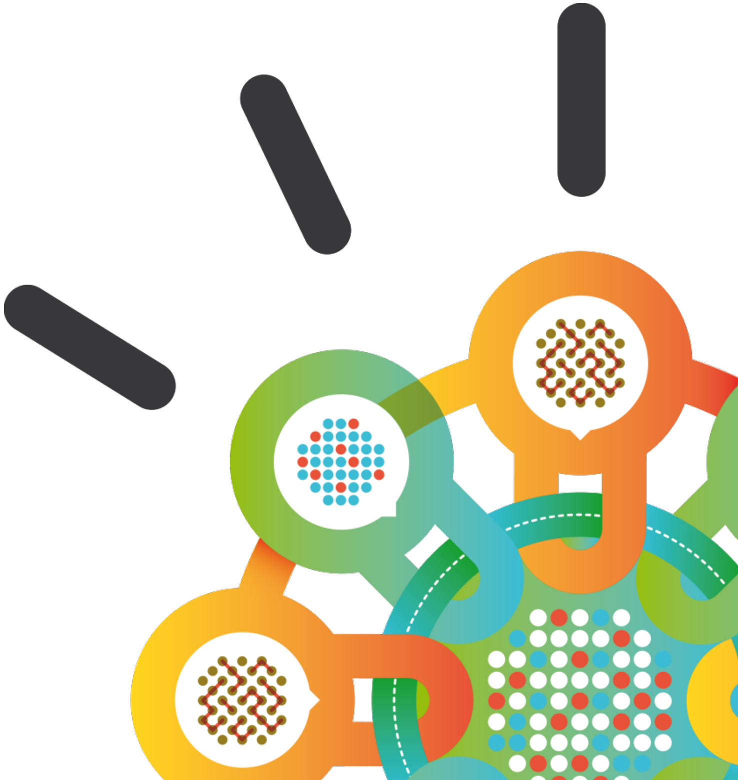
Security Intelligence.
Think Integrated.

IBM Security Trusteer

Malware Based Frauds & Countermeasures

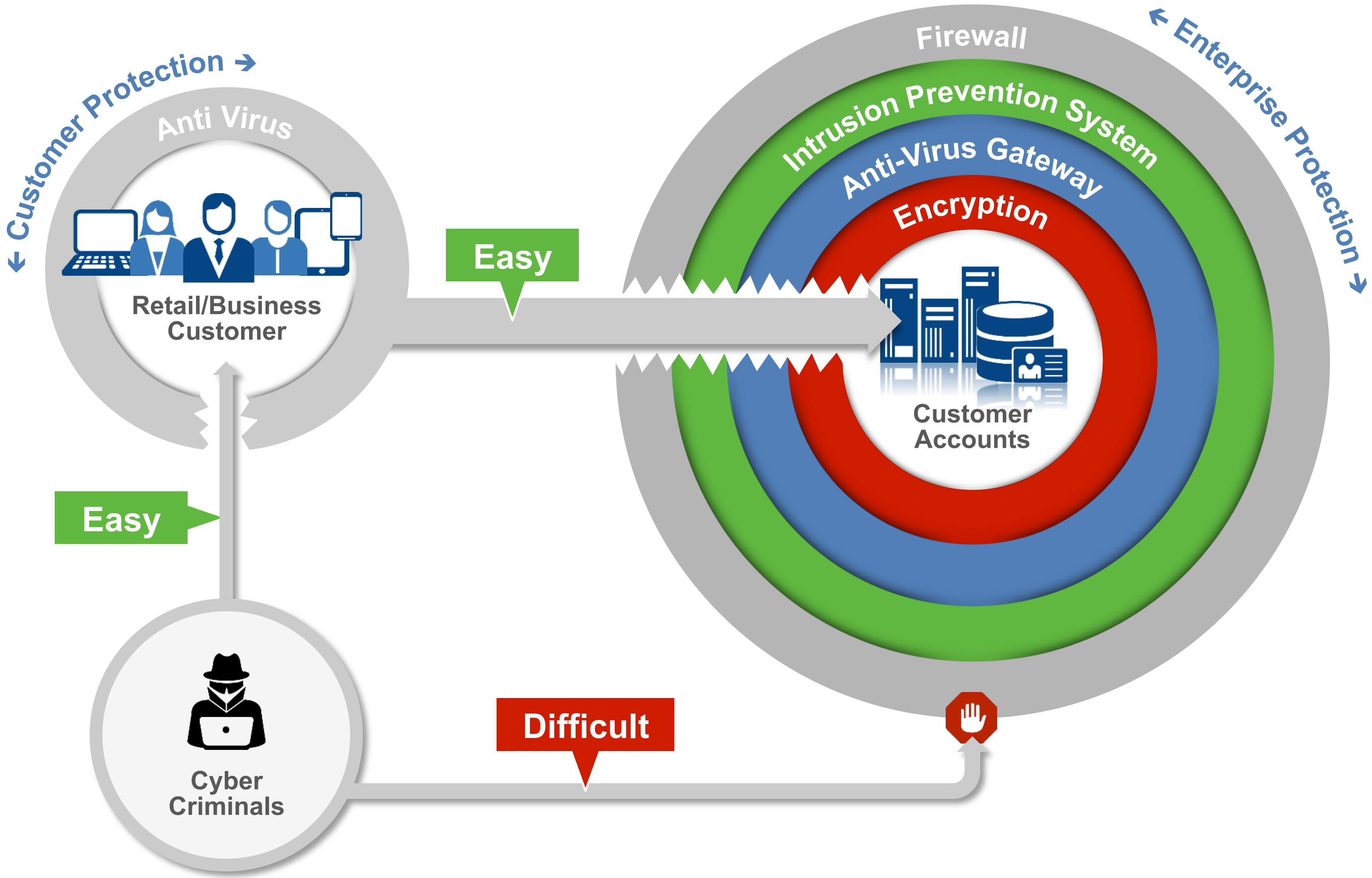


Massimiliano Rijllo

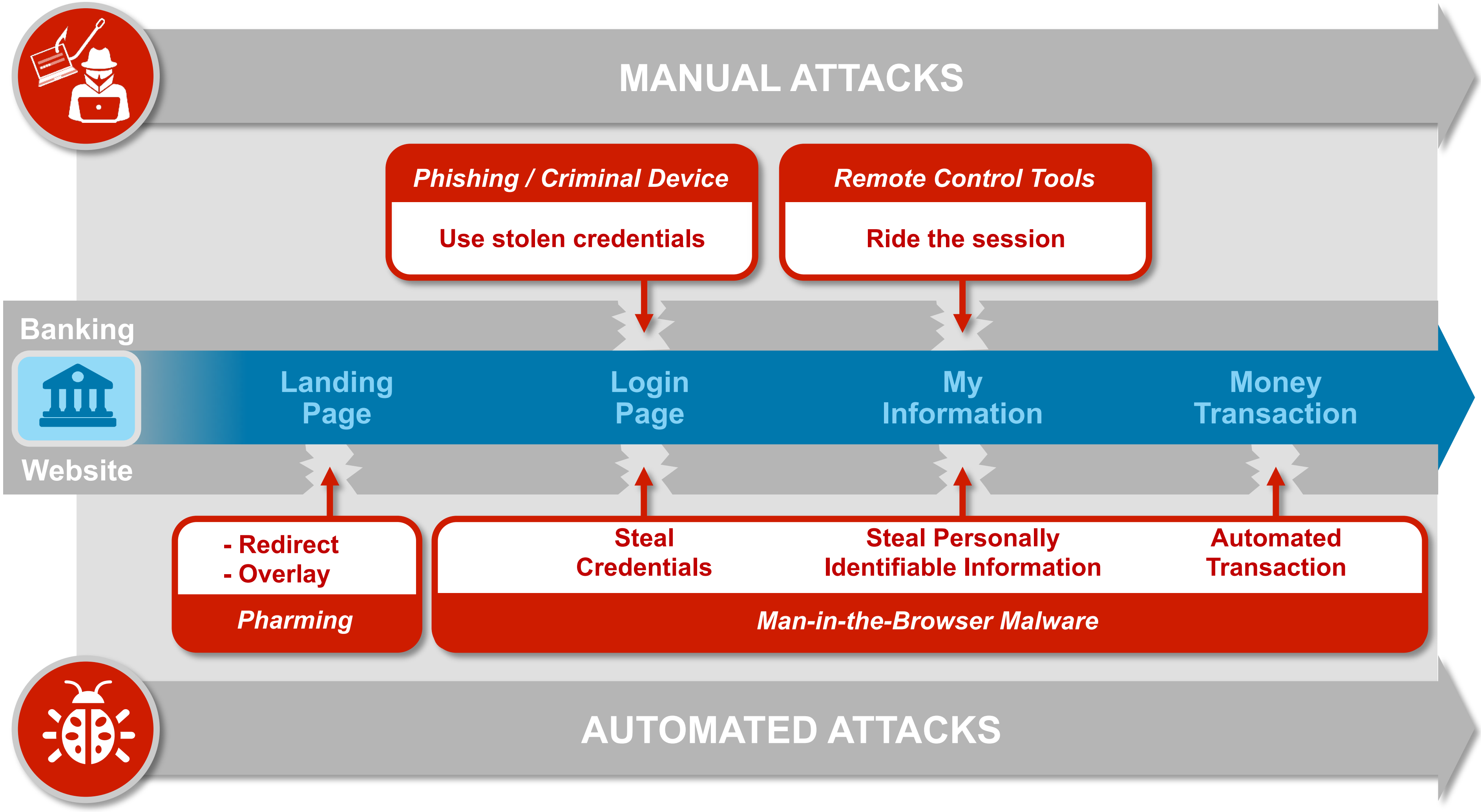
Web Fraud Sales Leader Italy

novembre 23, 2014

Criminals attack the weak link



Fraud attack methods evolve quickly



MANUAL ATTACKS

Phishing / Criminal Device

Use stolen credentials

Remote Control Tools

Ride the session

Banking Website

Landing Page

Login Page

My Information

Money Transaction

- Redirect
- Overlay

Pharming

Steal Credentials

Steal Personally Identifiable Information

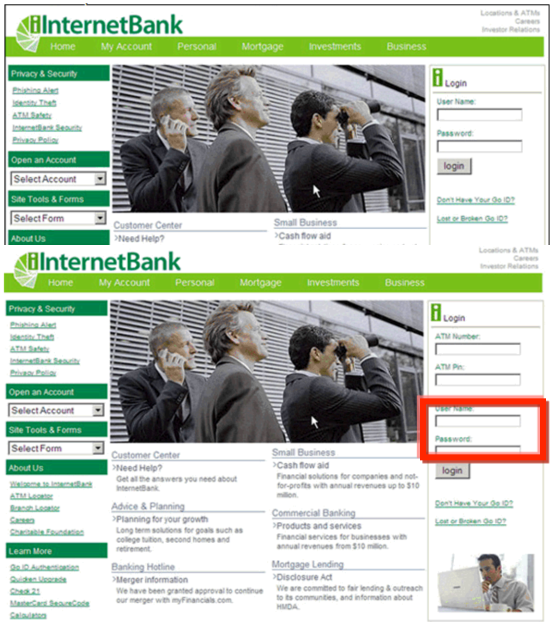
Automated Transaction

Man-in-the-Browser Malware

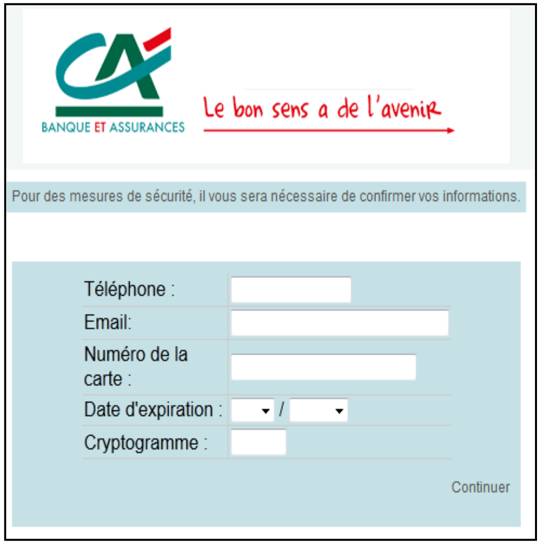
AUTOMATED ATTACKS

Fraud attack methods evolve quickly

Man-in-the Browser Malware



Man-in-the Browser Malware



Pour des mesures de sécurité, il vous sera nécessaire de confirmer vos informations.

Téléphone :

Email:

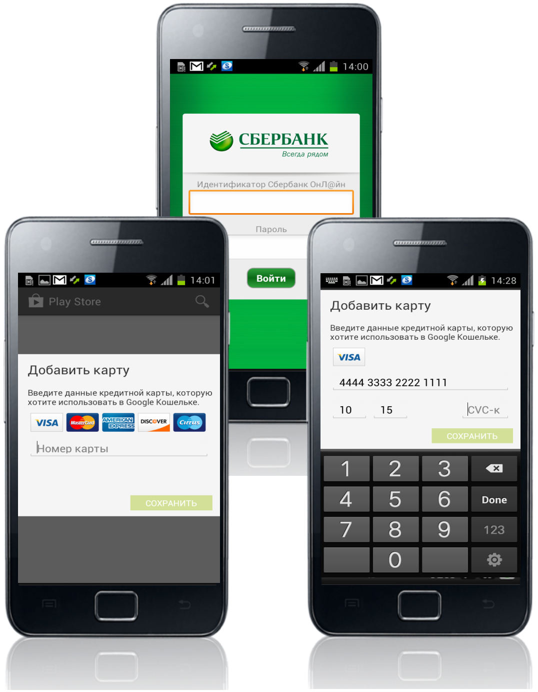
Numéro de la carte :

Date d'expiration : /

Cryptogramme :

Continuer

Mobile Malware



Идентификатор Сбербанк ОнЛ@йн

Пароль

Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

Номер карты

СОХРАНИТЬ

Добавить карту

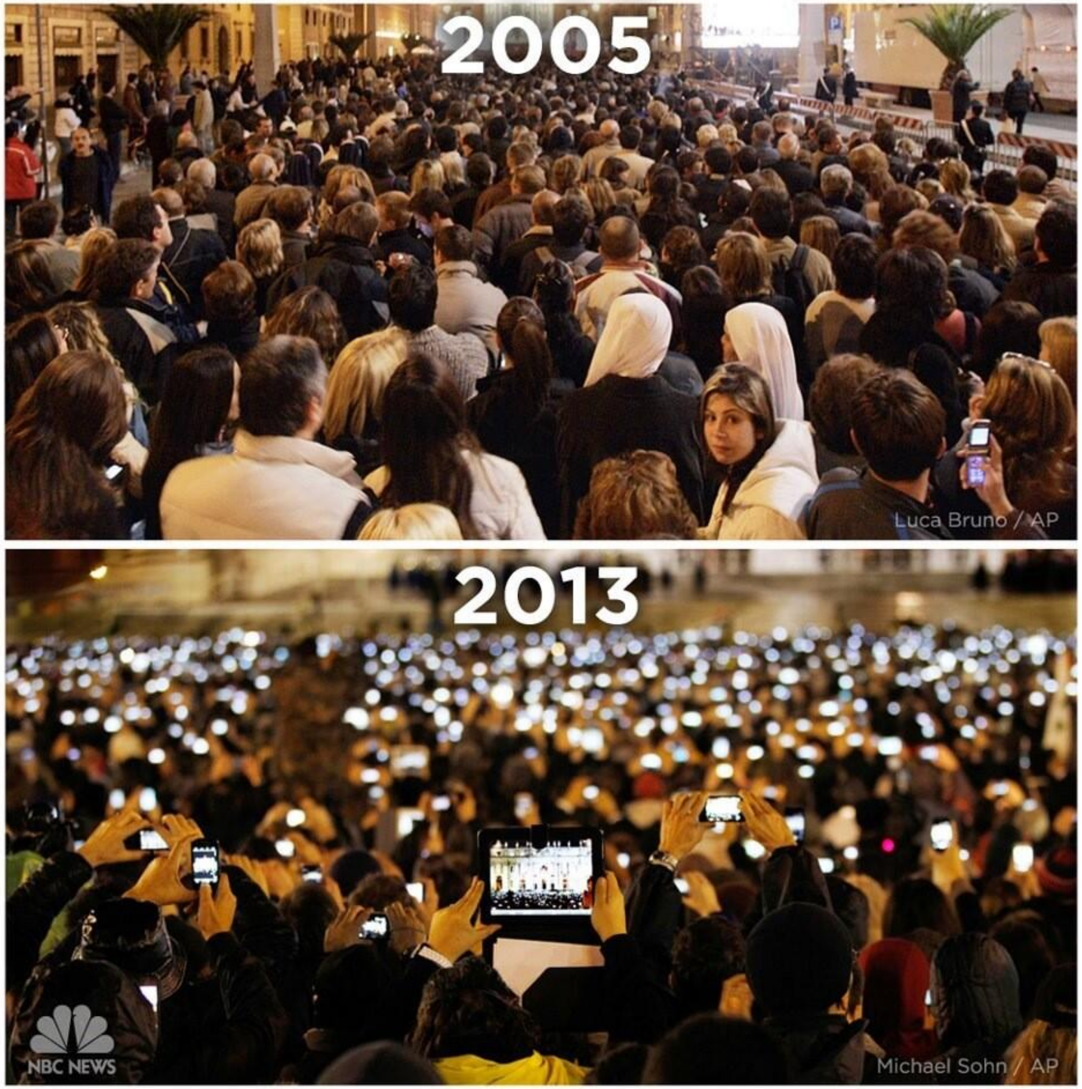
Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

4444 3333 2222 1111

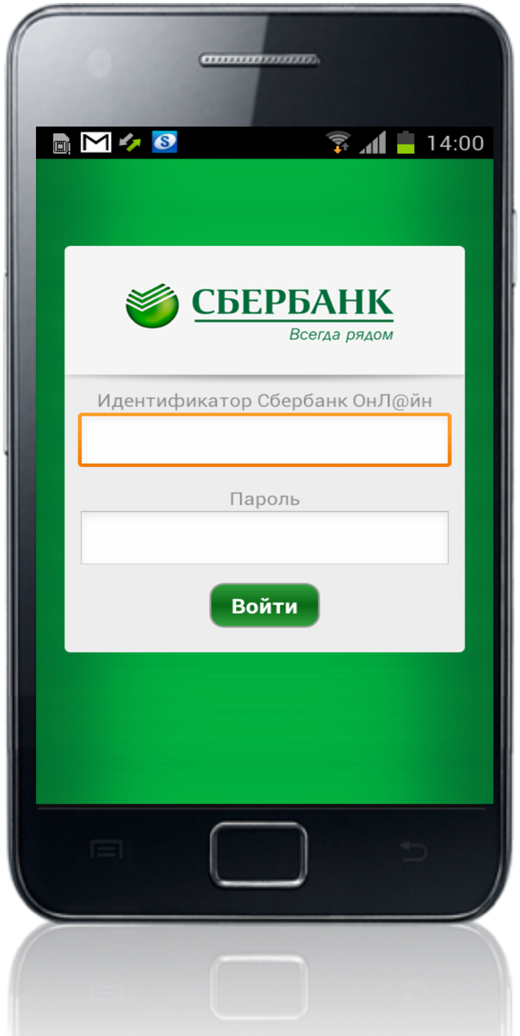
10 15 CVC-к

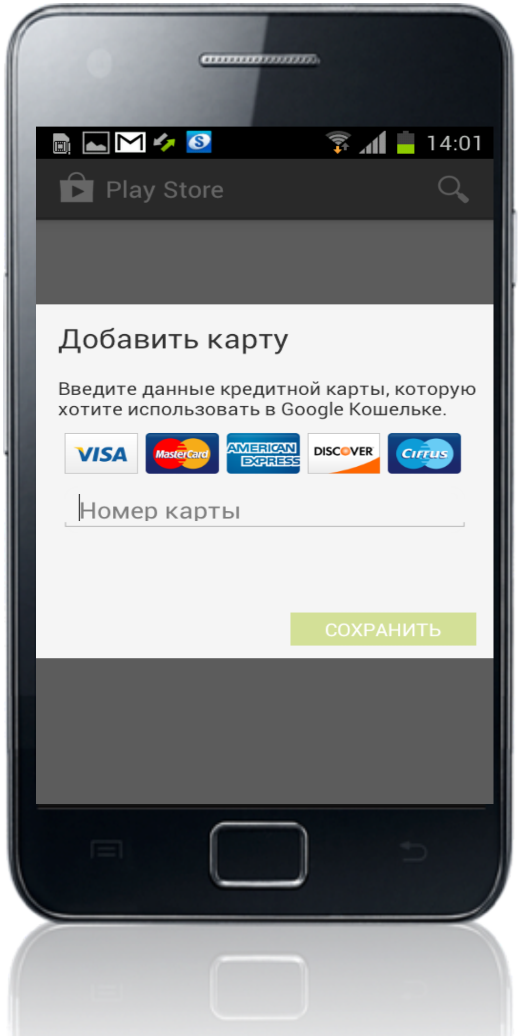
СОХРАНИТЬ

How Times Have Changed…



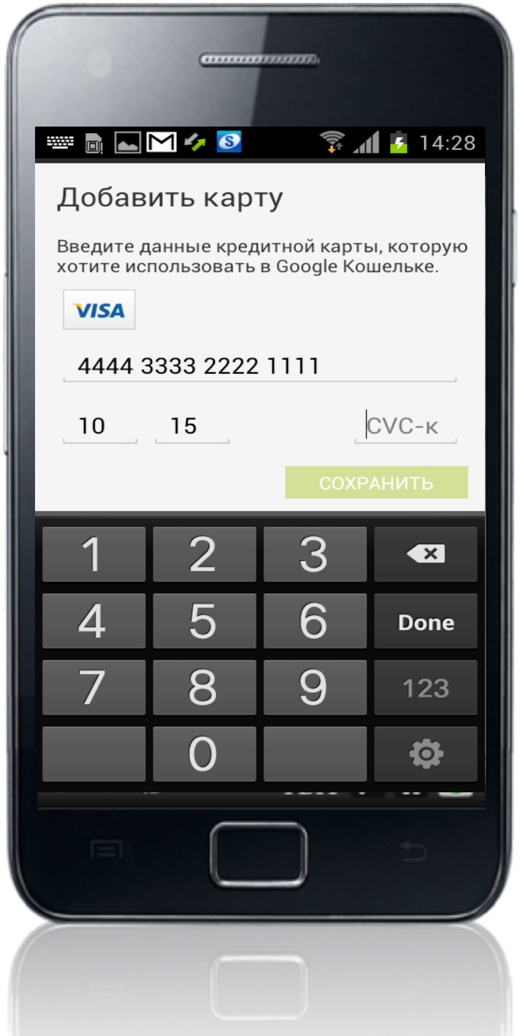
Overlay Mobile Attack





Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.



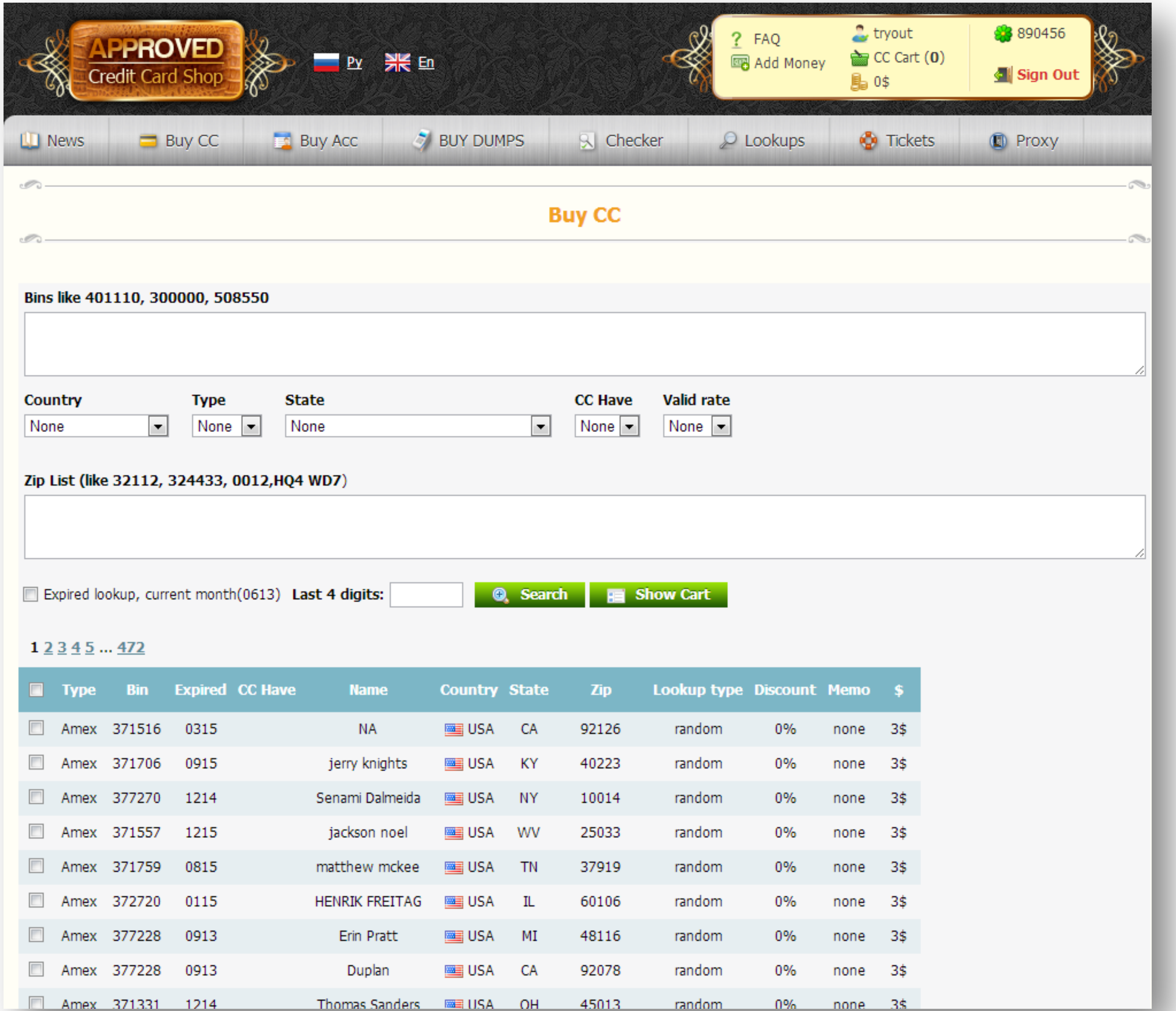
Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

4444 3333 2222 1111

10 15 CVC-к

Credit Card Store



Buy CC

Bins like 401110, 300000, 508550

Country	Type	State	CC Have	Valid rate
None	None	None	None	None

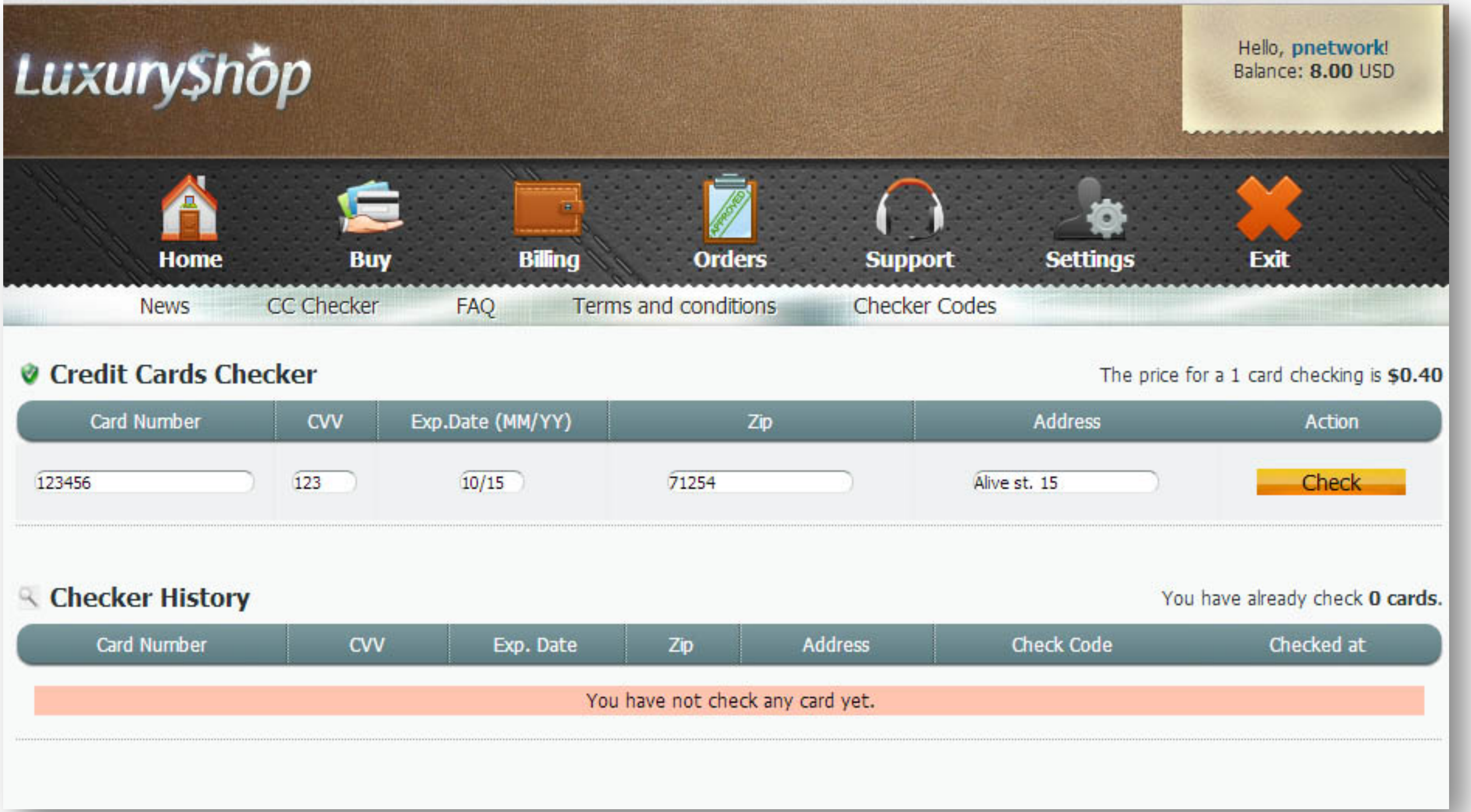
Zip List (like 32112, 324433, 0012,HQ4 WD7)

□ Expired lookup, current month(0613) **Last 4 digits:** Search Show Cart

1 2 3 4 5 ... 472

□	Type	Bin	Expired	CC Have	Name	Country	State	Zip	Lookup type	Discount	Memo	$
□	Amex	371516	0315		NA	USA	CA	92126	random	0%	none	3$
□	Amex	371706	0915		jerry knights	USA	KY	40223	random	0%	none	3$
□	Amex	377270	1214		Senami Dalmeida	USA	NY	10014	random	0%	none	3$
□	Amex	371557	1215		jackson noel	USA	WV	25033	random	0%	none	3$
□	Amex	371759	0815		matthew mckee	USA	TN	37919	random	0%	none	3$
□	Amex	372720	0115		HENRIK FREITAG	USA	IL	60106	random	0%	none	3$
□	Amex	377228	0913		Erin Pratt	USA	MI	48116	random	0%	none	3$
□	Amex	377228	0913		Duplan	USA	CA	92078	random	0%	none	3$
□	Amex	371331	1214		Thomas Sanders	USA	OH	45013	random	0%	none	3$

Credit Card Checkers



Hello, pnetwork!
Balance: 8.00 USD

Credit Cards Checker

The price for a 1 card checking is $0.40

Card Number	CVV	Exp.Date (MM/YY)	Zip	Address	Action
123456	123	10/15	71254	Alive st. 15	Check

Checker History

You have already check 0 cards.

Card Number	CVV	Exp. Date	Zip	Address	Check Code	Checked at

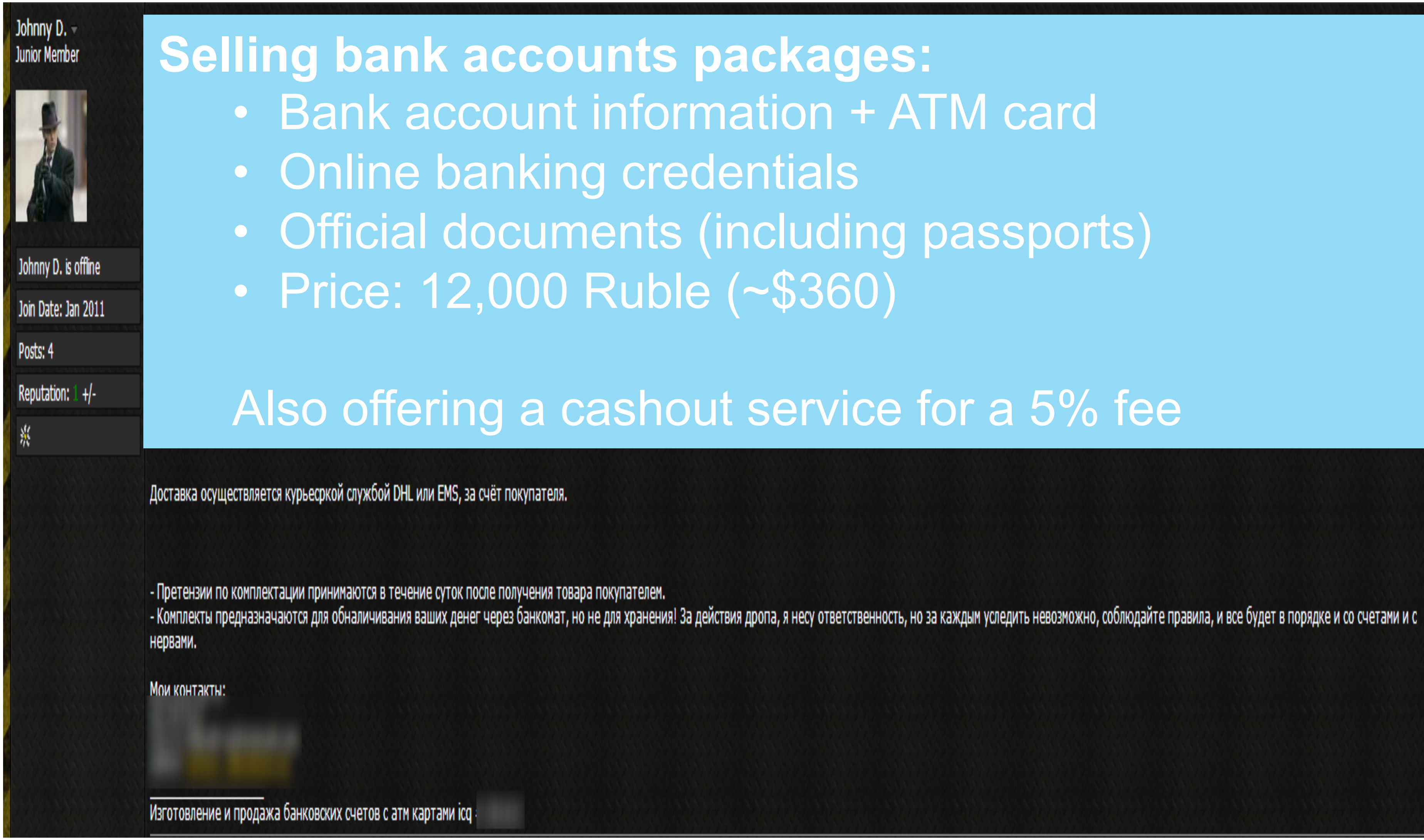
You have not check any card yet.

Identity Services

Selling bank accounts packages:

- Bank account information + ATM card
- Online banking credentials
- Official documents (including passports)
- Price: 12,000 Ruble (~$360)

Also offering a cashout service for a 5% fee



Johnny D.
Junior Member

Johnny D. is offline

Join Date: Jan 2011

Posts: 4

Reputation: 1 +/-

Доставка осуществляется курьесркой службой DHL или EMS, за счёт покупателя.

- Претензии по комплектации принимаются в течение суток после получения товара покупателем.
- Комплекты предназначаются для обналичивания ваших денег через банкомат, но не для хранения! За действия дропа, я несу ответственность, но за каждым уследить невозможно, соблюдайте правила, и все будет в порядке и со счетами и с нервами.

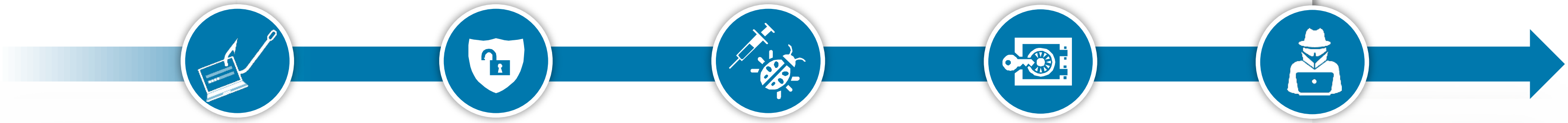
Мои контакты:

[redacted]

Изготовление и продажа банковских счетов с атм картами icq : [redacted]

A loosing battle ?

1. Humans will always make mistakes
2. System and application vulnerabilities continue to emerge
3. Malware detection will always lag



Social Engineering
Phishing

Vulnerability
Exploit

Malware
Infection

Fraud Scheme
Execution

Money
Loss

SECURITY

Gameover ZeuS adds nasty trick

Crypto t

By Richard Chi

Cybercrime Losses Top $400 Billion Worldwide, Study Claims

By Jeremy Kirk
Mon, June 09, 2014

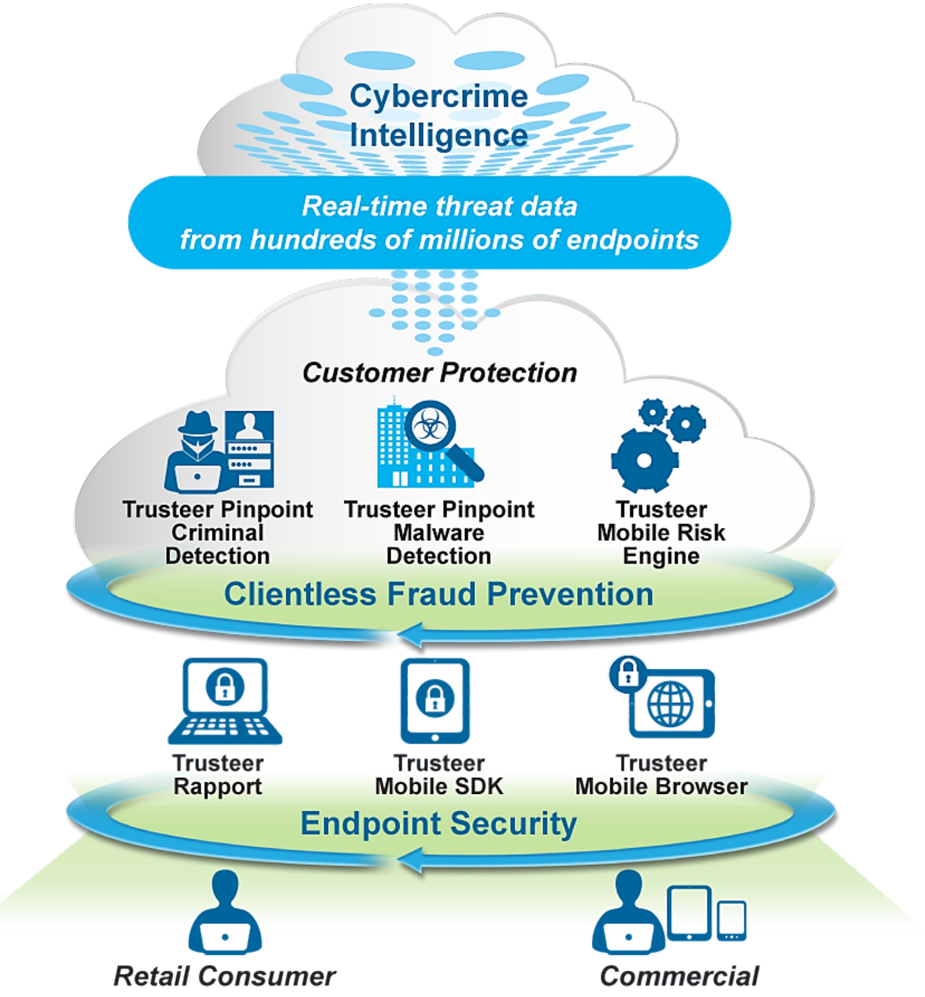
Cybercrime worries and costs on the rise

June 10, 2014, 3:00 pm MDT

User vs Cyber Crime…

Cybercrime prevention architecture

Comprehensive platform for fraud detection and prevention


Cybercrime Intelligence
Real-time threat data from hundreds of millions of endpoints
Customer Protection
Trusteer Pinpoint Criminal Detection
Trusteer Pinpoint Malware Detection
Trusteer Mobile Risk Engine
Clientless Fraud Prevention
Trusteer Rapport
Trusteer Mobile SDK
Trusteer Mobile Browser
Endpoint Security
Retail Consumer
Commercial

Clientless Fraud Prevention

- **Trusteer Pinpoint Criminal Detection**
  Conclusive detection of criminals and account takeover attempts
- **Trusteer Pinpoint Malware Detection**
  Accurate, real-time malware detection
- **Trusteer Mobile Risk Engine**
  Conclusive detection of mobile-fraud risks from compromised end user and criminal-owned devices

Endpoint Security

- **Trusteer Rapport**
  Prevents and removes financial malware and detects phishing attacks
- **Trusteer Mobile SDK**
  Embedded security library for native apps that detects compromised / vulnerable devices
- **Trusteer Mobile Browser**
  Secure, risk-based mobile web access

Why IBM Trusteer?

- **450+ leading global organizations put their TRUST in us**
- **270,000,000+ protected endpoints**

Prevent “Root Cause” of Fraud

Improve Your Customer Experience

Reduce Operational Impact

Utilize Real-time Intelligence Service

7/10 Top U.S. Banks

9/10 Top U.K. Banks

4/5 Top Canadian Banks

2/4 Top Japanese Banks

Major European Banks

IBM Trusteer delivers quantifiable results

100%

Reduction in *Online Fraud*

Many Global Customers

30%

Reduction in *Cross Channel Fraud* in 6 months

Top 5 U.S. Bank

50%

Reduction in *Risk Engine False Positives*

Top 5 U.K. Bank

80%

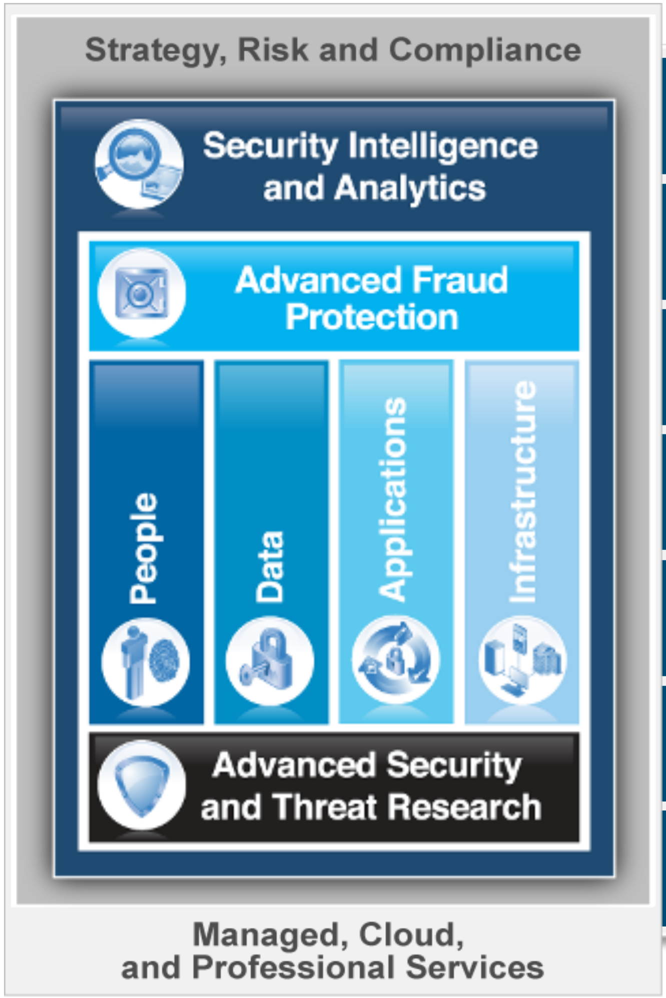
Reduction in *Phone Channel Fraud* in 2 weeks

Top 10 U.K. Bank

IBM Security

Integrated capabilities delivered across a comprehensive security framework

The IBM Security Framework


Strategy, Risk and Compliance
Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Managed, Cloud, and Professional Services

Detect, analyze, and prioritize threats	QRadar
Reduce fraud and malware	Trusteer
Manage users and their access	Identity and Access Management
Discover and harden valuable assets	InfoSphere Guardium
Secure critical business applications	AppScan
Protect infrastructure against attacks	Network and Endpoint Protection
Monitor and evaluate today's threats	IBM X-Force

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.