PHISHING: ONE SHOT, MANY VICTIMS!

06.05.2017 - Andrea Draghetti

HACK IN BO®
Spring 2017 Edition

$ whoami

Phishing Analysis and Contrast @ D3Lab

Team Member @ BackBox Linux

Phishing

Il Phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

{Wikipedia}

HACK IN BO®
Spring 2017 Edition

Che cos'è il Phishing?

Un problema delle vie urinarie

? %

Un tentativo di frode

? %

Fonte: http://www.today.it/poll/ad_ecostore_03 - Sondaggio presente dal 27 Ottobre 2016

Che cos'è il Phishing?

Un problema delle vie urinarie

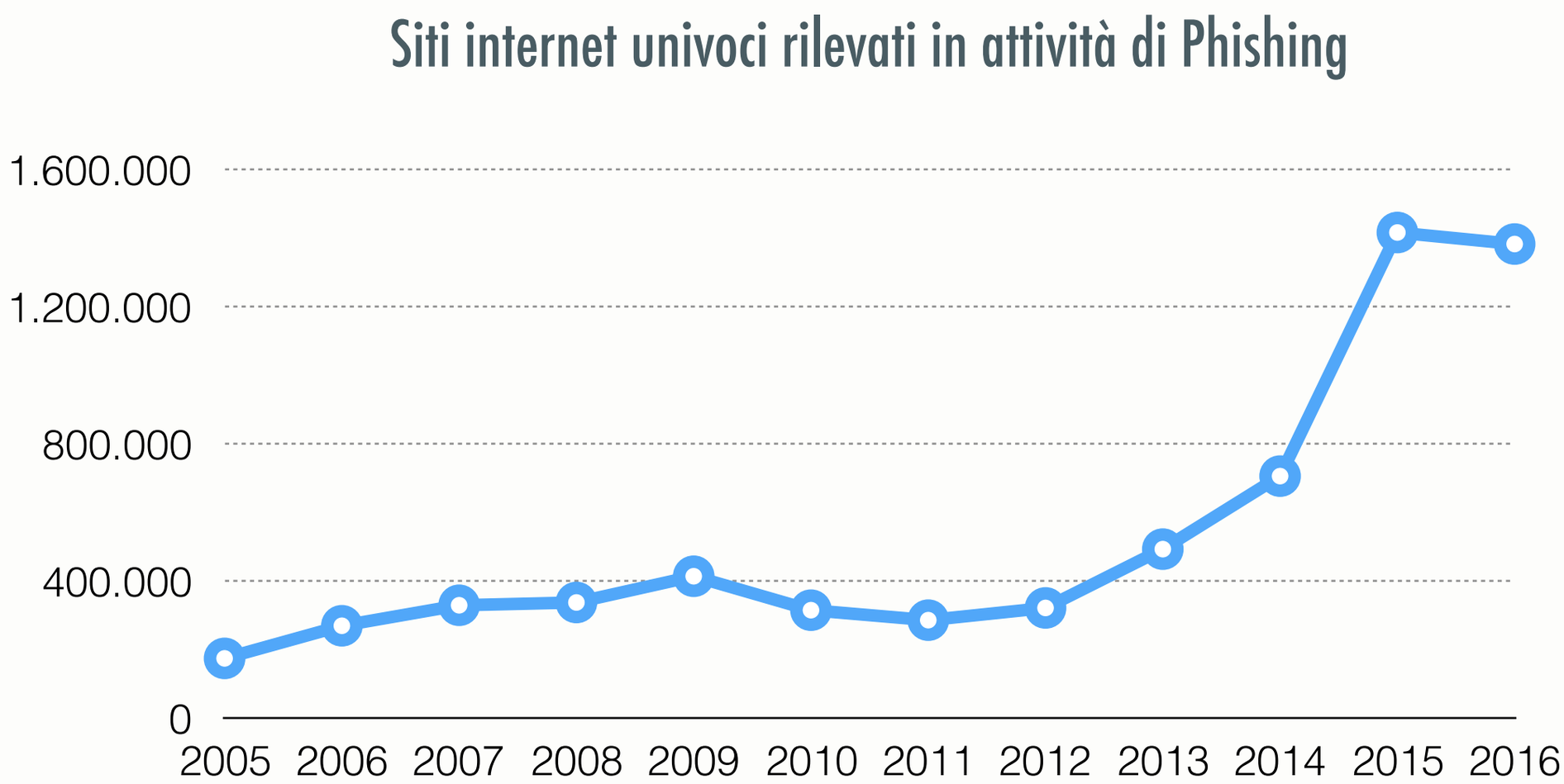
46 %

Un tentativo di frode

54 %

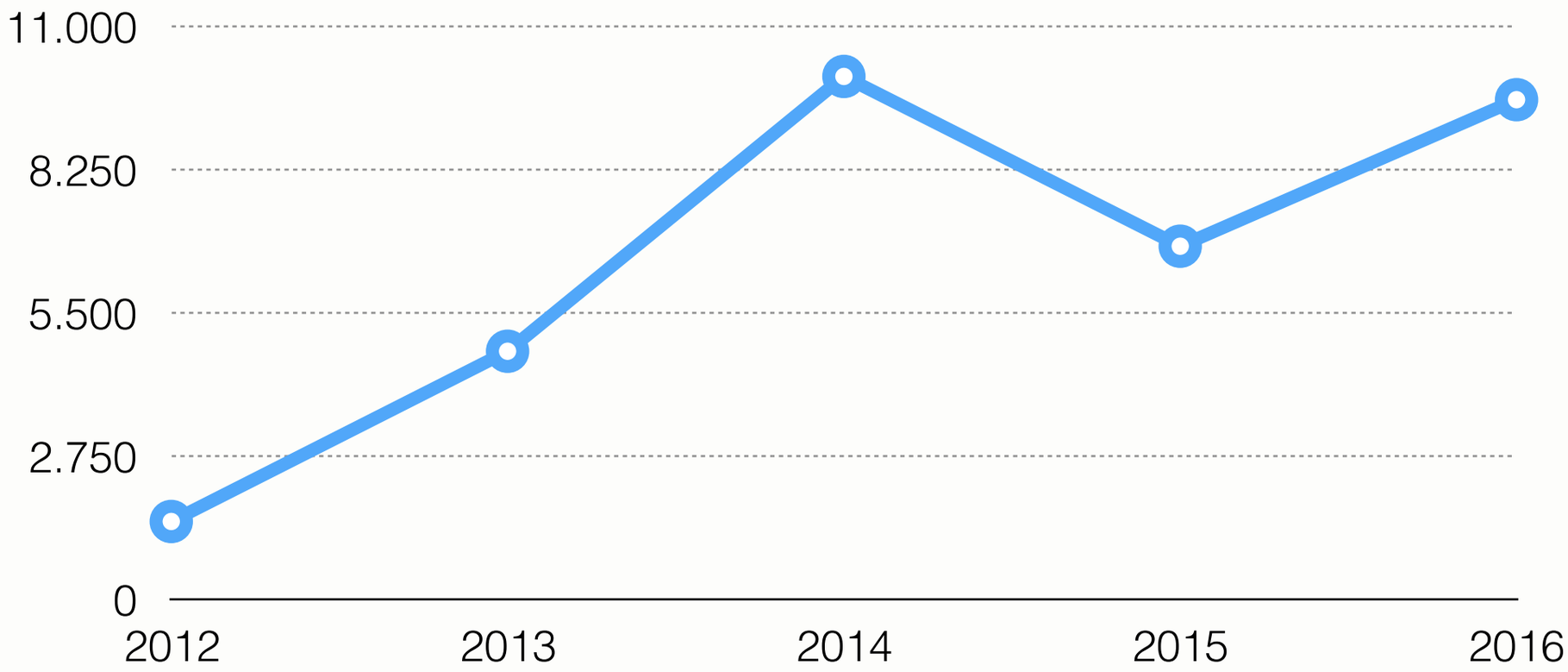
Fonte: http://www.today.it/poll/ad_ecostore_03 - Sondaggio presente dal 27 Ottobre 2016

Statistiche Internazionali

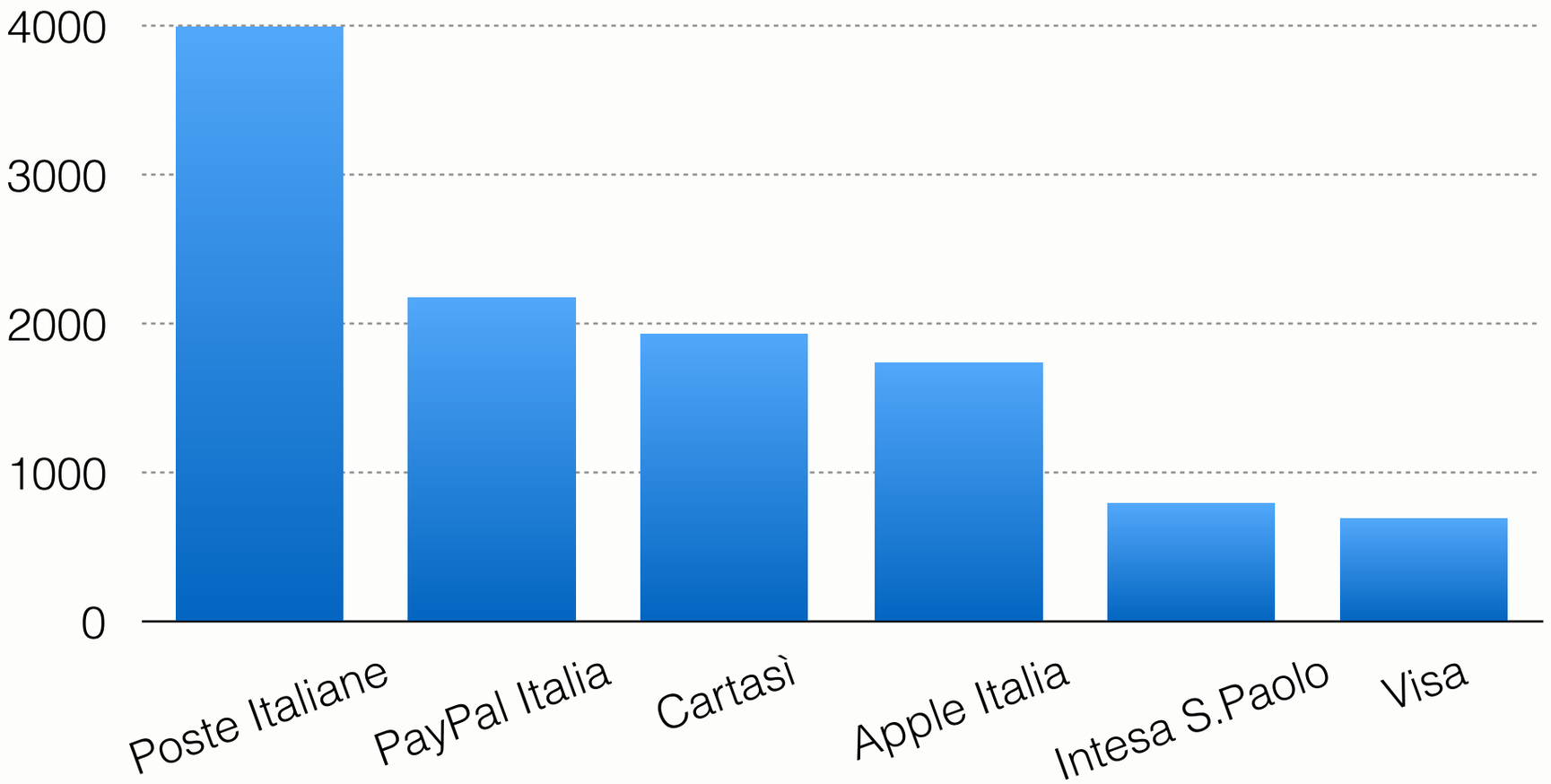


Fonte: Anti-Phishing Working Group

Statistiche Italiane



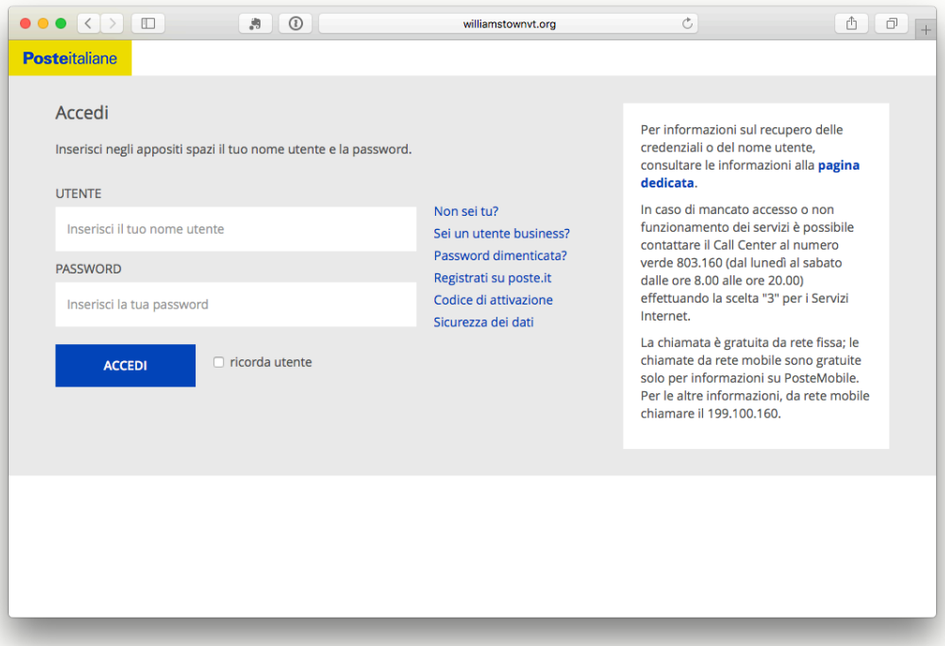
Principali Enti Italiani Colpiti

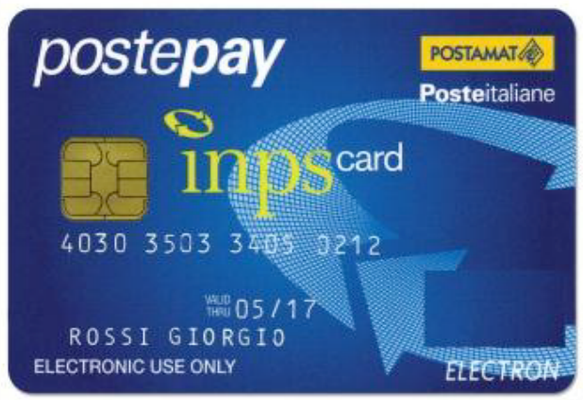


(2012-2016)

HACK IN BO®
Spring 2017 Edition

Cashout su INPS Card



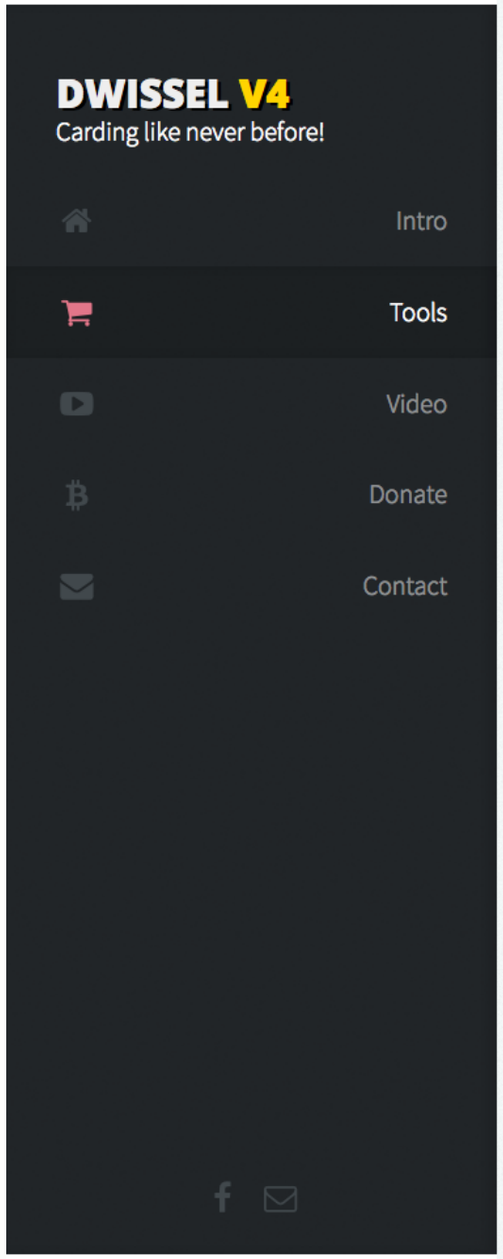


Indagine Forze di Polizia
1,5 milioni euro + 280 mila euro

Marzo 2017

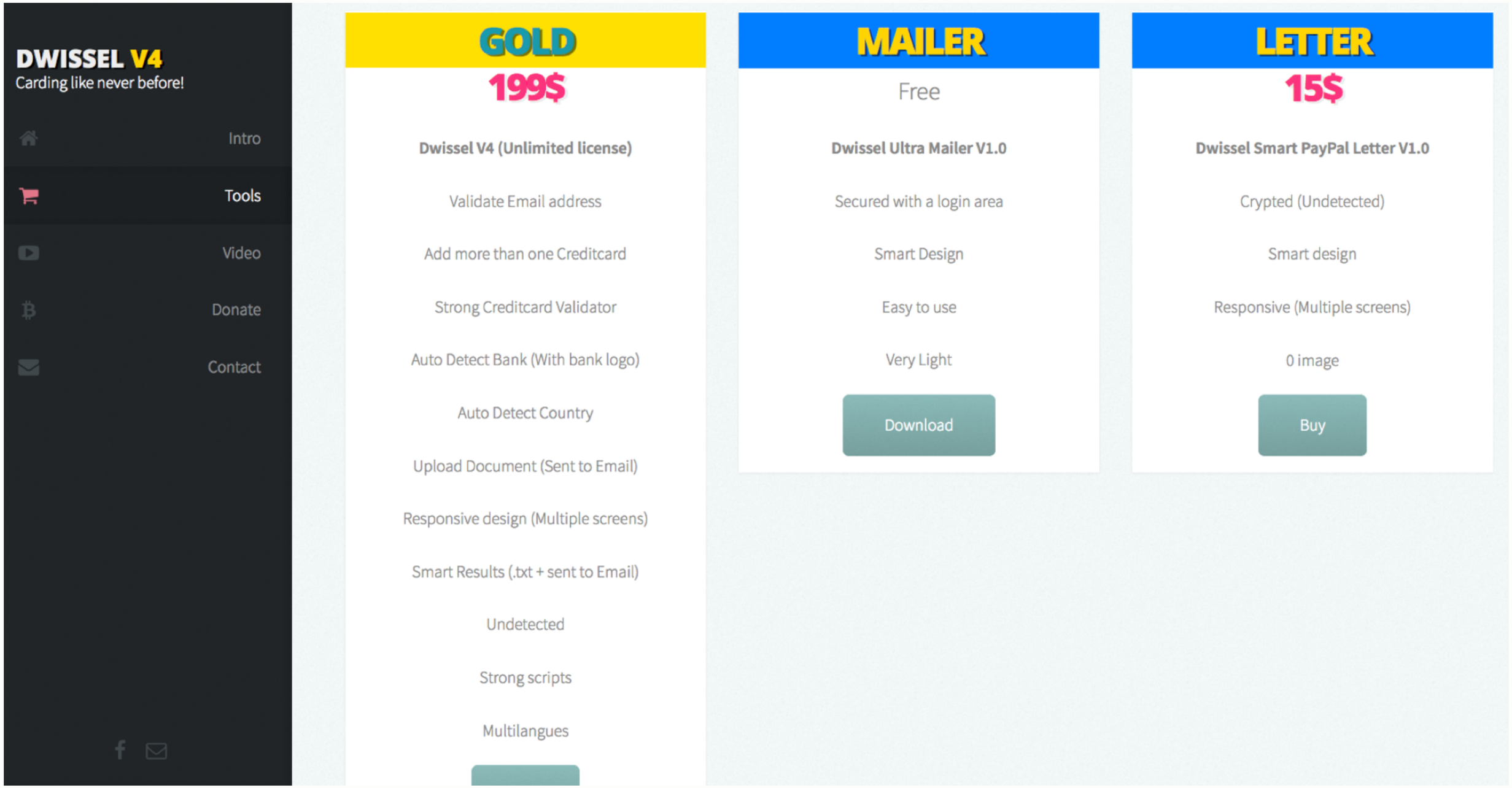
HACK IN BO®
Spring 2017 Edition

Phishing as a Service



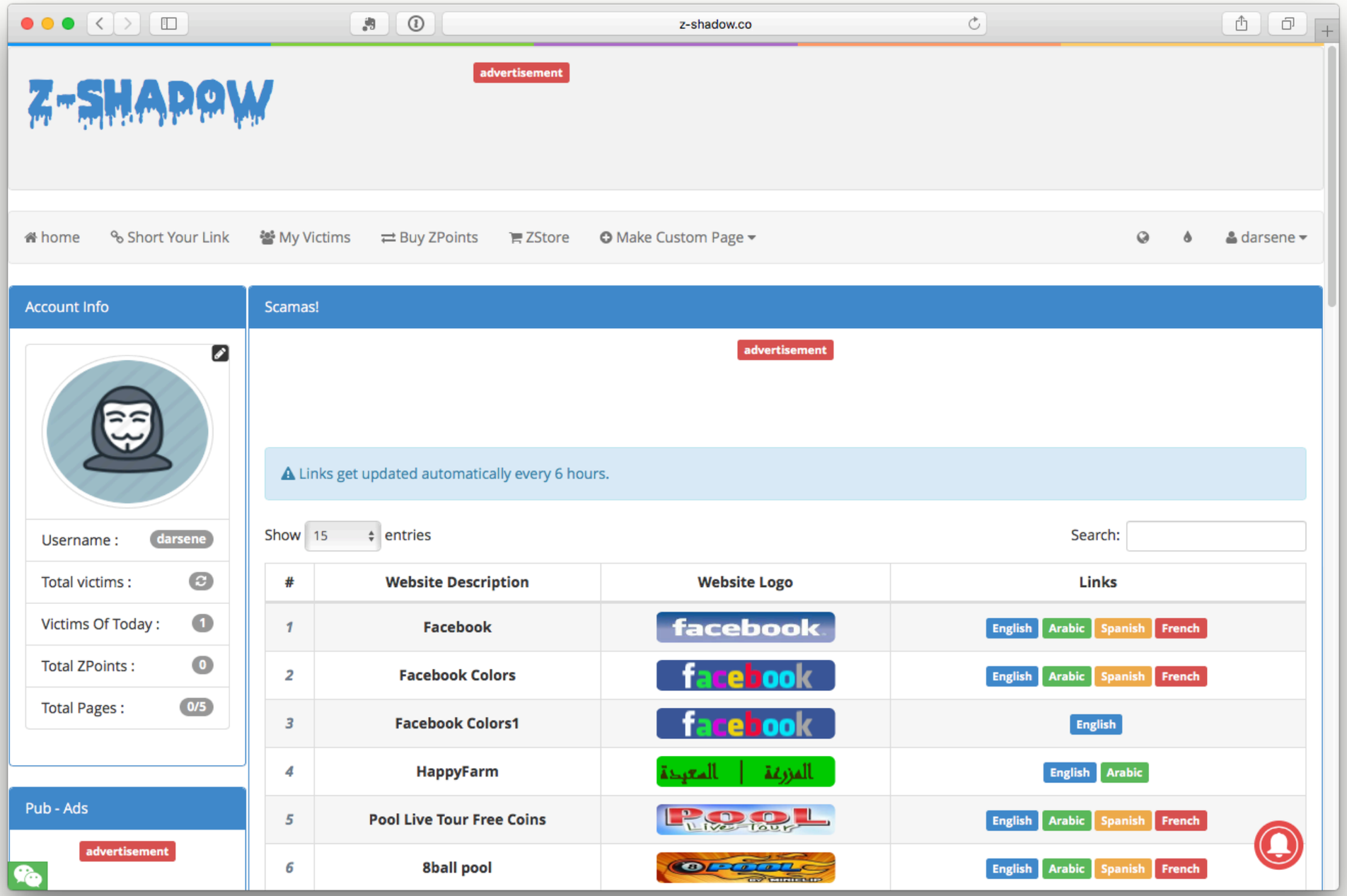
TRIAL	PREMIUM	SILVER
Free	60$/month	100$/70 days
Dwissel V4 (7 days trial)	**Dwissel V4 (30 days license)**	**Dwissel V4 (70 days license)**
Validate Email address	Validate Email address	Validate Email address
Add more than one Creditcard	Add more than one Creditcard	Add more than one Creditcard
Strong Creditcard Validator	Strong Creditcard Validator	Strong Creditcard Validator
Auto Detect Bank (With bank logo)	Auto Detect Bank (With bank logo)	Auto Detect Bank (With bank logo)
Auto Detect Country	Auto Detect Country	Auto Detect Country
Upload Document (Sent to Email)	Upload Document (Sent to Email)	Upload Document (Sent to Email)
Responsive design (Multiple screens)	Responsive design (Multiple screens)	Responsive design (Multiple screens)
Smart Results (.txt + sent to Email)	Smart Results (.txt + sent to Email)	Smart Results (.txt + sent to Email)
Undetected	Undetected	Undetected
Strong scripts	Strong scripts	Strong scripts
Multilangues	Multilangues	Multilangues
Download	Buy	Buy

Phishing as a Service



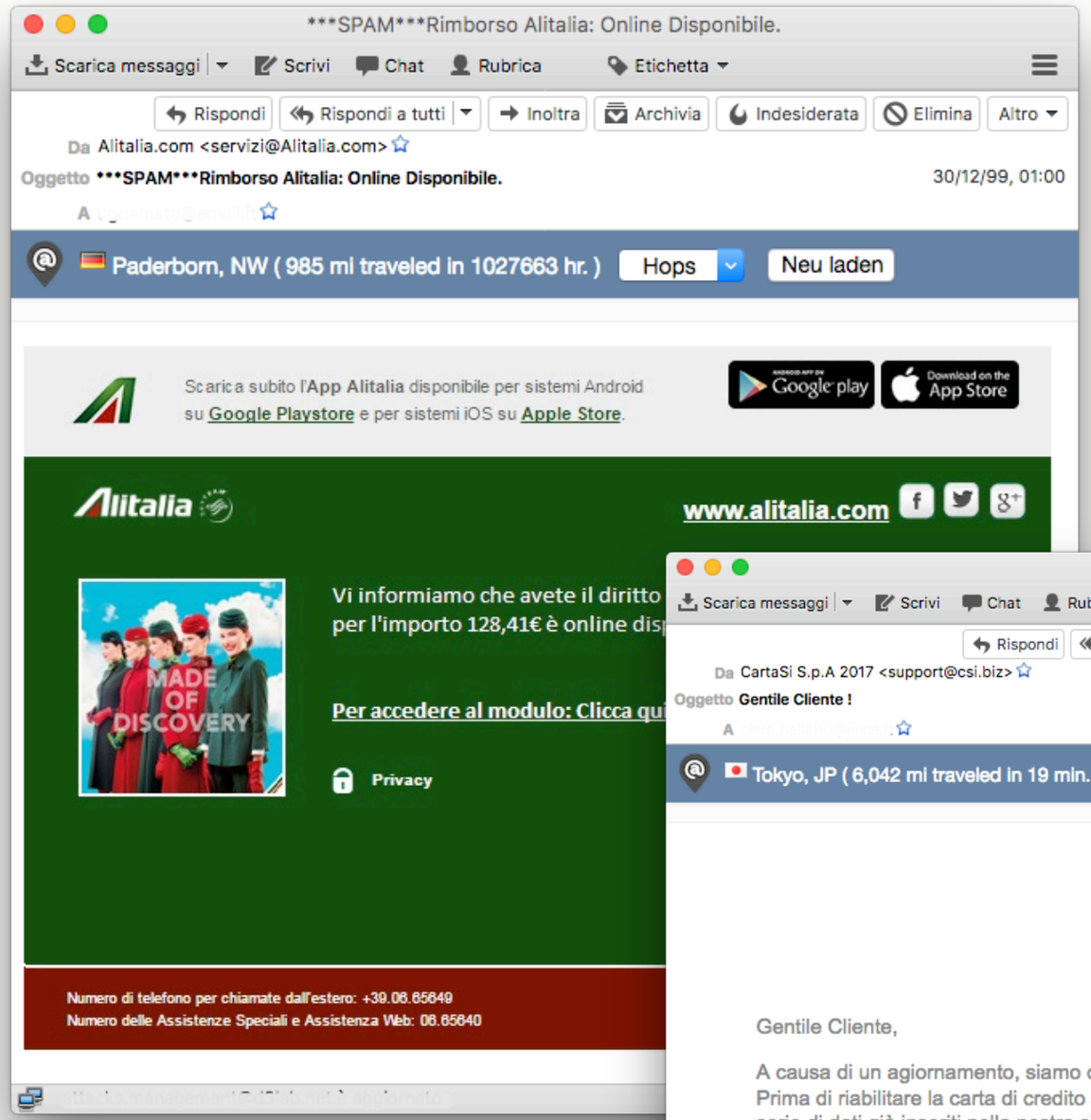
HACK IN BO®
Spring 2017 Edition

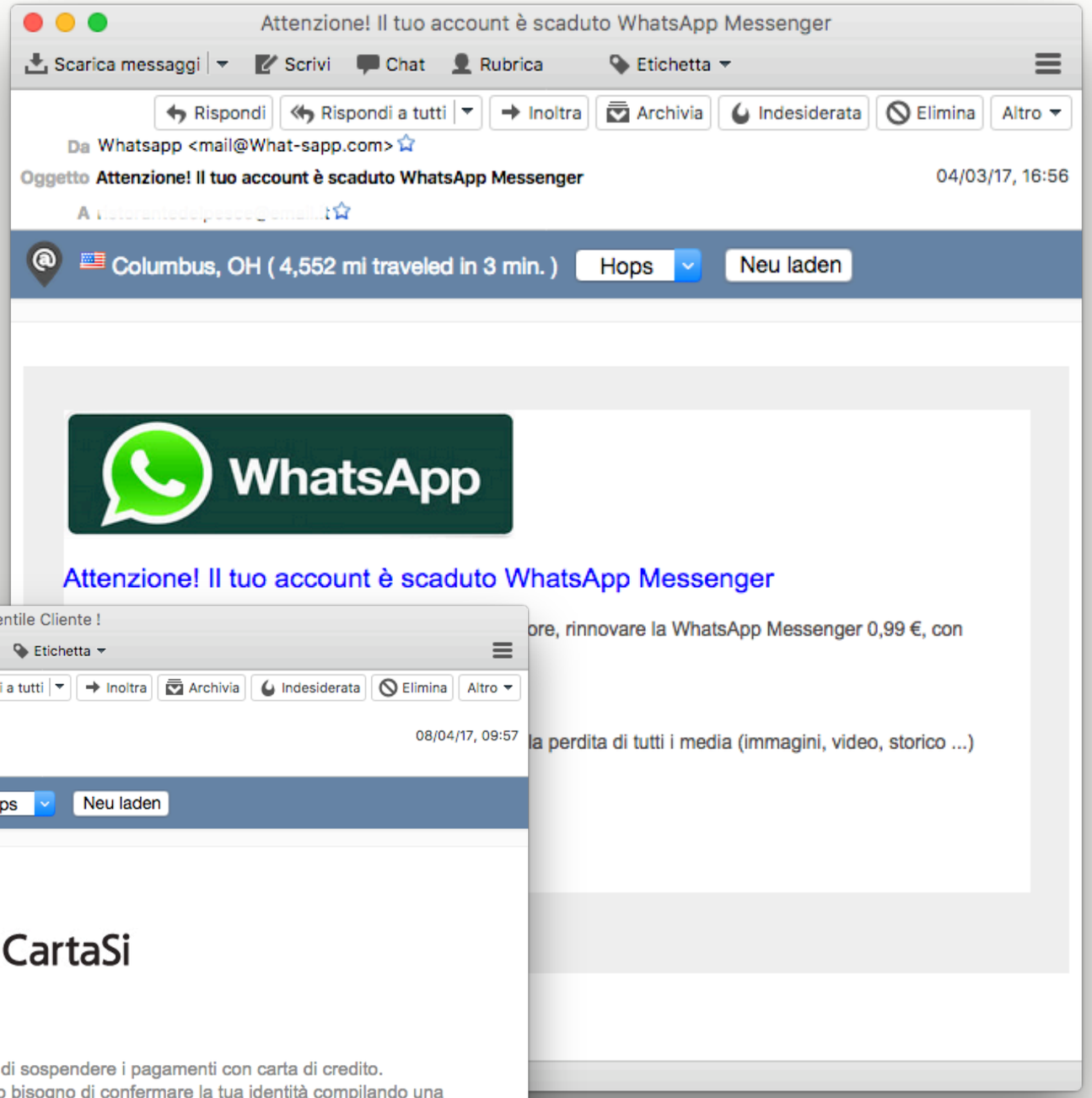
Phishing as a Service

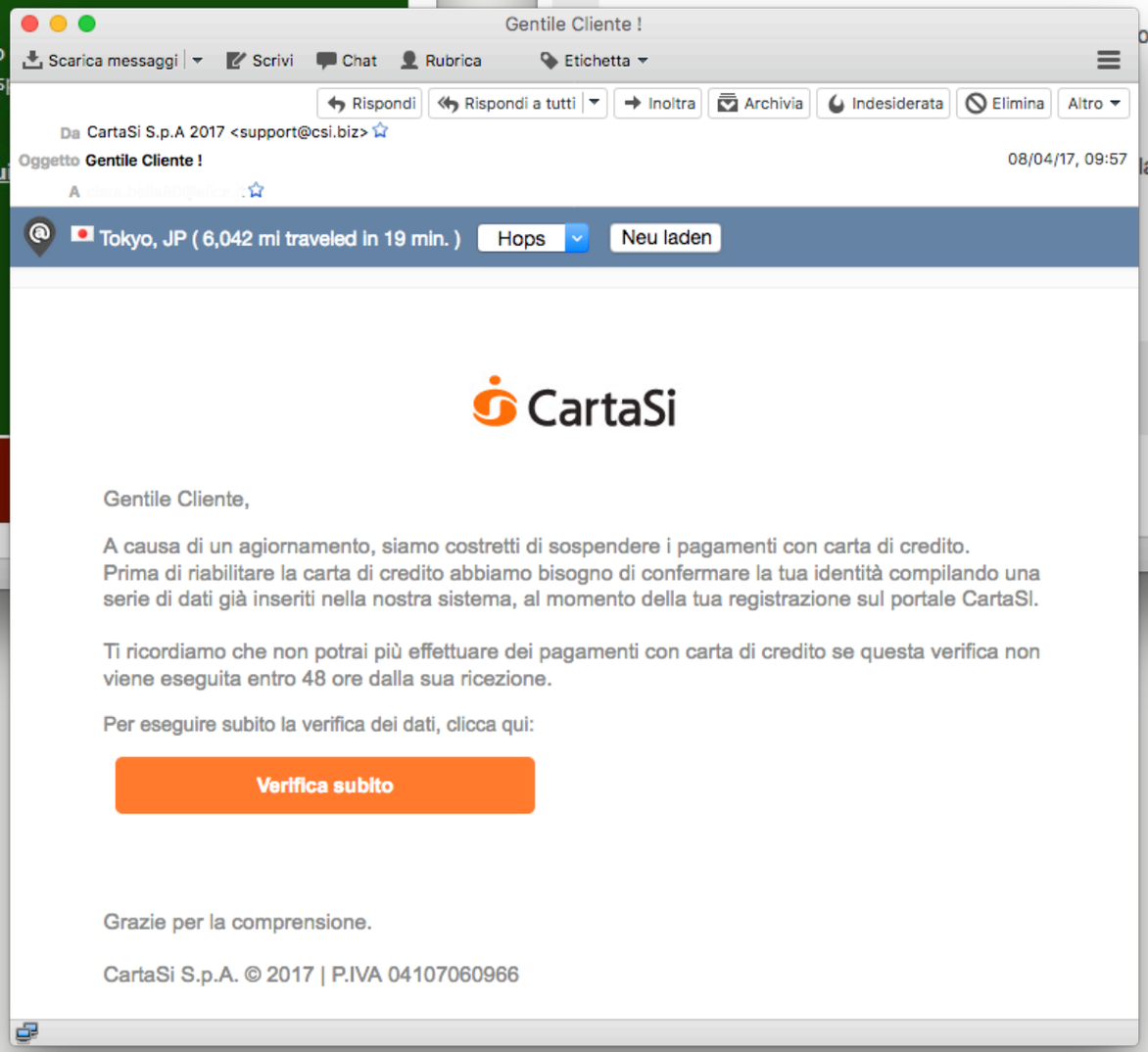


HACK IN BO®
Spring 2017 Edition

Diffusione: eMail

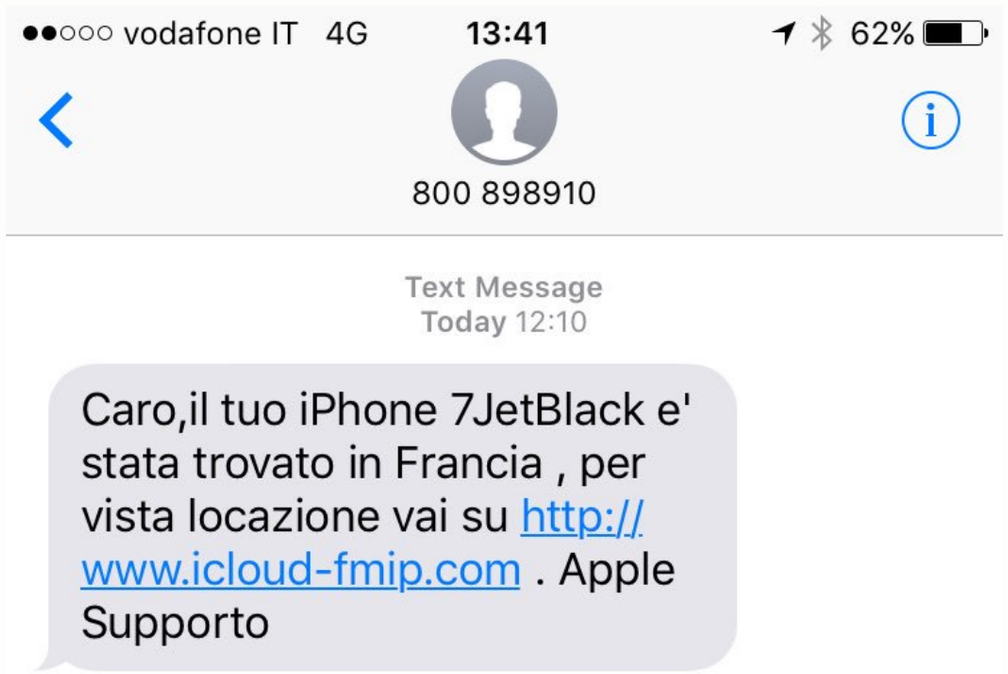






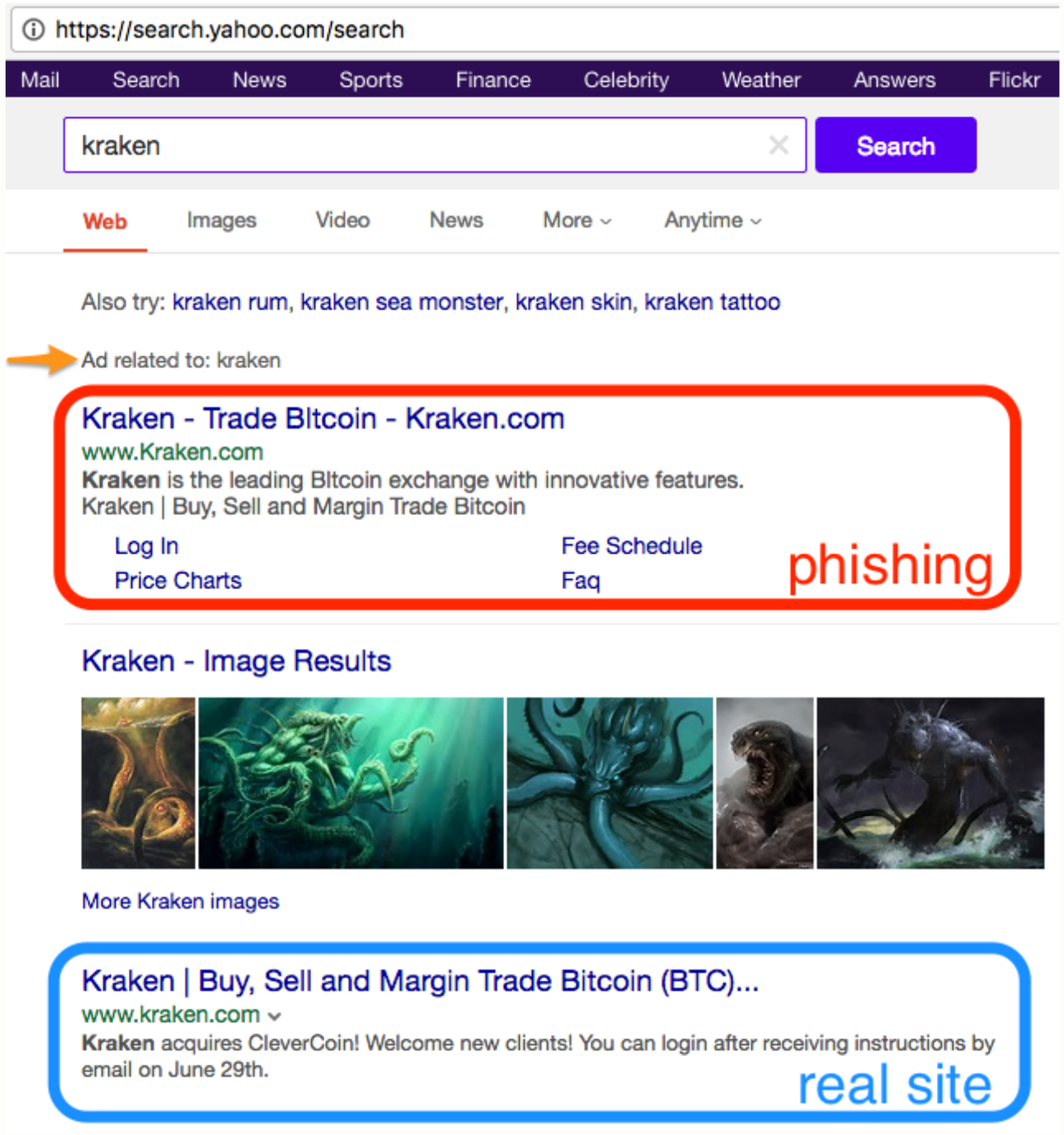
HACK IN BO®
Spring 2017 Edition

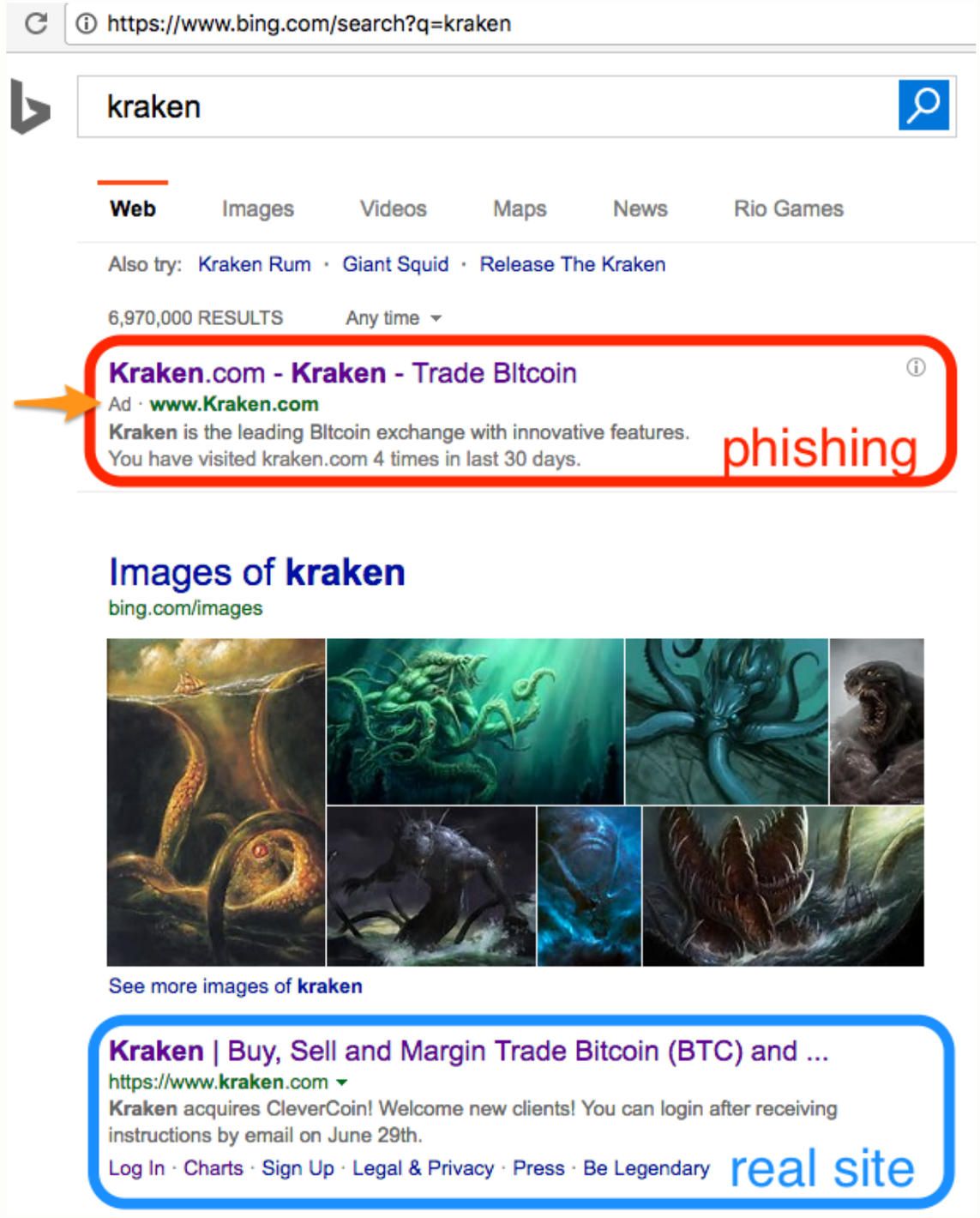
Diffusione: SMS



HACK IN BO®
Spring 2017 Edition

Diffusione: Ads





HACK IN BO®
Spring 2017 Edition

http://blog.kraken.com/post/148976188862/kraken-phishing-warning

Tecniche: Random Path

Sottodomini e Sottodirectory random per evitare le BlackList

http://www.chebancait.**random**.azaklarodunkofte.com/wps/portal/Istituzionale/

http://www.ingdirect.it.**random**.demosearchgtallsports.com/.ingdirect**random**/

http://www.postepay.it.**random**.it.iliel.xyz/agg/**random**/

Tecniche: Shorturl e Redirect

http://adf.ly/1mRu8u?**random**?

↓

http://www.megaline.co/Alhv9?**random**?

↓

http://**random**.totnuw.for-our.info?**random**?

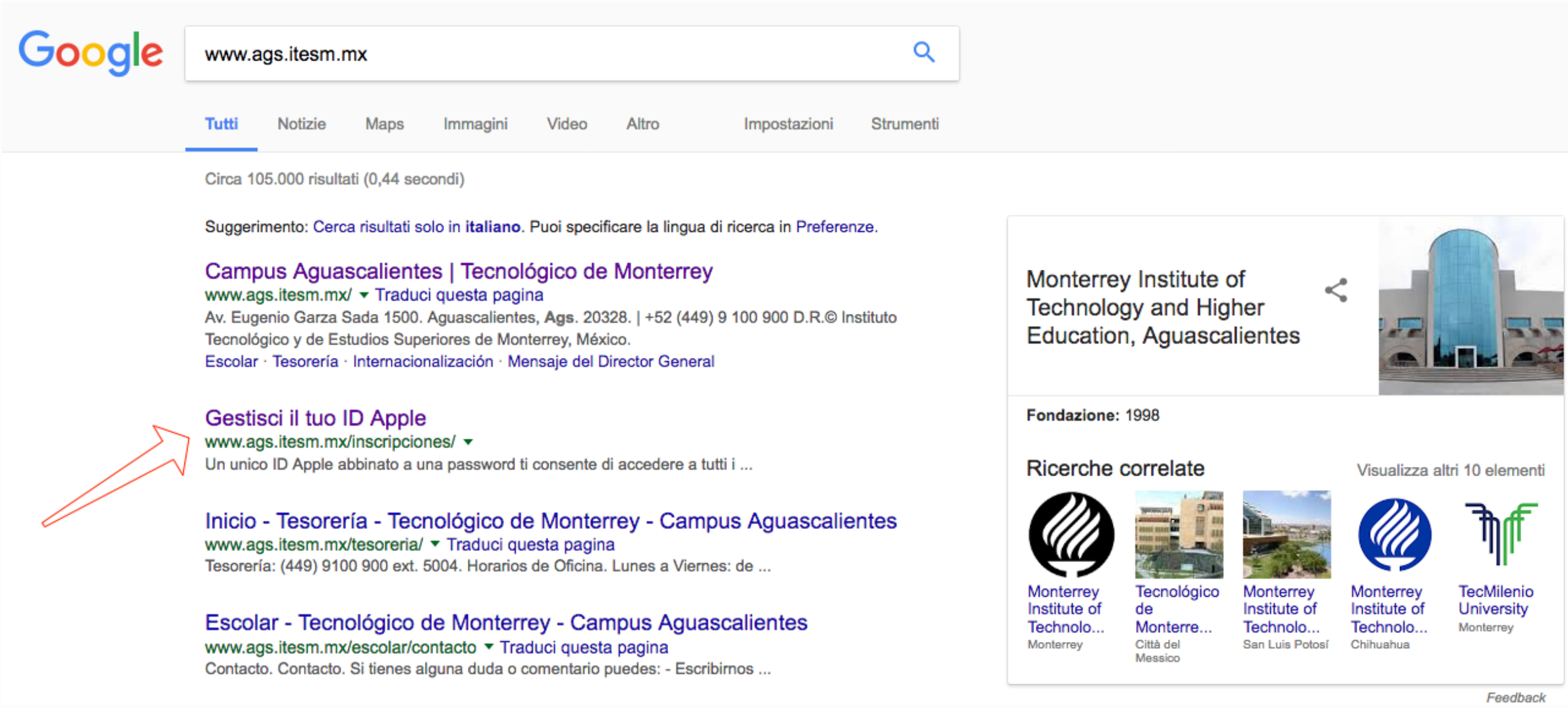
↓

http://postesecurelogin.posta.it.bancaposta.foo-autenticazione.**random**.lopamuser.for-our.info/hescientiststravelled/ontworesearchvessels/almostkilometresfrom/ichangtothenearbyhree/loginfile/

Tecniche: Shorturl e Redirect

https://www.google.no/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi
mx4fKnbPTAhWCiywKHYjHCWgQFggwMAE&url=**http://**
www.ags.itesm.mx/inscripciones/
&usg=AFQjCNGOANaZ8ewUjshair7YIZTzeCq7yA

Tecniche: Shorturl e Redirect



HACK IN BO®
Spring 2017 Edition

Tecniche: Filtri GeoIP

bots.php

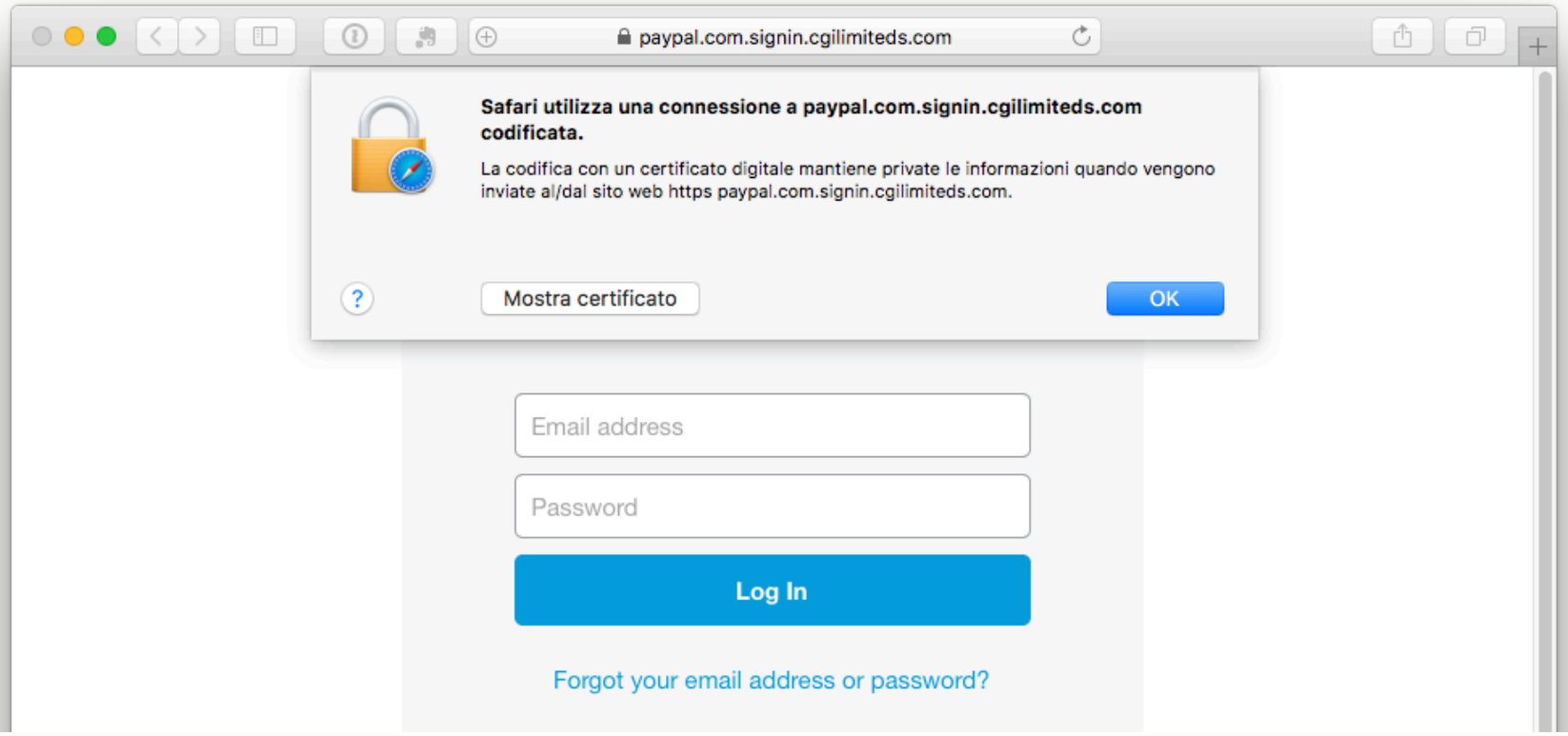
lang.php | bots.php

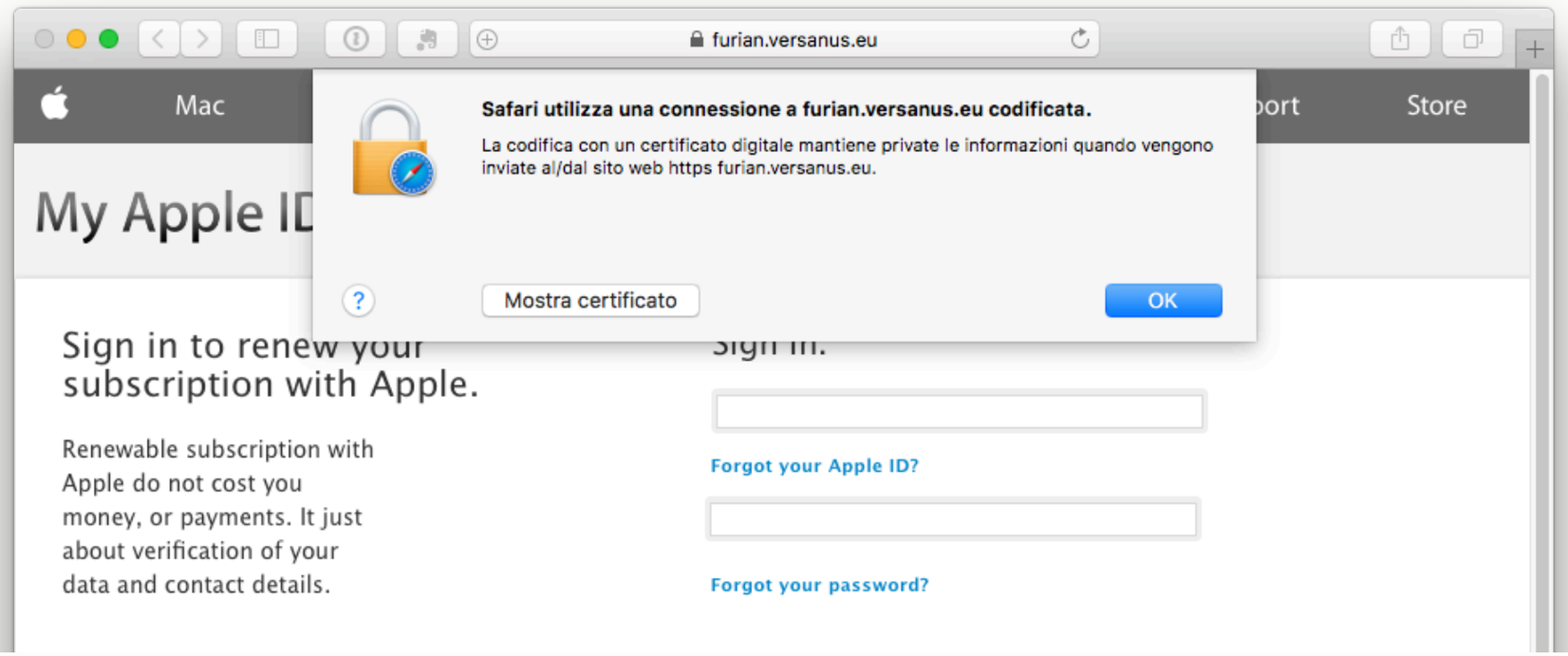
```php
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words =
array("above","google","softlayer","amazonaws","cyveillance","phishtank","dreamhost","netpilot","calyxinstitute
","tor-exit", "msnbot","p3pwgdsn","netcraft","trendmicro", "ebay", "paypal", "torservers", "messagelabs",
"sucuri.net", "crawler");
foreach($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {
    header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");

    }
}
$bannedIP = array("^81.161.59.*", "^66.135.200.*", "^66.102.*.*", "^38.100.*.*", "^107.170.*.*", "^149.20.*.*",
"^38.105.*.*", "^74.125.*.*",  "^66.150.14.*", "^54.176.*.*", "^38.100.*.*", "^184.173.*.*", "^66.249.*.*",
"^128.242.*.*", "^72.14.192.*", "^208.65.144.*", "^74.125.*.*", "^209.85.128.*", "^216.239.32.*",
"^74.125.*.*", "^207.126.144.*", "^173.194.*.*", "^64.233.160.*", "^72.14.192.*", "^66.102.*.*", "^64.18.*.*",
"^194.52.68.*", "^194.72.238.*", "^62.116.207.*", "^212.50.193.*", "^69.65.*.*", "^50.7.*.*", "^131.212.*.*",
"^46.116.*.* ", "^62.90.*.*", "^89.138.*.*", "^82.166.*.*", "^85.64.*.*", "^85.250.*.*", "^89.138.*.*",
"^93.172.*.*", "^109.186.*.*", "^194.90.*.*", "^212.29.192.*", "^212.29.224.*", "^212.143.*.*", "^212.150.*.*",
"^212.235.*.*", "^217.132.*.*", "^50.97.*.*", "^217.132.*.*", "^209.85.*.*", "^66.205.64.*", "^204.14.48.*",
"^64.27.2.*", "^67.15.*.*", "^202.108.252.*", "^193.47.80.*", "^64.62.136.*", "^66.221.*.*", "^64.62.175.*",
"^198.54.*.*", "^192.115.134.*", "^216.252.167.*", "^193.253.199.*", "^69.61.12.*", "^64.37.103.*",
"^38.144.36.*", "^64.124.14.*", "^206.28.72.*", "^209.73.228.*", "^158.108.*.*", "^168.188.*.*",
"^66.207.120.*", "^167.24.*.*", "^192.118.48.*", "^67.209.128.*", "^12.148.209.*", "^12.148.196.*",
"^193.220.178.*", "68.65.53.71", "^198.25.*.*", "^64.106.213.*", "^91.103.66.*", "^208.91.115.*",
"^199.30.228.*");
if(in_array($_SERVER['REMOTE_ADDR'],$bannedIP)) {
     header('HTTP/1.0 404 Not Found');
     exit();
} else {
     foreach($bannedIP as $ip) {
          if(preg_match('/' . $ip . '/',$_SERVER['REMOTE_ADDR'])){
               header('HTTP/1.0 404 Not Found');
               die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
          }
     }
}

?>
```

Caratteri: 2.308 · Posizione: 11 - 2.295 · Parole: 191

HACK IN BO®
Spring 2017 Edition

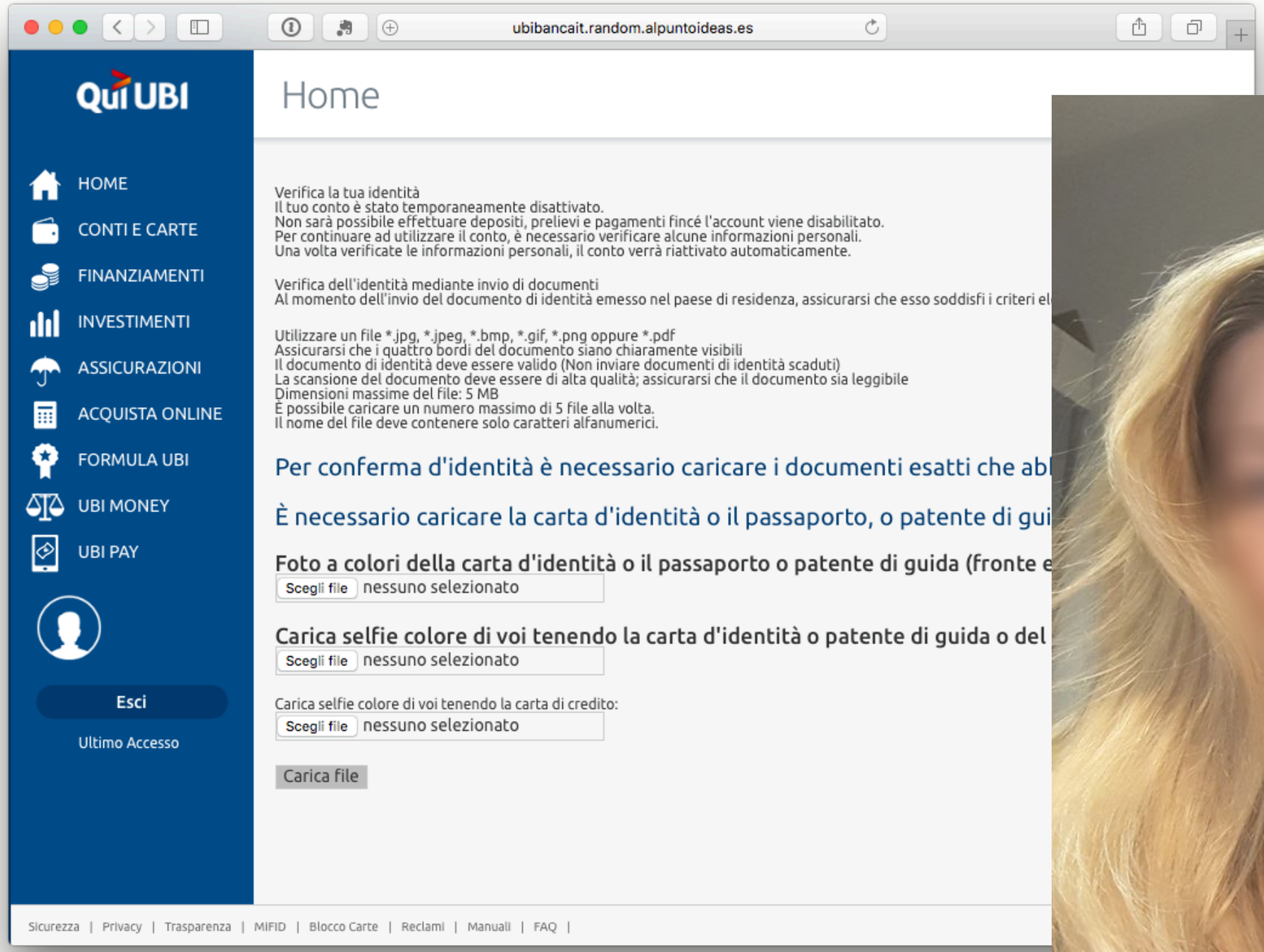
Tecniche: Certificati SSL

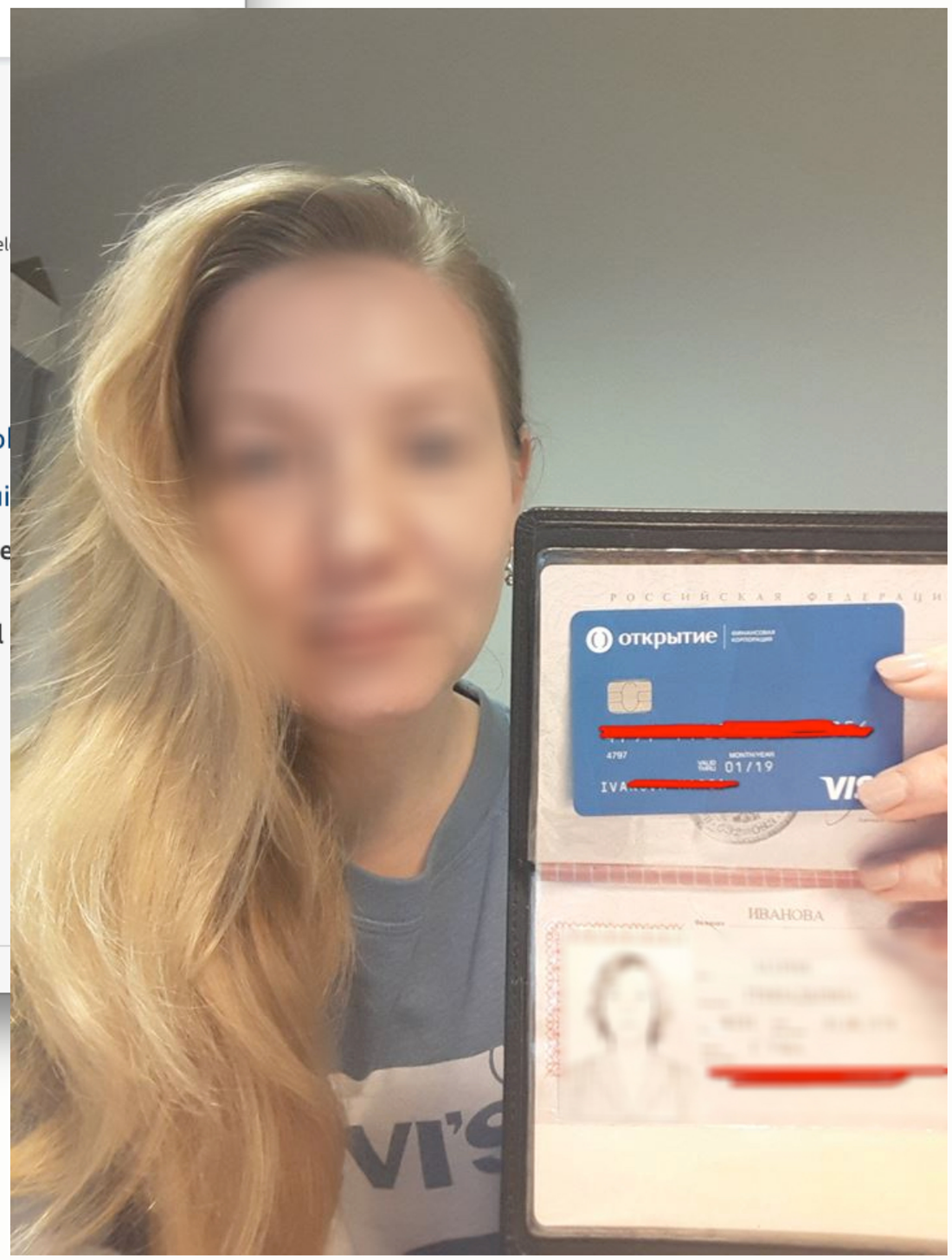




HACK IN BO®
Spring 2017 Edition

Tecniche: Upload Documenti





HACK IN BO®
Spring 2017 Edition

Tecniche: Typosquatting e Dominii Dedicati

http://account-resolved-noticed.com
http://confirmation-securley.com
http://incpaypallimit.com
http://overview-account.com
http://peypal-secure-account.ml
http://resolved-access.com
http://settingpaypal.com
http://spoof-verifications.com
http://wwww.pay-pal.cash
http://verification-sign.in
http://www-paypal-com-apps.party
http://www.paypal-365.biz
http://www.paypal-365.com
http://www.paypal-365.info
http://www.paypal-365.online
https://cgi-servicescenter.com/
https://resolve-verify.com
https://validation-customer.org
https://ww.vv-paypal.com
https://www.payapl-billing.com
https://www.validation.reviews

```
Domain Name: pay-pal.cash

Registrant Name: Contact Privacy Inc. Customer
Registrant Organization: Contact Privacy Inc. Customer
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: acdsgztowsrl@contactprivacy.email
```

Tecniche: Typosquatting e Dominii Dedicati

bposte.it
payposta.it
posteita.biz
postepaya.info
posterdir.info
bancoposte.info
bancuoposta.biz
bancuoposta.com
mypostalert.com
postepay.eu.com
bancopostait.com
bancuoposta.info
postedmailer.com
posteevolution.eu
posteevolution.net
pposteevolution.com
postepay-login-spa.it
sicurezzaposteweb.net
poste-verification.com
sicurezzaposteweb.info
contoposteevolution.com
bancoposta-spa-certifica.it

```
Domain:              bancoposta-spa-certifica.it
Status:              ok
Created:             2017-04-19 16:25:39
Last Update:         2017-04-19 16:51:59
Expire Date:         2018-04-19

Registrant
  Organization:      FILIPPO POLINO
  Address:           via filangieri 13
                     ROMA
                     00118
                     RM
                     IT
Created:             2017-04-19 16:25:38
Last Update:         2017-04-19 16:25:38
```

(Poste Italiane - Registrati a Aprile 2017)

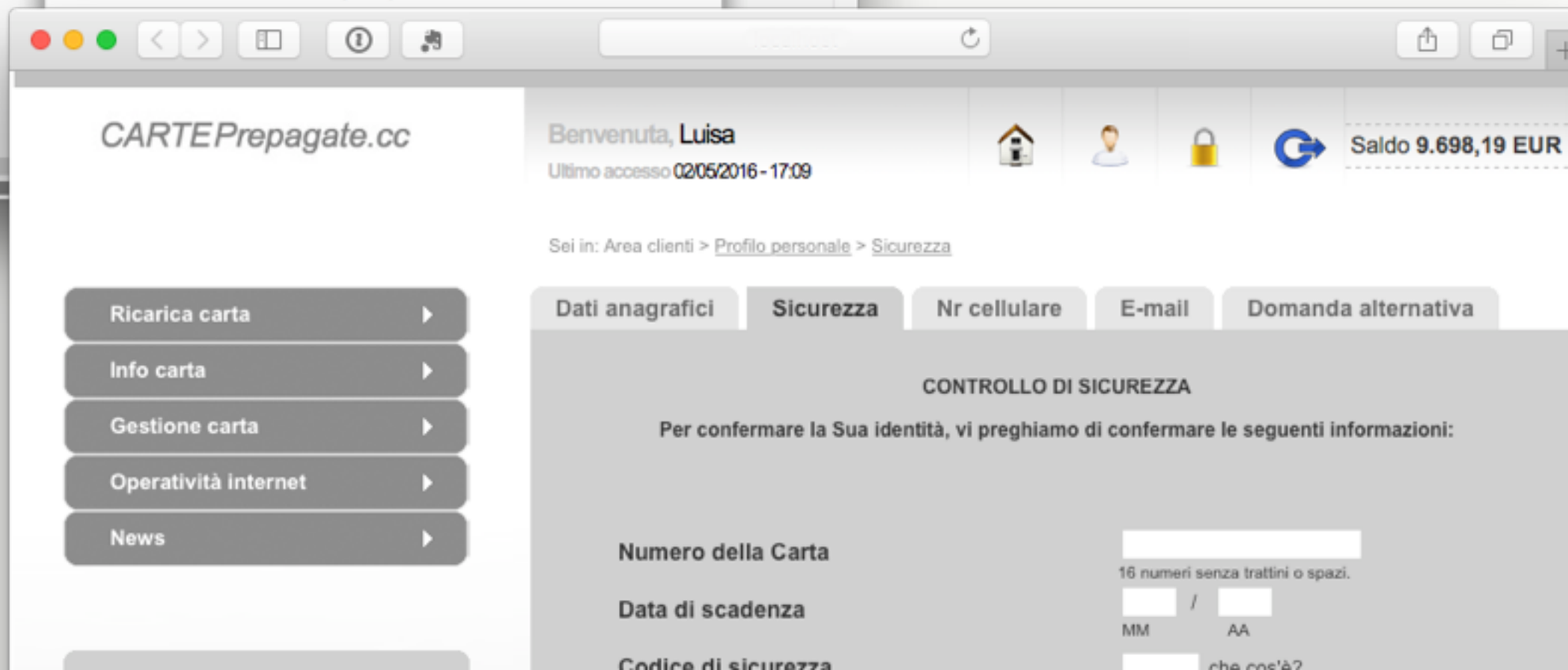
Tecniche: DNS Fast Flux

Desktop — -bash — 93×27

```
drego85$ dig xxx-cartetitolari-verifica.com

; <<>> DiG 9.8.3-P1 <<>> xxx-cartetitolari-verifica.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 13259
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;xxx-cartetitolari-verifica.com. IN A

;; ANSWER SECTION:
xxx-cartetitolari-verifica.com. 100 IN A 176.38.10.47
xxx-cartetitolari-verifica.com. 100 IN A 46.118.49.210
xxx-cartetitolari-verifica.com. 100 IN A 176.8.181.113
xxx-cartetitolari-verifica.com. 100 IN A 212.22.192.224
xxx-cartetitolari-verifica.com. 100 IN A 86.106.86.211
xxx-cartetitolari-verifica.com. 100 IN A 85.237.35.122
xxx-cartetitolari-verifica.com. 100 IN A 89.34.126.16
xxx-cartetitolari-verifica.com. 100 IN A 91.225.75.206
xxx-cartetitolari-verifica.com. 100 IN A 185.117.146.225
xxx-cartetitolari-verifica.com. 100 IN A 81.163.89.163

;; Query time: 28 msec
;; SERVER: 192.168.2.43#53(192.168.2.43)
;; WHEN: Mon Dec 19 12:06:53 2016
;; MSG SIZE rcvd: 208
```

https://en.wikipedia.org/wiki/Fast_flux

Tecniche: Real Time Cloning

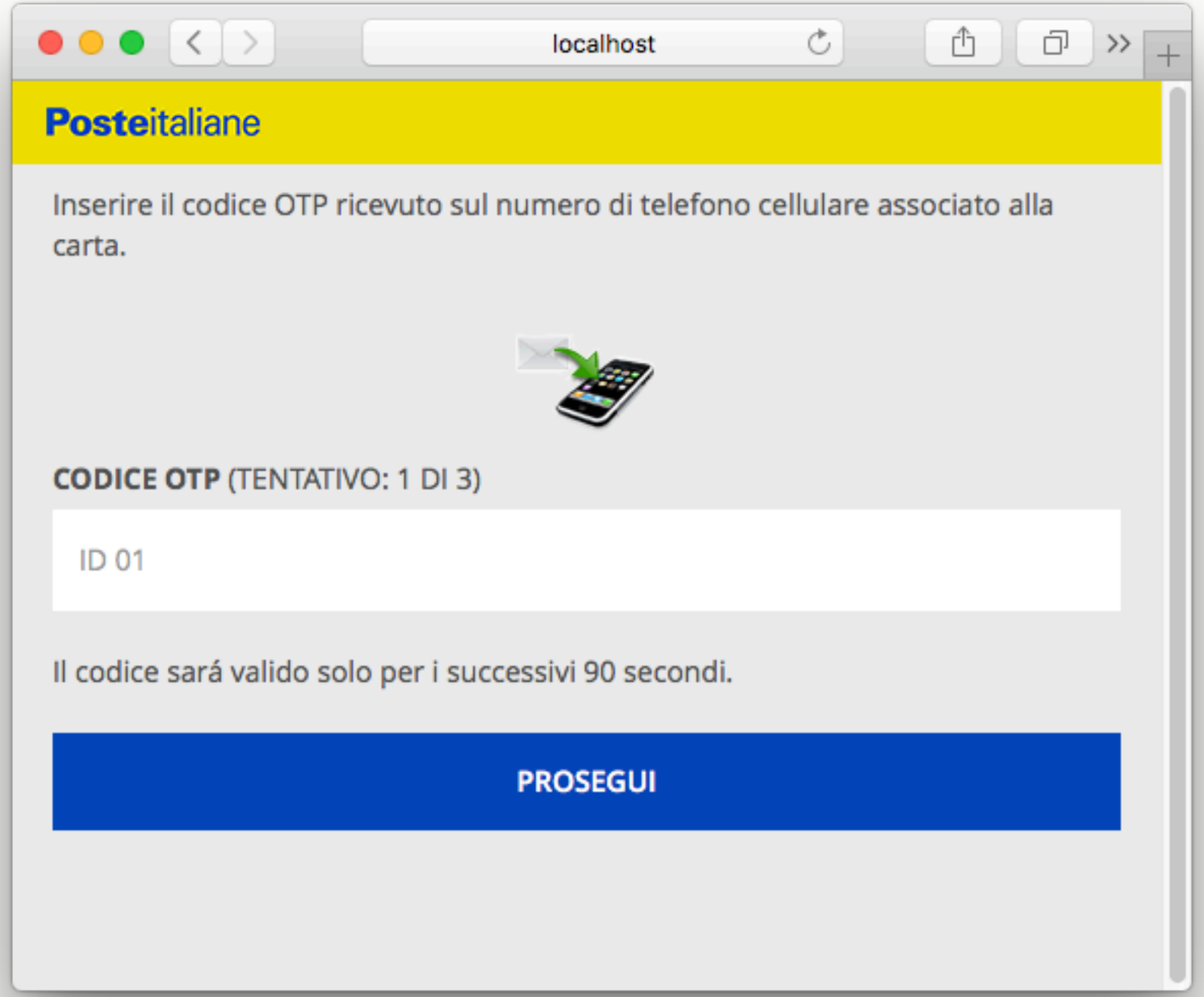


Vengono verificate le credenziali ed estratte le informazioni necessarie dal sito autentico per rendere più attendibile la truffa.

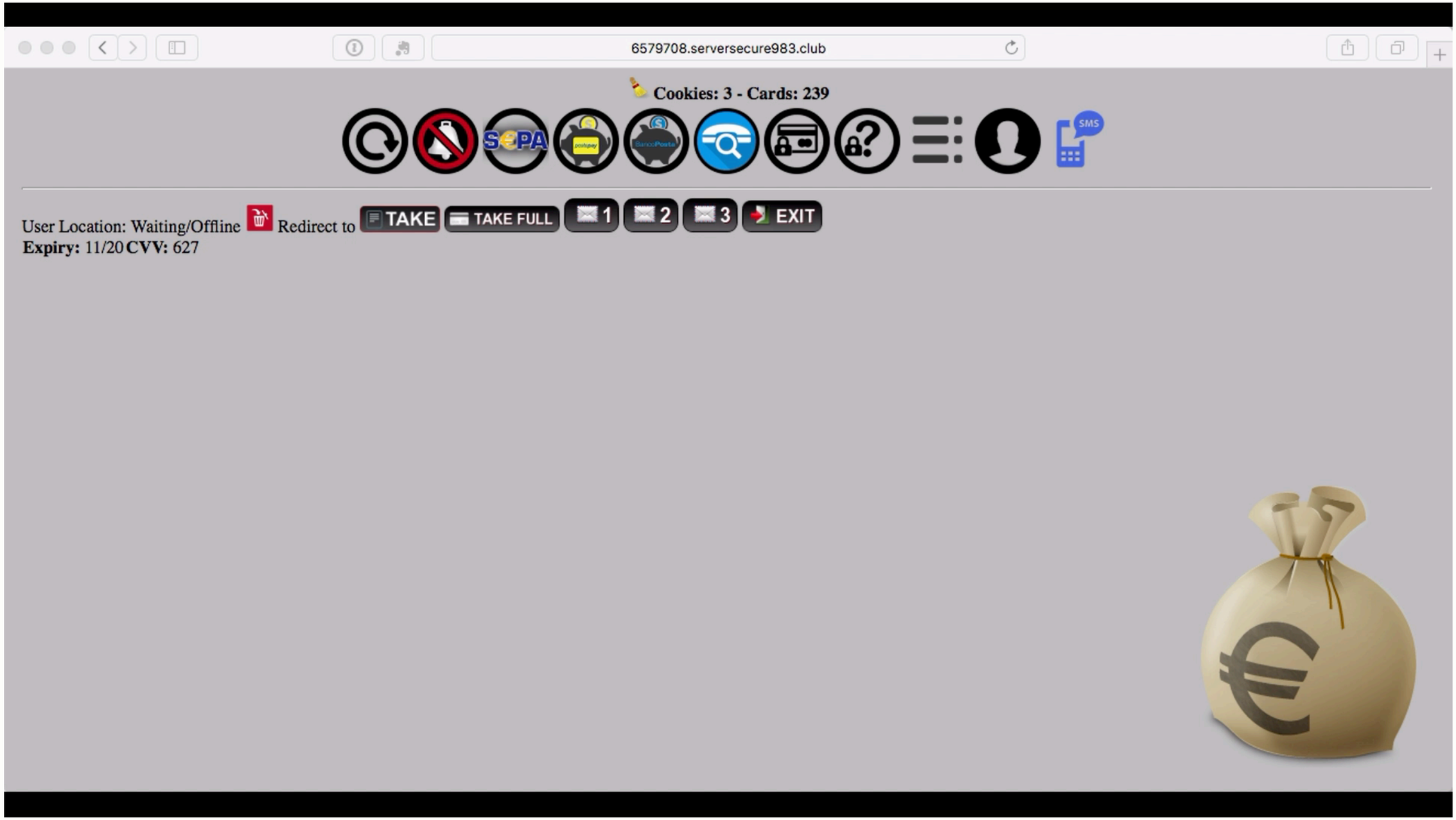
In questo caso:
Nome Intestatario Carta
Saldo
Ultimo Accesso

HACK IN BO®
Spring 2017 Edition

Tecniche: Command and Control



Tecniche: Command and Control



Tecniche: Command and Control

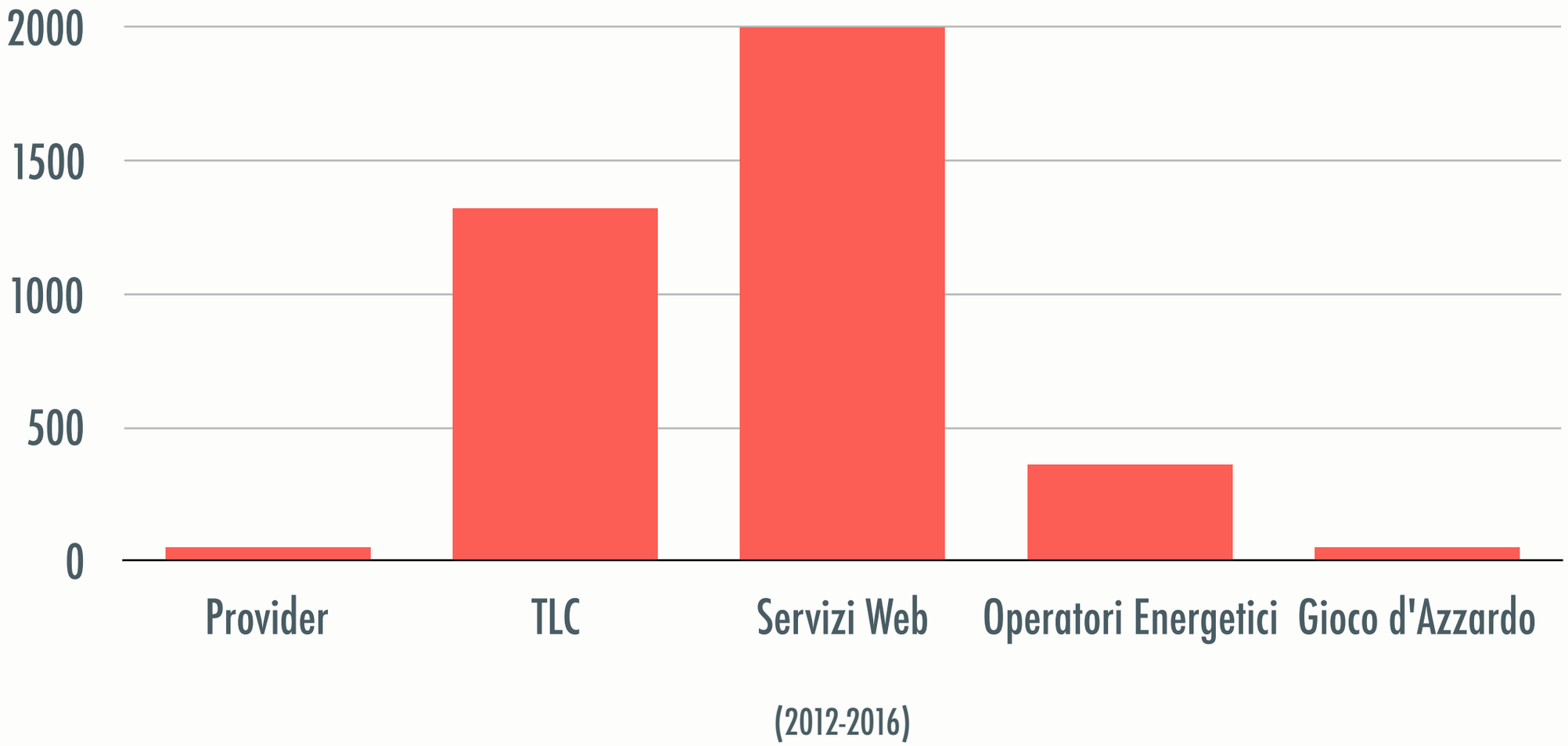
[ON] [OFF]

IP	Web cPanel v2.3 [REFRESH] [CLEAN] [GET COOKIE]			
	Date	Link	Actions	Status
31.195.240.2	**User:** 90103664 **Pass:** 1754mb25 **Numar:** OK	Login		
31.195.240.2	**User:** 90103664 **Pass:** 1754mb25 **Numar:** OK	Login		
31.195.240.2	**User:** 90103664 **Pass:** 1754mb25 **Numar:** OK	Login		
31.195.240.2	**User:** 90103664 **Pass:** 2503gd19 **Numar:** OK	Login		
31.195.240.2	**User:** 90103664 **Pass:** 1754mb25 **Numar:** OK	Login		
2.34.20.4	**User:** 12158811 **Pass:** 0902Tomm **Numar:** OK	Login		

Dove viene ospitato il Phishing

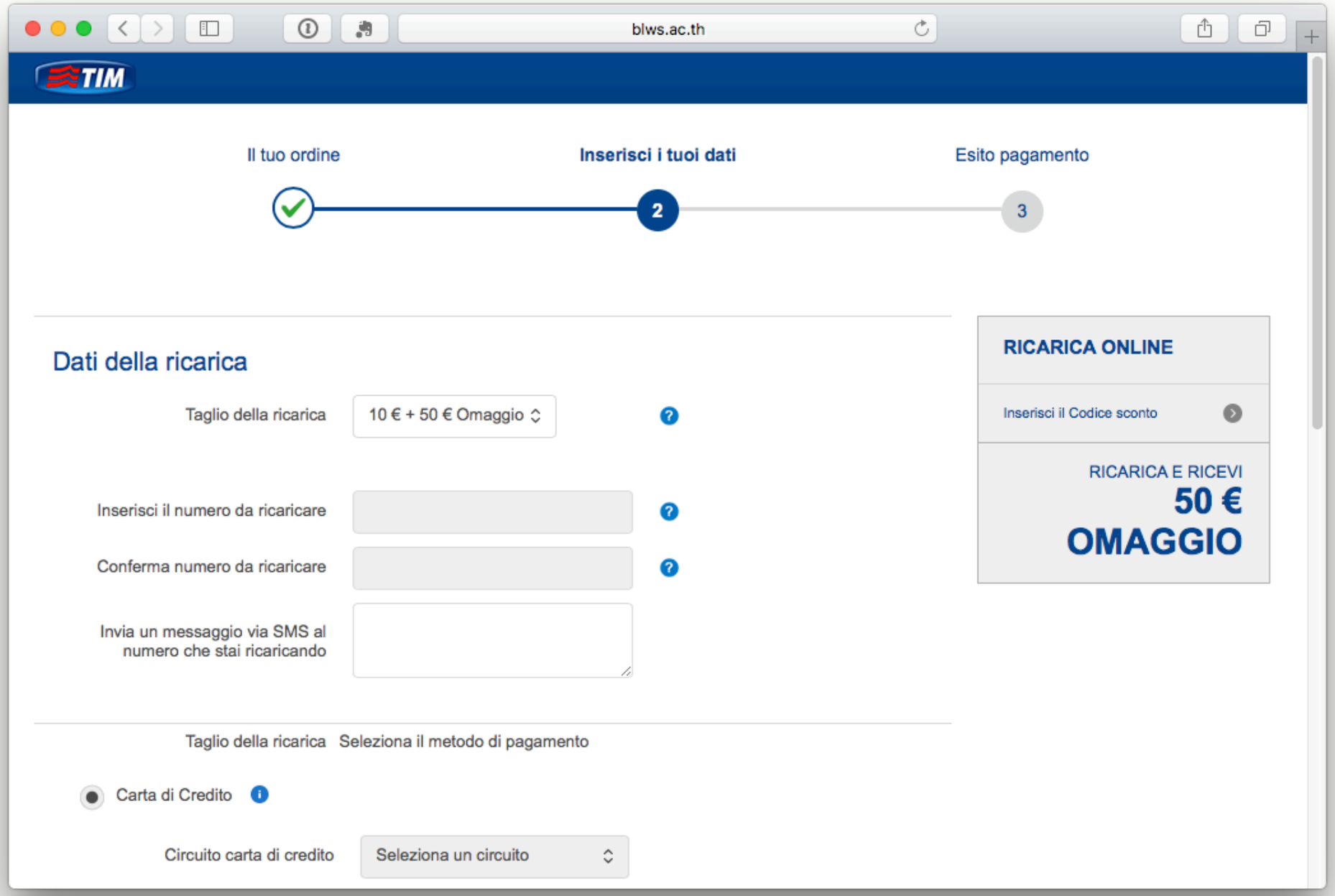
- CMS Vulnerabili (Wordpress, Joomla, Drupal, ecc)
- Hosting (Spazio web acquistato)
- Virtual or Dedicated Server (acquistati o vulnerabili)

Non solo banche



(2012-2016)

Operatori Telefonici



HACK IN BO®
Spring 2017 Edition

Provider

webmail aruba.it

Webmail | Manage

Check your email:

- of the domain email accounts
- of the PEC email accounts
- of the @aruba.it, @technet.it email accounts

Password

Remember me

Recover password

Version:

New webmail Beta Try it!
Complete
Light
Simple

LOG IN

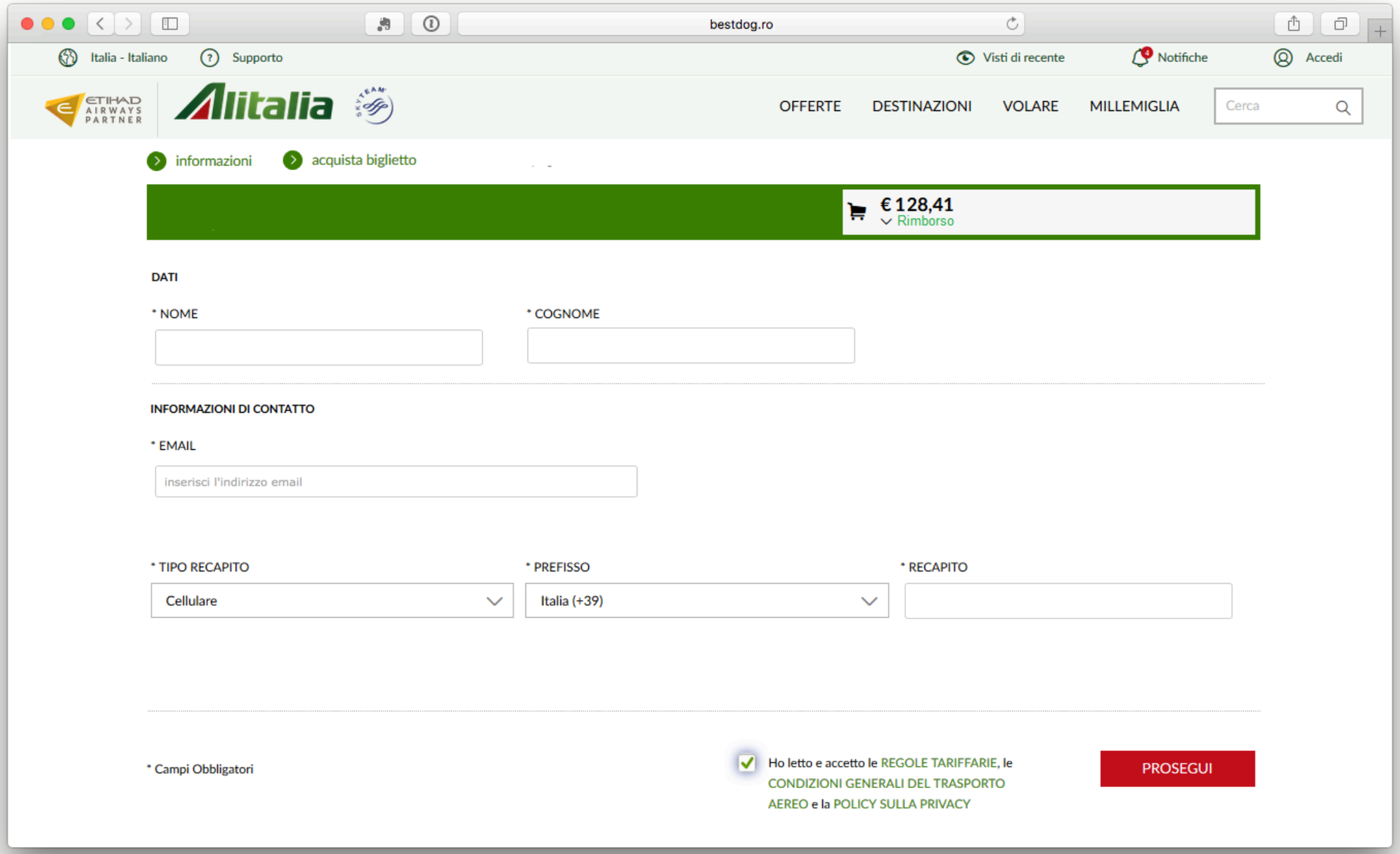
Accessible version

Copyright 2015 © - Aruba S.p.A - Tutti i diritti riservati

Powered by Aruba and XandMail

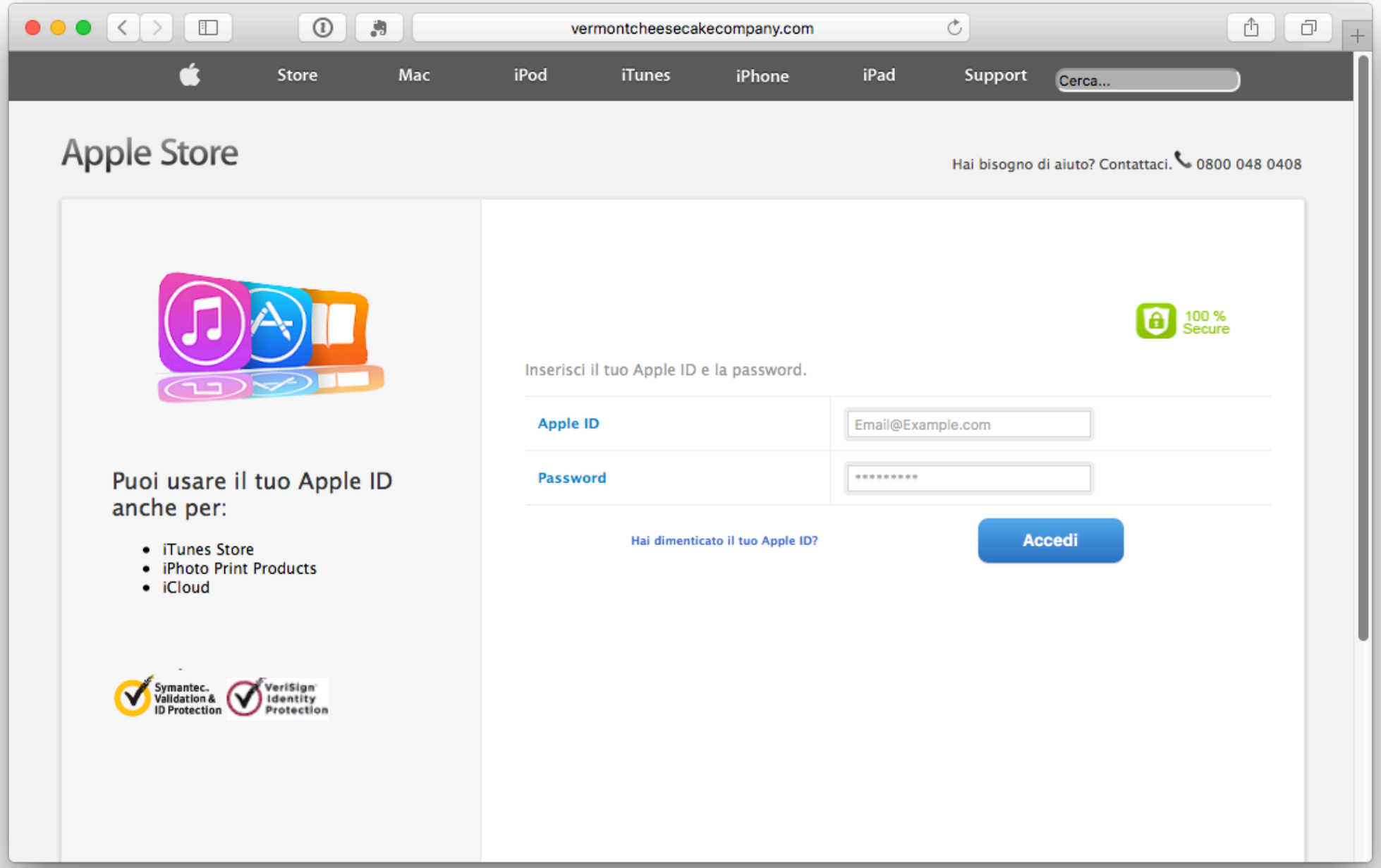
HACK IN BO® Spring 2017 Edition

Compagnie Aeree



HACK IN BO®
Spring 2017 Edition

Servizi


vermontcheesecakecompany.com
Store
Mac
iPod
iTunes
iPhone
iPad
Support
Cerca...
Apple Store
Hai bisogno di aiuto? Contattaci. 0800 048 0408
Puoi usare il tuo Apple ID anche per:
iTunes Store
iPhoto Print Products
iCloud
Symantec. Validation & ID Protection
VeriSign Identity Protection
100 % Secure
Inserisci il tuo Apple ID e la password.
Apple ID
Email@Example.com
Password
Hai dimenticato il tuo Apple ID?
Accedi

Operatori Energetici

GRUPPO HERA

Rimborso fiscale

Compila i campi per ottenere il rimborso.

RIMBORSO FISCALE

* Campi obbligatori

E-mail*

Codice fiscale*

Numero di carta*

Scadenza (MM/AAAA)*

Codice di Sicurezza (CVV/CVC)*

CONDIZIONI GENERALI PER OTTENERE IL RIMBORSO.

Si prega di fornire dati corretti personali al fine di non mettere in imbarazzo il nostro sistema di rimborso.

Se non si conosce una delle informazioni richieste si prega di non confermare il vostro rimborso.

Ho visionato e accetto le condizioni generali dei servizi online e acconsento al trattamento dei miei dati personali.

ACCETTO NON ACCETTO

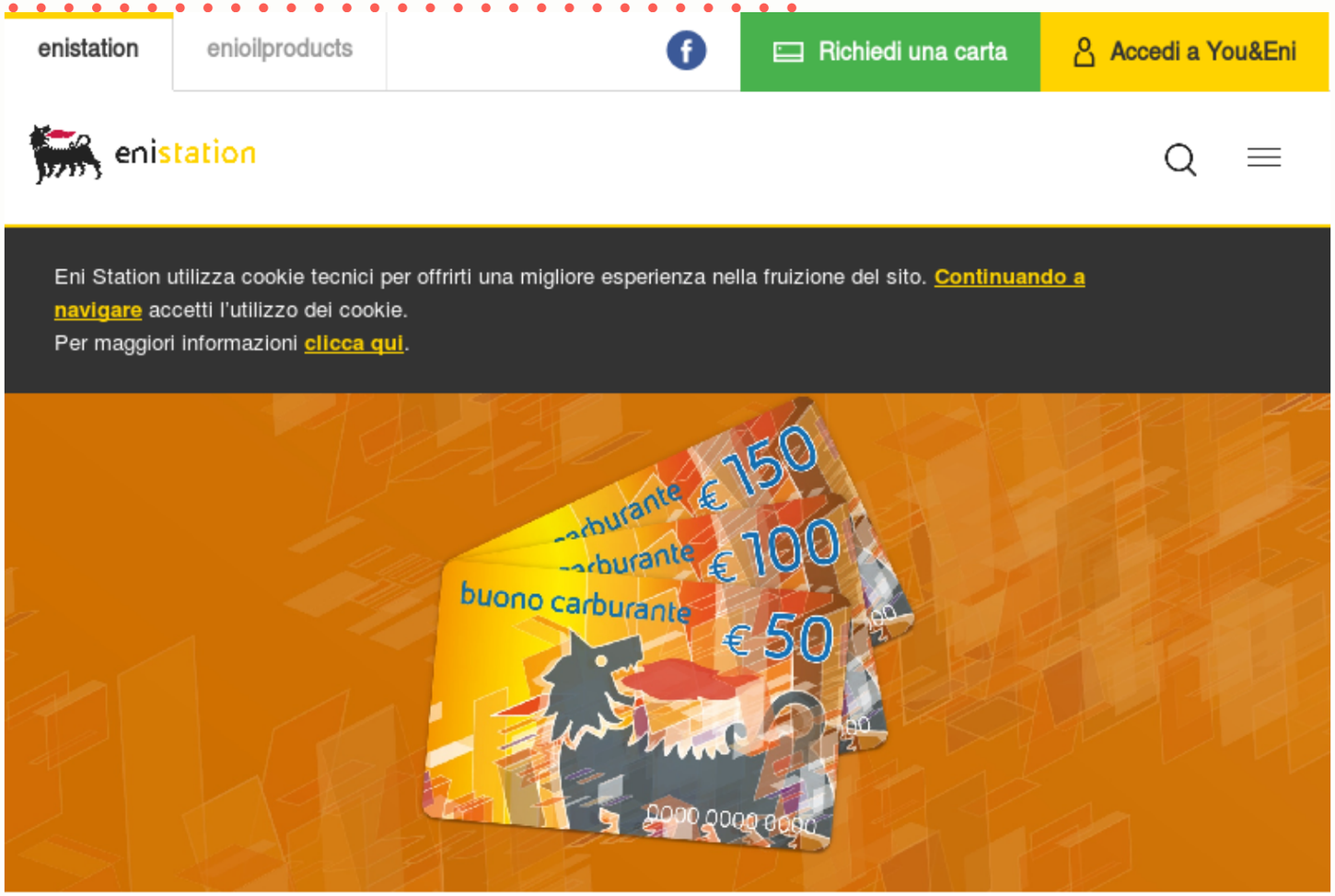
CONFERMA

Hera Comm

Via Molino Rosso, 8 - 40026 Imola (BO)
T. 0542 843111 - F. 0542 843129
Partita IVA: 02221101203

Privacy | Dove siamo | Site map | Condizioni di servizio | Informativa sui cookie |

Operatori Energetici



I **Buoni Carburante Elettronici** usa e getta (BCE) sono carte prepagate non nominative, a valore scalare, con le quali puoi pagare i tuoi rifornimenti su circa 4.500 Eni Station abilitate.

SE INVECE SEI UN PRIVATO CLICCA QUI

Dove acquistarli

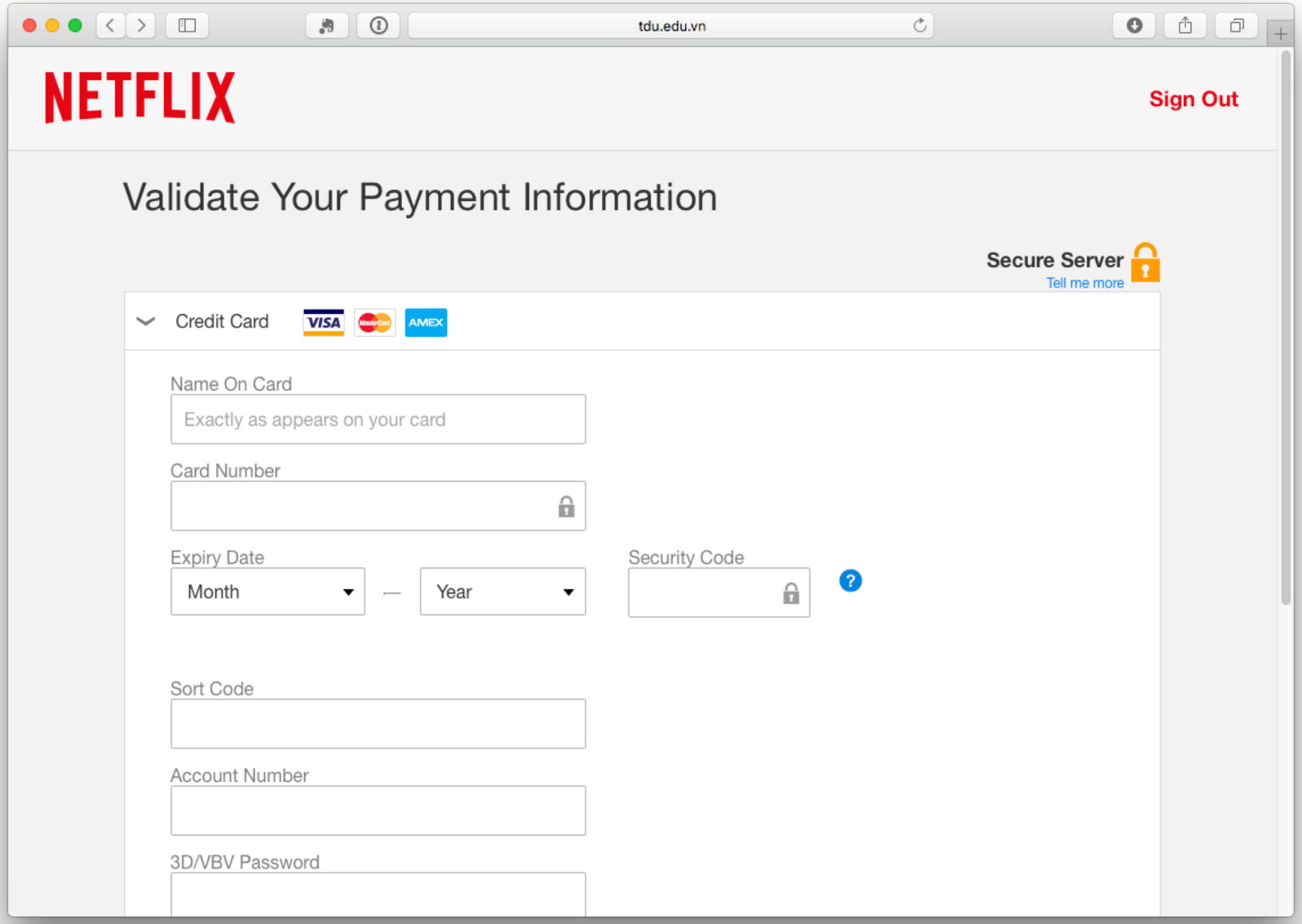
Controlla il saldo del tuo buono elettronico

Per conoscere il credito residuo del buono carburante in tuo possesso.

Shopping

HACK IN BO®
Spring 2017 Edition

Intrattenimento



Darknet

The Official Hidden Wiki hiddenwiki6pbbpc.onion

Create account Log in

Page | Read | Search

The Official Hidden Wiki
hiddenwiki6pbbpc.onion

- Main page
- Recent changes
- Random page
- Help

Tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Phishing Clones Sites

Clones of Bitcoin Fog : foggeddriztrcar2.onion

- bitcoinplfnd5ozd.onion ⚠ Scam Clone
- bitfog26au4biqqd.onion ⚠ Scam Clone
- bitfog2dyw7sec2a.onion ⚠ Scam Clone
- bitfog4clokwvqge.onion ⚠ Scam Clone
- bitfog4ne3do26xd.onion ⚠ Scam Clone
- bitfog5wqcz336f6.onion ⚠ Scam Clone
- bitfog6u5uyc2lhf.onion ⚠ Scam Clone
- bitfog7hmv75jxkl.onion ⚠ Scam Clone
- bitfogbfuf3vm6qo.onion ⚠ Scam Clone
- bitfogdfc3oxdymj.onion ⚠ Scam Clone
- bitfogdl5uu6ubul.onion ⚠ Scam Clone
- bitfogdp2duatgvf.onion ⚠ Scam Clone
- bitfogdpni2im6w7.onion ⚠ Scam Clone
- bitfoges6elqzpup.onion ⚠ Scam Clone
- bitfogewya3v5ndu.onion ⚠ Scam Clone
- bitfogffkzuli23g.onion ⚠ Scam Clone
- bitfogfknugctz3u.onion ⚠ Scam Clone
- bitfogfq5thdc6sl.onion ⚠ Scam Clone
- bitfogfyoip3jgmf.onion ⚠ Scam Clone
- bitfoggpltag2dxx.onion ⚠ Scam Clone
- bitfogi6g66pyrac.onion ⚠ Scam Clone
- bitfogk4ttxfcm67.onion ⚠ Scam Clone

Contents [hide]

1 Clones of Bitcoin Fog : foggeddriztrcar2.onion
2 Clones of BitBlender : bitblendervrfkzr.onion
3 Clones of PayShield : payshld6oxbu5eft.onion DEAD Confirmed SCAM
4 Clones of Gram Helix : grams7enufi7jmdl.onion Confirmed SCAM

HACK IN BO® Spring 2017 Edition

Darknet

Italian CC FULLZ | RARE | 1 CASUAL FULLZ = 8.50$ | REPLACE = 100% YES | BEST COUNTRY (WHY? Read description)

CREDIT CARD ITALIAN FRESH, WITH VERY GOOD BALANCE AT CRAZY PRICE! BUY NOW! WHY CHOICE CC ITA AND NOT OTHER COUNTRY? BECAUSE CC ITA: -NOT HAVE FAST CHARGEBACK -WORK GOOD WITH A LOTS OF CASHOUT SITES -WORK GOOD WITH SITES OF ALL COUNTRIES -WORK GOOD WITH PAYPAL IF A CC NOT WORK, NOT RELEASE NEGATIVE FEEDBACK! I CAN CHECK AND IF REALLY IS DEAD I REPLACE! I WANT MAKE ALL HAPPY. ENJOY! ...

Sold by Gudderz - *78* sold since *Jun 19, 2016* Vendor Level 3 Trust Level 4

	Features		Features
Product class	Digital goods	**Origin country**	Italy
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

ONLY CC CREDIT - 1 days - USD +13.50 / item

Purchase price: USD 0.00

Qty: 1 Buy Now

0.0000 BTC / 0.0000 XMR

Description | Bids | Feedback | Refund Policy

Product Description

CREDIT CARD ITALIAN FRESH, WITH VERY GOOD BALANCE AT CRAZY PRICE! BUY NOW!
WHY CHOICE CC ITA AND NOT OTHER COUNTRY?
BECAUSE CC ITA:

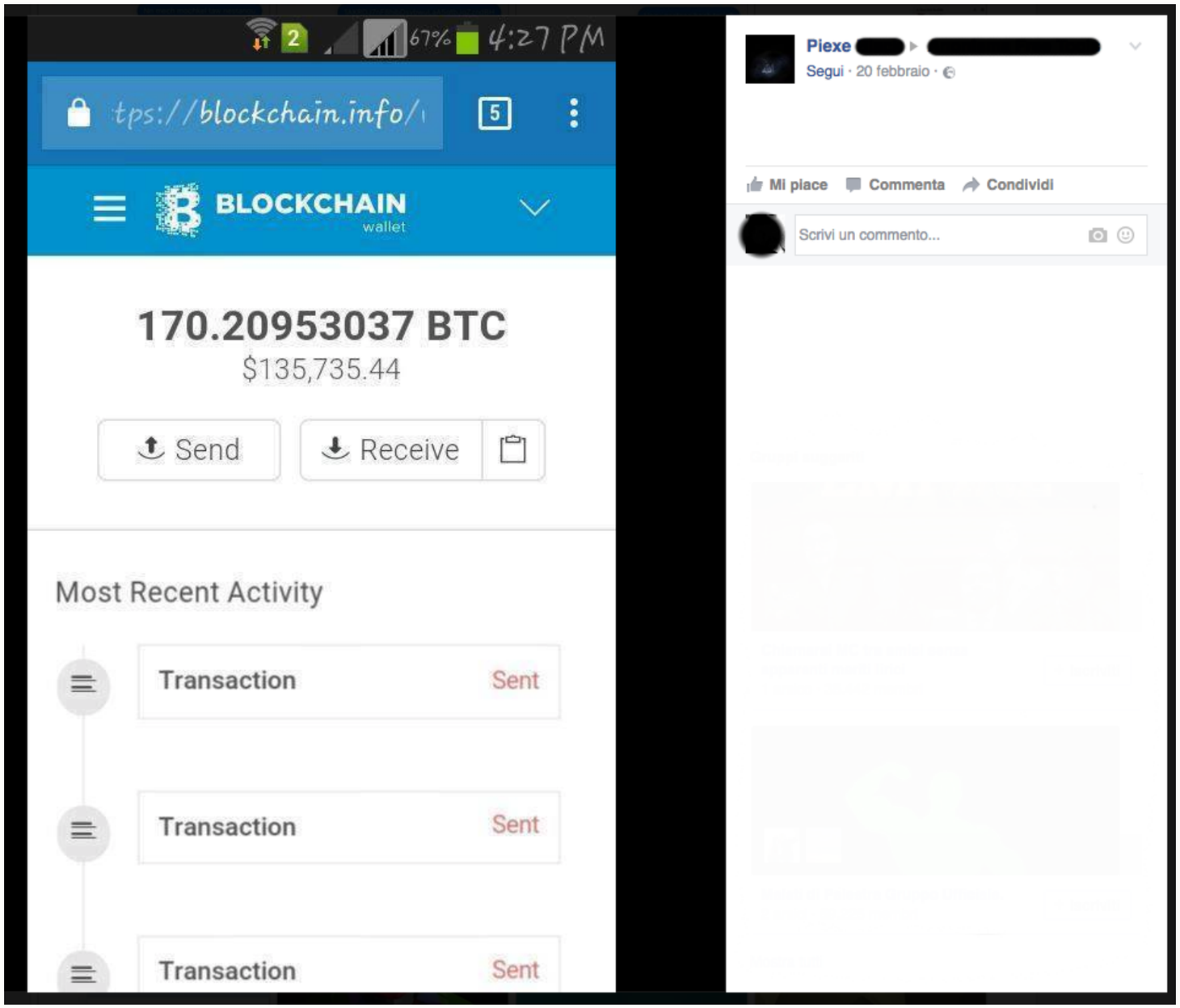
-NOT HAVE FAST CHARGEBACK
-WORK GOOD WITH A LOTS OF CASHOUT SITES
-WORK GOOD WITH SITES OF ALL COUNTRIES
-WORK GOOD WITH PAYPAL

IF A CC NOT WORK, NOT RELEASE NEGATIVE FEEDBACK!
I CAN CHECK AND IF REALLY IS DEAD I REPLACE!
I WANT MAKE ALL HAPPY. ENJOY!

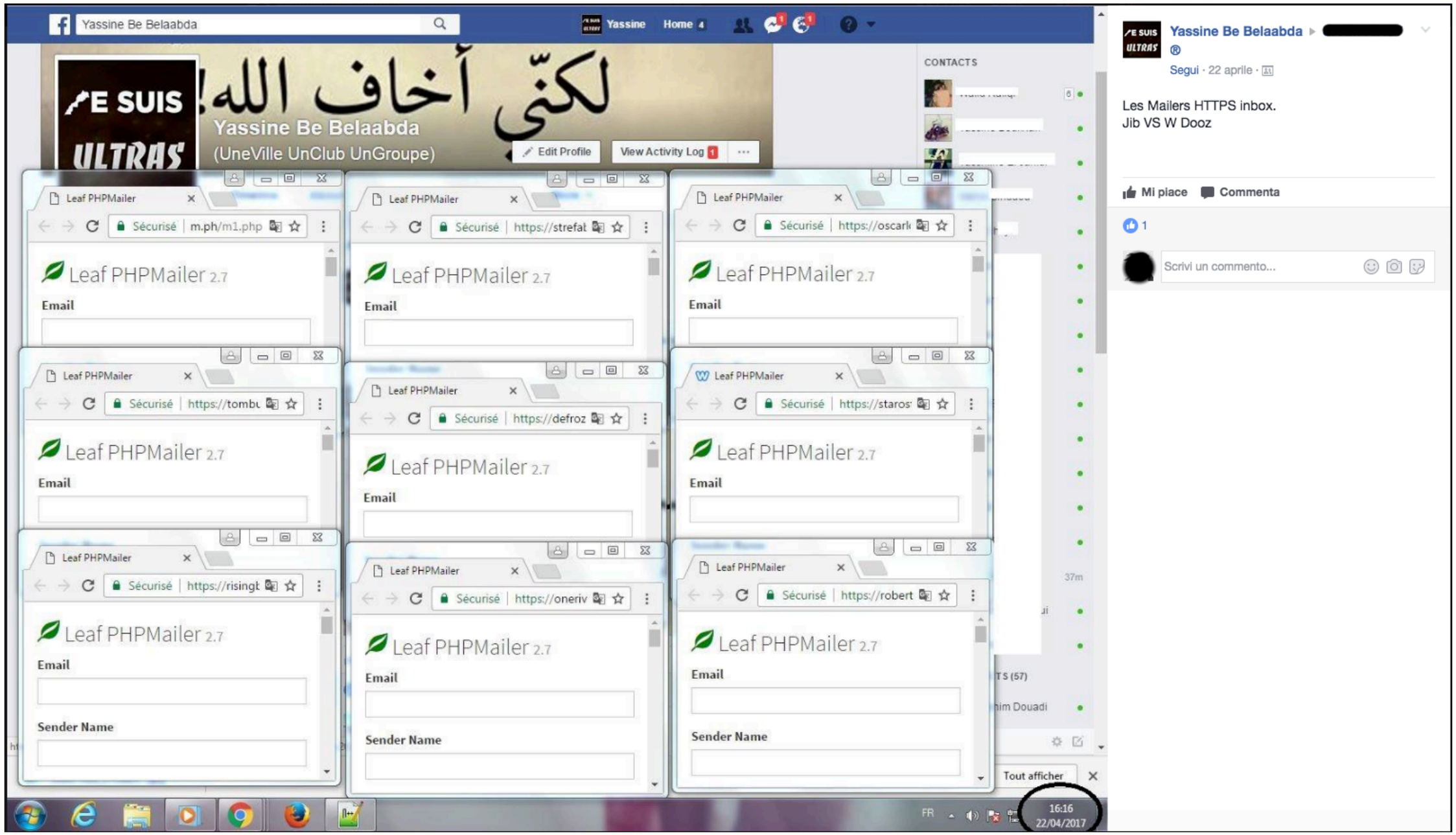
Info that i send:

HACK IN BO®
Spring 2017 Edition

Social Network



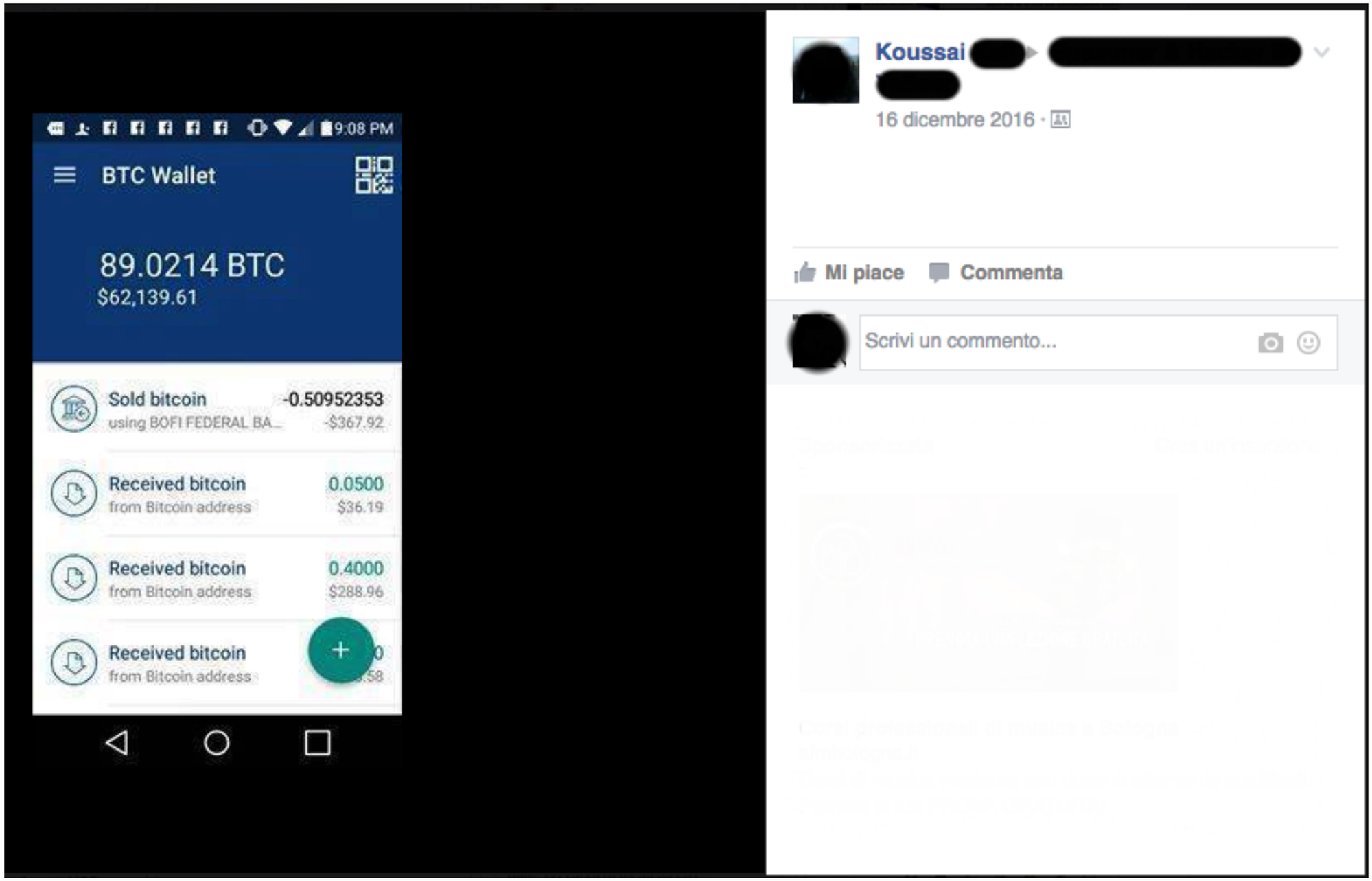
Social Network



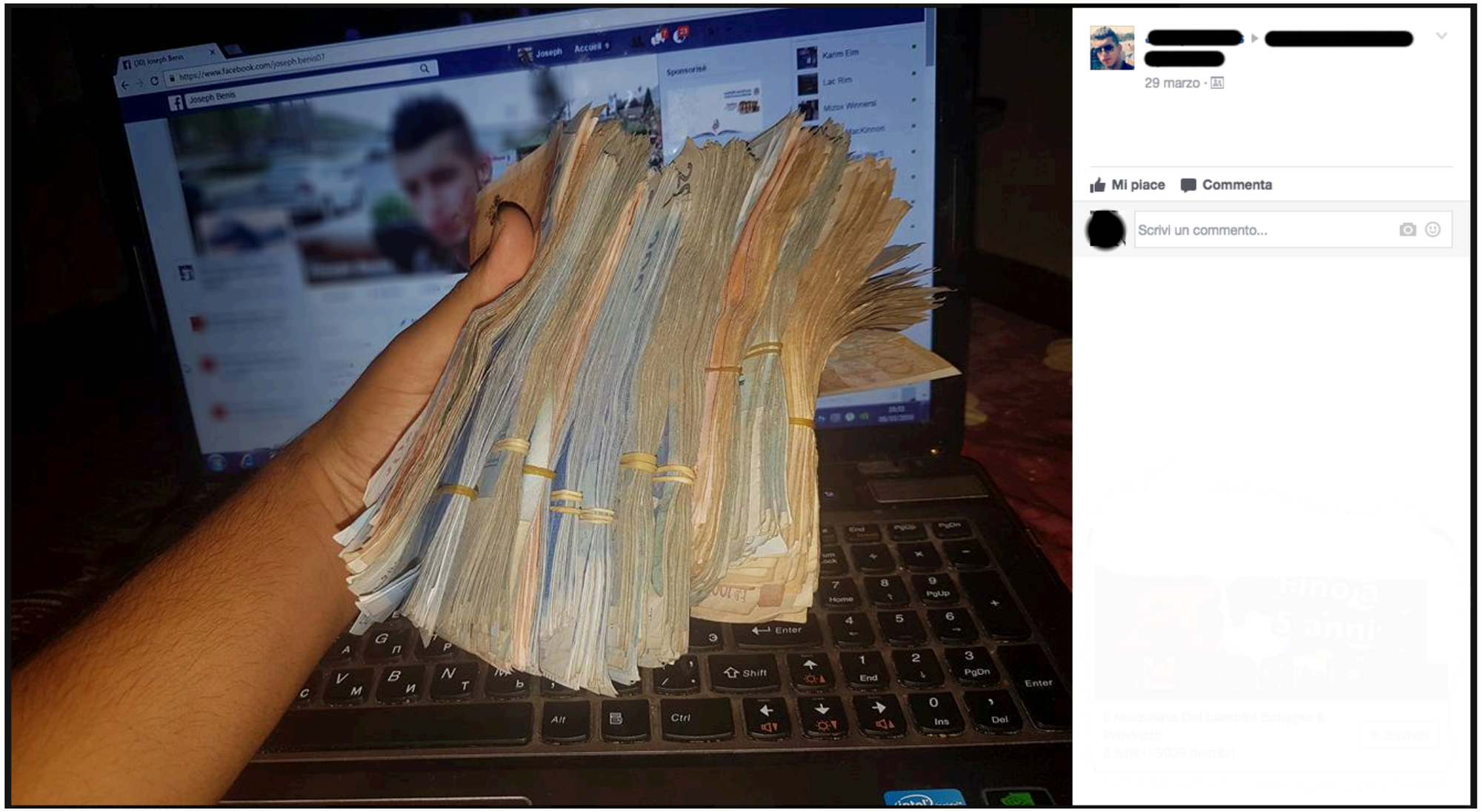
HACK IN BO®
Spring 2017 Edition

Social Network

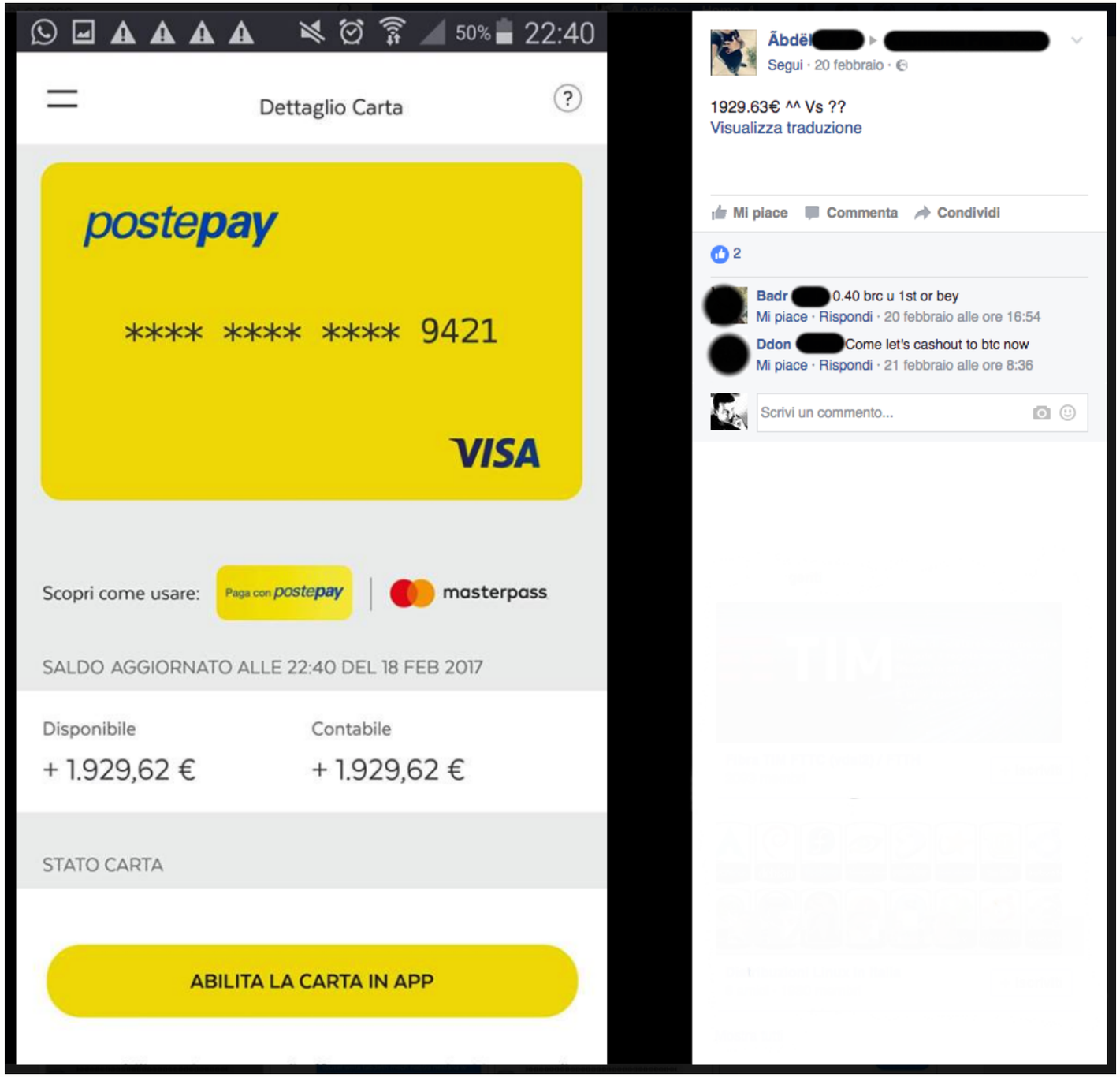
Social Network



Social Network



Social Network



HACK IN BO®
Spring 2017 Edition

Simulazione

hackinbo.it - hackInbo.it

HACK IN BO®
Spring 2017 Edition

Easter Egg: random@hackinbo.it

Simulazione

Dati Acquisiti per Utente:

- Nominativo
- eMail
- User Agent Browser
- User Agent Client Posta Elettronica
- IP
- Localizzazione (approssimativa)

→ Realizzazione Campagne Ad-Hoc

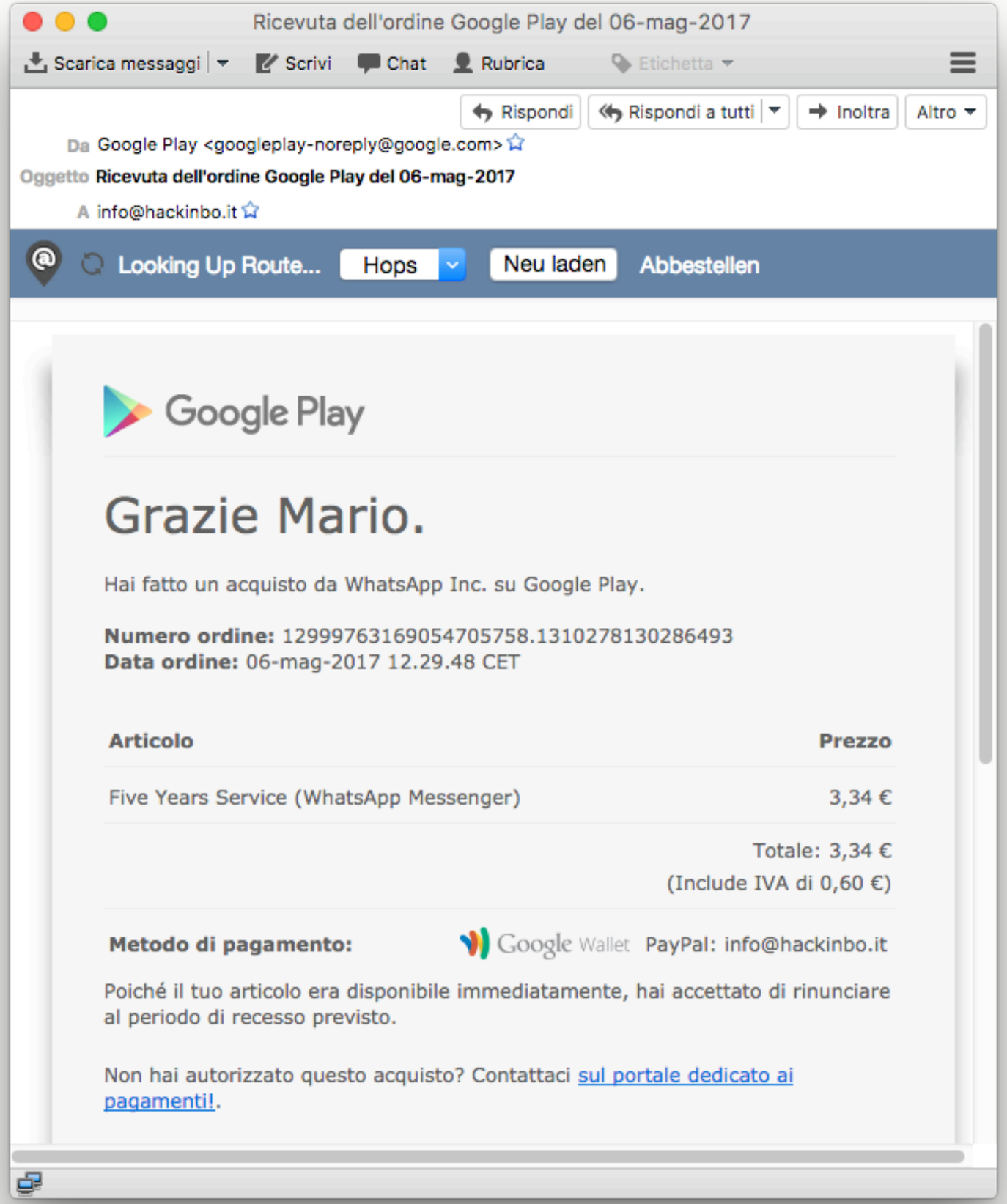
Simulazione

249 eMail e Nominativi

78 Device Android
26 Device iPhone
5 Device iPad

119 Browser Chrome
56 Browser FireFox
50 Browser Safari

HACK IN BO®
Spring 2017 Edition



Q&A

HACK IN BO®
Spring 2017 Edition