



ON PHISHING

MODI OPERANDI AND INVESTIGATION CHALLENGES

PROTEUS PROJECT

Polícia Judiciária

Lisboa, Portugal – Outubro 2015




Agenda

- Identity theft definition
- Phishing MO
- Why homebanking
- Approaching the MO
- Tackling the difficulties



First remarks

- “ ... all others pay cash!”
- Thomas Stearns Elliot:
 - “[...] Where is the life we have lost in living?
Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information? [...]”

T. S. Elliot, “The Rock” (1936)



Definitions

PHISHING

- ID theft?
- Burglary?
- Fraud?
- Crime?
- Technique?

THEFT

FACTS!

Step 2: Choose the payment method

☐ Credit Card:

- ☐ PayPal
- ☐ amazonpayments[™] (USA Only) **New!**
- ☐ Google Checkout
- ☐ clickandbuy
- ☐ 3iFt

☒ Moneybookers: moneybookers.com

Credit Card:

- ☐ VISA
- ☐ MasterCard
- ☐ AMERICAN EXPRESS
- ☐ JCB
- ☐ Diners Club International

Debit Cards:

- ☐ BLEUE
- ☐ VISA

eWallets:

- ☐ eWallet

☐ Cash:

- ☐ Pay By Cash
- ☐ Western Union **New!**
- ☐ rftbu

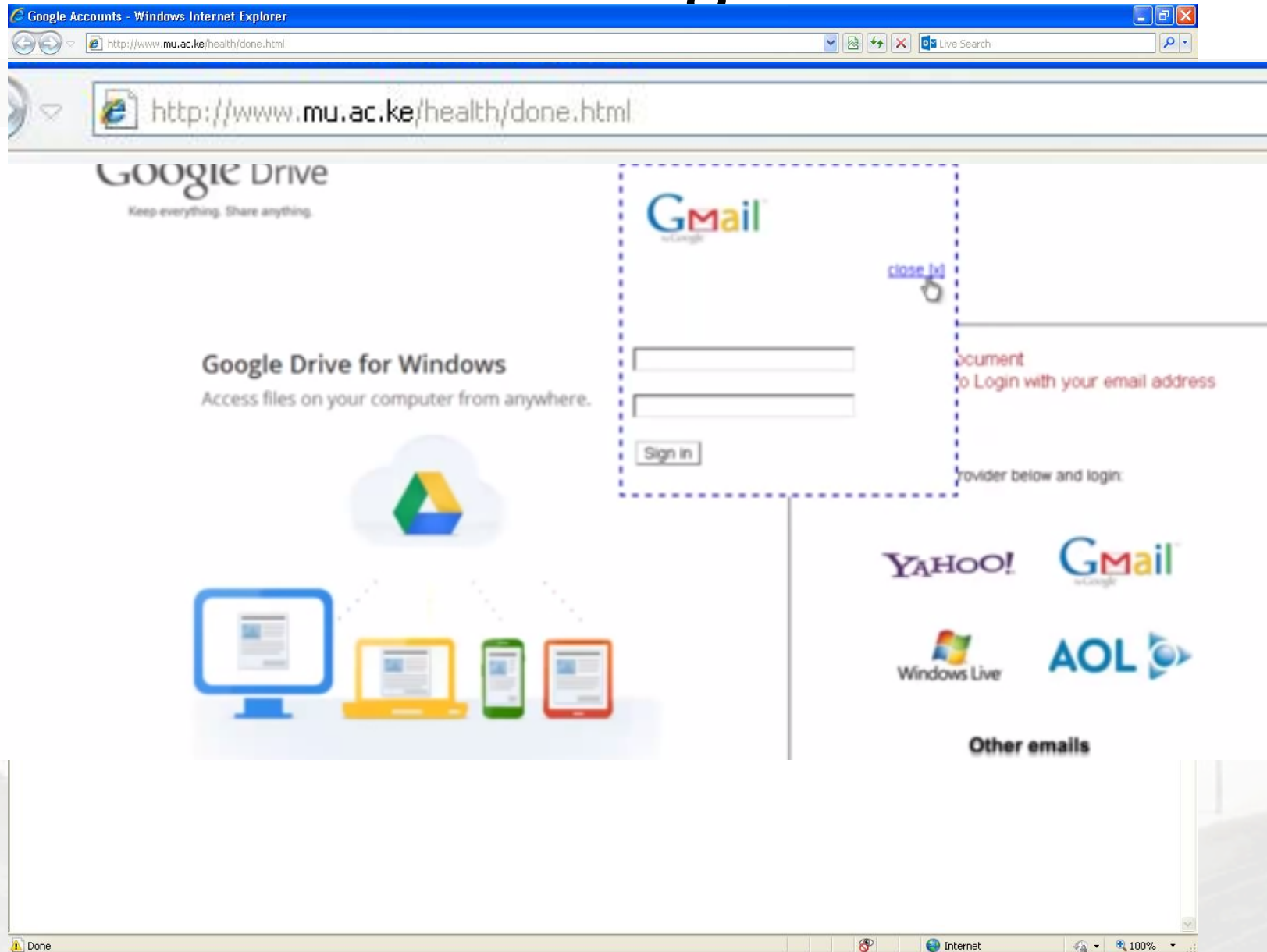
☐ SMS Billing:

- ☐ Pay by Mobile paymo (Boku)
- ☐ onebip **New!**

☐ Scratch Card: paysafecard (EURO)



Phishing MO





Phishing MO

- Gmail / generic mail account

“[...]we observed that, once logged in, manual hijackers profile the victim’s account and spend an average of 3 minutes to assess the value of the account before exploiting it or abandoning the process. This step entails searching through the victim’s email history for banking details or messages that the victim had previously flagged as important[...]”

Burstzein, Elie *et al* (see references)

- Main uses:
 - Ordering bank transactions
 - Continue phishing scam



Phishing MO

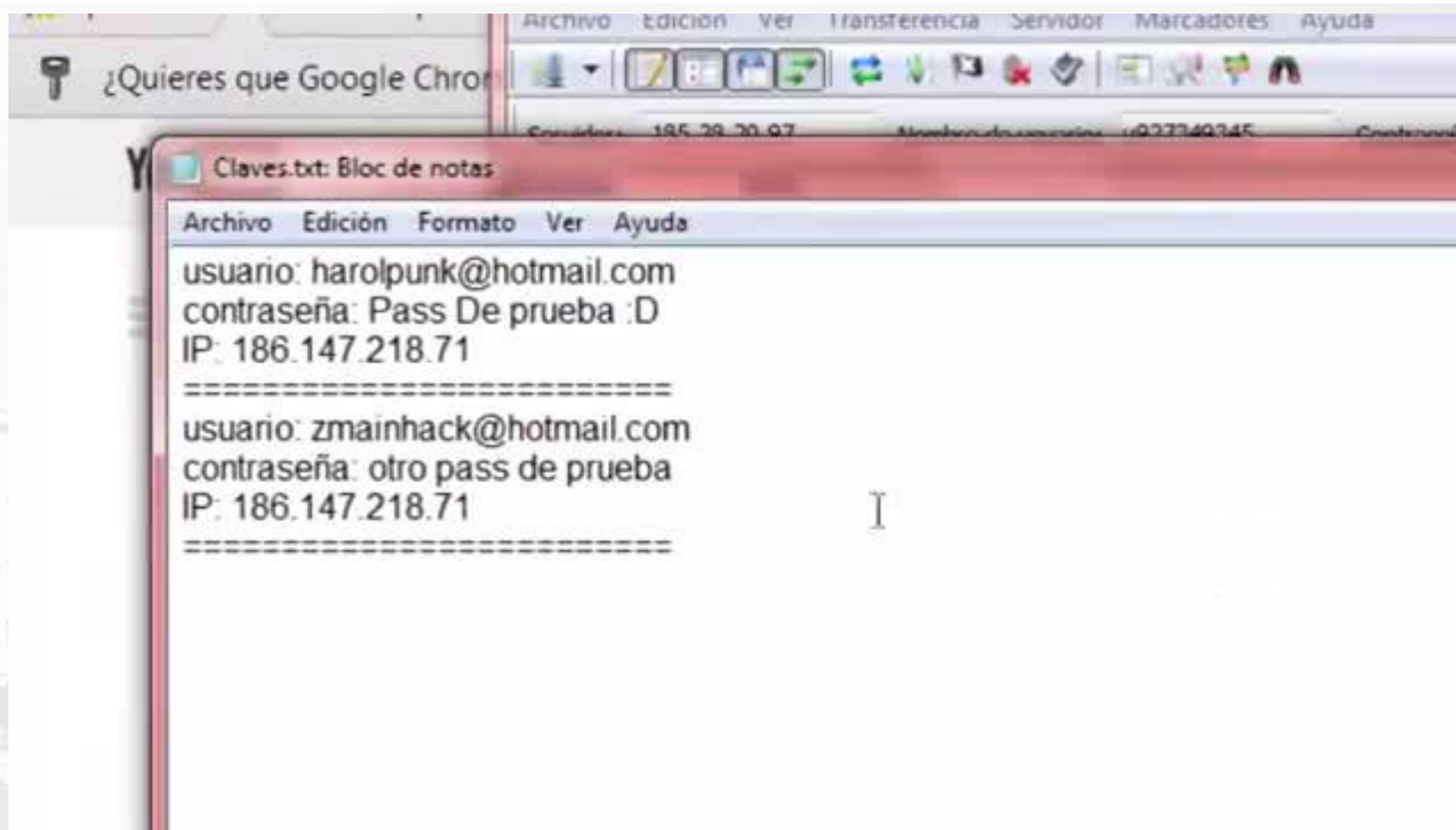
- Facebook / generic social network account

[MOV](#)





Phishing MO





Phishing MO

- Facebook / generic social network account
- Main uses:
 - “Mugged-in-...”



Phishing MO

Resources

- i. Mail account
- ii. Social networks
- iii. Financial / Banking / Bet

Any log-in account

Hardware

- i. PC
- ii. MAC
- iii. Mobile

Any device

Source

- i. E-mail
- ii. URL
- iii. Phone contact / SMS

Any contact mean



Phishing MO

- Quotes:

“[...] We argue that phishing is the attack vector of choice for manual hijackers as it is easier and cheaper to perform than other mean to compromise accounts[...]

Burstzein, Elie *et al* (see references)

“[...] Subjects often decided whether a stimulus was legitimate or not based on the content, as opposed to the signs of authenticity.. [...] emails that requested passwords upfront were considered phishy, whereas emails that only appeared to contain information were considered safe. This is a problem, as users could be drawn to a site by an email that appears to be for information only, and once at the site asked for credentials.”

Jakobsson, Markus *et al* (see references)

“While companies can invest in increased ICT security which in turn requires criminals to innovate their own technical capability, it is harder to upgrade the “human firewall”. [...] The overall effectiveness of phishing campaigns, which was formerly 10-20%, increased in 2014. Research shows that 23% of recipients who receive a phishing messages will open it and a further 11% will continue to open any attachments.”

Europol, IOCTA 2015



Phishing MO

- Step by step:
 - Define target, scam tools, and dissemination;
 - Assure a way to receive the illicit profit;
 - Assure the fund transfer
 - Collect the benefit after laundering



Why homebanking

The Client

- i. Easy access to savings;
- ii. Secure access to savings;

The Bank

- i. Easier (and cheaper) access to savings;
- ii. Cost/benefit security in granting access to savings;

The Criminal

- i. Easy access to others' savings;
- ii. Dummy security in access to savings;



Why homebanking

A secure system...

- Username/password combination
- Transaction password
- Matrix security card
- SMS token
- Token device

... or is it?

- Social engineering / ID theft
- Phone company compromise
- man in the middle



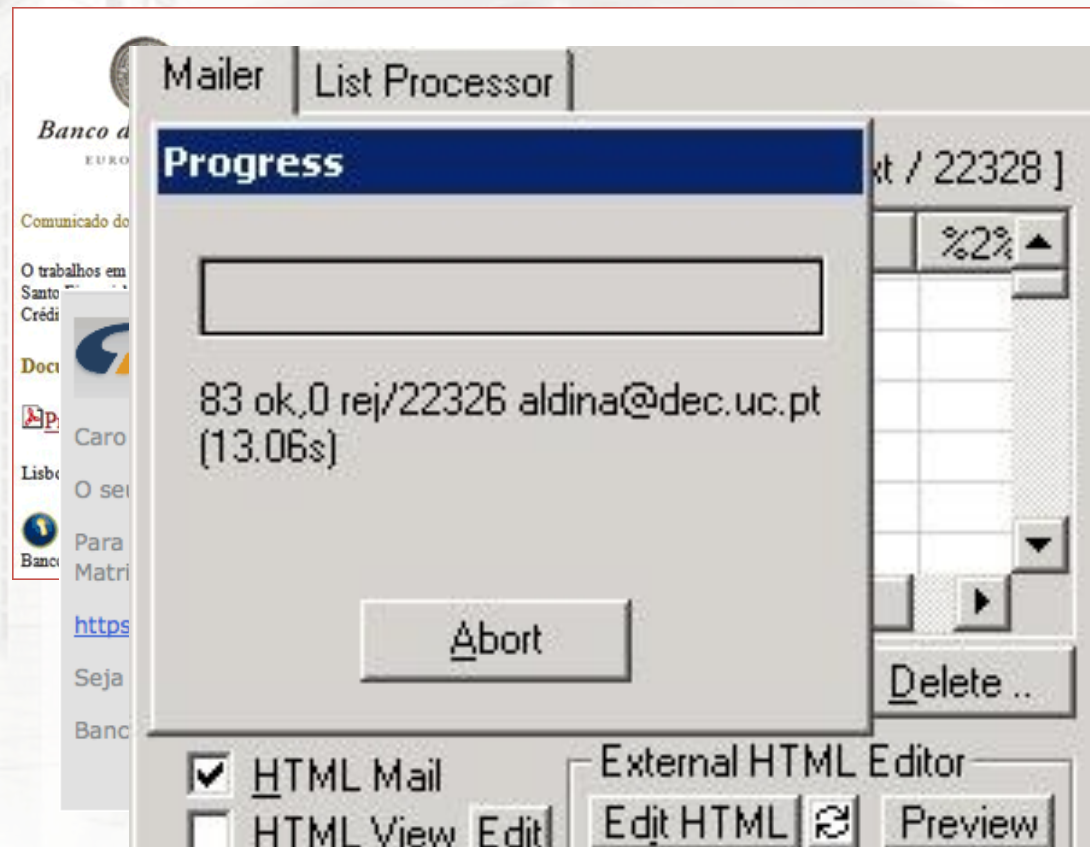
Approaching the MO

- i. Developing the identity theft tools, and its dissemination
- ii. Gathering multiple destination accounts, where the funds will afterwards be transferred to
- iii. Entering the victim's online banking service, ordering the funds transfer
- iv. Rewarding the structure



i. Developing the identity theft tools, and its dissemination

- Spam – unsolicited e-mail





i. Developing the identity theft tools, and its dissemination

```
NIB: 0033 0017558 05
IBAN: PT50 0033 0017 558 05
Código SWIFT: BCOMPTPL
Titulares da Conta: LUCIO
MARIA
Morada da Conta:
2855-276 CORROIOS
*****
"codUser": "comandos1",
"passPosKL": "1*:4|2*:6|3*:0|",
"passPosSite": "4*:5|7*:8|6*:0|",
"specialPos": "5",
"telemovel": "96",
"contribuinte": "176",
"valueSpecialPos": "2",
"Saldo": "Saldo Disponível:151,16",
```

```
NIB: 0033 000166 05
IBAN: PT50 0033 0001 66 05
Código SWIFT: BCOMPTPL
Titulares da Conta: CRISTINA
Morada da Conta:
1600-176 LISBOA
"codUser": "chsnd07",
"passPosKL": "3*:6|4*:1|6*:4|",
"passPosSite": "5*:2|1*:8|2*:5|",
"specialPos": "7",
"telemovel": "91",
"contribuinte": "",
"valueSpecialPos": "0",
"Saldo": "Saldo Disponível:441,37"
```

[Report that this download is safe](#)

Cancel

Security Warning

Could not be verified. Are you sure you want to run this

File name: HRPRO.exe

Publisher: Unknown Publisher

Type: Application

Version: 10.130.0.52

Run

Cancel

This file does not have a valid digital signature that verifies its identity. You should only run software from publishers you trust. Do you want to run this file? I decide what software to run?



i. Developing the identity theft tools, and its dissemination

- Active contribution from the victim

caixadirecta on-line

Bem-vindo ao Caixadirecta

53*****81
1*****8

[Voltar ao CGD.pt](#)

002:8020	156:1726	335:5610	708:4711	872:6448
005:1115	210:8920	370:3388	714:8387	889:3417
021:0304	260:1153	383:8648	723:4279	927:7824
028:9612	267:4211	443:3705	740:1738	935:6145
031:3288	293:4806	474:6322	750:3481	941:0792
064:7793	307:6743	601:8257	761:1758	944:1984
071:9144	309:7500	603:9934	771:8196	961:5160
092:4762	310:9512	651:2354	777:3369	971:7764
093:2952	311:1930	689:1865	800:9930	977:0736
153:6816	324:2554	705:8029	811:0260	987:0260

F
G
H
-

Segurança na Caixa Geral de Depósitos.

[Continuar](#)

Caixa Geral de Depósitos
A Caixa Geral de Depósitos é um membro associado do Euronext Lisbon que é uma sociedade registada na CMVM com o número 125.
(c) 1995 - 2012 Caixa Geral de Depósitos, SA. Todos os direitos reservados.
Site optimizado para Internet Explorer 6, 7 e 8, Mozilla Firefox 2 e 3, Opera 8 e 9 e (Mac/Win) Safari 3 e 4, para a resolução de 1024px por 768px.



ii. Gathering multiple destination accounts

- Need to assure a destination account (money mule)



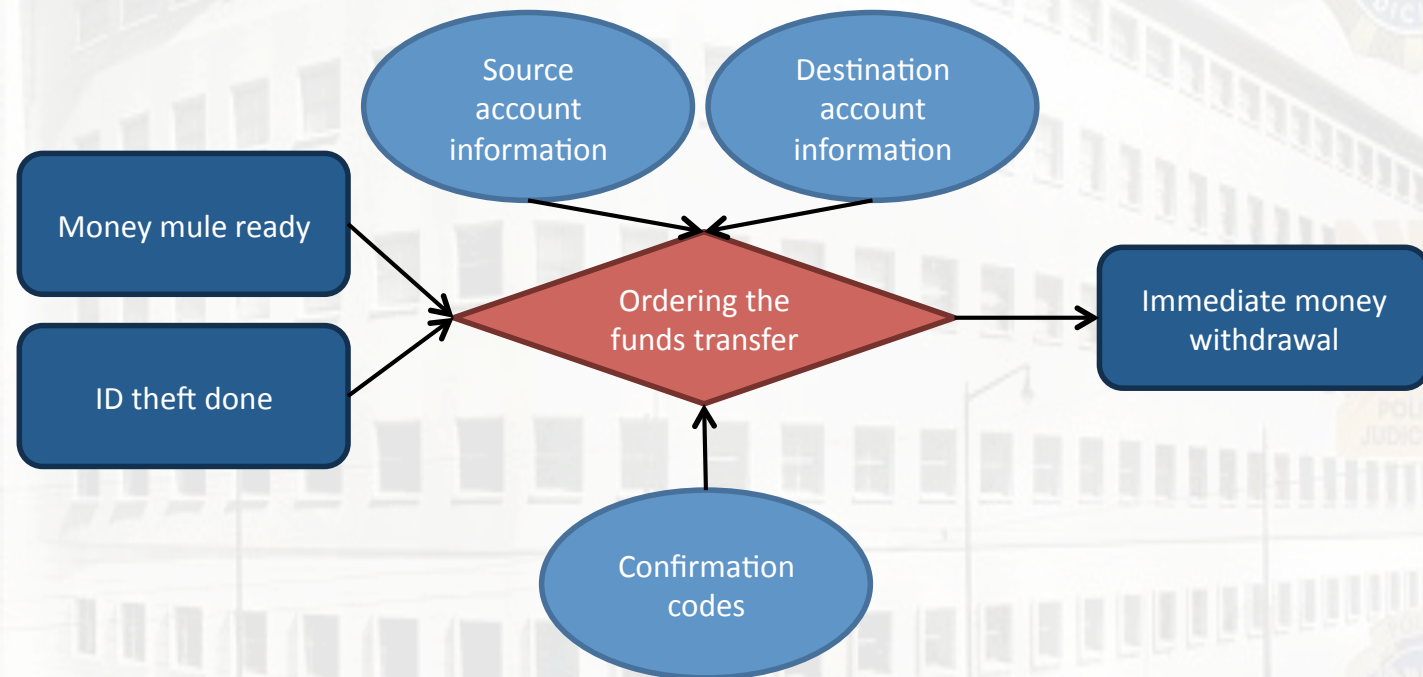
€

- i. Job scam
- ii. Social environment



iii. Entering the victim's online banking service

- Simultaneous criminal structure action





iv. Rewarding the structure

- i. Job scam:
 - i. Money withdrawal in a branch
 - ii. International money transfer outside the classical banking system
 - iii. Payment deducted from money mule's fee
- ii. Social environment:
 - i. POS with limited ID demands
 - ii. Immediate funds distribution



Tackling the difficulties

The costs of the crime:

- For the victim / bank
- For the trust in banking system
- For the society



Tackling the difficulties

The need for proactivity

Restricted access to information/evidence:

- Bank and phone accounts
- IP and internet traffic information



Tackling the difficulties

International cooperation

- Job scam
 - Eastern coorelation;
 - Quick mutation and territorial coverage
 - Minimum three jurisdictions involved
- Social environment
 - South-american coorelation
 - Major focus on minorities as facilitators
 - Minimum two jurisdictions involved



References

- Burstzein, Elie *et al* – “Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild”, Google, Inc *et* University of California, San Diego, 2014;
- Elliot, Thomas S., “The rock”, 1936, *apud* Rodrigues, Fernando C. e Ramos, Luís, “Ontem um anjo disse-me”, Ed. Europa-América, 1995;
- Jakobsson, Markus *et al* – “What Instills Trust? A Qualitative Study of Phishing”, Indiana University, Bloomington and RavenWhite Inc., 2007.



ON PHISHING

MODI OPERANDI AND INVESTIGATION CHALLENGES

Carlos Nunes

Inspector

Polícia Judiciária

Tel: (+351) 211967841

carlos.nunes@pj.pt