Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago

Mauro Lance
Chief Operating Officer
PCI Security Standards Council

Mauro Lance
Gerente de Operaciones, PCI Security Standards Council

- 20 años de experiencia directiva en Chile, China, Francia y los Estados Unidos
- MIT Media Lab, MIT CSAIL/W3C, Web Foundation, PUCV
- Especialización:
  - Tecnología y Ciberseguridad
  - Gobiernos Corporativos
  - Finanzas y Logística
  - Equipos de Alto Desempeño
- Educación:
  - MBA, Suffolk University
  - Ingeniero Comercial, PUCV


Valparaíso
Santiago
Santa Cruz
San Fernando

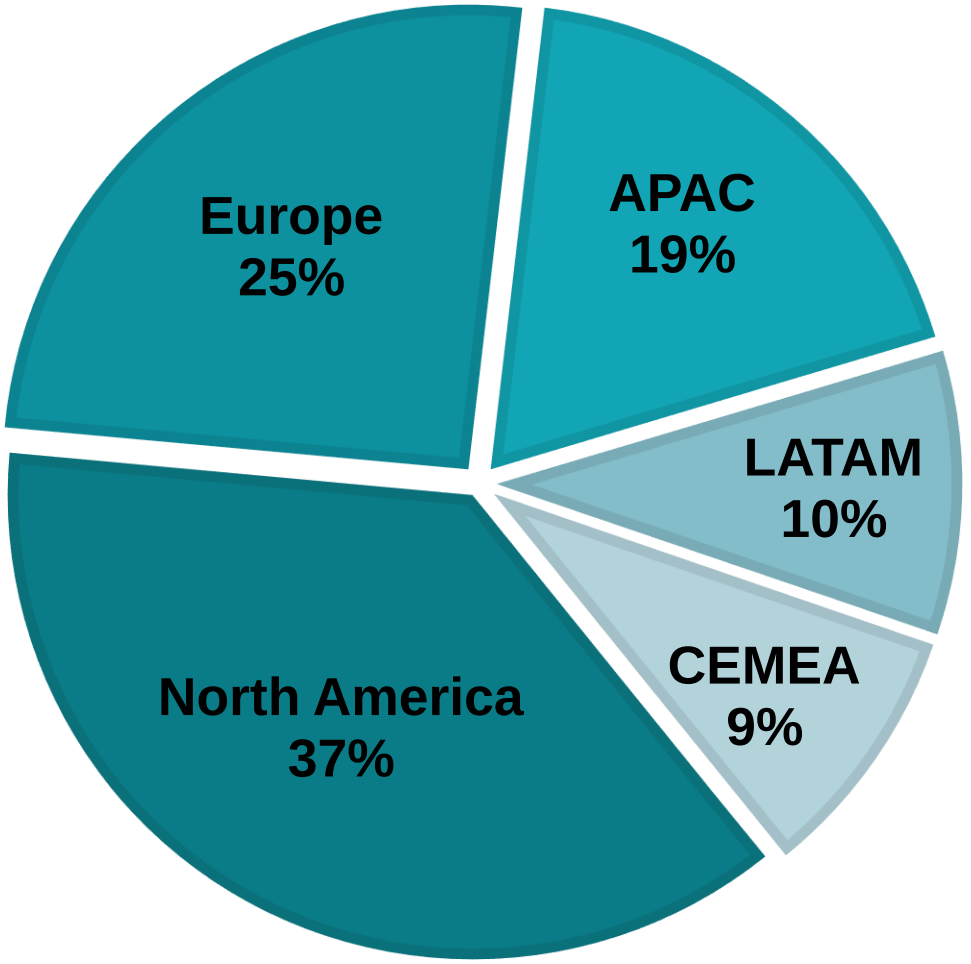
- Ubicuidad de las Tarjetas de Pago a Nivel Mundial
- Cibercrimen y Ciberseguridad
- El Consejo PCI
- La Colaboración es la Solución
- Preguntas y Respuestas

Ubicuidad de las Tarjetas de Pago a Nivel Mundial

Número de transacciones sin efectivo a nivel mundial alcanzó 358 mil millones en 2013.

Fuente: Capgemini/RBS World Payments Report 2015

PARTICIPACIÓN REGIONAL EN NÚMERO DE TRANSACCIONES SIN EFECTIVO A NIVEL MUNDIAL (2013)



Fuente: Capgemini/RBS World Payments Report 2015

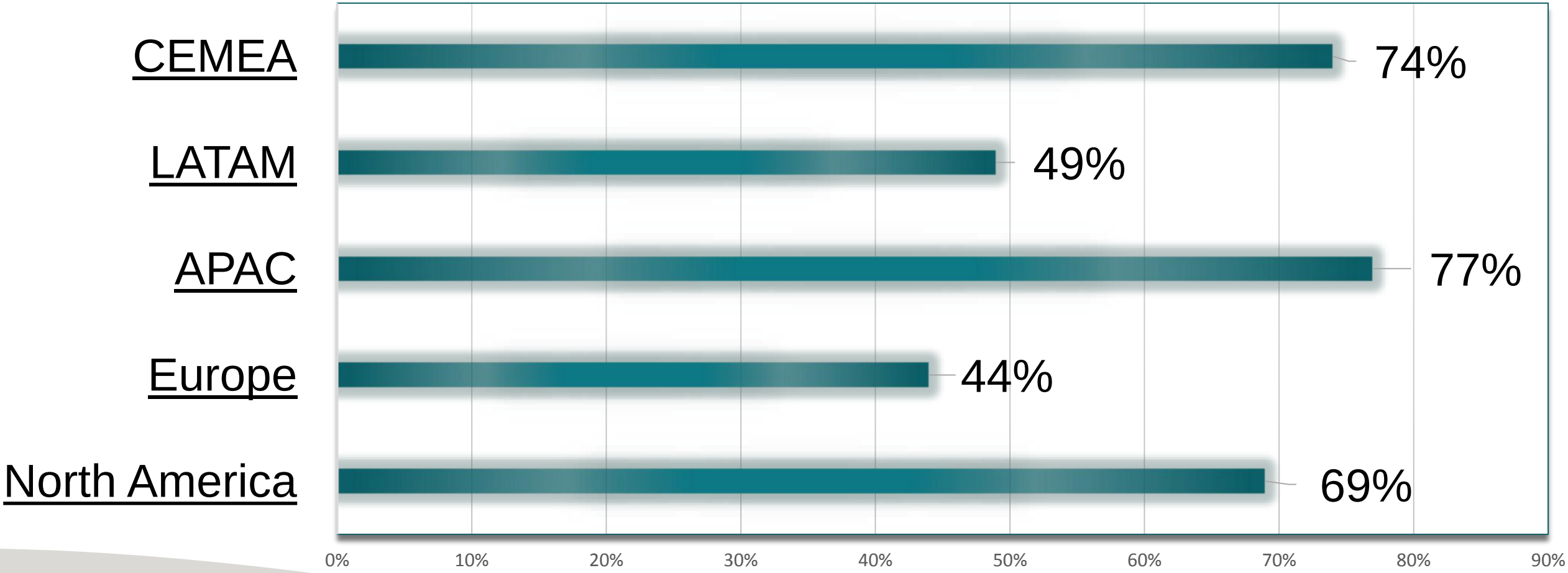
A nivel mundial en 2013…

358.000.000.000 Transacciones Sin Efectivo (100%)

223.969.500.000 Transacciones con Tarjetas de Pago (63%)

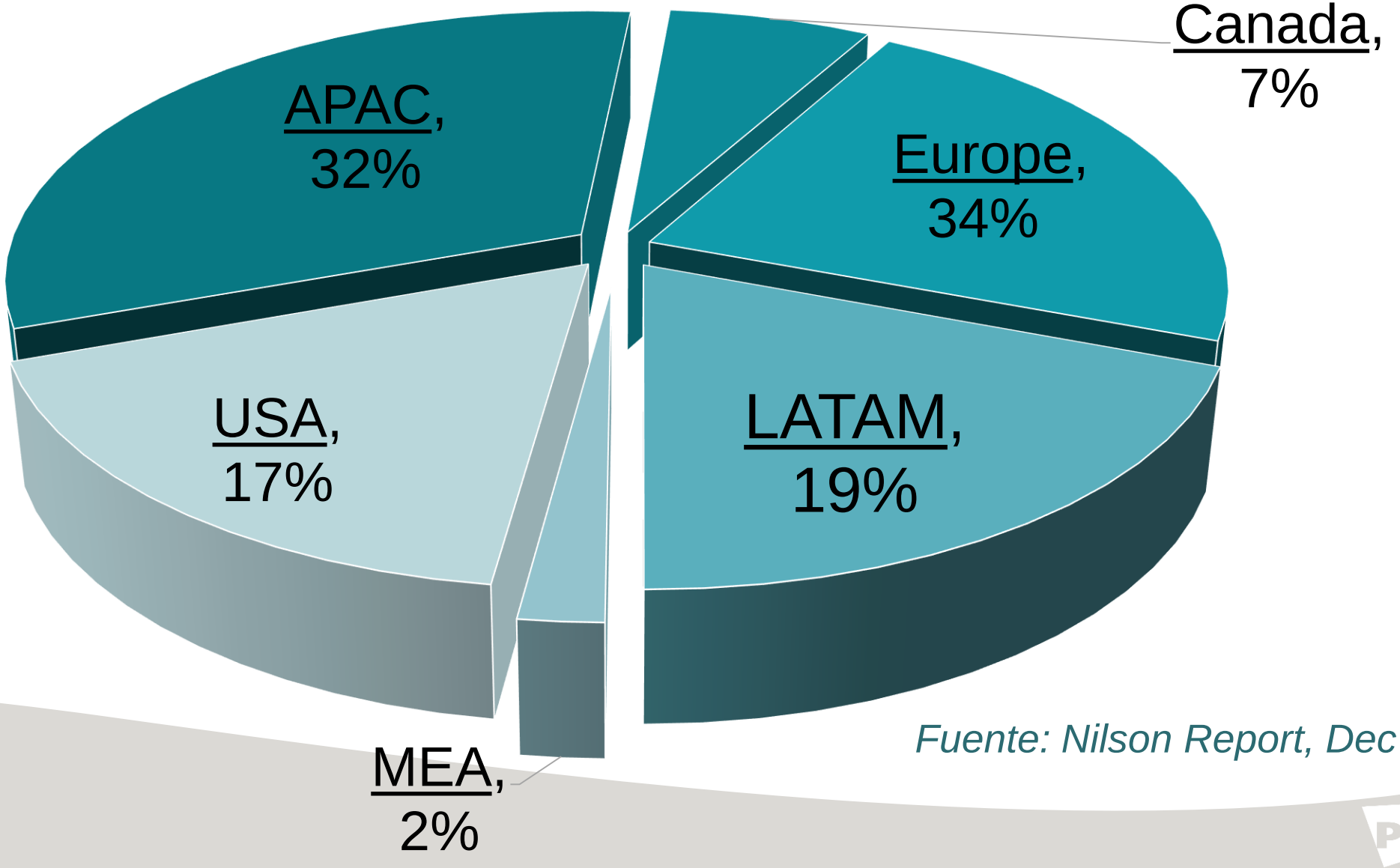
Fuente: Capgemini/RBS World Payments Report 2015

Participación de Tarjetas de Pago en Total de Transacciones Sin Efectivo a Nivel Mundial, por Regiones (2013)



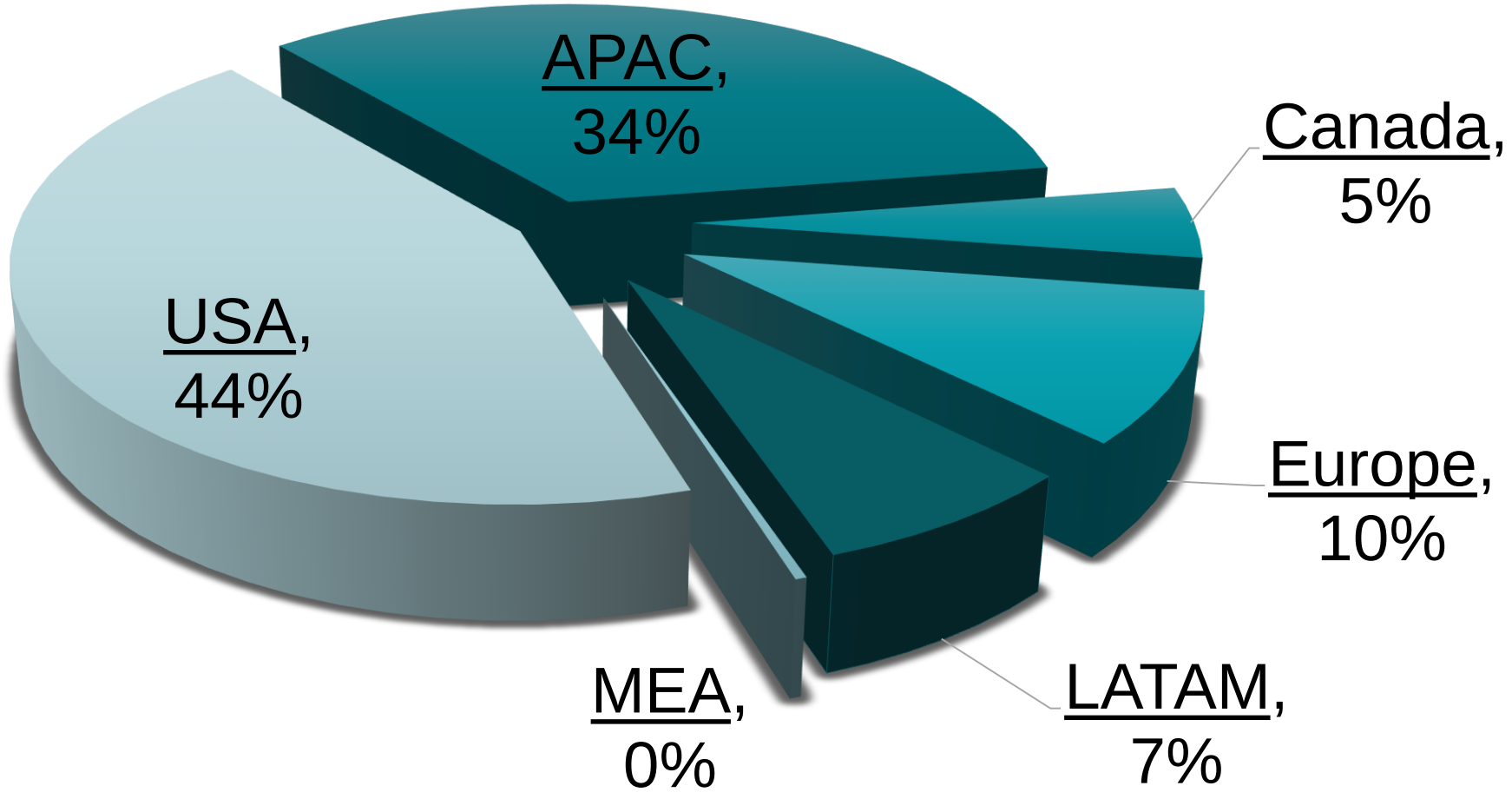
Fuente: Capgemini/RBS World Payments Report 2015

Participación Regional en los 150 Principales Emisores a Nivel Mundial (2014)



Fuente: Nilson Report, Dec 2015

Participación Regional en Monto Impago de los 150 Principales Emisores a Nivel Mundial (2014)



Fuente: Nilson Report, Dec 2015

Cibercrimen y Ciberseguridad

El costo anual del crimen informático para la industria se ha incrementado a aproximadamente 465 mil millones de dólares.

- Allianz, 2014

Las grandes empresas tienen en promedio 14 incidentes de seguridad al año. Las pequeñas empresas tienen en promedio 4.

- HM Information Security Breaches Survey, 2015

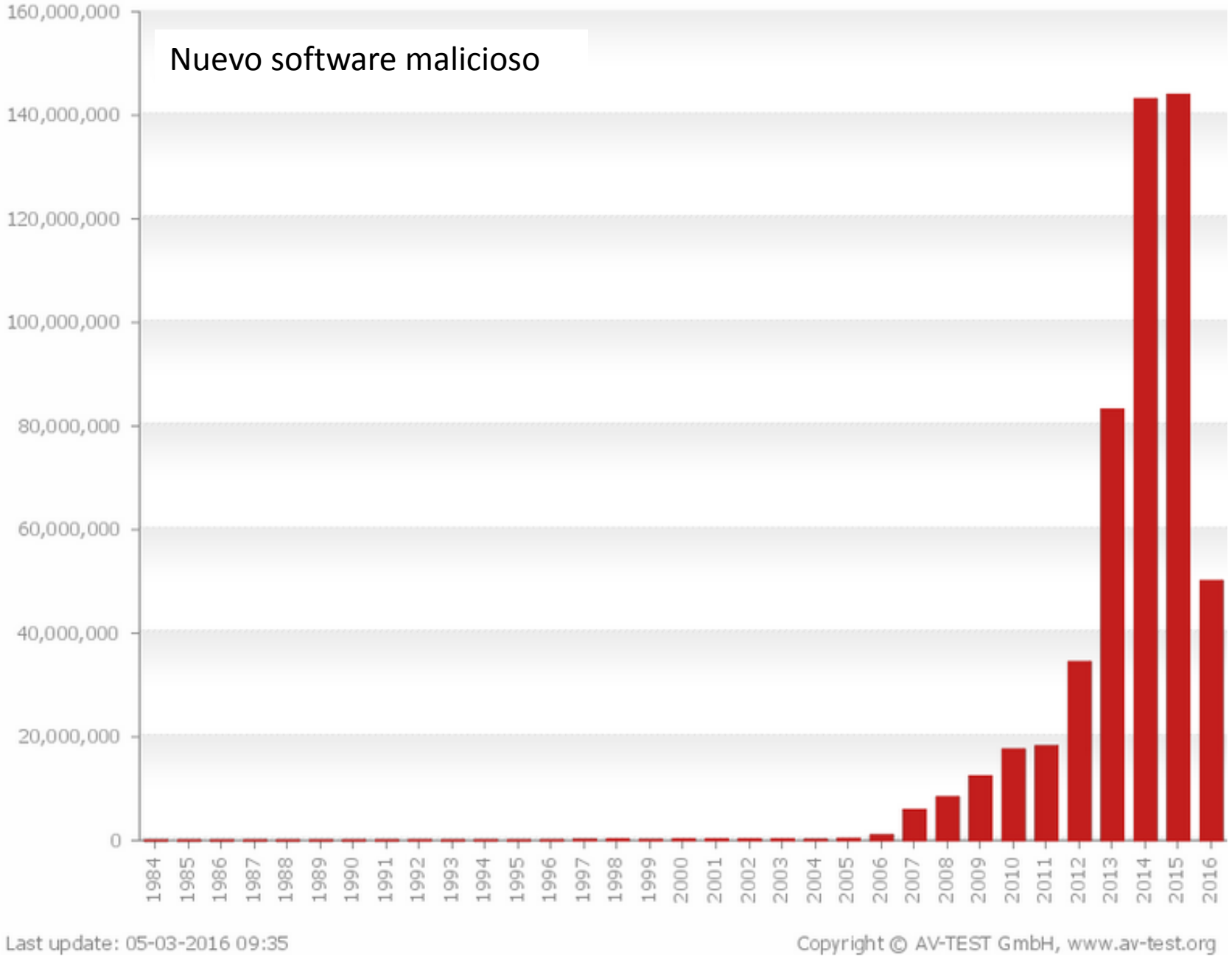
Número de Sitios Web Activos para Suplantación de Identidad (Phishing) en Diciembre 2004: 1.707

Fuente: Anti-Phishing Working Group, Inc.

Número de Sitios Web Activos para Suplantación de Identidad (Phishing) en Diciembre 2015: 65.885

Fuente: Anti-Phishing Working Group, Inc.

El crecimiento del software malicioso a nivel mundial ha explotado…



Número de computadores infectados con software malicioso a nivel mundial 2011

Ranking	País	Tasa de Contagio
1	China	54.10%
2	Taiwan	47.15%
3	Turquía	42.75%
4	Rusia	41.22%
5	Perú	39.99%
6	Ecuador	38.03%
7	España	37.93%
8	Argentina	37.52%
9	Polonia	36.90%
10	Chile	36.63%

- Fuente: Anti-Phishing Working Group, Inc. 2012

Los criminales son profesionales

Video: Men Place Card Skimmer on ATM Store Machine

Video Credit: Harry Williby
https://www.youtube.com/watch?v=y83ZgzuFBSE

Evolución constante de los medios de pago

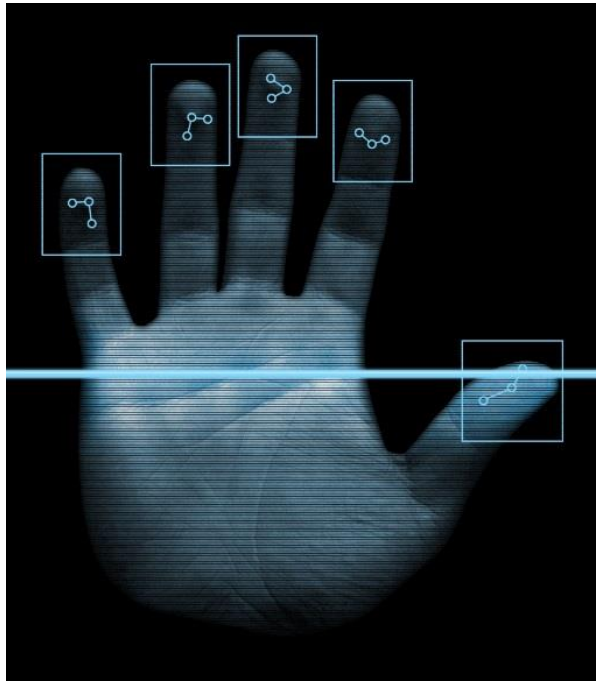
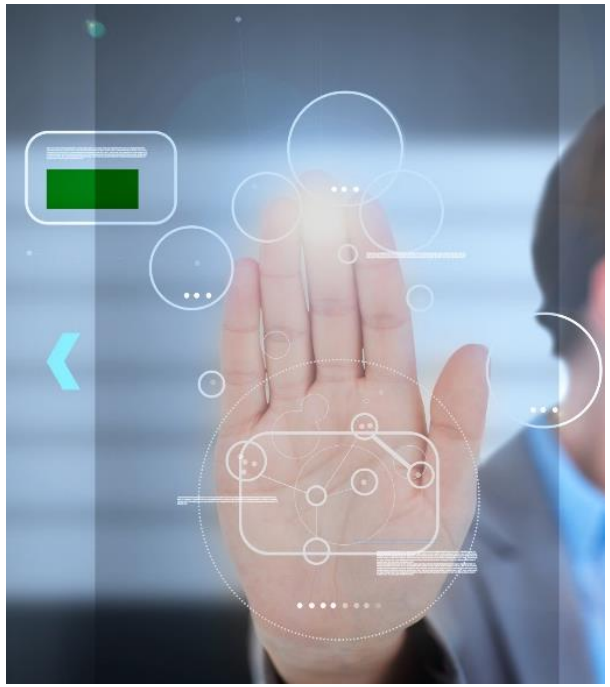
Pasado

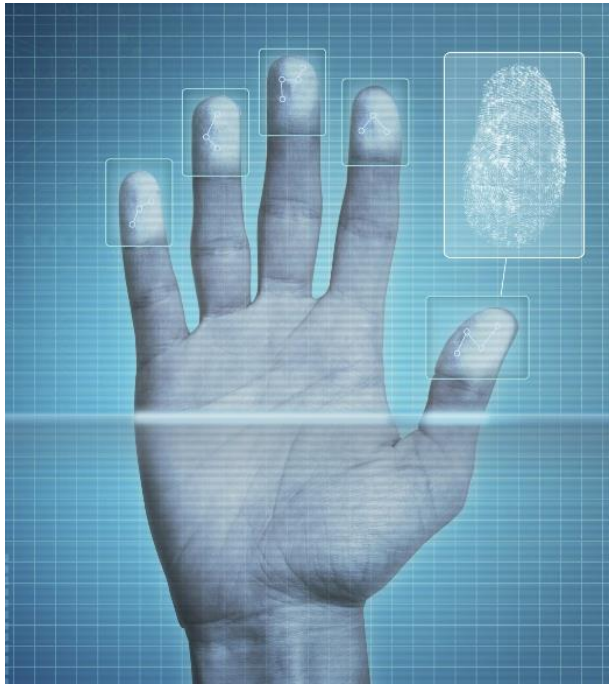
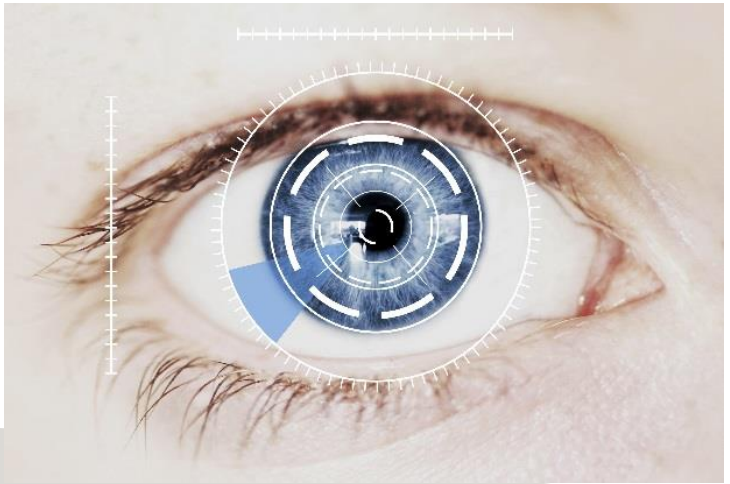
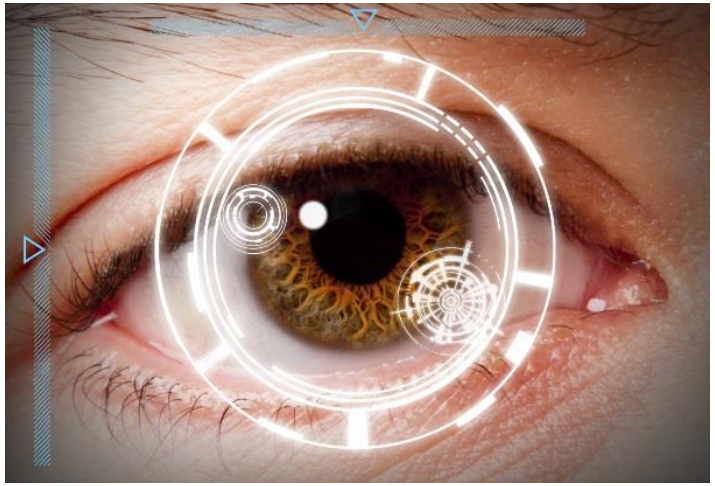
Evolución constante de los medios de pago

Pasado

Amenazas Actuales

- Contraseñas débiles
- Inyección SQL
- Suplantación de Identidad (Phishing)
- Software Malicioso (Malware)
- Vectores de Ataque Remoto
- Parchado Inadecuado

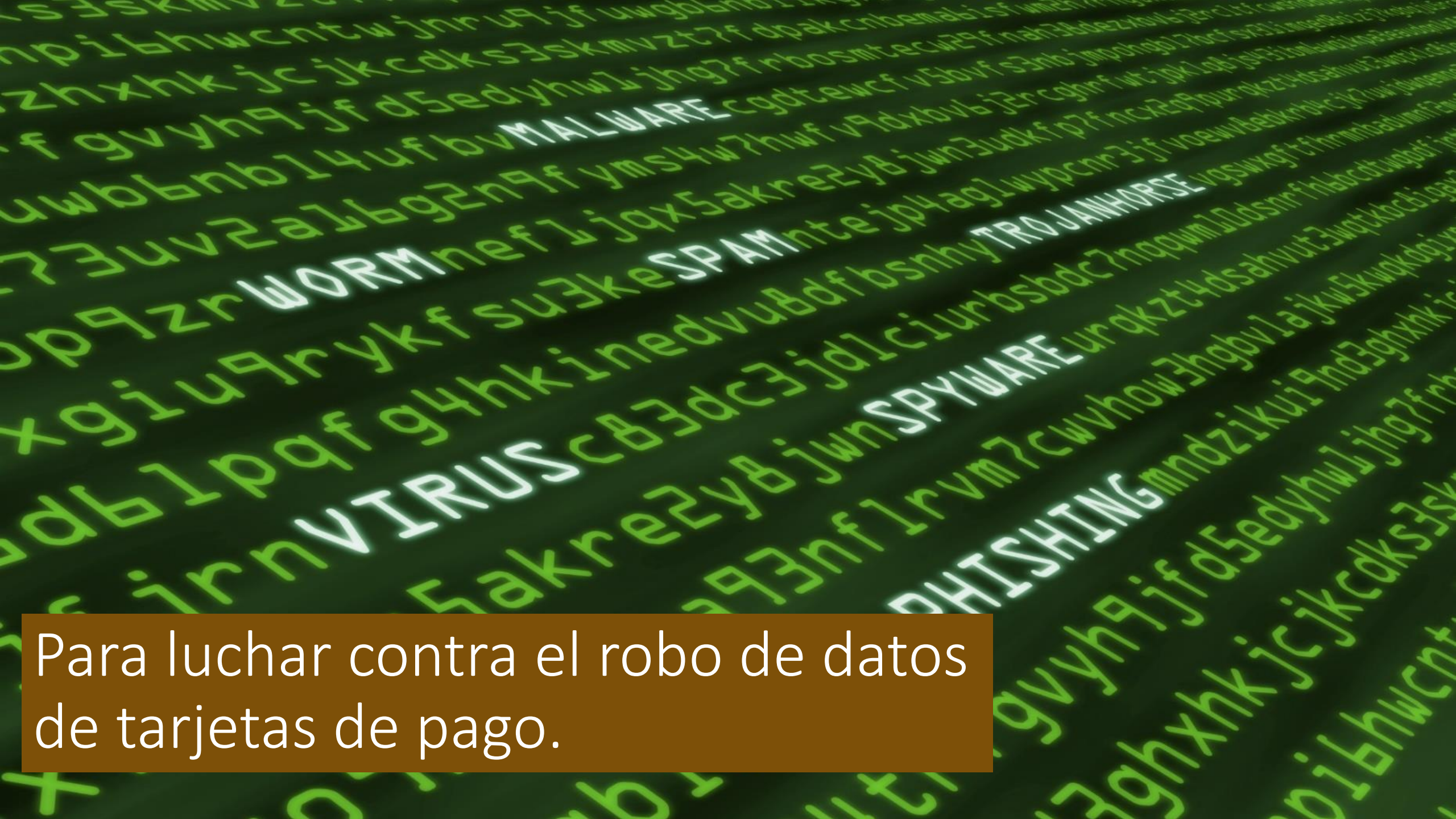

Futuras Amenazas

- Fraude con Tarjetas No Presentes
- Vulnerabilidades de Pagos sin Contacto
- Vulnerabilidades de Dispositivo Mobil (Wallets)
- Extorsión

La seguridad requiere una mentalidad de alerta 24 horas, 7 días a la semana…

… no es una vez al año y listo.

¿Por qué existe el Consejo?



Para luchar contra el robo de datos de tarjetas de pago.


10TH
PCi
Security
Standards Council
Anniversary • 2006 - 2016

Miembros Fundadores

Un Objetivo Común

Protejer, Eliminar, Devaluar los Datos de Pago

Con Estándares, Guías, Educación y Tecnologías tales como Cifrado de Punto a Punto (P2PE) y Tokenización

Gobierno Corporativo del Consejo PCI

Consejo Asesor

Comité Ejecutivo

Organizaciones Participantes

Comité de Administración (Normas y Programas)

Task Forces & Grupos de Trabajo

Grupos de Interés

Comité Ejecutivo

Mike Matan
American Express

Gina Gobeyn
Discover

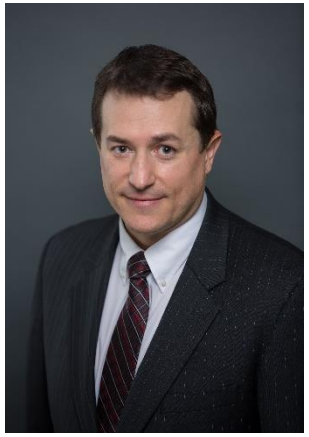
Lib de Veyra
JCB International

Bruce Rutherford
MasterCard

Karteek Patel
Visa Inc.
(2016 Chairperson)

Equipo Ejecutivo

Stephen Orfei
Gerente General



Troy Leach
Gerente de Tecnologias

Jeremy King
Director de Relaciones Internacionales

Mauro Lance
Gerente de Operaciones

John Fitzsimmons
Vice Presidente de Relaciones Públicas

Consejo Asesor

Estándares, Mejores Prácticas, Capacitación, Certificación, Alertas a la Industria

Equipos de Venta

Softwares de Pago

Entornos de Comercios y Proveedores de Servicios

Certificación – Equipos, Soluciones y Software de Pago, Empresas Asesoras e Investigadoras

Capacitación – Asesores, Investigadores

Cobertura

Ecosistema de equipos de pago, aplicaciones, infraestructura, y usuarios

Los estándares PCI evolucionan constantemente

- Retroalimentación
- Investigación
- Amenazas

Los estándares PCI evolucionan constantemente

PCI Security Standards Council

Comité de Administración

Responsable de la mantención de las normas PCI

Responsable de gestionar los programas y operaciones diarias del Consejo

Grupos de Trabajo

Grupos de Trabajo:
Rango específico de trabajo

Fuerzas de Trabajo:
Iniciativas de corto plazo

Grupos Especiales de Interés

Los objetivos para cada SIG se desarrollan en base a presentaciones en las Reuniones Comunitarias

Contenido basado en objetivos y especialización de sus participantes

Los participantes del SIG son voluntarios, coordinan objetivos y elaboran borradores

Se acuerdan?

Video Credit: Harry Williby
https://www.youtube.com/watch?v=y83ZgzuFBSE

PCI DSS Requisito 9.9

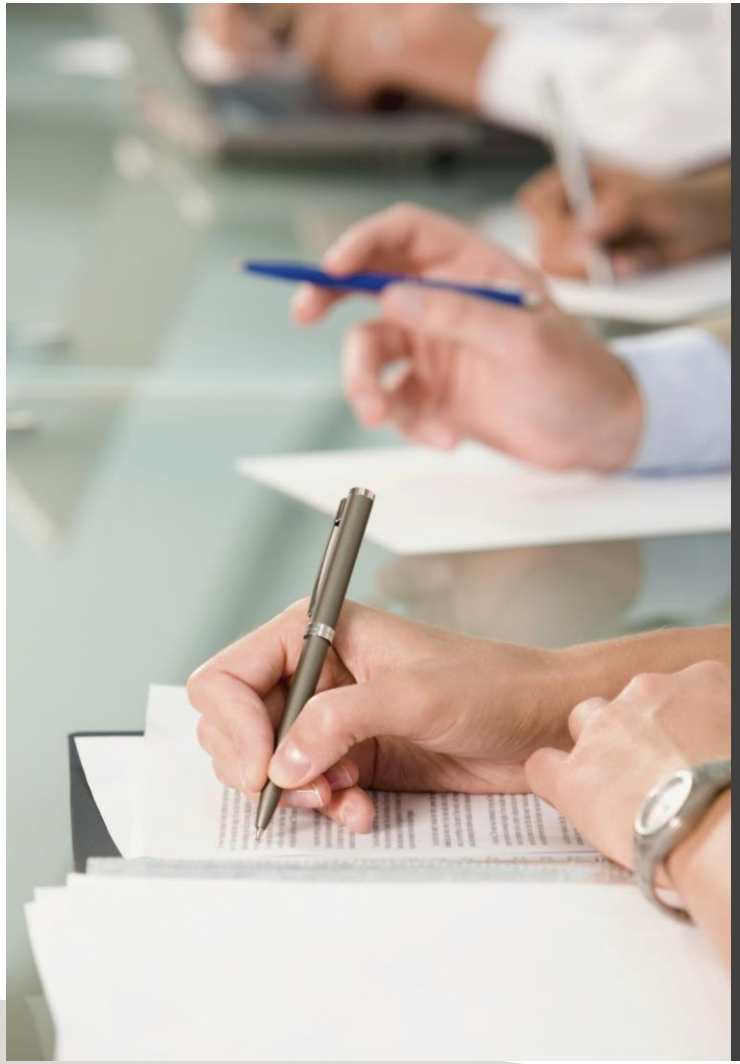
Proteja de alteraciones y sustituciones a los dispositivos que interactúan físicamente con las tarjetas para captar sus datos.

Procedimientos de prueba
9.9 Examine las políticas y procedimientos documentados para verificar que incluyen: • Mantenimiento de una lista de dispositivos • Inspección periódica de dispositivos para buscar alteraciones y sustituciones • Capacitación del personal para tomar conciencia de conductas sospechosas e informar alteraciones o sustituciones en dispositivos
9.9.1 Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única
9.9.2 Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento).
9.9.3 Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos.

Programas para Apoyar la Implementación de los Estándares

- PCI Data Security Standard
- Approved Scanning Vendor
- Payment Application DSS
- Qualified Integrator and Reseller
- Point to Point Encryption
- PIN Transaction Standards
- PCI Forensic Investigator

Cursos de Capacitación



- ✓ Internal Security Assessor (ISA)
- ✓ Point-to-Point Encryption (P2PE) Qualified Security Assessors - QSA (P2PE)Awareness Training
- ✓ PCI Essentials
- ✓ Qualified Integrators and Resellers (QIR)™
- ✓ Qualified Security Assessor (QSA)
- ✓ PCI Professional Program (PCIP)™
- ✓ Approved Scanning Vendor (ASV)
- ✓ Payment Application Qualified Security Assessor (PA-QSA)

Para mas información, visite:
www.pcisecuritystandards.org/training

PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL EXPANDS TRAINING IN SOUTH AMERICA

Chilean Payment Leaders – Transbank, Redbanc and Nexus - Join with PCI Council to Deliver First Internal Security Assessor Training in the Country

SANTIAGO, **Chile**, 4 September 2015 —Transbank, Redbanc and Nexus are the first Chilean companies to join with the Payment Card Industry Security Standards Council (PCI SSC) to train Internal Security Assessors (ISAs) in the region. Internal Security Assessors are responsible for examining cybersecurity planning and execution at the largest retailers in the country, ensuring that retailers use PCI SSC's proven security standards to protect customers' payment and personal information collected during transactions.

"By joining forces to make the first Chilean ISA class a reality, these key players in the country's payment card industry are moving data security forward another important step," said PCI Security Standards Council Chief Operating Officer Mauro Lance. "These companies understand that securing the payment chain is an industry-wide challenge, and by collaborating with each other it's easier to protect information on a national scale. This is exactly the industry synergy that the Council is trying to foster, and we're pleased to have Transbank, Redbanc and Nexus on board."

Using PCI Data Security Standards has proven to improve security of payment data and customer information, yet many organizations confuse compliance with the standards at a point in time – when assessed once per year - with ongoing, year-round protection. The ISA curriculum trains payment and IT security professionals on how to be vigilant in protecting payment data with programs that increase and sustain higher levels of security. The course provides best practices and tools for creating controls to secure cardholder data against breaches at all times.

La colaboración es la solución

La Colaboración Global es Crítica

29

Empresas miembros del Consejo Asesor a nivel mundial

741

Organizaciones Participantes a nivel mundial

Miembros Afiliados

10

Marcas Europeas de Tarjetas Domésticas

3

Asociaciones de Pago en Europa

Cooperación con Gobiernos y Cuerpos de Ley y Orden

INTERPOL

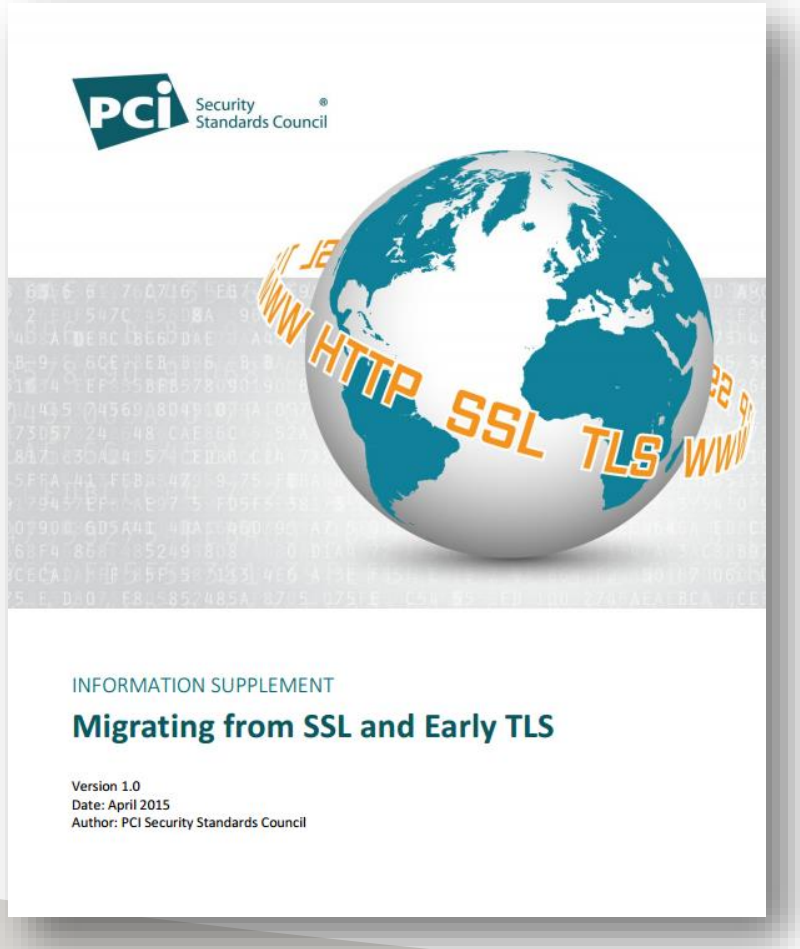
EUROPOL

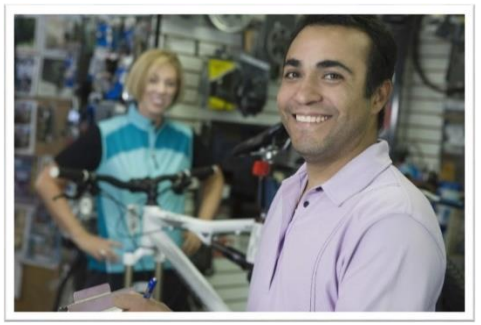
FINANCIAL SERVICES ISAC

Trabajando con el Comercio

PCI Security Standards Council

Grupo de Trabajo para Pequeños Comerciantes





Comunidad de profesionales a nivel mundial

2.047
Asesores QSAs

1.657
Asesores Internos ISAs

2.396
Profesionales PCI

El Consejo PCI capacita mas de

6.000

profesionales al año

Colaboración Regional

El Consejo PCI existe para servir a la industria

En todas las brechas que nuestro equipo forense ha investigado en los últimos 10 años, no se ha encontrado ninguna empresa que estuviese en cumplimiento *(con el estándar)* al momento de la brecha - esto demuestra la importancia del cumplimiento con PCI DSS.

- Verizon's 2015 PCI Compliance Report

Recursos

Skimming

A Resource Guide from the PCI Security Standards Council

WHAT IS SKIMMING?

Skimming is copying payment card numbers and personal identification numbers (PIN) 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 (ATM), and kiosks that captures the information from the magnetic stripe.

FACTS & FIGURES

$2 billion
The estimated global cost of skimming[1]

$50,000
The average loss from skimming crime[2]

Skimming-related counterfeit card fraud is the leading type of third-party card fraud[3]

92%
Skimming is the #1 ATM c… globally making up 92% o… attacks at the ATM[1]

From Jan-Apr 2015, the nu… of attacks on debit cards … ATMs reached the highes… that period in at least 20…

All amounts are in U.S. Dollars

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 plastic 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 VIDEOS

Safeguard Against Skimming

ATM SKIMMER

The ATM Scam

RELATED INDUSTRY RESOURCES

Skimming the Surface

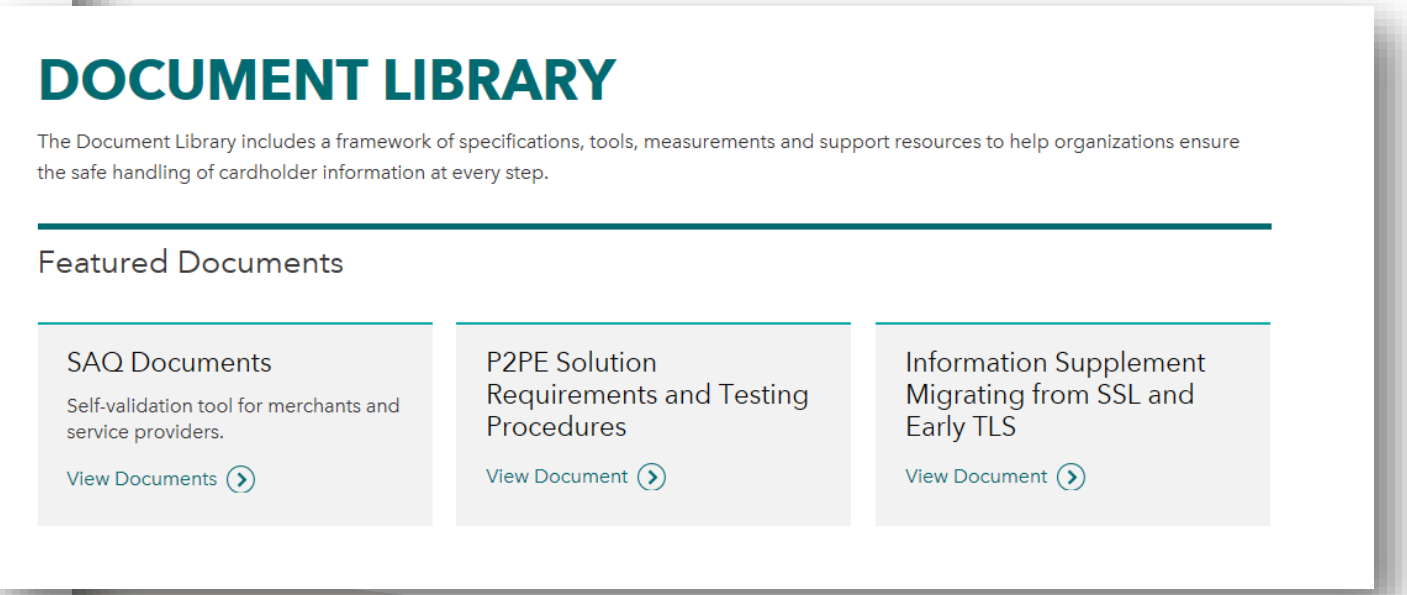
All About Skimmers

Skimming is a Scam

1: Source: ATMmarketplace.com 2: Source: Aite Group 3: Source: Mercator Advisory Group 4: Source: FICO

PCI Security Standards

Nuestra biblioteca de recursos está a disposición de la industria en forma gratuita: **www.pcisecuritystandards.org/document_library**



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.

Featured Documents

SAQ Documents

Self-validation tool for merchants and service providers.

View Documents

P2PE Solution Requirements and Testing Procedures

View Document

Information Supplement Migrating from SSL and Early TLS

View Document

Palabras finales…

Preguntas y Respuestas

Muchas Gracias!

PCI Security Standards Council®