and a woman are seated at a desk in a server room, working on multiple computer monitors. The room is dimly lit with blue light from the screens and server racks in the background.

The global impact of huge cyber security events such as the WannaCry ransomware epidemic has taken the threat from cybercrime to another level. Banks and other major businesses are now targeted on a scale not seen before.

- Europol

Leading Causes of Data Breaches



**Weak and
default
passwords**



**Unpatched
software**



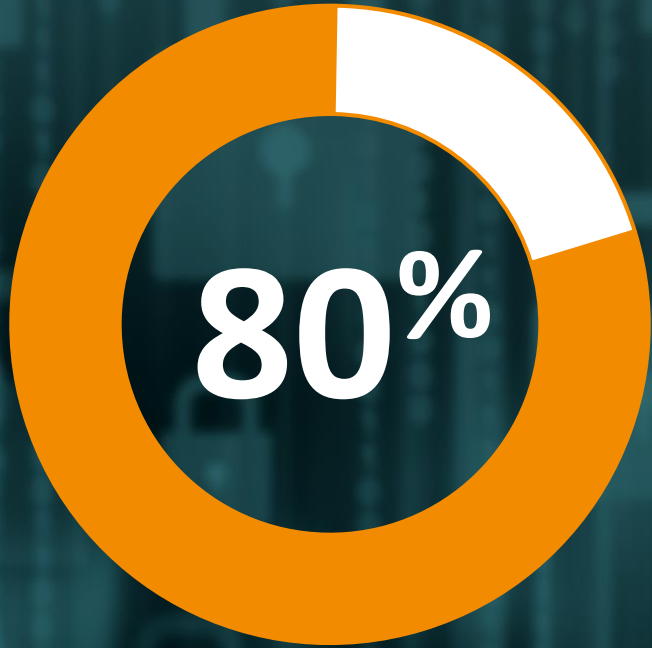
**Insecure
Remote
Access**



81%

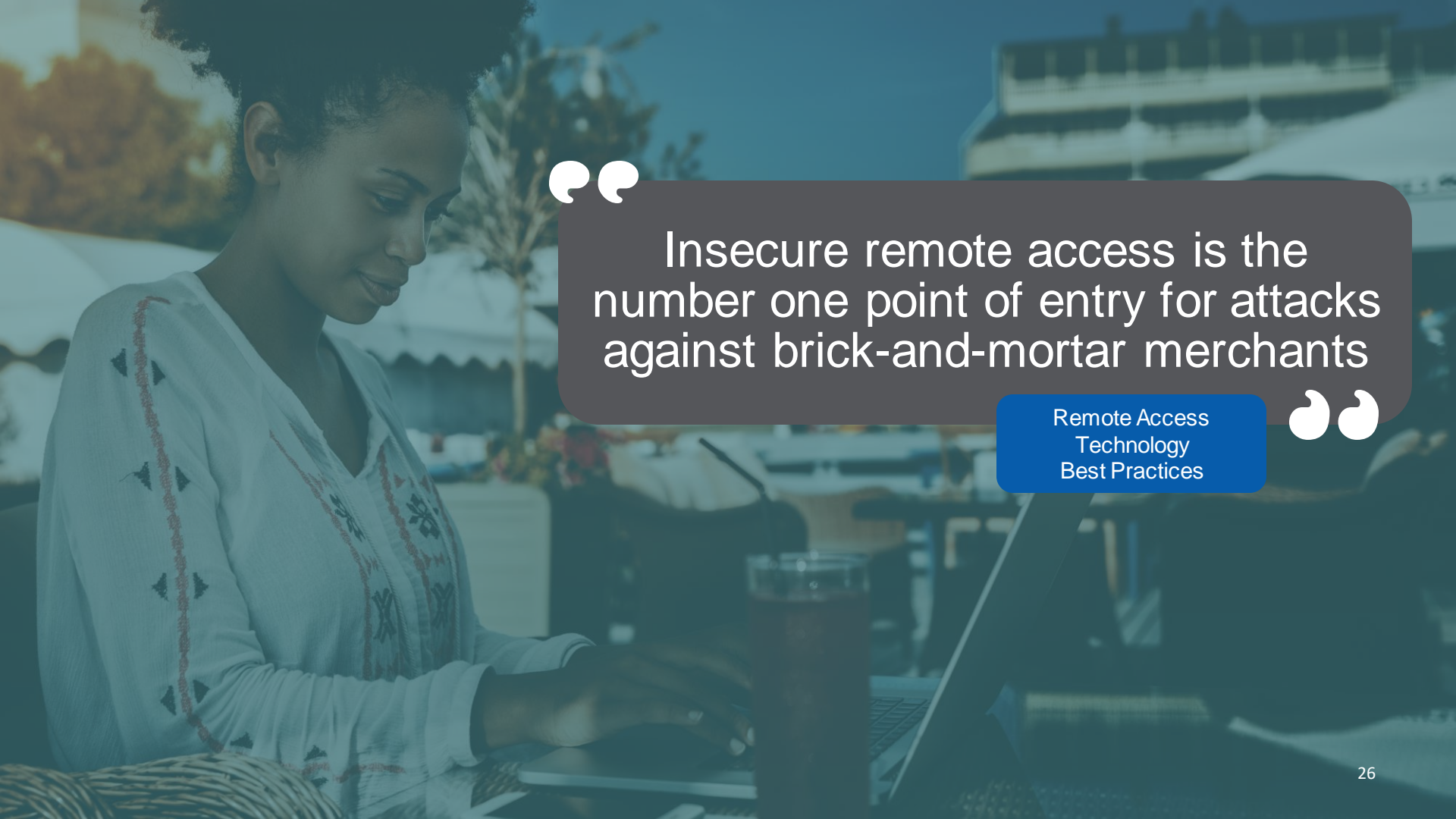
of hacking-related breaches succeeded through stolen passwords, default or weak passwords.

**Verizon
Data Breach Investigation Report
(DBIR)**



Of the majority of hacking attacks could be prevented by strengthening passwords and installing patches.

Verizon Data Breach Investigation Report (DBIR)



“ Insecure remote access is the number one point of entry for attacks against brick-and-mortar merchants ”

Remote Access
Technology
Best Practices

POS Attacks Lead to Breaches

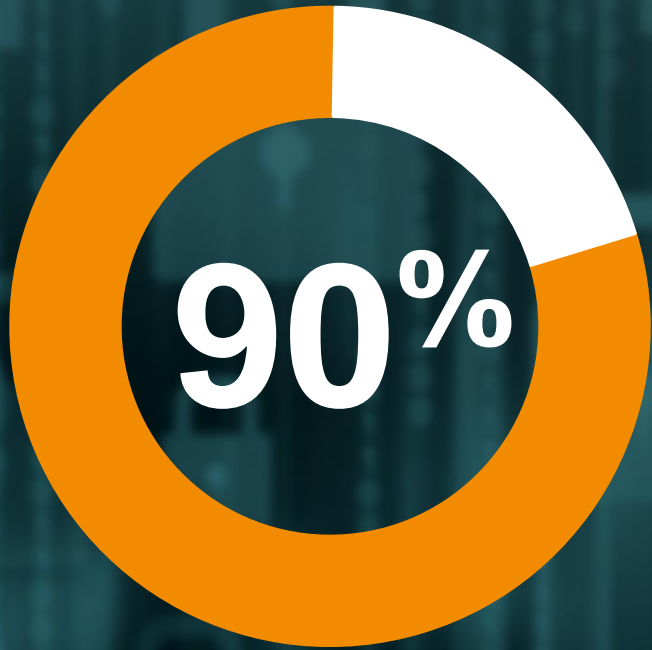


“At 40%, payment card data is the #1 type of data targeted in a breach.”

2018 Trustwave Global Security Report

“The chances of being struck by lightning this year are 1 in 960,000. When it comes to experiencing a data breach, the odds are as high as 1 in 4.”

2017 Ponemon Cost of Data Breach Study



**of all accommodation
breaches were POS breaches.**

2018 Verizon Data Breach Investigations Report (DBIR)

Small Merchant Resources

PCISSC.org/Merchants



GUIDE TO SAFE PAYMENTS

Simple guidance for understanding the risk to small business, security basics to protect against payment data theft, and where to go for help.



















































COMMON PAYMENT SYSTEMS

Real-life visuals to help identify what type of payment system a small business uses, the kinds of risks associated with their system, and actions they can take to protect it.

How do you protect your business?

The good news is, you can start protecting your business today with these security basics:

 Use strong passwords and change default ones	 Protect your card data and only store what you need	 Inspect payment terminals for tampering	 Use trusted business partners and know how to contact them	 Install patches from your vendors	 Protect in-house access to your card data
Cost 	Cost 	Cost 	Cost 	Cost 	Cost 
Ease 	Ease 	Ease 	Ease 	Ease 	Ease 
Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 
 Don't give hackers easy access to your systems	 Use anti-virus software	 Scan for vulnerabilities and fix issues	 Use secure payment terminals and solutions	 Protect your business from the Internet	 For the best protection, make your data useless to criminals
Cost 	Cost 	Cost 	Cost 	Cost 	Cost 
Ease 	Ease 	Ease 	Ease 	Ease 	Ease 
Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 	Risk Mitigation 

These security basics are organized from easiest and least costly to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the "Risk Mitigation" column.

Small Merchant Resources

PCISSC.org/Merchants



QUESTIONS TO ASK YOUR VENDORS

A list of the common vendors small business rely on and specific questions to ask them to make sure they are protecting customer payment data.



GLOSSARY OF PAYMENT AND INFORMATION SECURITY TERMS

Simplified glossary, based on PCI DSS Glossary and with extra definitions specific to small merchants.

What is a “Small Merchant”?

PCISSC.org/Merchants



- Typically an independently-owned and operated business
- With a single location or a few locations
- With limited or no IT budget
- Often with no IT personnel

Whether a small merchant is required to validate PCI compliance is determined by the payment brands or acquirer

Current Small Merchant Materials



Small Merchant materials released in 2016 provided:

- Education and awareness
- Simple security steps to address critical risks

Small Merchant materials updated in 2018 to provide:

- Clearer e-commerce guidance
- More types of payment diagrams for small merchants
- New, easy-to-understand DSE Evaluation Tool to help with validation

PCI Data Security Essentials Evaluation Tool

PCISSC.org/SmallMerchantTool

PCI DATA SECURITY ESSENTIALS EVALUATION TOOL FOR SMALL MERCHANTS



The PCI Data Security Essentials Resources for Small Merchants provides security basics to protect against payment data theft and to help small merchants simplify their security and reduce their risk. The Data Security Essentials Evaluation Tool provides an alternative for eligible small merchants to learn more about their security posture and perform a preliminary evaluation to understand how they are meeting these security basics for safe payments.

Each merchant's acquirer (merchant bank), in coordination with the applicable payment brands, determines which merchants are eligible to use Data Security Evaluation forms. We encourage small merchants to review Data Security Essentials Resources for Small Merchants, talk to your acquirers for instructions on how to complete and submit a Data Security Essentials evaluation, and start your path to better security and simpler validation today



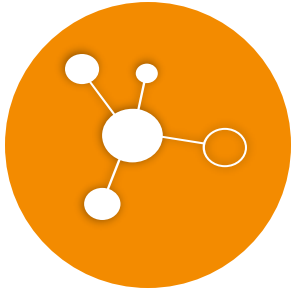
PCI Data Security Essentials Evaluation Tool

PCISSC.org/SmallMerchantTool

Security Practice	How have you implemented this practice?	Additional Information as Needed
A. Use strong passwords and change default ones Passwords are vital for security of your payment systems and card data. The confidentiality of all passwords should be protected and passwords should be changed if there is any suspicion of misuse. This includes all passwords you and your staff (including permanent full-time and part-time workers, contractors, consultants, etc.) use to log into or connect to your payment systems, computers, and other equipment. In addition, much equipment comes with default passwords "out of the box" (like "password" or "admin"). Hackers easily guess these out-of-the-box passwords since they are commonly known and often left unchanged. See " It's time to change your password " at www.PCIStandards.org .		
1. You and your staff change passwords for computer access regularly, at least every 90 days.	<input type="checkbox"/> I do this consistently. <input type="checkbox"/> I do this sometimes. <input type="checkbox"/> This is N/A to my business environment (explain). <input type="checkbox"/> I do not know / I do not understand. <input type="checkbox"/> I do not do this (explain).	
2. You and your staff make all passwords for computer access in your business unique and hard to guess: 7 or more characters and a combination of upper- and lower-case letters, numbers, and symbols. Consider using a passphrase as your password; you can make it personal and easy for you to remember.	<input type="checkbox"/> I do this consistently. <input type="checkbox"/> I do this sometimes. <input type="checkbox"/> This is N/A to my business environment (explain). <input type="checkbox"/> I do not know / I do not understand. <input type="checkbox"/> I do not do this (explain).	
3. Immediately, you change out-of-the-box default passwords from your equipment and/or software suppliers. If you do not know where these passwords are or how to change them, find out from your payment system vendor or supplier, the individual who set up your payment system, or your merchant bank.	<input type="checkbox"/> I do this consistently. <input type="checkbox"/> I do this sometimes. <input type="checkbox"/> This is N/A to my business environment (explain). <input type="checkbox"/> I do not know / I do not understand. <input type="checkbox"/> I do not do this (explain).	



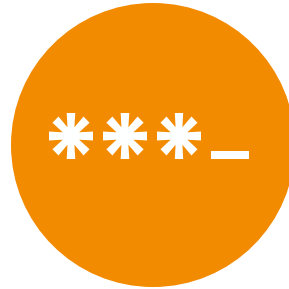
Help Us Help Them



Share these resources with your small merchant customers



Let small merchants know the simple things they can do today



Help small merchants understand and address risks with remote access and default passwords



Use secure remote access into small merchant systems and help them manage it

Questions About Small Merchant Resources?



Co-branding?
Where are the documents?
Are paper versions available?

Find the documents at:

<https://www.PCISSC.org/Merchants>

PCI Resources for Securing Payment Data



PEOPLE

Hire qualified and trusted partners and train your staff to understand payment data security essentials.

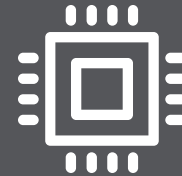
[Learn more about training and qualified security professionals](#)



PROCESS

Put the right policies and practices in place to make payment security a priority every day.

[Learn more about the PCI Data Security Standard \(PCI DSS\)](#)



TECHNOLOGY

Make sure you are using the right technology and implementing it correctly to get the best security and business benefits.

[Learn more about secure technology](#)

People: Qualified Integrator and Reseller™

What Types of Organizations Employ QIRs?

- Certified POS Technicians
- Merchants
 - Retail
 - IT
 - Hospitality
 - Healthcare
 - Restaurant
- Financial Institutions
- Processors
- Service Providers



Who Becomes a QIR?

Technician
Integrator
Developer
Engineer
Implementer
Software
Installer
Reseller

What Do QIRs Actually Do?

- Ensure installation is implemented in a manner that addresses high-priority risks
- Protect confidential and sensitive information
- Support investigations by PCI Forensic Investigators
- Ongoing support/maintenance is in accordance with both application vendor guidance and PCI DSS



Key Security Controls for QIRs

PAYMENT DATA SECURITY ESSENTIAL

Patching

WHAT'S THE RISK?

80% of security incidents are caused by unpatched software.

Often, vulnerabilities (flaws or holes) made by programmers when they create the code become the #1 or 2 most common reasons for security alerts. These vulnerabilities often become the "back door" for attackers to enter your system and steal payment data.

PATCHING BEST PRACTICES

Test: installation of security patches is crucial to minimize the risk of being targeted. It is important for you to know that your software is being regularly patched with patches and only is responsible to install the ones:

- Identify which vendors need your updates.
- Test updates before you install them on your systems.
- Test your updates before patching.
- Notify your vendors about patches.

RESOURCES

- The [PCI Security Standards Council's Patching Best Practices](#) is a resource that provides guidance on how to patch your systems.
- The [PCI Security Standards Council's Patching Best Practices](#) is a resource that provides guidance on how to patch your systems.
- The [PCI Security Standards Council's Patching Best Practices](#) is a resource that provides guidance on how to patch your systems.

PAYMENT DATA SECURITY ESSENTIAL

Strong Passwords

WHAT'S THE RISK?

81% of security incidents are caused by weak passwords.

Weak passwords are a major security risk because they are easy to guess. Attackers can use automated tools to try thousands of passwords per second. If your passwords are weak, your systems are vulnerable to being hacked.

PASSWORD BEST PRACTICES

To minimize the risk of being hacked, passwords should change and be different from one another and never share them with other individuals (even in your organization).

- Change your passwords regularly**: Test your passwords like a thief. Don't use the same password for multiple systems.
- Don't share passwords**: Never use the same password for multiple systems.
- Make passwords hard to guess**: Use a mix of uppercase and lowercase letters, numbers, and symbols. Avoid using common words or phrases.

RESOURCES

- The [PCI Security Standards Council's Password Best Practices](#) is a resource that provides guidance on how to create strong passwords.
- The [PCI Security Standards Council's Password Best Practices](#) is a resource that provides guidance on how to create strong passwords.

PAYMENT DATA SECURITY ESSENTIAL

Secure Remote Access

WHAT'S THE RISK?

#1 reason for security incidents is insecure remote access.

Remote access is a common way for attackers to gain access to your systems. If your remote access is insecure, your systems are vulnerable to being hacked.

REMOTE ACCESS BEST PRACTICES

To minimize the risk of being hacked, it is important for you to change how and where your remote access is used. Only allow remote access when necessary:

- Limit use of remote access.
- Require use of multi-factor authentication.
- Require unique identifiers.

RESOURCES

- The [PCI Security Standards Council's Remote Access Best Practices](#) is a resource that provides guidance on how to secure remote access.
- The [PCI Security Standards Council's Remote Access Best Practices](#) is a resource that provides guidance on how to secure remote access.

QIR Value

- Recognition of criticality of security controls applied during installation
- Merchant trust in the quality, reliability and consistency of work
- Part of larger community of security professionals



QIR Value

- Industry recognized credential that follows the individual
- Public recognition of professional achievement
- Competitive career advantage



People: PCI Professionals

What Types of Organizations Employ PCIPs?

- Merchants
 - Retail
 - IT & Telecom
 - Hospitality
 - Finance
 - Food
- Financial Institutions
- Acquirers
- Service Providers



Who Becomes a PCIP?

Internal Auditor
Technical Writer
President / CEO
GRC Program Manager
Engagement Manager
Finance Analyst
Office Manager
Central Key Manager
Data Center Manager
Credit Card Fraud Manager
Engineer
Staff Attorney
QA Director
Retail IT Business Analyst
Treasury Manager
Project Manager
Web Systems Engineer
Vice President
eCommerce Manager
LAN/WAN Support
Assistant Vice President
Application Developer
Network Coordinator
Application Engineer
Crypto Lead
Manager IT
Head of Payments
System Engineer
Studio Head
Business Applications Analyst
Data Breach Specialist
IT Manager

What Do PCIPs Actually Do?

- Write/review PCI policies and procedures
- Owning and managing PCI DSS controls
- Work with ISA/QSA
- Advise internally on PCI projects
- Train staff on PCI DSS
- Input and maintenance of PCI processes



PCIP Value

- PCI DSS subject matter experts
- Confidence in interpreting requirements
- Ability to interact with other PCI entities
- PCI compliance often extends across many parts of an organization...



PCIP Value

- Become part of the PCIP Community
- Industry recognized credential that follows the individual
- Public recognition of professional achievement
- Competitive career advantage



Case Studies

Instructor-led PCIP training classes available

[VIEW SCHEDULE](#)



PCI PROFESSIONAL (PCIP)[™] QUALIFICATION

The Payment Card Industry Professional is an individual, entry-level qualification in payment security information and provides you with the tools to build a secure payment environment and help your organization achieve PCI compliance. This renewable career qualification is not affected by changes in employment assignments and stays in effect as long as the individual continues to meet requirements. This three-year credential also provides a great foundation for other PCI qualifications.



[DOWNLOAD COURSE DESCRIPTION](#)

[VIEW BIT9 CASE STUDY >](#)

[VIEW EXCENTUS CASE STUDY >](#)



- PCI SSC website under “Training and Qualification”
- Interested? Email us at PCIP@pcisecuritystandards.org







Other PCI Resources

https://www.pcisecuritystandards.org/document_library



Contact Change Your Language 



[Get Started](#)  [Assessors & Solutions](#)  [Document Library](#) [Training & Qualification](#)  [About Us](#)  [Get Involved](#)  [Newsroom](#)  [FAQs](#)

DOCUMENT LIBRARY



The Document Library includes a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.

PCI Guidance and Best Practices

Defending Against Phishing & Social Engineering Attacks A Resource Guide from the PCI Security Standards Council

Hackers use phishing and other social engineering methods to target organizations with legitimate-looking emails and social media posts. These attacks are providing confidential information to attackers. These attacks are serious cyberhacks that put your customers at risk. Vigilance, business awareness, and security are key to defending against these attacks.

Skimming

A Resource Guide from the PCI Security Standards Council

WHAT IS SKIMMING?

Skimming is copying payment card numbers and personal identification numbers (PINs) and using them to make counterfeit cards, siphon money from bank accounts and make fraudulent purchases.

Criminals install equipment at merchant locations, on point-of-sale (POS) devices, automated teller machines (ATMs), and kiosks that captures the information from the magnetic stripe.

FACTS & FIGURES

\$2 billion
The estimated global cost of skimming*

\$50,000
The average loss from skimming crime**

Skimming-related counterfeit card fraud is the leading type of third-party card fraud*

92%
Skimming is the #1 ATM crime globally making up 92% of all attacks at the ATM*

From Jan-Apr 2016, the number of attacks on debit cards used at ATMs reached the highest level for that period in at least 20 years**



HANDHELD SKIMMER

Handheld skimmers used by corrupt staff are very small, fitting in the palm of a hand. Despite their size, these devices can store a significant amount of cardholder data.



POS TERMINAL SKIMMER

Skimming devices hidden within the terminal are invisible, and neither the merchant staff nor the cardholder will know that a card was skimmed.



ATM SKIMMER

Criminals may not use a single attack against a device, but can use a combination of attack scenarios. In this attack we see an overlay has been placed on the ATM's card reader to capture the card data, and an additional overlay was added to the screen that allowed for a hidden camera to capture the PIN.

IN-DEPTH BACKGROUND MATERIALS



Skimming Prevention - Overview of Best Practices for Merchants
Skimming Prevention - Best Practices for Merchants
ATM Security Guidelines

RELATED INDUSTRY RESOURCES

Skimming the Surface
All About Skimmers
Skimming is a Scam
The ATM Scam

All amounts are in U.S. Dollars

RELATED VIDEOS



Safeguard Against Skimming



The ATM Scam

* Source: All Threat Intelligence Group
** Source: Visa Group
*** Source: MasterCard Advisory Group
**** Source: FICO

- Building a security awareness program
- Protecting against malware
- Skimming prevention
- Defending against phishing attacks
- Working with third parties
- Maintaining PCI DSS compliance
- Accepting payments with a mobile phone
- PCI DSS compliance in the cloud

PCI Resource Center



Server Time: 10:54:08 AM
Welcome back, you are logged in as **eterry**.

Resource Center

PCI SSC

PCIP Training/Requal

CPE Hours

Operations

Logout

Home

PCIP Portal

My Account

Consolidated Statement

Your Benefits



Community Meeting

You are eligible to attend the annual PCI Community Meetings

PCIP Newsletters

Get the quarterly *PCIP Professional Update* newsletter delivered to your inbox

CPE Credits

Receive six (6) Continuing Education (CPE) credits for the eLearning course / seven (7) for the instructor-led course.

Recognition

Get a PCI Professional certificate (suitable for printing and framing)

Exclusive PCIP Logo

You will be authorized to use the PCIP logo to create your own personal brand (use on resumes, email signatures and other professional communications)

Demonstrate Your Qualifications to the World

You will be included on a listing on the PCI website - searchable by name or certificate number



Save the Date for 2019 Events



India

13 March
New Delhi, India



Latin America

15 August
São Paulo, Brazil



North America

17 – 19 September
Vancouver, BC, Canada



Europe

22 – 24 October
Dublin, Ireland



Asia-Pacific

20 – 21 November
Melbourne, Australia

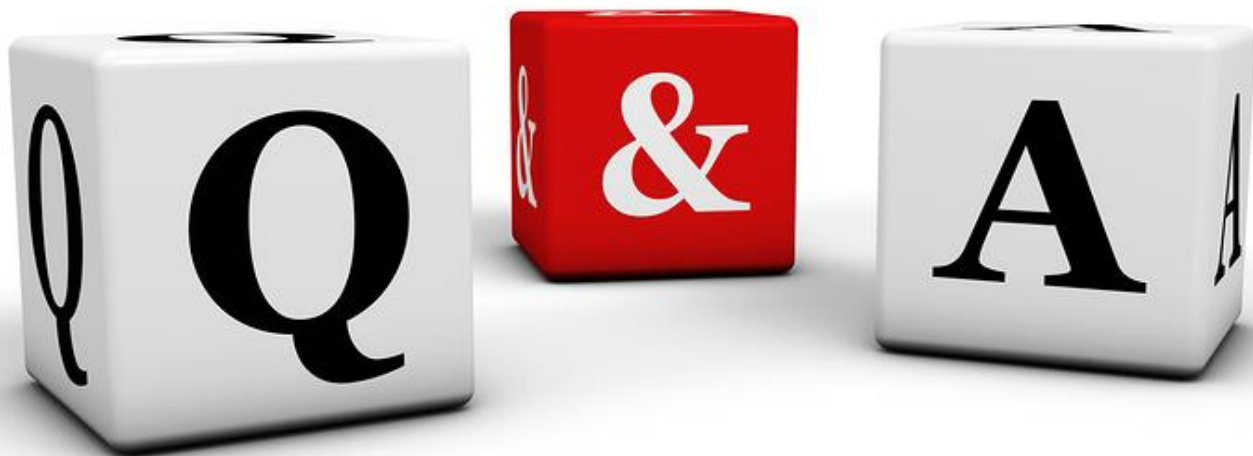


events.pcisecuritystandards.org



Help Secure Payment Data

pcisecuritystandards.org



- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: [Conexxus.org](https://www.linkedin.com/company/conexxus.org)
- Follow us on Twitter: [@Conexxusonline](https://twitter.com/Conexxusonline)