



PHISHING: ONE SHOT, MANY VICTIMS!

06.05.2017 - Andrea Draghetti

HACKINBO®
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}

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



Un tentativo di frode

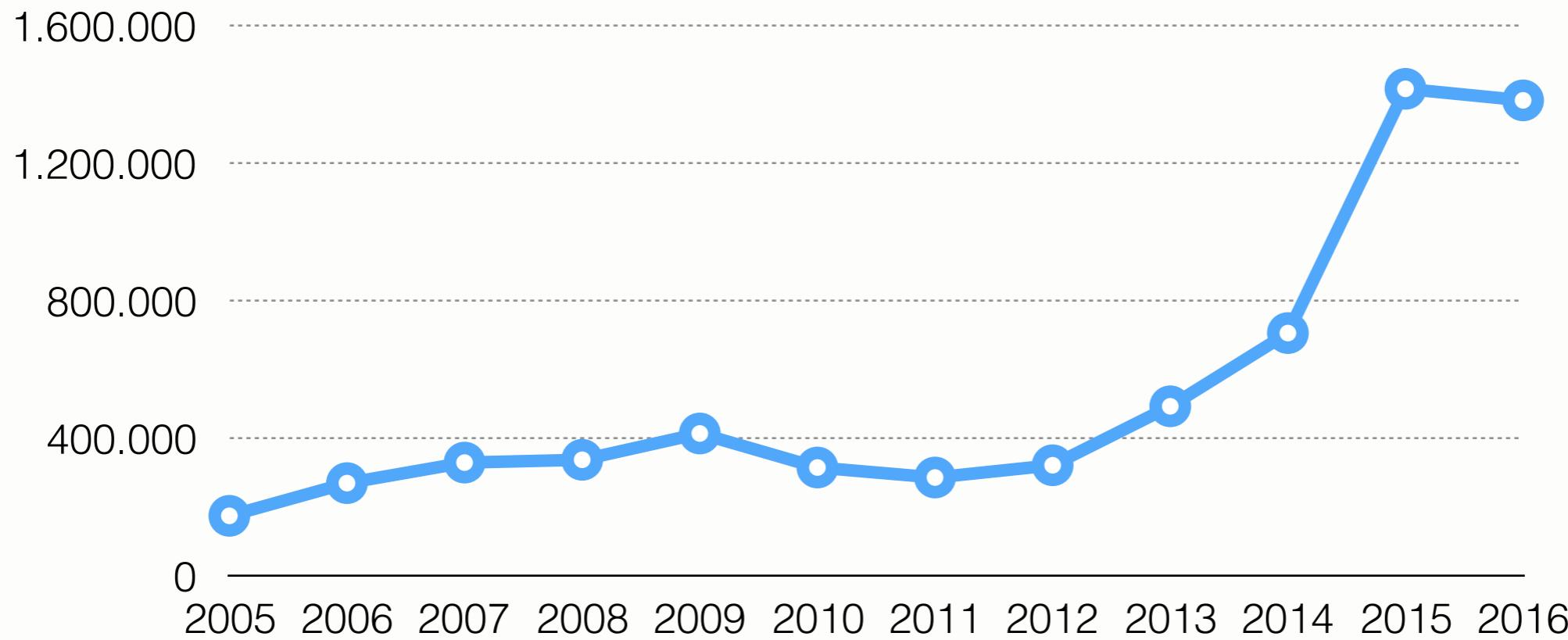


Fonte: http://www.today.it/poll/ad_ecostore_03 - Sondaggio presente dal 27 Ottobre 2016

Statistiche Internazionali

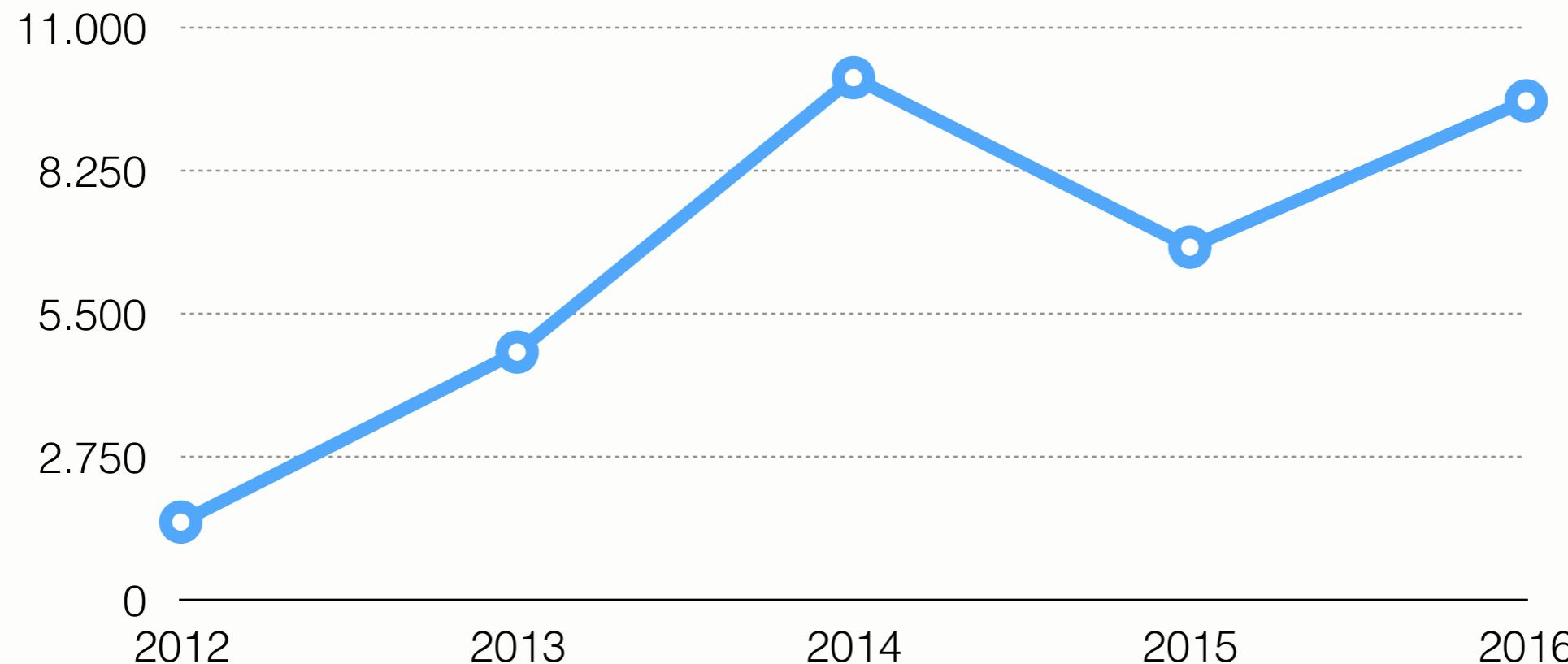
• • • • • • • • • • • • • • • • • •

Siti internet univoci rilevati in attività di Phishing



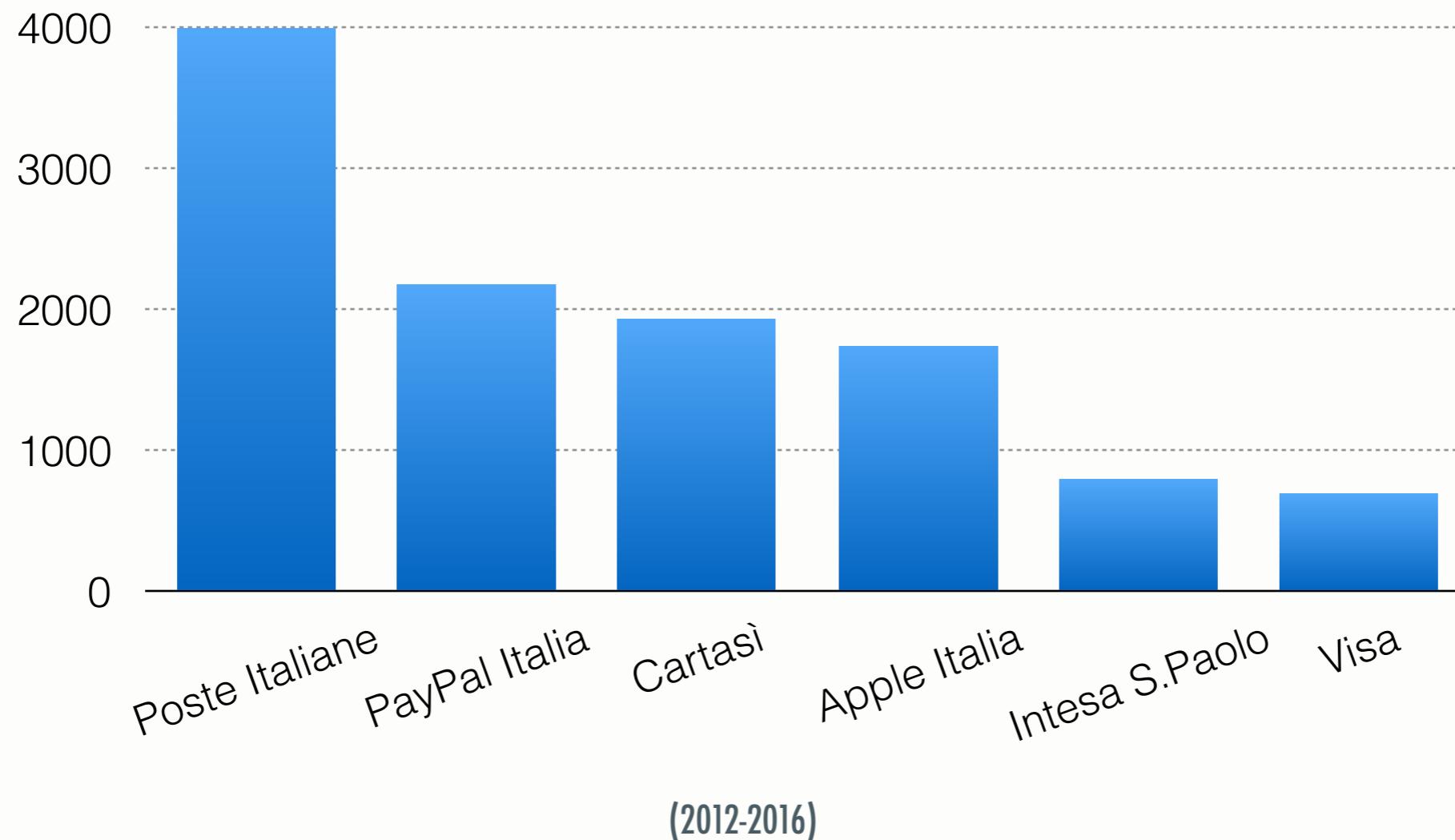
Fonte: Anti-Phishing Working Group

Statistiche Italiane

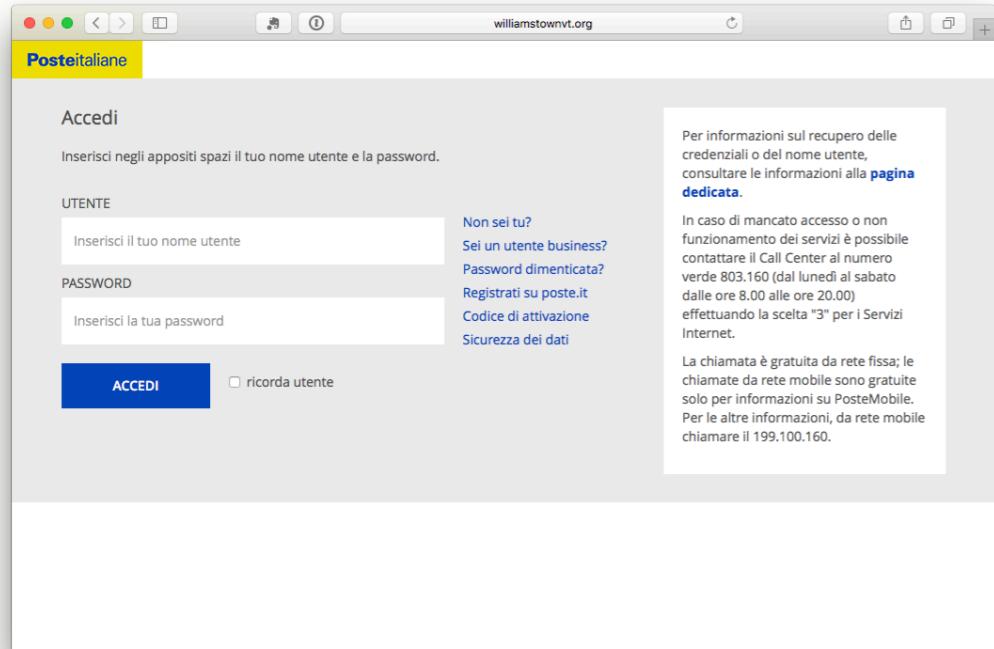


Principali Enti Italiani Colpiti

• •



Cashout su INPS Card



williamstownvt.org

Poste italiane

Accedi

Inserisci negli appositi spazi il tuo nome utente e la password.

UTENTE

Inserisci il tuo nome utente

Non sei tu?

Sei un utente business?

Password dimenticata?

Registrati su poste.it

Codice di attivazione

Sicurezza dei dati

PASSWORD

Inserisci la tua password

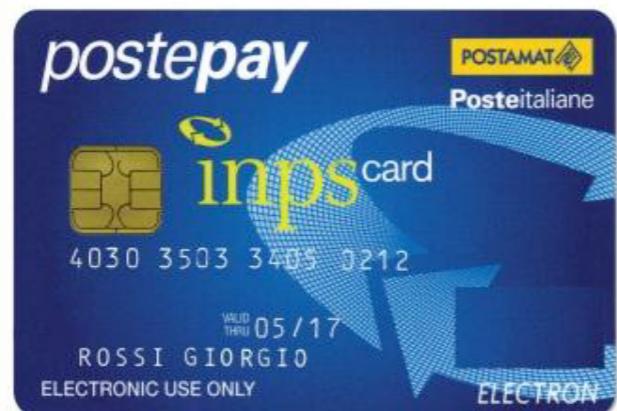
ACCEDI

ricorda utente

Per informazioni sul recupero delle credenziali o del nome utente, consultare le informazioni alla [pagina dedicata](#).

In caso di mancato accesso o non funzionamento dei servizi è possibile contattare il Call Center al numero verde 803.160 (dal lunedì al sabato dalle ore 8.00 alle ore 20.00) effettuando la scelta "3" per i Servizi Internet.

La chiamata è gratuita da rete fissa; le chiamate da rete mobile sono gratuite solo per informazioni su PosteMobile. Per le altre informazioni, da rete mobile chiamare il 199.100.160.



Indagine Forze di Polizia
1,5 milioni euro + 280 mila euro
Marzo 2017

Phishing as a Service

DWISSEL V4		TRIAL	PREMIUM	SILVER
Dwissel V4	Carding like never before!	Free	60\$ /month	100\$ /70 days
	Intro	Dwissel V4 (7 days trial)	Dwissel V4 (30 days license)	Dwissel V4 (70 days license)
	Tools	Validate Email address	Validate Email address	Validate Email address
	Video	Add more than one Creditcard	Add more than one Creditcard	Add more than one Creditcard
	Donate	Strong Creditcard Validator	Strong Creditcard Validator	Strong Creditcard Validator
	Contact	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

.....

DWISSEL V4	GOLD 199\$	MAILER	LETTER 15\$
Carding like never before!	Dwissel V4 (Unlimited license)	Free	Dwissel Smart PayPal Letter V1.0
Intro	Validate Email address	Dwissel Ultra Mailer V1.0	Crypted (Undetected)
Tools	Add more than one Creditcard	Secured with a login area	Smart design
Video	Strong Creditcard Validator	Smart Design	Responsive (Multiple screens)
Donate	Auto Detect Bank (With bank logo)	Easy to use	0 image
Contact	Auto Detect Country	Very Light	Buy
	Upload Document (Sent to Email)	Download	
	Responsive design (Multiple screens)		
	Smart Results (.txt + sent to Email)		
	Undetected		
	Strong scripts		
	Multilangues		

Phishing as a Service

• • • • •

The screenshot shows a web browser window for the URL `z-shadow.co`. The interface is divided into two main sections: 'Account Info' on the left and 'Scamas!' on the right.

Account Info:

- Profile picture: A stylized mask icon.
- Username: `darsene`
- Total victims: 0
- Victims Of Today: 1
- Total ZPoints: 0
- Total Pages: 0/5

Scamas!:

A message at the top states: "⚠ Links get updated automatically every 6 hours."

#	Website Description	Website Logo	Links
1	Facebook		English Arabic Spanish French
2	Facebook Colors		English Arabic Spanish French
3	Facebook Colors1		English
4	HappyFarm		English Arabic
5	Pool Live Tour Free Coins		English Arabic Spanish French
6	8ball pool		English Arabic Spanish French

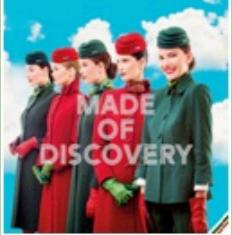
A red bell icon is located in the bottom right corner of the 'Scamas!' section.

Diffusione: eMail

SPAMRimborso Alitalia: Online Disponibile.

Da Alitalia.com <servizi@Alitalia.com>☆
Oggetto ***SPAM***Rimborso Alitalia: Online Disponibile.
30/12/99, 01:00
A Paderborn, NW (985 mi traveled in 1027663 hr.) Hops Neu laden

Scarica subito l'App Alitalia disponibile per sistemi Android su [Google Playstore](#) e per sistemi iOS su [Apple Store](#).

 www.alitalia.com f t g+

MADE OF DISCOVERY
Vi informiamo che avete il diritto per l'importo 128,41€ è online disponibile.
Per accedere al modulo: Clicca qui


Numero di telefono per chiamate dall'estero: +39.06.65649
Numero delle Assistenze Speciali e Assistenza Web: 06.65640


Gentile Cliente,
A causa di un aggiornamento, siamo costretti di sospendere i pagamenti con carta di credito.
Prima di riabilitare la carta di credito abbiamo bisogno di confermare la tua identità compilando una serie di dati già inseriti nella nostra sistema, al momento della tua registrazione sul portale CartaSi.
Ti ricordiamo che non potrai più effettuare dei pagamenti con carta di credito se questa verifica non viene eseguita entro 48 ore dalla sua ricezione.
Per eseguire subito la verifica dei dati, clicca qui:
[Verifica subito](#)
Grazie per la comprensione.
CartaSi S.p.A. © 2017 | P.IVA 04107060966


Spring 2017 Edition

Attenzione! Il tuo account è scaduto WhatsApp Messenger

Scarica messaggi | Scrivi | Chat | Rubrica | Etichetta | Rispondi | Rispondi a tutti | Inoltra | Archivia | Indesiderata | Elimina | Altro | Da Whatsapp <mail@What-sapp.com>☆
Oggetto Attenzione! Il tuo account è scaduto WhatsApp Messenger 04/03/17, 16:56
A Columbus, OH (4,552 mi traveled in 3 min.) Hops Neu laden

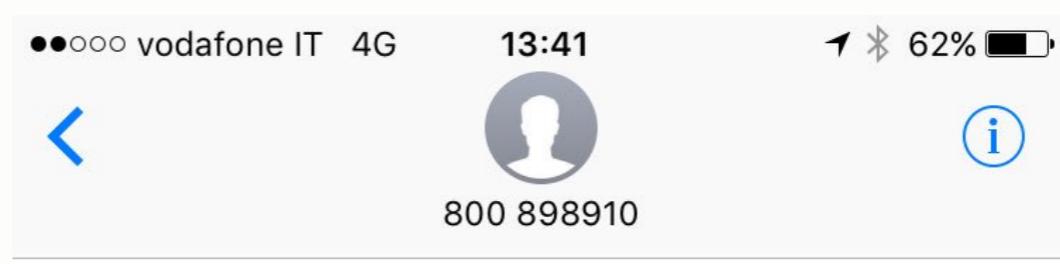
 WhatsApp

Attenzione! Il tuo account è scaduto WhatsApp Messenger

Gentile Cliente !
Da CartaSi S.p.A 2017 <support@csi.biz>☆
Oggetto Gentile Cliente ! 08/04/17, 09:57
A Tokyo, JP (6,042 mi traveled in 19 min.) Hops Neu laden


Gentile Cliente,
A causa di un aggiornamento, siamo costretti di sospendere i pagamenti con carta di credito.
Prima di riabilitare la carta di credito abbiamo bisogno di confermare la tua identità compilando una serie di dati già inseriti nella nostra sistema, al momento della tua registrazione sul portale CartaSi.
Ti ricordiamo che non potrai più effettuare dei pagamenti con carta di credito se questa verifica non viene eseguita entro 48 ore dalla sua ricezione.
Per eseguire subito la verifica dei dati, clicca qui:
[Verifica subito](#)
Grazie per la comprensione.
CartaSi S.p.A. © 2017 | P.IVA 04107060966

Diffusione: SMS



Caro,il tuo iPhone 7JetBlack e' stata trovato in Francia , per vista locazione vai su <http://www.icloud-fmip.com> . Apple Supporto

Diffusione: Ads

① <https://search.yahoo.com/search>

Mail Search News Sports Finance Celebrity Weather Answers Flickr

kraken X

Web Images Video News More ▾ Anytime ▾

Also try: kraken rum, kraken sea monster, kraken skin, kraken tattoo

Ad related to: kraken

Kraken - Trade Bitcoin - Kraken.com
www.Kraken.com
Kraken is the leading Bitcoin exchange with innovative features.
Kraken | Buy, Sell and Margin Trade Bitcoin

Log In Fee Schedule
Price Charts Faq

phishing

Kraken - Image Results



More Kraken images

Kraken | Buy, Sell and Margin Trade Bitcoin (BTC)...
www.kraken.com ▾
Kraken acquires CleverCoin! Welcome new clients! You can login after receiving instructions by email on June 29th.

real site

① <https://www.bing.com/search?q=kraken>

kraken 🔍

Web Images Videos Maps News Rio Games

Also try: Kraken Rum • Giant Squid • Release The Kraken

6,970,000 RESULTS Any time ▾

Kraken.com - Kraken - Trade Bitcoin
Ad · www.Kraken.com
Kraken is the leading Bitcoin exchange with innovative features.
You have visited kraken.com 4 times in last 30 days.

phishing

Images of kraken
bing.com/images



See more images of kraken

Kraken | Buy, Sell and Margin Trade Bitcoin (BTC) and ...
[https://www.kraken.com](http://www.kraken.com) ▾
Kraken acquires CleverCoin! Welcome new clients! You can login after receiving instructions by email on June 29th.

real site

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/.ingdirectrandom/>

<http://www.postepay.it.random.it.iliel.xyz/agg/random/>

Tecniche: Shorturl e Redirect

.....

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



http://www.megoline.co/Alhv9?random?



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



**http://postesecurelogin.posta.it.bancaposta.foo-
autenticazione.random.lojamuser.for-our.info/hescientiststravelled/
ontwo research vessels/almostkilometresfrom/ichangtothe nearbyree/
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=AFQjCNGOANaZ8ewUjs hair7YIZTzeCq7yA](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=AFQjCNGOANaZ8ewUjs hair7YIZTzeCq7yA)

Tecniche: Shorturl e Redirect

• •

Google 

Tutti Notizie Maps Immagini Video Altro Impostazioni Strumenti

Circa 105.000 risultati (0,44 secondi)

Suggerimento: Cerca risultati solo in italiano. Puoi specificare la lingua di ricerca in Preferenze.

Campus Aguascalientes | Tecnológico de Monterrey
www.agc.itesm.mx/ ▾ Traduci questa pagina
Av. Eugenio Garza Sada 1500. Aguascalientes, Ags. 20328. | +52 (449) 9 100 900 D.R.© Instituto Tecnológico y de Estudios Superiores de Monterrey, México.
Escolar · Tesorería · Internacionalización · Mensaje del Director General

Gestisci il tuo ID Apple
www.agc.itesm.mx/inscripciones/ ▾
Un unico ID Apple abbinato a una password ti consente di accedere a tutti i ...

Inicio - Tesorería - Tecnológico de Monterrey - Campus Aguascalientes
www.agc.itesm.mx/tesoreria/ ▾ Traduci questa pagina
Tesorería: (449) 9100 900 ext. 5004. Horarios de Oficina. Lunes a Viernes: de ...

Escolar - Tecnológico de Monterrey - Campus Aguascalientes
www.agc.itesm.mx/escolar/contacto ▾ Traduci questa pagina
Contacto. Contacto. Si tienes alguna duda o comentario puedes: - Escribirnos ...



Monterrey Institute of Technology and Higher Education, Aguascalientes 


Fondazione: 1998

Ricerche correlate


Monterrey Institute of Technolo... Monterrey


Tecnológico de Monterre... Città del Messico


Monterrey Institute of Technolo... San Luis Potosí


Monterrey Institute of Technolo... Chihuahua


TecMilenio University Monterrey

Visualizza altri 10 elementi

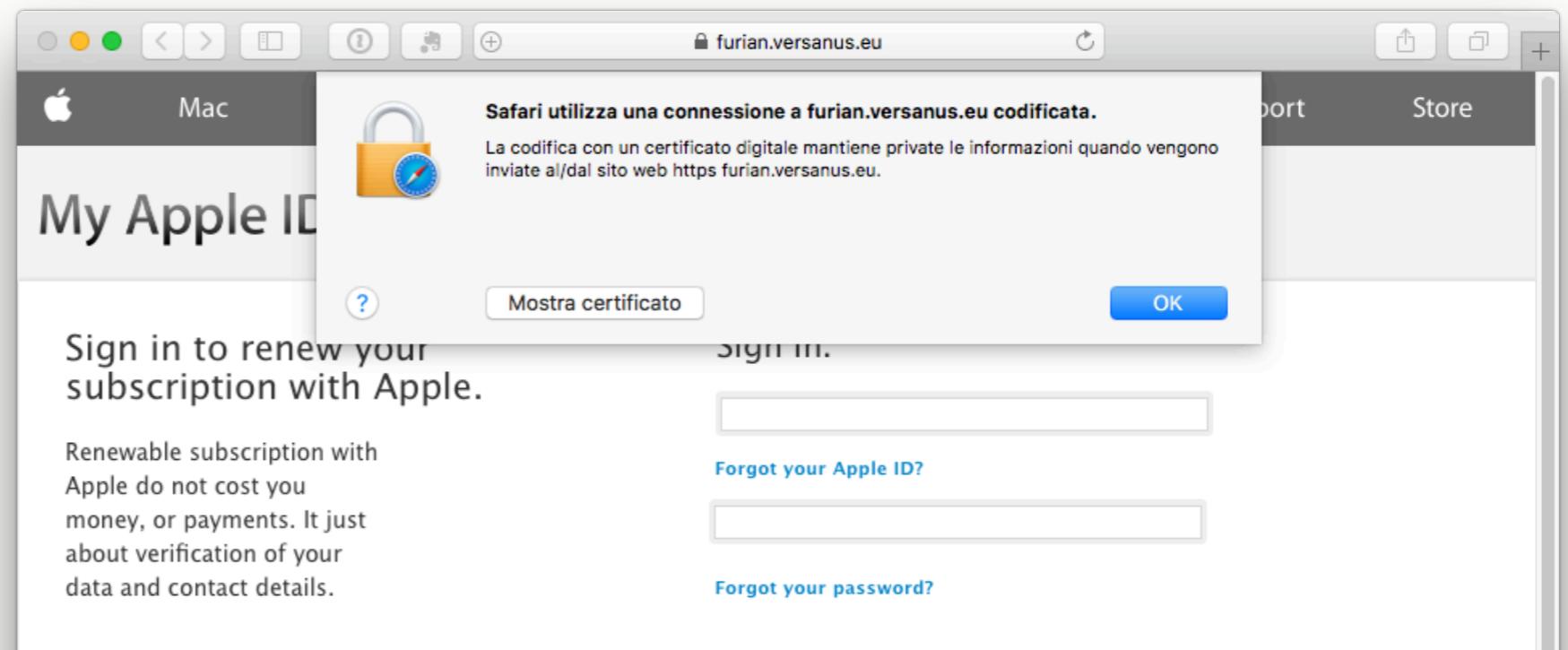
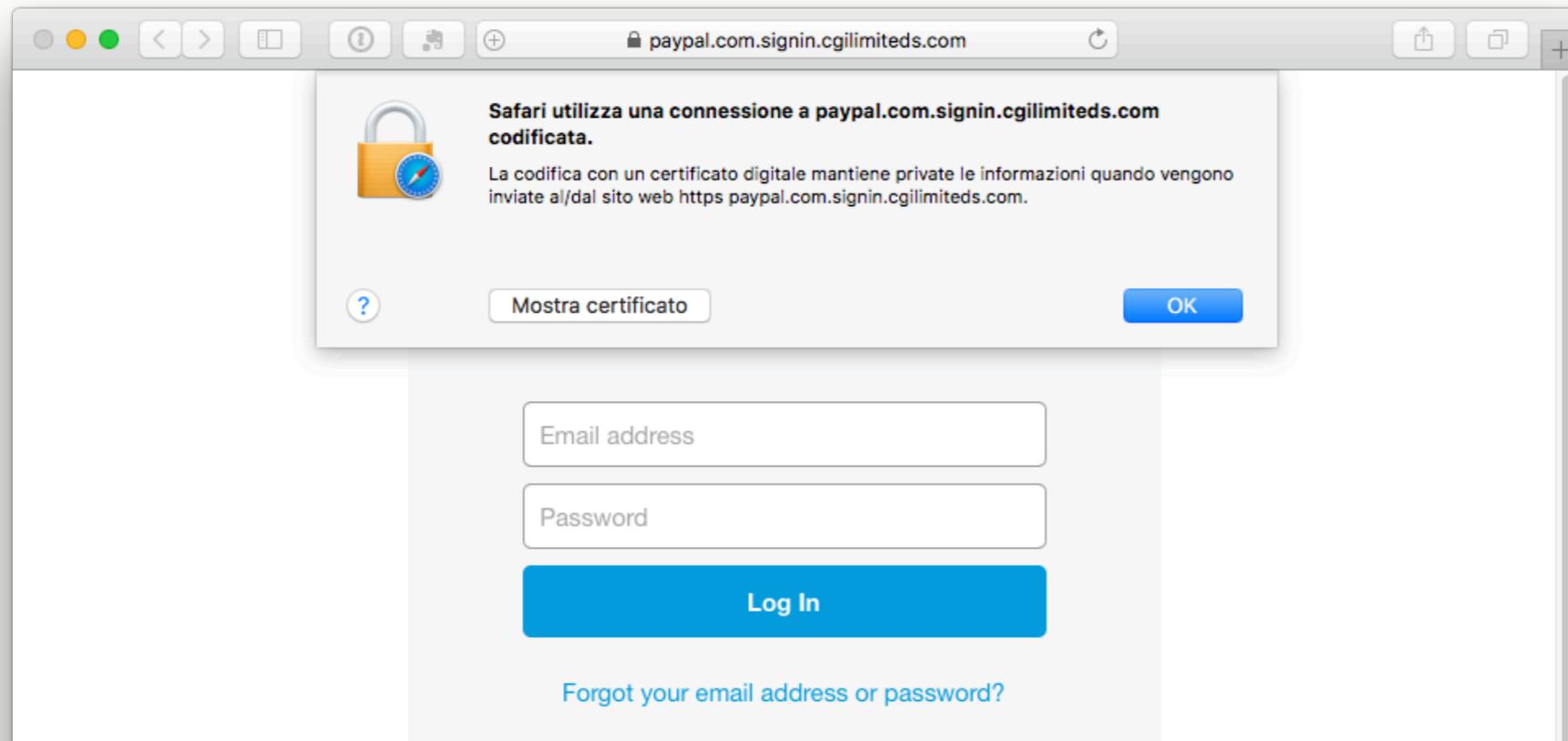
Feedback

Tecniche: Filtri GeolP

```
bots.php ~
lang.php          bots.php +  
  
3 $hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);  
4 $blocked_words =  
5     array("above", "google", "softlayer", "amazonaws", "cyveillance", "phishtank", "dreamhost", "netpilot", "calyxinstitute  
6     ", "tor-exit", "msnbot", "p3pwgdsn", "netcraft", "trendmicro", "ebay", "paypal", "torservers", "messagelabs",  
7     "sucuri.net", "crawler");  
8     foreach($blocked_words as $word) {  
9         if (substr_count($hostname, $word) > 0) {  
10             header("HTTP/1.0 404 Not Found");  
11             die("<h1>404 Not Found</h1>The page that you have requested could not be found.");  
12     }  
13     $bannedIP = array("^81.161.59.*", "^66.135.200.*", "^66.102.*.*", "^38.100.*.*", "^107.170.*.*", "^149.20.*.*",  
14     "^38.105.*.*", "^74.125.*.*", "^66.150.14.*", "^54.176.*.*", "^38.100.*.*", "^184.173.*.*", "^66.249.*.*",  
15     "^128.242.*.*", "^72.14.192.*", "^208.65.144.*", "^74.125.*.*", "^209.85.128.*", "^216.239.32.*",  
16     "^74.125.*.*", "^207.126.144.*", "^173.194.*.*", "^64.233.160.*", "^72.14.192.*", "^66.102.*.*", "^64.18.*.*",  
17     "^194.52.68.*", "^194.72.238.*", "^62.116.207.*", "^212.50.193.*", "^69.65.*.*", "^50.7.*.*", "^131.212.*.*",  
18     "^46.116.*.*", "^62.90.*.*", "^89.138.*.*", "^82.166.*.*", "^85.64.*.*", "^85.250.*.*", "^89.138.*.*",  
19     "^93.172.*.*", "^109.186.*.*", "^194.90.*.*", "^212.29.192.*", "^212.29.224.*", "^212.143.*.*", "^212.150.*.*",  
20     "^212.235.*.*", "^217.132.*.*", "^50.97.*.*", "^217.132.*.*", "^209.85.*.*", "^66.205.64.*", "^204.14.48.*",  
21     "^64.27.2.*", "^67.15.*.*", "^202.108.252.*", "^193.47.80.*", "^64.62.136.*", "^66.221.*.*", "^64.62.175.*",  
22     "^198.54.*.*", "^192.115.134.*", "^216.252.167.*", "^193.253.199.*", "^69.61.12.*", "^64.37.103.*",  
23     "^38.144.36.*", "^64.124.14.*", "^206.28.72.*", "^209.73.228.*", "^158.108.*.*", "^168.188.*.*",  
24     "^66.207.120.*", "^167.24.*.*", "^192.118.48.*", "^67.209.128.*", "^12.148.209.*", "^12.148.196.*",  
25     "^193.220.178.*", "68.65.53.71", "^198.25.*.*", "^64.106.213.*", "^91.103.66.*", "^208.91.115.*",  
      "^199.30.228.*");  
13     if(in_array($_SERVER['REMOTE_ADDR'], $bannedIP)) {  
14         header('HTTP/1.0 404 Not Found');  
15         exit();  
16     } else {  
17         foreach($bannedIP as $ip) {  
18             if(preg_match('/' . $ip . '/', $_SERVER['REMOTE_ADDR'])) {  
19                 header('HTTP/1.0 404 Not Found');  
20                 die("<h1>404 Not Found</h1>The page that you have requested could not be found.");  
21             }  
22         }  
23     }  
24 ?>  
Caratteri: 2.308 · Posizione: 11 - 2.295 · Parole: 191
```

Tecniche: Certificati SSL

• •



Tecniche: Upload Documenti

• • • • •

ubibancit.random.alpuntoideas.es

QuiUBI

- HOME**
- CONTI E CARTE**
- FINANZIAMENTI**
- INVESTIMENTI**
- ASSICURAZIONI**
- ACQUISTA ONLINE**
- FORMULA UBI**
- UBI MONEY**
- UBI PAY**

Esci

Ultimo Accesso

Sicurezza | Privacy | Trasparenza | MIFID | Blocco Carte | Reclami | Manuali | FAQ |

Home

Verifica la tua identità
Il tuo conto è stato temporaneamente disattivato.
Non sarà possibile effettuare depositi, prelievi e pagamenti finché l'account viene disabilitato.
Per continuare ad utilizzare il conto, è necessario verificare alcune informazioni personali.
Una volta verificate le informazioni personali, il conto verrà riattivato automaticamente.

Verifica dell'identità mediante invio di documenti
Al momento dell'invio del documento di identità emesso nel paese di residenza, assicurarsi che esso soddisfi i criteri elencati di seguito:

Utilizzare un file *.jpg, *.jpeg, *.bmp, *.gif, *.png oppure *.pdf
Assicurarsi che i quattro bordi del documento siano chiaramente visibili
Il documento di identità deve essere valido (Non inviare documenti di identità scaduti)
La scansione del documento deve essere di alta qualità; assicurarsi che il documento sia leggibile
Dimensioni massime del file: 5 MB
È possibile caricare un numero massimo di 5 file alla volta.
Il nome del file deve contenere solo caratteri alfanumerici.

Per conferma d'identità è necessario caricare i documenti esatti che abbiano:

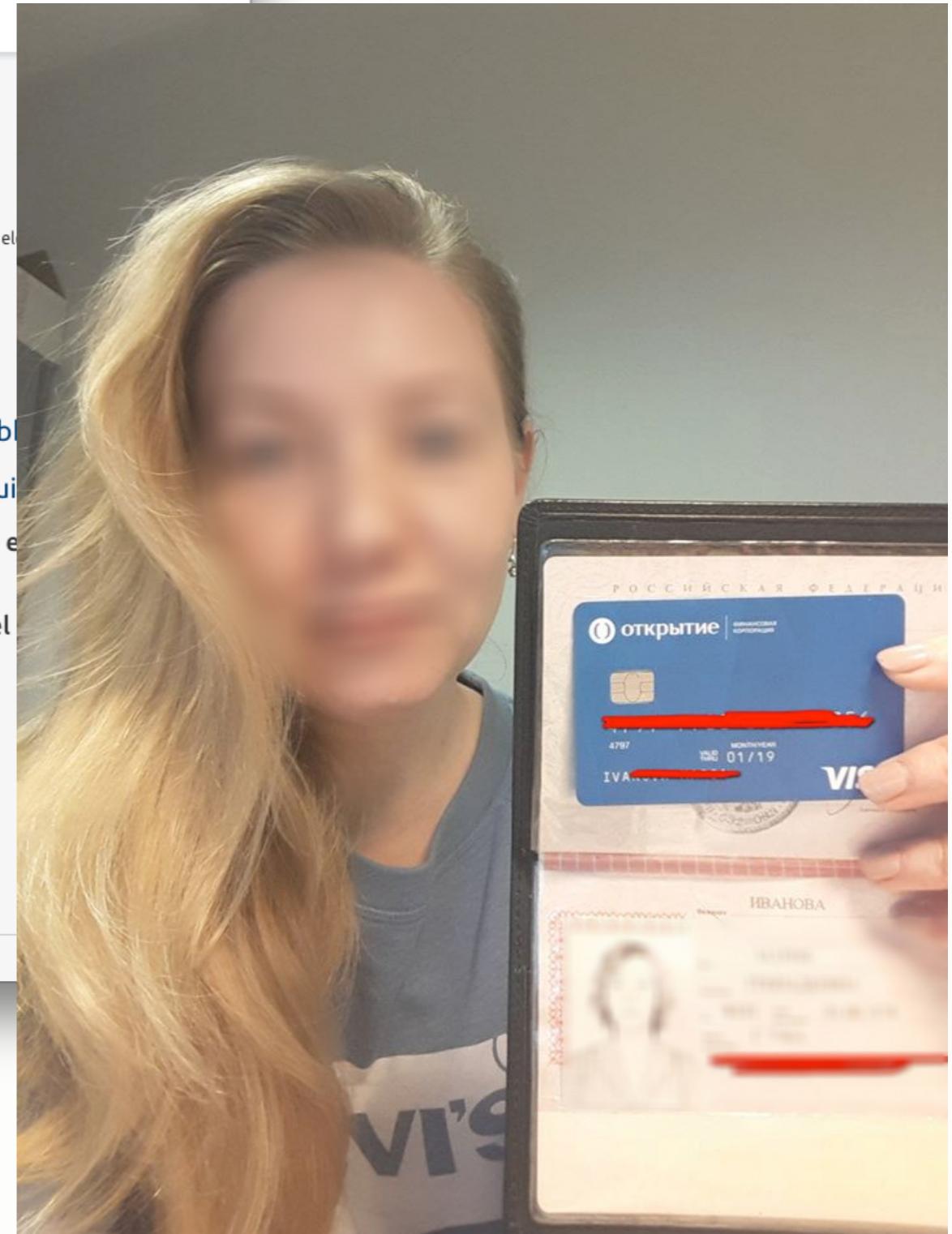
È necessario caricare la carta d'identità o il passaporto, o patente di guida.

Foto a colori della carta d'identità o il passaporto o patente di guida (fronte e retro).

Carica selfie colore di voi tenendo la carta d'identità o patente di guida o del passaporto.

Carica selfie colore di voi tenendo la carta di credito:

Carica file



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://www.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

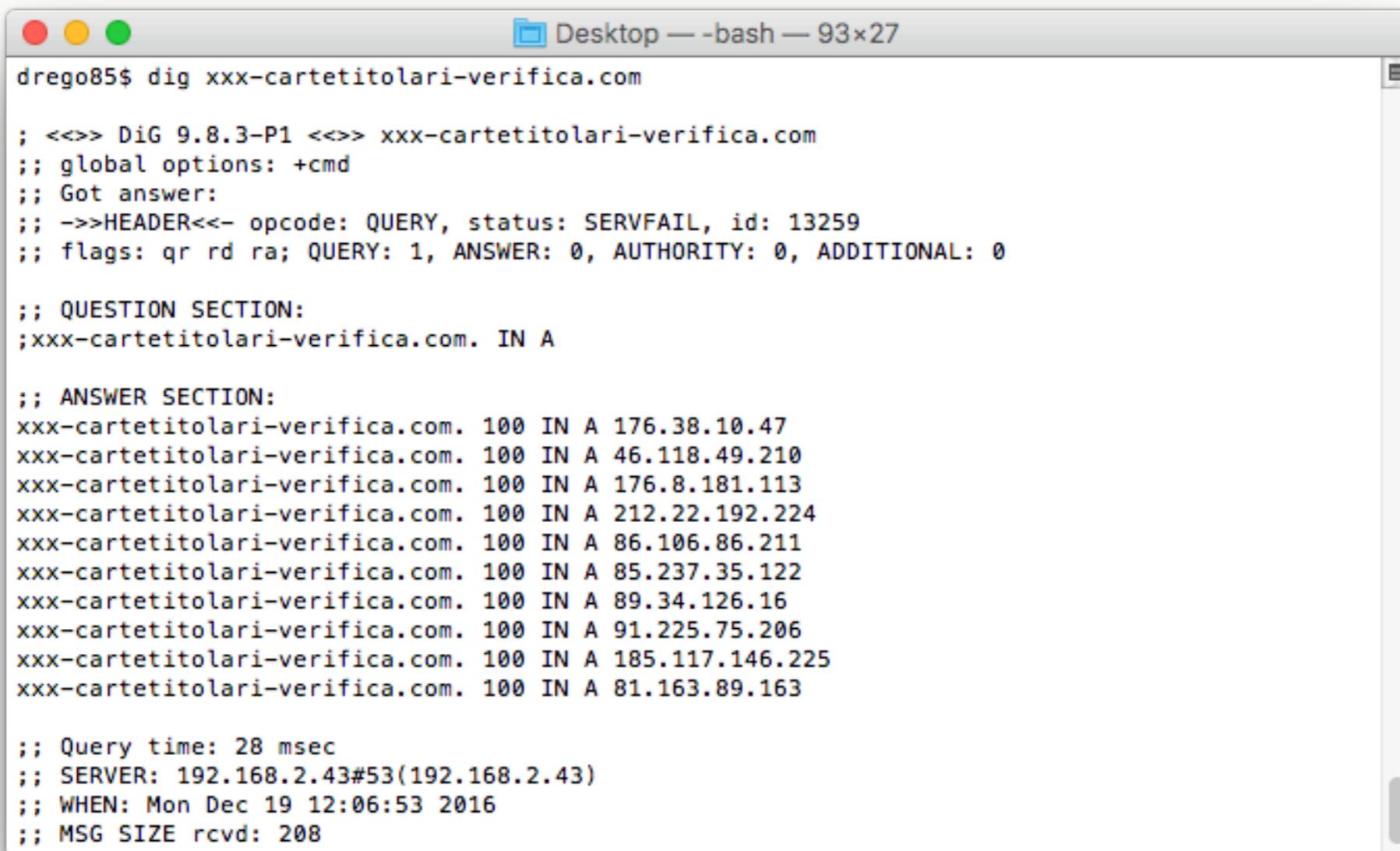
Tecniche: Typosquatting e Dominii Dedicati

.....

bposte.it	Domain:	bancoposta-spa-certifica.it
payposta.it	Status:	ok
posteita.biz	Created:	2017-04-19 16:25:39
postepaya.info	Last Update:	2017-04-19 16:51:59
posterdir.info	Expire Date:	2018-04-19
bancoposte.info	Registrant	
bancuoposta.biz	Organization:	FILIPPO POLINO
bancuoposta.com	Address:	via filangieri 13
mypostalert.com		ROMA
postepay.eu.com		00118
bancopostait.com		RM
bancuoposta.info		IT
postedmailer.com	Created:	2017-04-19 16:25:38
posteevolution.eu	Last Update:	2017-04-19 16:25:38
posteevolution.net		
pposteevolution.com		
postepay-login-spa.it		
sicurezzaposteweb.net		
poste-verification.com		
sicurezzaposteweb.info		
contoposteevolution.com		
bancoposta-spa-certifica.it		

Tecniche: DNS Fast Flux

• •



```
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



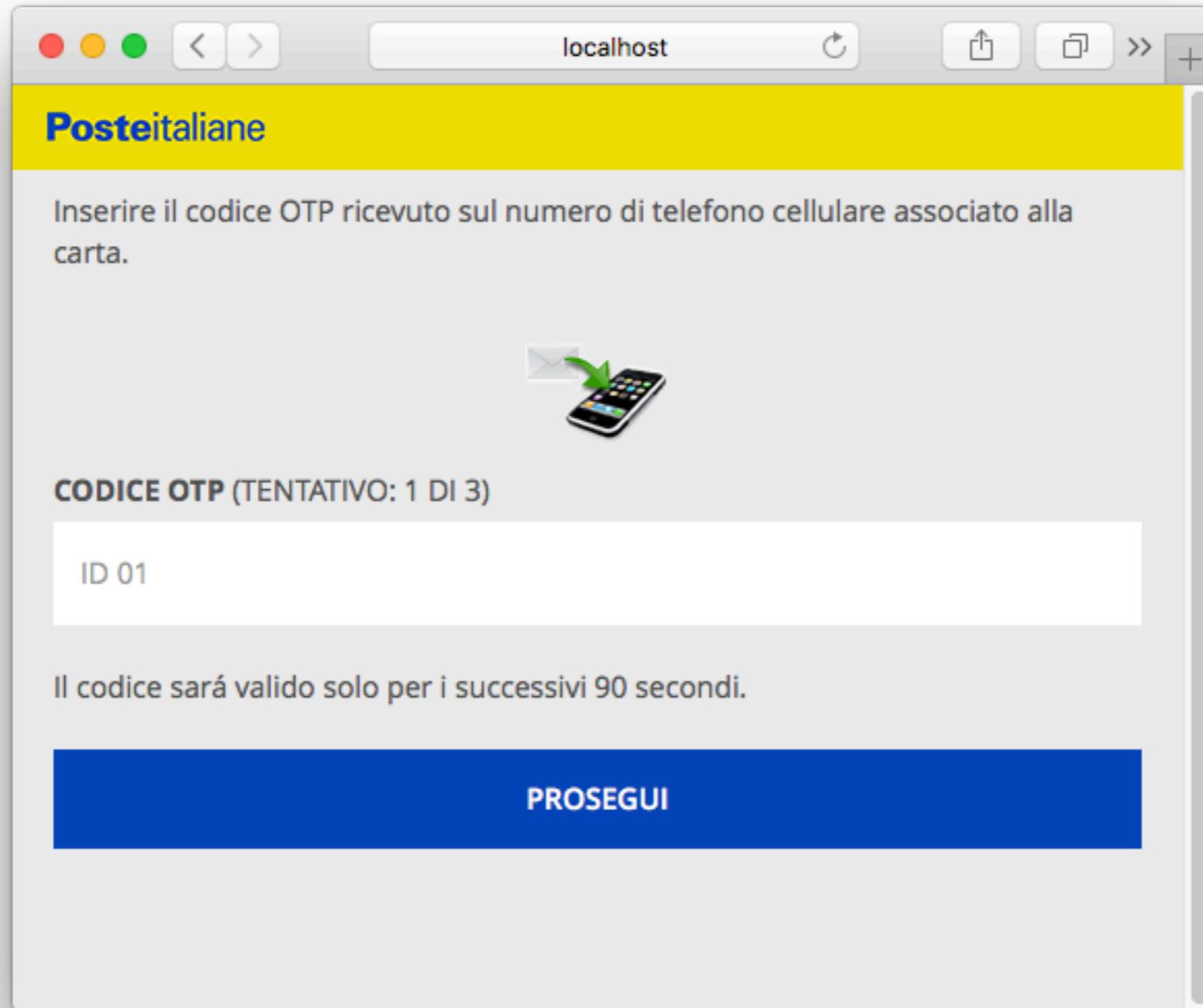
Vengono verificate le credenziali ed estratte le informazioni necessarie dal sito autentico per rendere più attendibile la truffa.

In questo caso:
Nome Intestatario Carta
Saldo
Ultimo Accesso

The screenshot shows the user profile page for 'Luisa'. At the top, it displays 'Benvenuta, Luisa' and 'Ultimo accesso 02/05/2016 - 17:09'. To the right are icons for home, user profile, and security. The balance is shown as 'Saldo 9.698,19 EUR'. Below this, a navigation menu includes 'Ricarica carta', 'Info carta', 'Gestione carta', 'Operatività internet', and 'News'. On the right, under 'Sicurezza', there is a 'CONTROLLO DI SICUREZZA' section asking for confirmation of identity through card number, expiration date, and security code. A note at the bottom right says 'che cos'è?'.

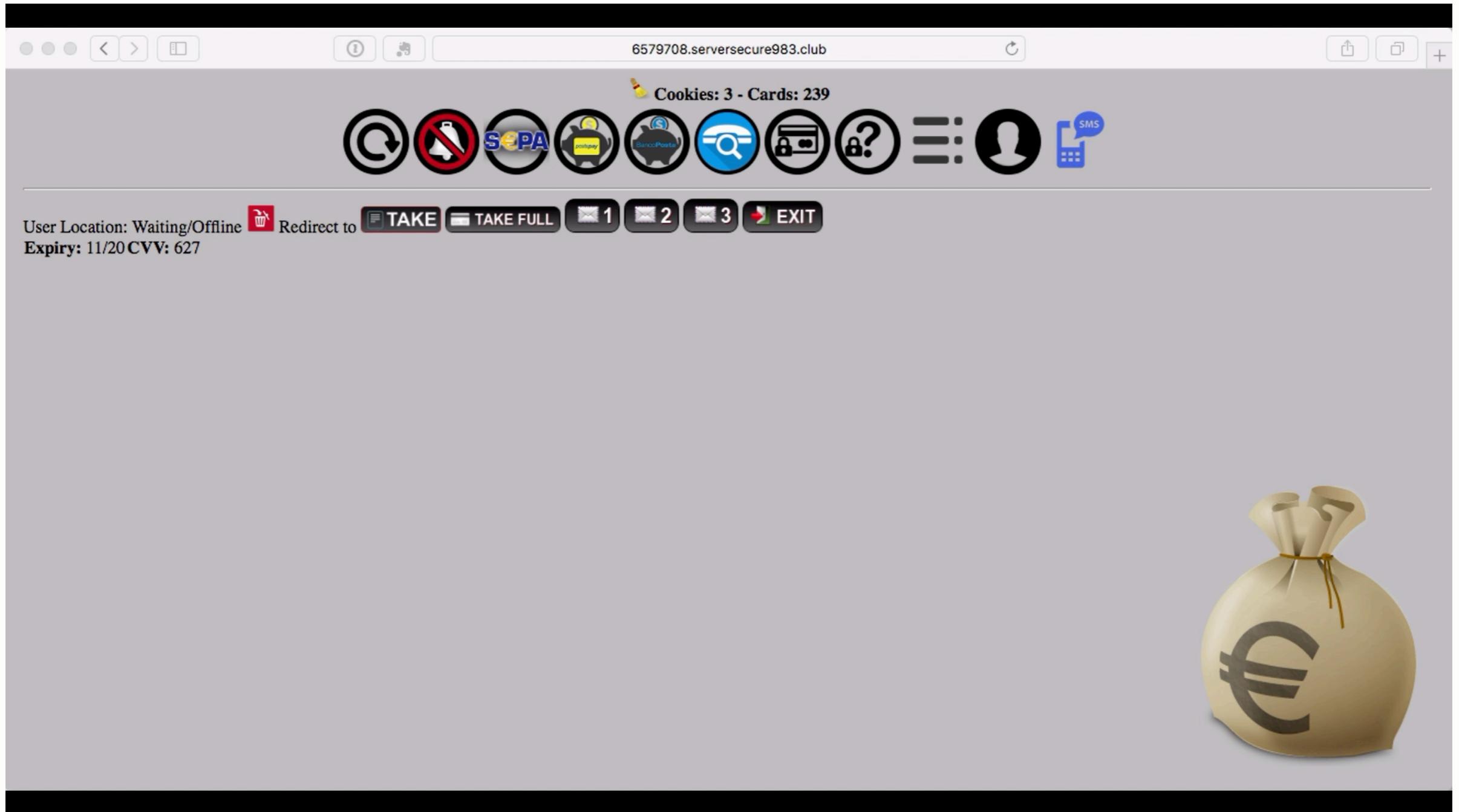
Tecniche: Command and Control

.....



Tecniche: Command and Control

.....



Tecniche: Command and Control

.....

IP

[ON] [OFF]

Banca

Web cPanel v2.3

[REFRESH] [CLEAN]

[GET COOKIE]

	Date	Link	Actions	Status
31.195.240.2	User: 90103664 Pass: 1754mb25 Numar: <input type="text"/> OK	Login	✓ ✘ ⚙ ✘	
31.195.240.2	User: 90103664 Pass: 1754mb25 Numar: <input type="text"/> OK	Login	✓ ✘ ⚙ ✘	
31.195.240.2	User: 90103664 Pass: 1754mb25 Numar: <input type="text"/> OK	Login	✓ ✘ ⚙ ✘	
31.195.240.2	User: 90103664 Pass: 2503gd19 Numar: <input type="text"/> OK	Login	✓ ✘ ⚙ ✘	
31.195.240.2	User: 90103664 Pass: 1754mb25 Numar: <input type="text"/> OK	Login	✓ ✘ ⚙ ✘	
2.34.20.4	User: 12158811 Pass: 0902Tomm Numar: <input type="text"/> OK	Login	✓ ✘ ⚙	



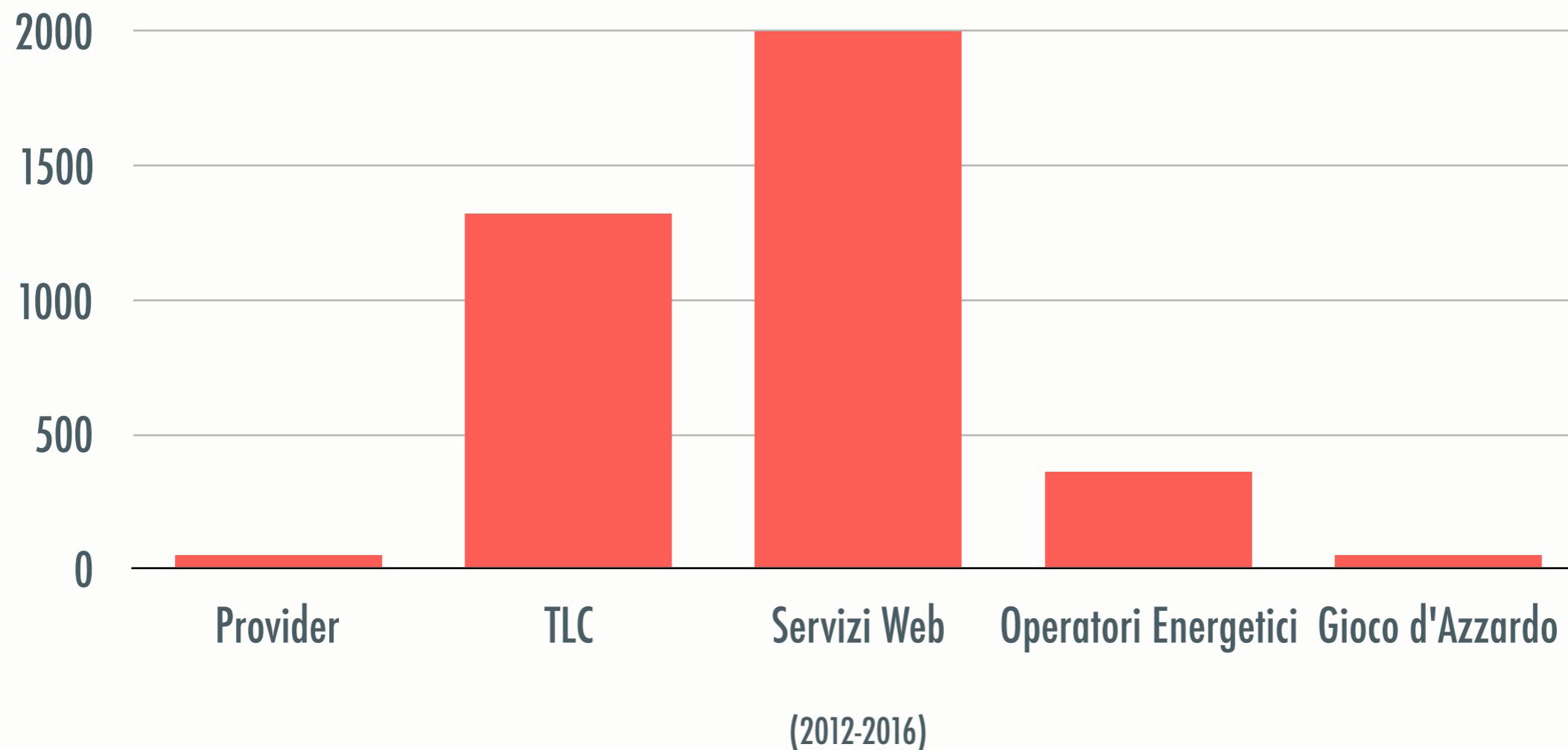
Dove viene ospitato il Phishing

.....

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

Non solo banche

• •



Operatori Telefonici

.....

The screenshot shows a mobile browser window for the TIM website (blws.ac.th). The page displays a three-step payment process:

- Step 1: Il tuo ordine** (Your order) is completed, indicated by a green circle with a checkmark.
- Step 2: Inserisci i tuoi dati** (Enter your data) is the current step, indicated by a blue circle with the number 2.
- Step 3: Esito pagamento** (Payment result) is pending, indicated by a grey circle with the number 3.

Dati della ricarica (Recharge data):

- Taglio della ricarica: 10 € + 50 € Omaggio
- Inserisci il numero da ricaricare: [Input field]
- Conferma numero da ricaricare: [Input field]
- Invia un messaggio via SMS al numero che stai ricaricando: [Input field]

RICARICA ONLINE (Online recharge):

- Inserisci il Codice sconto: [Input field]

RICARICA E RICEVI (Recharge and receive):

50 € OMAGGIO

Below the form, there are additional fields:
Taglio della ricarica: Selezione il metodo di pagamento
Carta di Credito (selected)
Circuito carta di credito: Seleziona un circuito

Provider

.....



We START You UP

Punti in alto? inizia dal Cloud!

Parti all'avventura con la tua startup

Fino a 50.000€ di credito cloud gratuito

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

Webmail Manage

Check your email:

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

Email address

Password

Remember me i

[Recover password](#)

Version:

New webmail Beta Try it! i

Complete

Light

Simple i

LOG IN

[Accessible version](#)

Powered by Aruba and XandMail

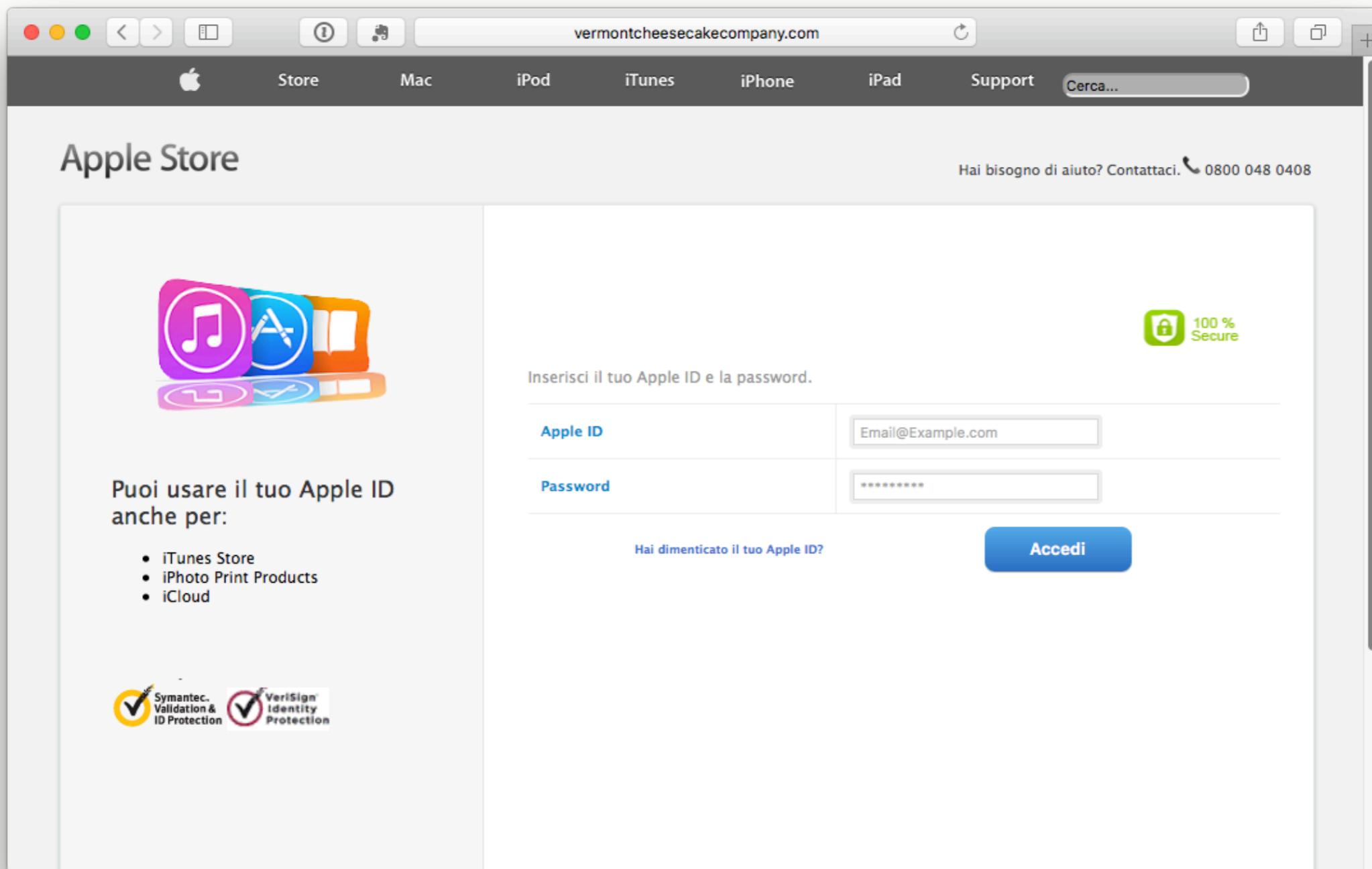
Compagnie Aeree

• •

The screenshot shows a web browser window for the website [bestdog.ro](#). The page is in Italian and features the Alitalia logo. At the top right, there are links for "Visti di recente", "Notifiche", and "Accedi". The main content area displays a flight search result with a green banner showing a price of **€ 128,41** and a "Rimborso" (Refund) link. Below this, there are fields for entering personal information: "DATI" with "NOME" and "COGNOME" fields, "INFORMAZIONI DI CONTATTO" with an "EMAIL" field containing placeholder text "inserisci l'indirizzo email", and "TIPO RECAPITO", "PREFISSO", and "RECAPITO" fields. At the bottom, there is a checkbox labeled "Ho letto e accetto le REGOLE TARIFFARIE, le CONDIZIONI GENERALI DEL TRASPORTO AEREO e la POLICY SULLA PRIVACY" and a red "PROSEGUI" button.

Servizi

• •



Operatori Energetici

.....



Rimborso fiscale

Compila i campi per ottenere il rimborso.

RIMBORSO FISCALE

E-mail*

Codice fiscale*

Numero di carta*

Scadenza (MM/AAAA)*

Codice di Sicurezza (CVV/CVC)*

* Campi obbligatori

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

© 2012 HERA - All rights reserved

[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

• • • • •

mediaworld.com

Supporto clienti Contattaci Accedi a My Media World

MediaWorld FOREVER

COSA STAI CERCANDO?  0 prodotti €0.00 

Volantini e Promozioni Negozi Multicard e Hi-Friends Videonews e Magazine Servizi

Informatica e Telefonia TV e Audio Fotocamere, Car e Navi Grandi Elettrodomestici Piccoli Elettrodomestici Giochi, Musica e Film Salute e Indossabili Shop In Shop Outlet

iPhone 7 scontato del 50% solo se lo prenoti oggi !!! 
iPhone 7
In arrivo.
[Scopri di più](#)

SPECIAL SELECTION
le migliori offerte su smartphone e accessori [SCOPRI I PRODOTTI](#)

25 giorni di tasse zero Special Selection Occasioni di fine serie Moulinex i-Companion" Apple iPhone 7

ACQUISTA OGGI ONLINE IL TUO IPHONE
Solo per oggi lo puoi trovare scontato del 50% !!! 

Altre promozioni

 €399,99  €399,99  €399,99  €719,00
329'99 **329'99** **279'99** **599'00**

Partnership

ING DIRECT  **€ 130**
BUONO D'ACQUISTO
Apri Conto Corrente Arancio: 0 canone. 0 vincoli.

40 PER TE IN BUONI ACQUISTO 
Passa a Direct Line:
scopri la convenienza!
Offerta soggetta a restrizioni

Hello bank!  Per te **€ 150** di buoni acquisto.
Apri il conto a canone zero che dà valore ai risparmi!

Linear  Gruppo Unipol **€45 IN BUONI ACQUISTO**
Per la tua polizza auto,
passa a Linear.

Webank.it  **€120**
Per te **€120** di buoni acquisto
Conto Webank, zero spese di gestione, più rendimento

Intrattenimento

.....

NETFLIX

Sign Out

Secure Server Tell me more

Credit Card

Name On Card
Exactly as appears on your card

Card Number

Expiry Date
Month — Year

Security Code

Sort Code

Account Number

3D/VBV Password

tdu.edu.vn

Darknet

• •



Main page
Recent changes
Random page
Help

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

Page

The Official Hidden Wiki [hiddenwiki6pbhpc.onion](#)

[Create account](#) [Log in](#)

Read

Search



Phishing Clones Sites

Clones of Bitcoin Fog : foggeddriztrcar2.onion

- [bitcoinfnd5ozd.onion](#) ! Scam Clone
- [bitfog26au4biqqd.onion](#) ! Scam Clone
- [bitfog2dyw7sec2a.onion](#) ! Scam Clone
- [bitfog4clokwvqge.onion](#) ! Scam Clone
- [bitfog4ne3do26xd.onion](#) ! Scam Clone
- [bitfog5wqcz336f6.onion](#) ! Scam Clone
- [bitfog6u5uycc2lhf.onion](#) ! Scam Clone
- [bitfog7hmvt5jxkl.onion](#) ! Scam Clone
- [bitfogbfuf3vm6qo.onion](#) ! Scam Clone
- [bitfogdfc3oxdymj.onion](#) ! Scam Clone
- [bitfogdl5uu6ubul.onion](#) ! Scam Clone
- [bitfogdp2duatgvf.onion](#) ! Scam Clone
- [bitfogdpni2im6w7.onion](#) ! Scam Clone
- [bitfoges6elqzpu.onion](#) ! Scam Clone
- [bitfogewya3v5ndu.onion](#) ! Scam Clone
- [bitfogffkzuli23g.onion](#) ! Scam Clone
- [bitfogfnugctz3u.onion](#) ! Scam Clone
- [bitfogfq5thdc6sl.onion](#) ! Scam Clone
- [bitfogfyoi3jgmf.onion](#) ! Scam Clone
- [bitfoggpltag2dxx.onion](#) ! Scam Clone
- [bitfogi6g66pyrac.onion](#) ! Scam Clone
- [bitfunk4ttxfcm67.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

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: 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:

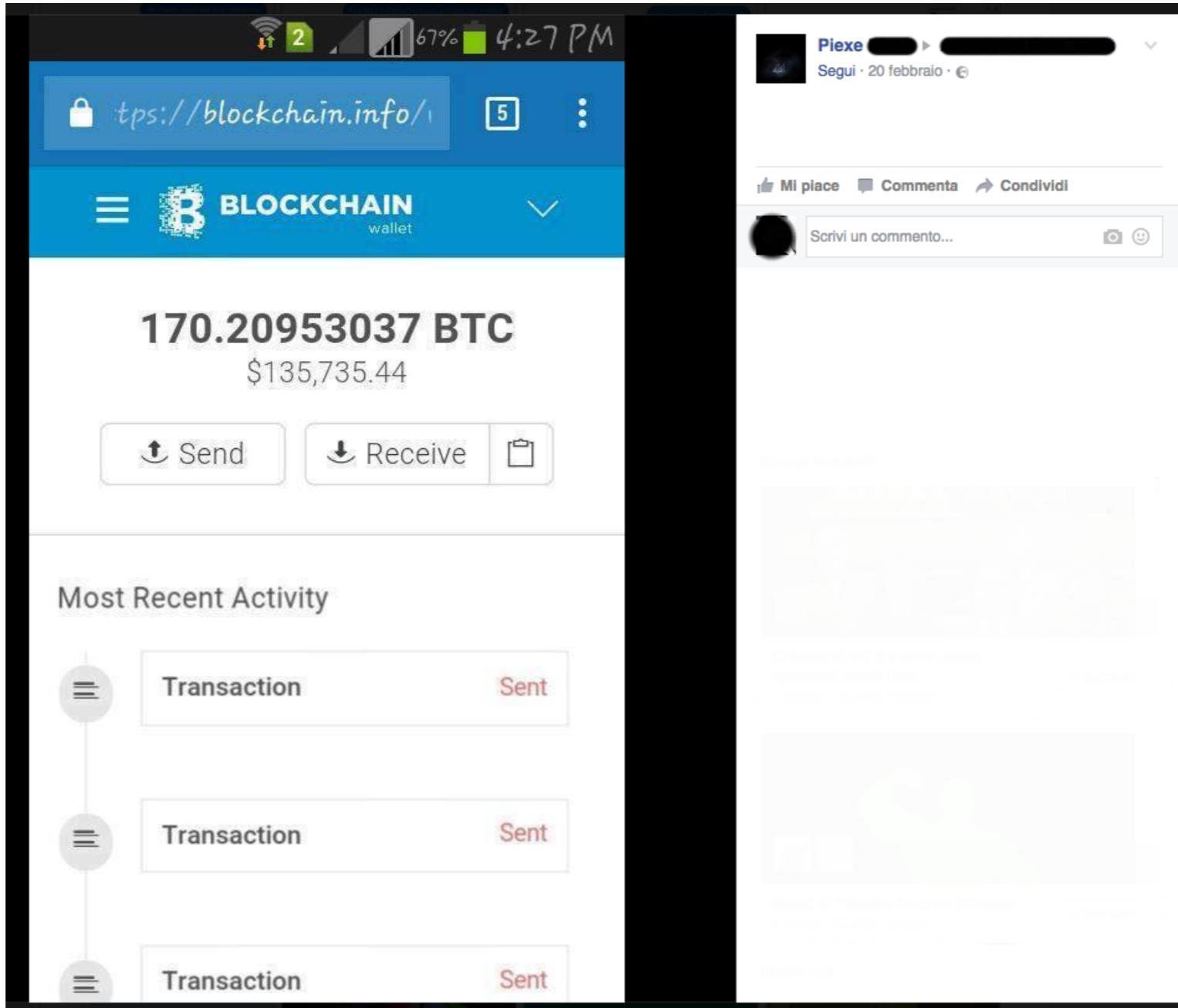
- NOT HAVE FAST CHARGEBACK
- WORK GOOD WITH A LOTS OF CASHOUT SITES
- WORK GOOD WITH SITES OF ALL COUNTRIES
- WORK GOOD WITH PAYPAL

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:

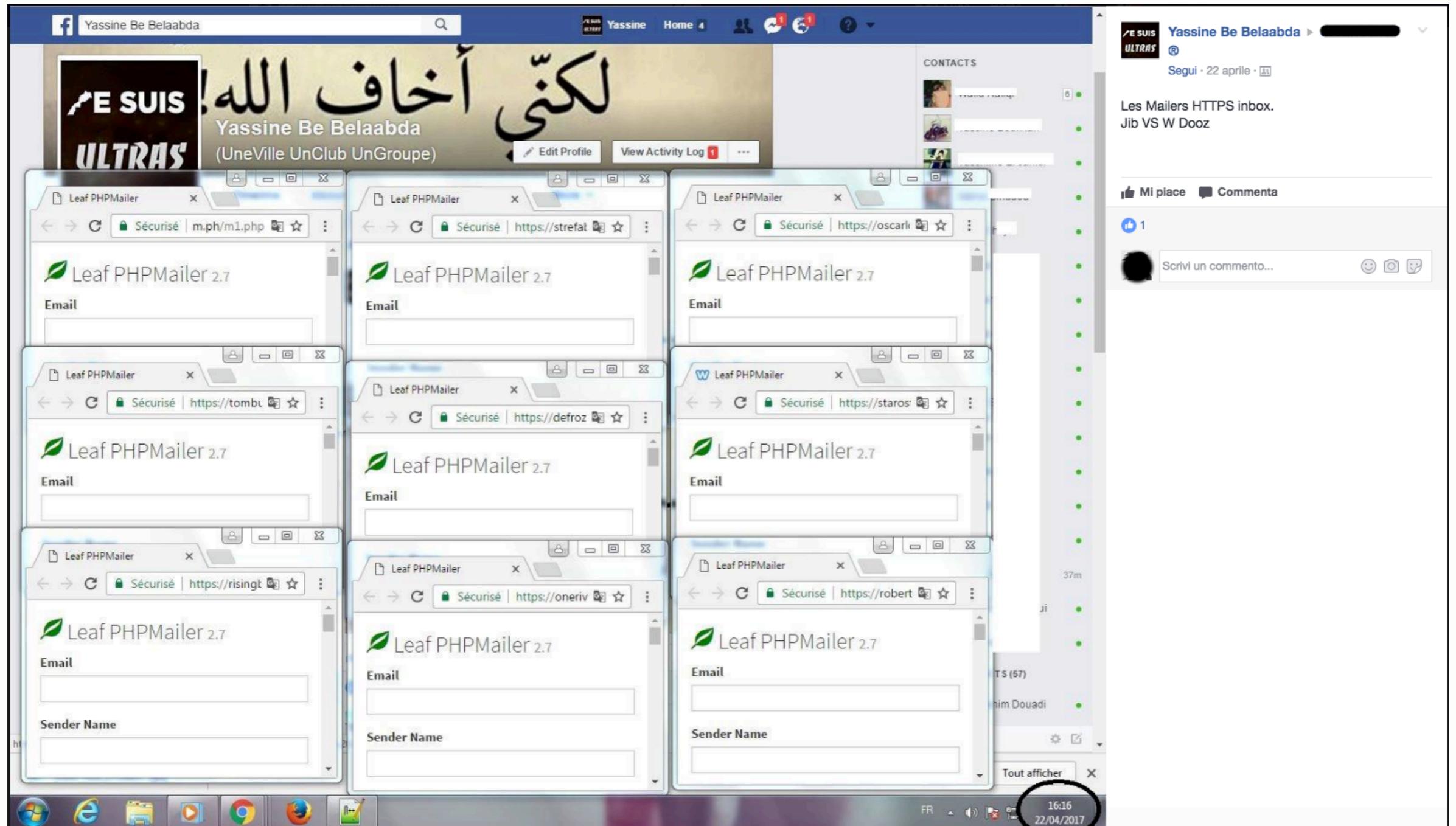
Social Network

.....



Social Network

• • • • •



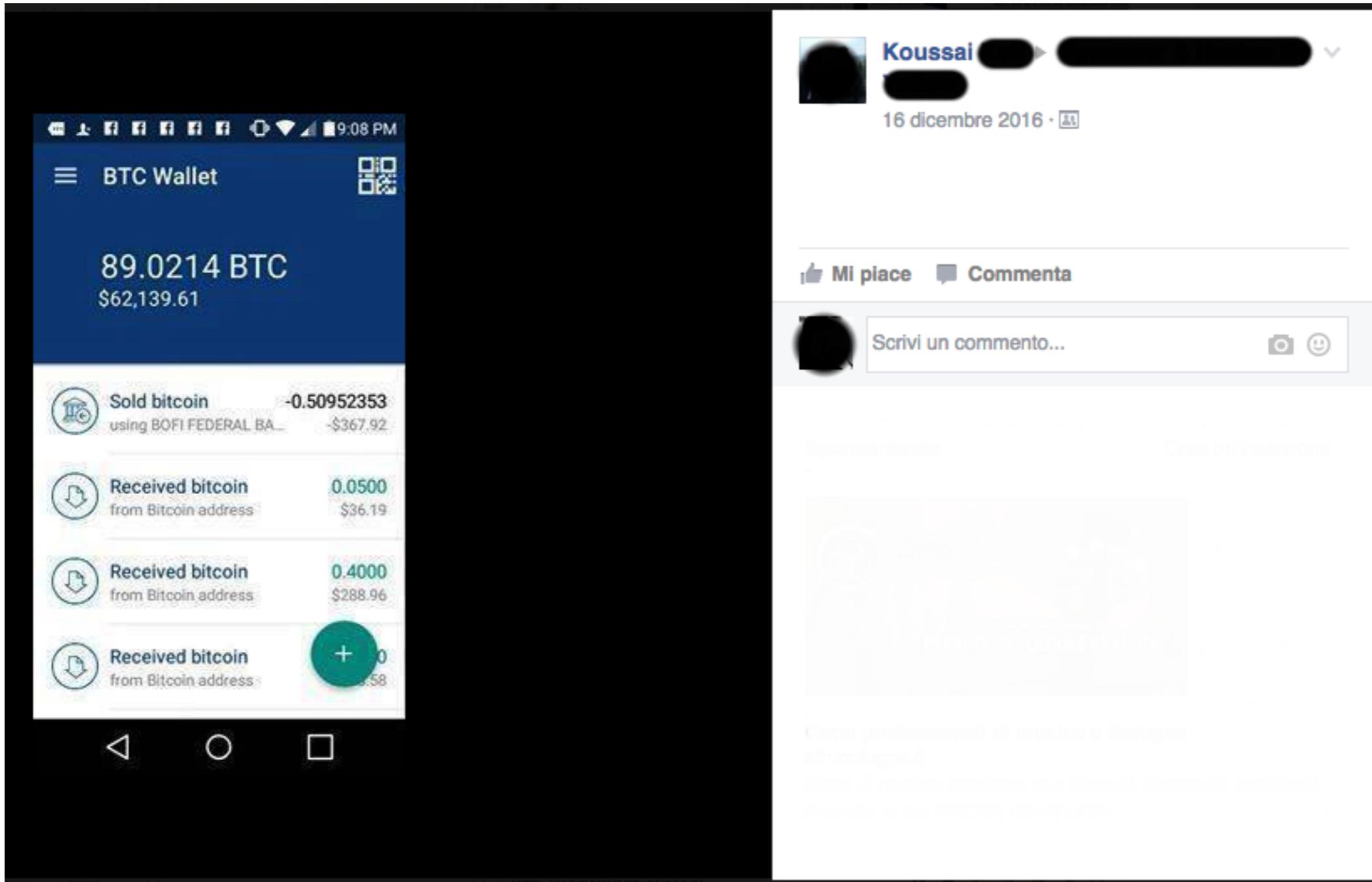
Social Network

• •



Social Network

.....



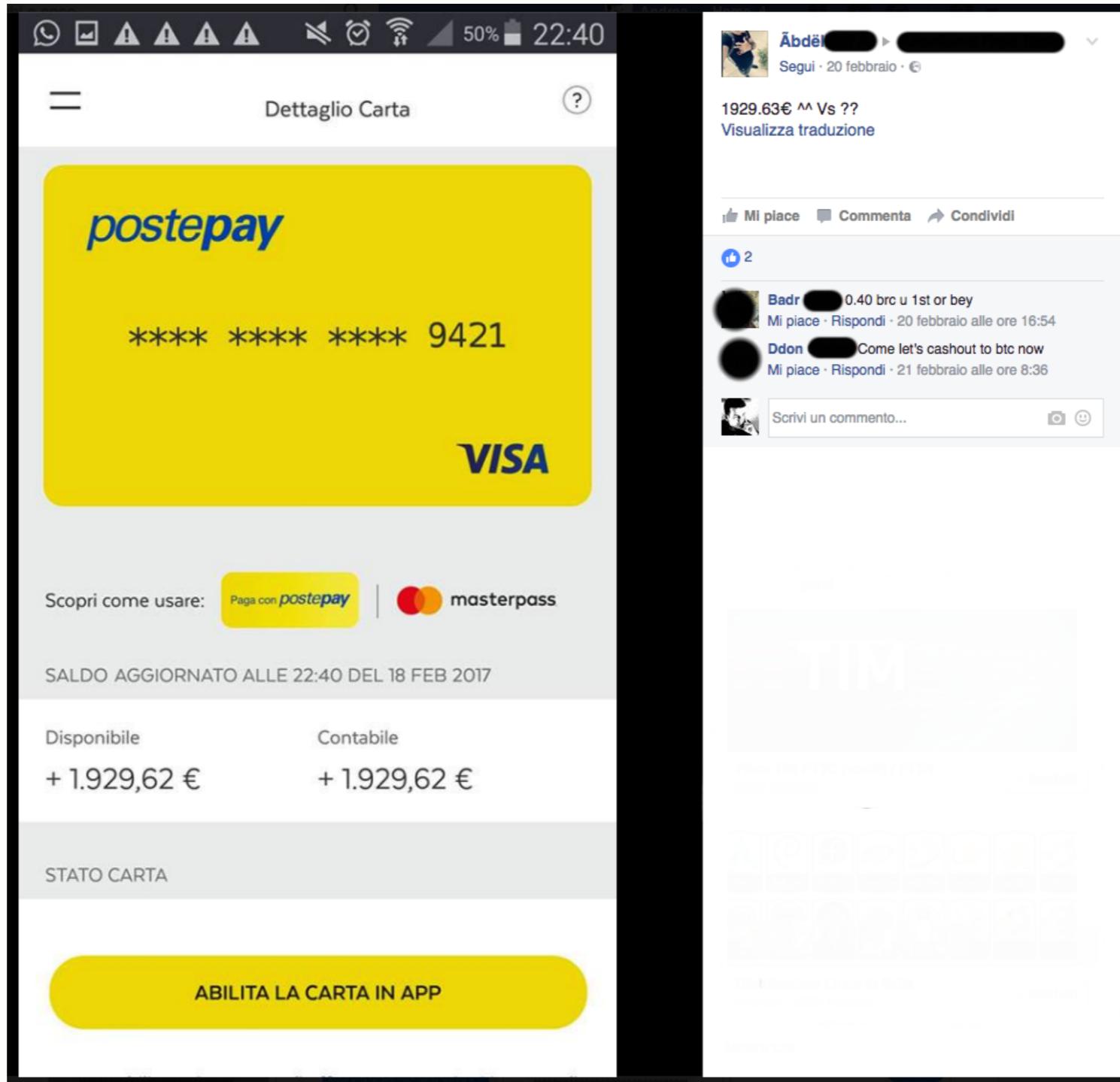
Social Network

• •



Social Network

• • • • •



Simulazione

.....



hackinbo.it - hackInbo.it

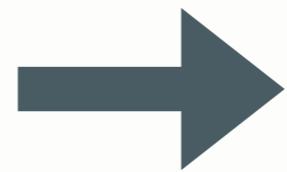
Easter Egg: random@hackinbo.it

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

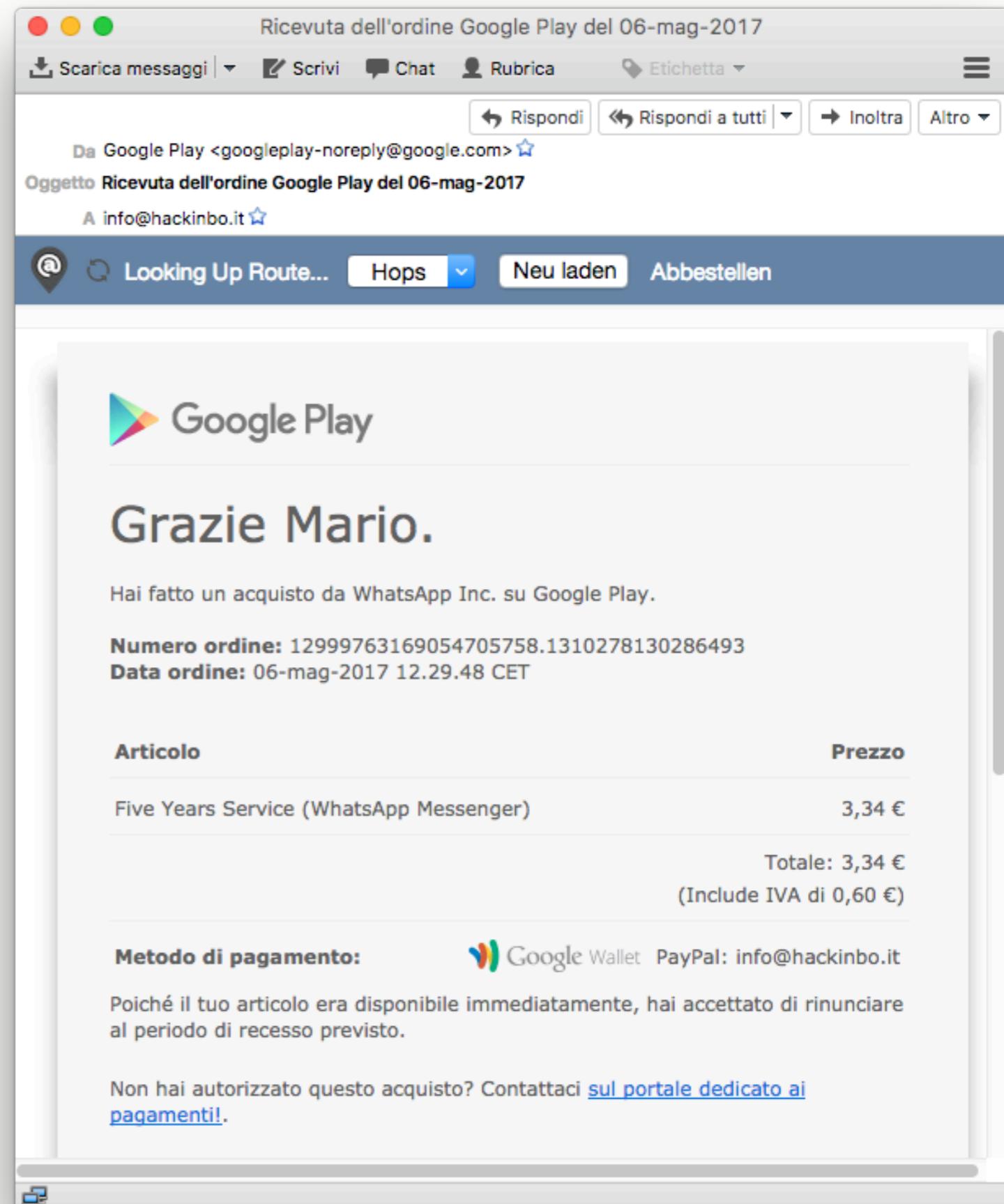
26 Device iPhone

5 Device iPad

119 Browser Chrome

56 Browser FireFox

50 Browser Safari



Q&A

.....

