



XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

LA INDUSTRIALIZACION DE LOS ATAQUES FINANCIEROS ON-LINE

Presentado por:
Mario Benedetti C.
BDM – Cono Sur

Organizado por



EASY SOLUTIONS
TOTAL FRAUD PROTECTION®

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Chaos in the Online Channel

Malware Explosion

Compound Attacks

Lack of integration



2012: The Year Malware Went Nuclear

05 December 2012



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

How to Stop What you Cannot See?

Most attacks are indirect



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

How to Stop What you Cannot See?

Good Intelligence is Hard to Come By



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

How to Stop What you Cannot See?

Attacks Usually Occur without Warning



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Weak Password?

Why passwords have never been weaker— and crackers have never been stronger

Thanks to real-world data, the keys to your digital kingdom are under assault.

by Dan Goodin - Aug 20 2012, 9:00pm EDT

HACKING 334

Facebook sees 600,000 compromised logins per day—0.06% of all logins

Facebook has released a statistic showing that fewer than one-tenth of one ...

by Jon Brodtkin - Oct 28 2011, 1:33pm EDT

22

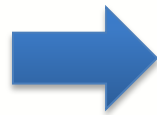
Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Attack and Counterattack



MITB

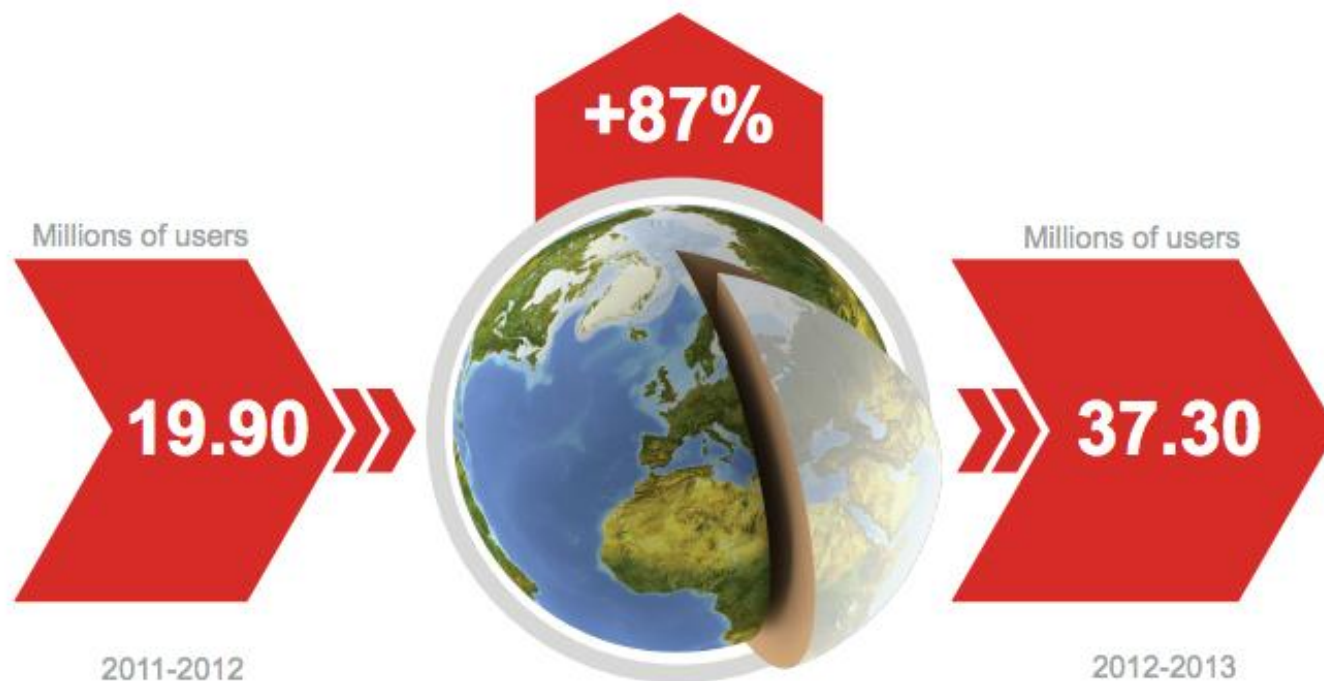
Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Phishing Trends – 2011 to 2013



Kaspersky, 2013

Organizado por

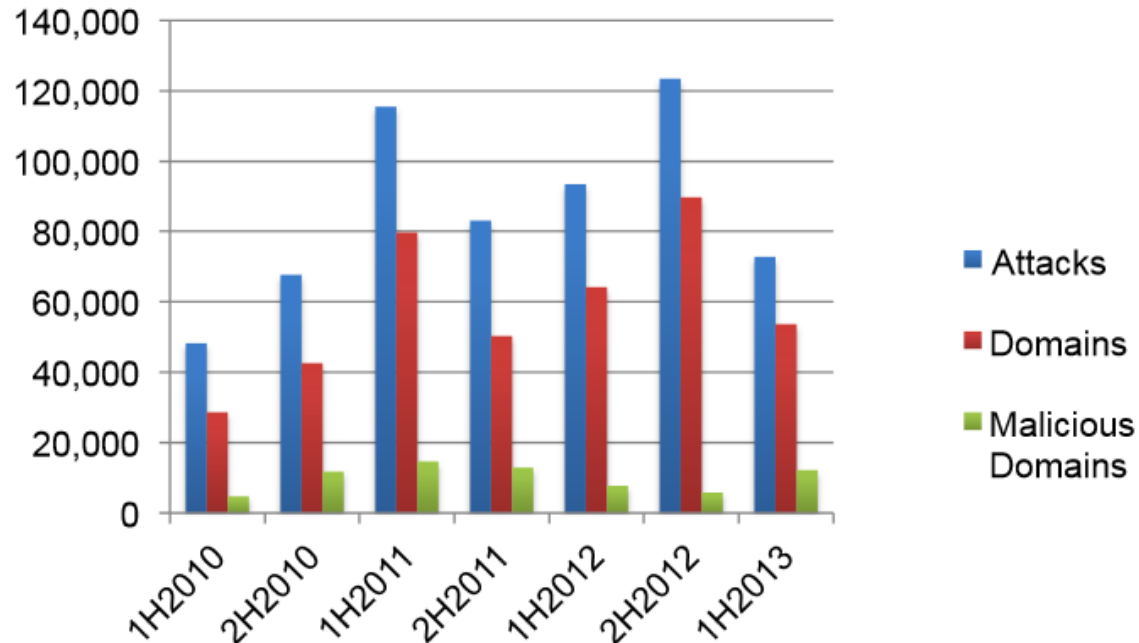


**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Phishing Trends – 2013

**Phishing Attacks, Domains
1H2010 - 1H2013**



Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Mobile Malware Growth – 1 year

TOTAL MOBILE MALWARE SAMPLES ACROSS ALL OPERATING SYSTEMS AT END OF Q1

Q1 2012



Q1 2013



+614%

Juniper Networks

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2007

Gozi Trojan - \$1000

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2009

Zeus Trojan - \$8000

SpyEye Trojan - \$6000

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2010

Zeus Trojan - \$8000 base

SpyEye Trojan - \$500 + modules

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2011

SpyEye Trojan - \$95

IcelX Trojan - \$1500 (unlimited)

Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2012

Explosion of Variants

\$100-\$10,000

Private Trojans

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Trojan Kit Prices

2013

Rapid Growth of Mobile Malware

\$100-\$10,000

Expansion of Variants

Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Mobile Malware Pricing

Pricing

Sample Toolkits & Service	Price (US\$) - March 2013	Example Descriptions
Mobile intrusion (keyloggers)	Open Source - 400	Java & Python Keyloggers, Mobistealth,
Mobile Intrusion (surveillance)	500 - 5,000	Re-engineered Finfisher, Finfisher Lite & FlexiSpy extended copies
Mobile malware for banking theft	10,000 - 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. Pth capabilities)
Mobile botnet (rental)	50 - 400	Hourly rates
Mobile botnets (operational & tailored source code)	4,000 - 30,000	Mobile ISP service, SMS, & Drive by
Mobile malware for black SEO and underground partnership programs	5,000 - 10,000	Used to traffic redirects, J2ME midlets, or standard applications for the popular platforms.
Mobile traffic by targeted country	10 - 30 per 1,000 hosts	Can be bought through special underground services (by area, by country)
Mobile SMS spam service	2-8 cents per 1 SMS	Mobile spamming
Mobile SMS spamming tool	30-50	SMS spammer by klychev v0.3
Mobile flooder (Skype or SIP)	30-80	Skype Flooder

Table 1: eCrime market current pricing (March 2013)

Anti-Phishing Working Group

www.celaes2013.com

Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Web Injection Examples

Bank of America  Sign In

Unrecognized computer

ATM or Debit Card Number^{*}:
(16 digits, no dashes or spaces)

ATM or Debit Card PIN^{*}:

ATM or Debit Card Identification Number (CVV)^{*}:

Expiry date^{*}:

Social Security Number or Tax Identification^{*}: - -

Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

The End Result

Global Hack Nets \$45
Million In ATM Crime Spree

ReadWrite Editors · May 10th, 2013

+1 3 Tweet 119 Share 14 Like 12



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

2013 FACES OF FRAUD: THE THREAT EVOLUTION

How Are Organizations Addressing Fraud, Cyberthreats?



Sponsored by



www.celaes2013.com

Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

> *Participants*

200

Chief Information Security Officers, Chief Information Officers, Directors of IT, and Senior IT Management at primarily **U.S. Financial Institutions**

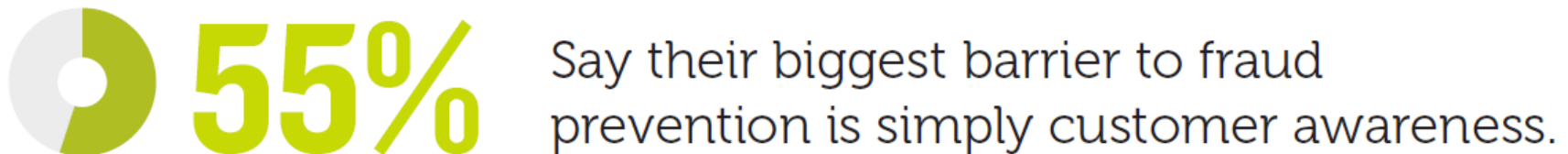
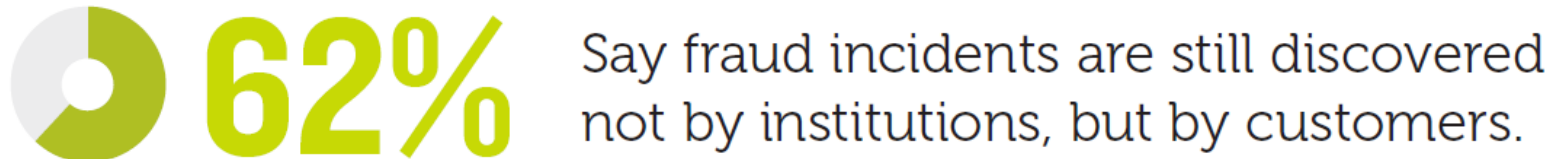
Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

> **Highlights**



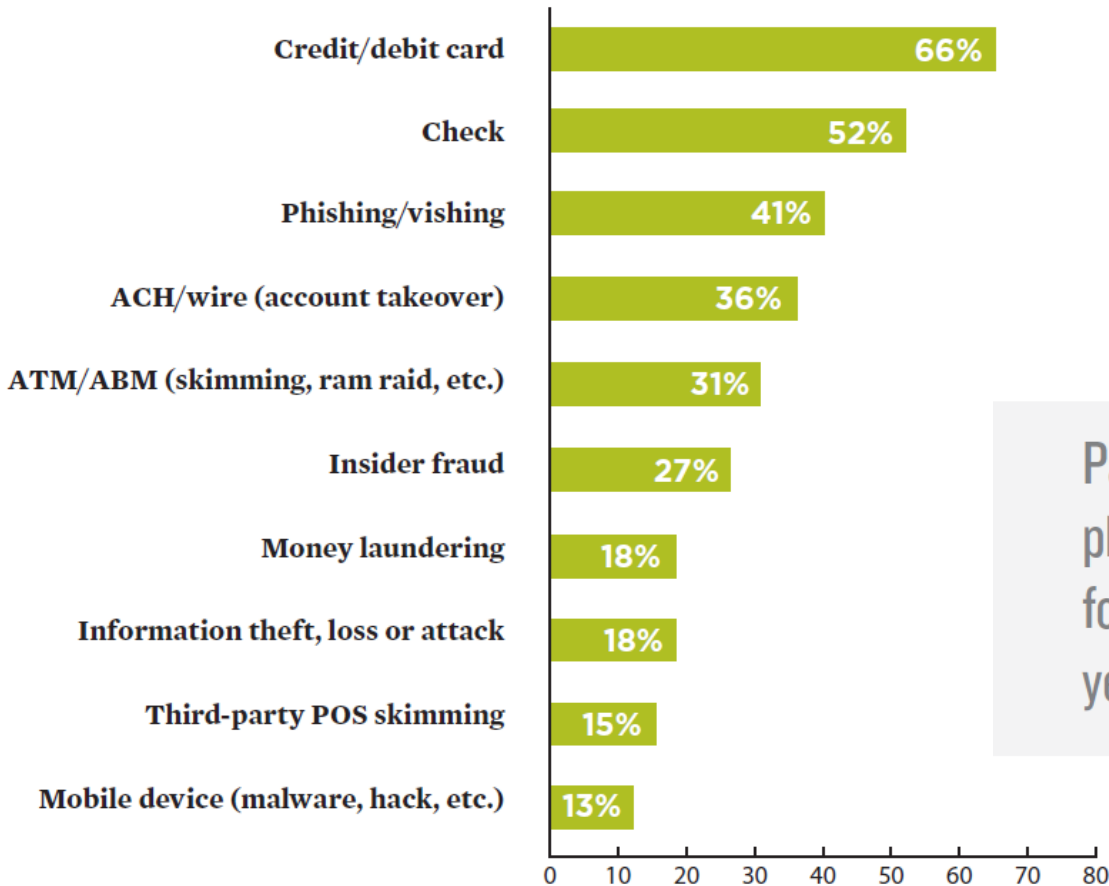
Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Which types of fraud have you experienced in the past year?



Payment card, check fraud and phishing/vishing are the top forms of fraud faced by this year's survey respondents.

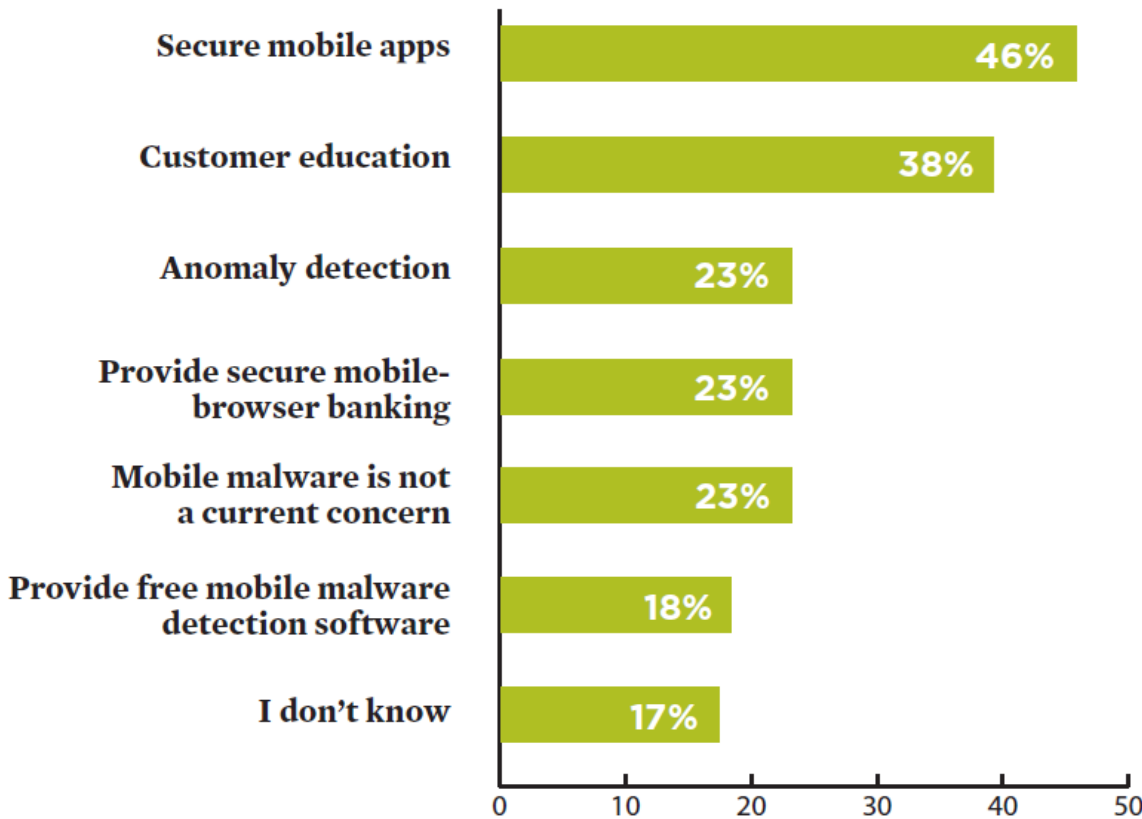
Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

How do you defend against **mobile malware** attacks?



Nearly one-quarter of survey respondents said this is not a current concern for them (despite the fact mobile malware increased

614%*

from March 2012 to March 2013).

[*Juniper Networks, June 2013](#)

Organizado por



XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES

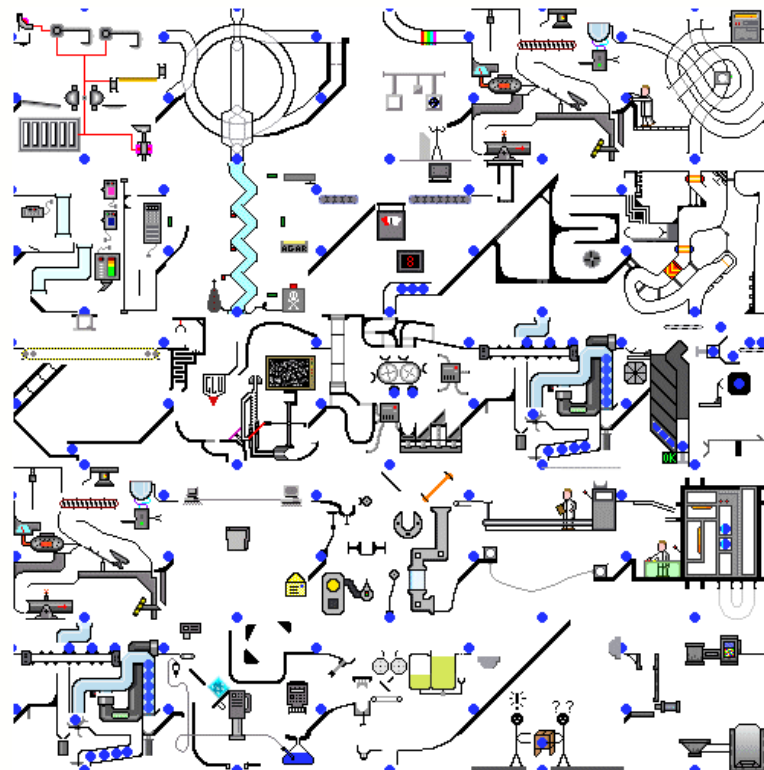
Lima, 25 - 26 de Noviembre, 2013

Complexity is the Enemy

Lack of flexibility

**Rigidity harms
innovation**

**Fraud is constantly
evolving**



Organizado por



**XXVIII Congreso Latinoamericano
de Seguridad Bancaria - CELAES**

Lima, 25 - 26 de Noviembre, 2013

Improve the Odds

Seek simplicity

Understand the changing
threat environment

Integrate data and tech

Build a flexible and layered
defense

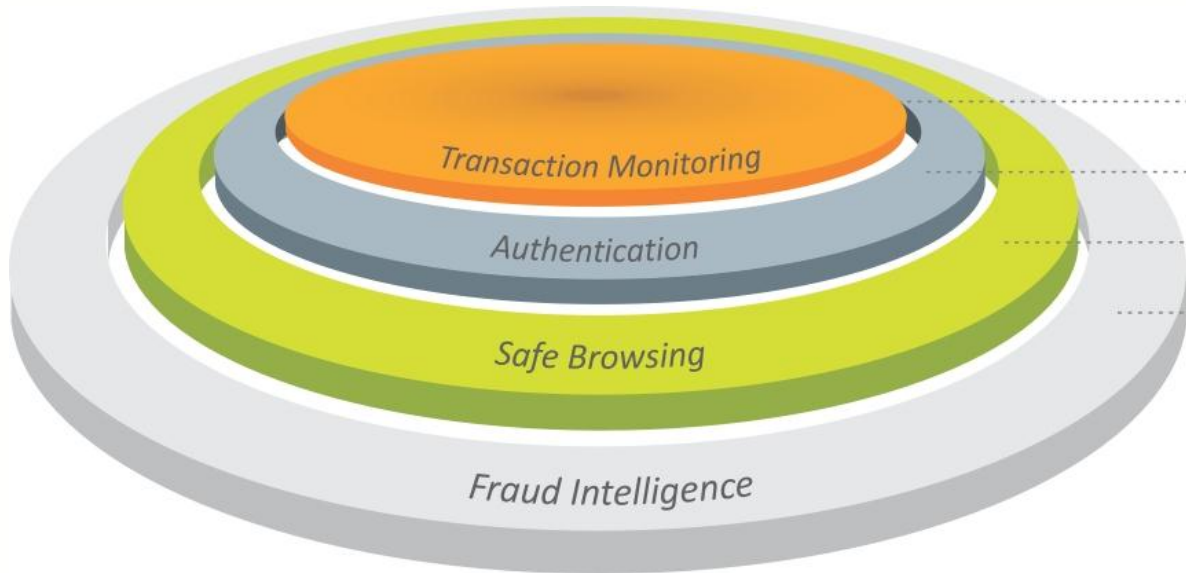


Organizado por



XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013



Organizado por



XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013



EASYSOLUTIONS
TOTAL FRAUD PROTECTION®

Follow us: @goeasysol

www.celaes2013.com