WordCamp Torrelodones 2023

Aspire... Espire...

Yoga 

para recuperar

tu sitio y tu reputación

después de un hackeo.

Néstor Angulo de Ugarte

#WCTorre

Néstor Angulo de Ugarte

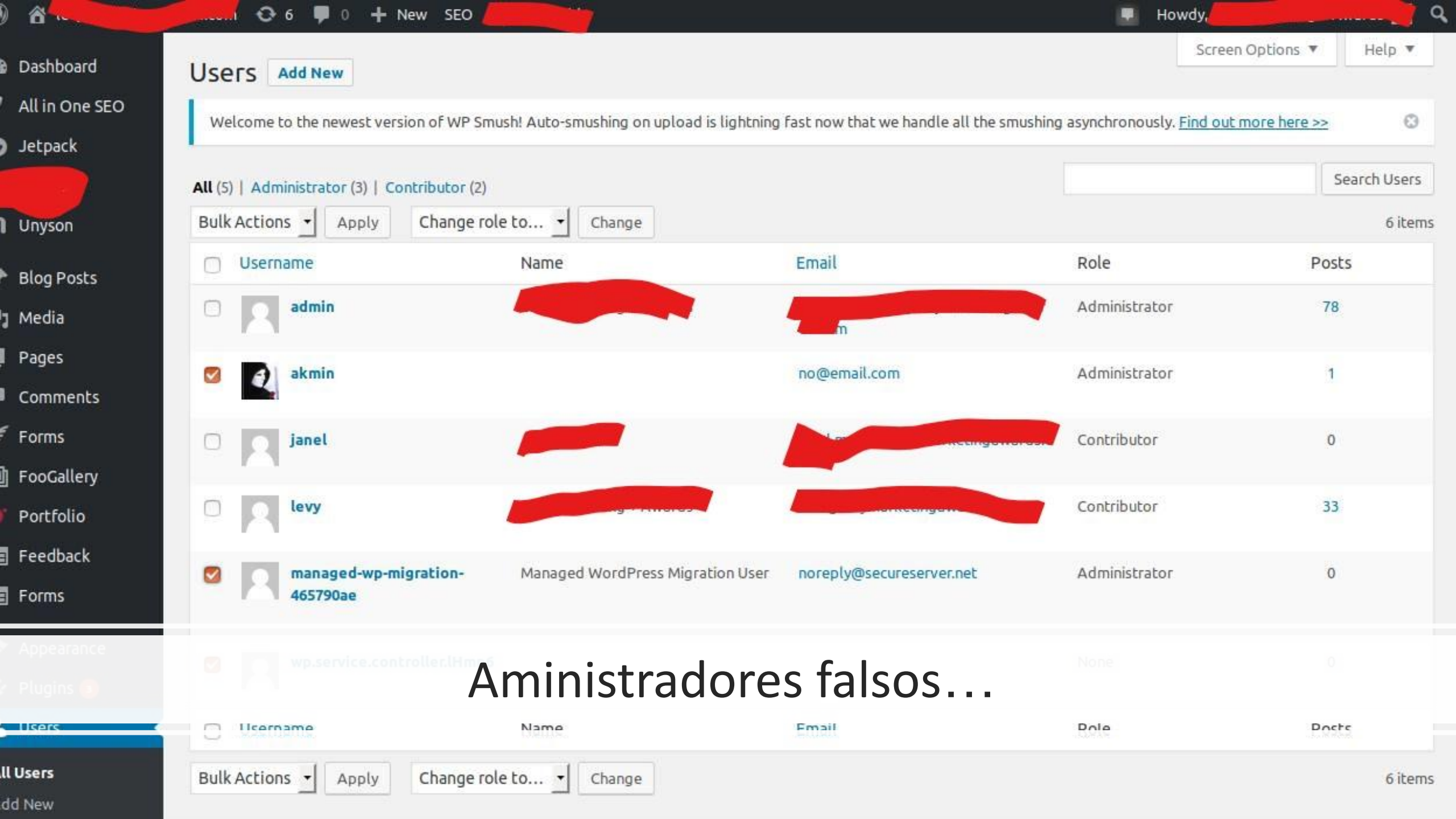
CISSP, Ingeniero Informático, emprendedor y Tecnólogo Humanista

< 2015 -> 4 empresas
2015 -> Sucuri.net
2017 -> GoDaddy WebSecurity

2023 -> Nuevo comienzo:
nestorangulo.pro

Twitter: **@pharar**

WordCamp Torrelodones 2023



Aministradores falsos…

Current Revision by
3 months ago (4 Mar @ 09:03)

Restore This Revision

Title

```
Hacked By BALA SNIPER
```

```
Hacked By GeNErAL
```

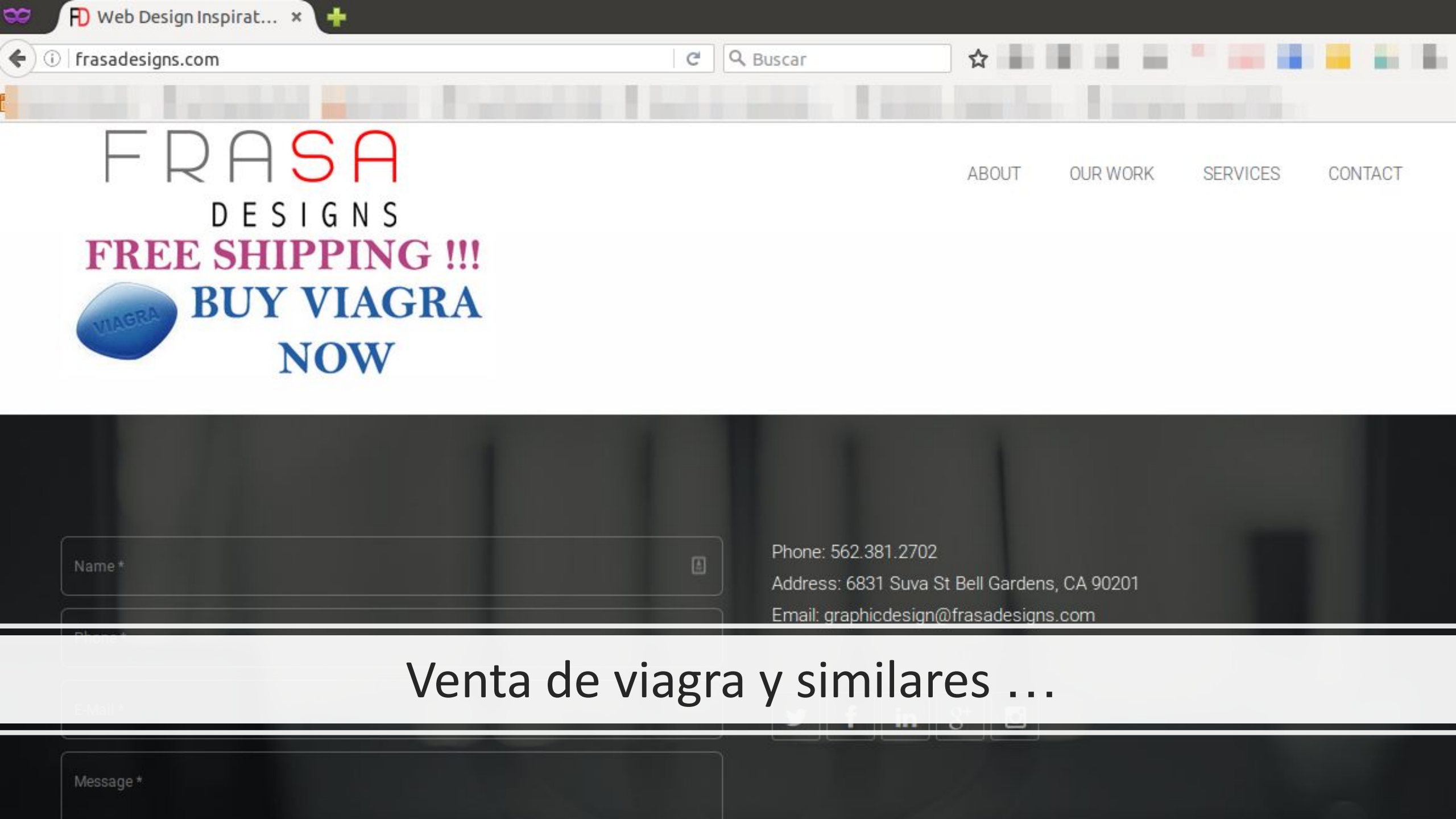
Content

```
<p>Hacked By BALA SNIPER<br />
 Kurdish Hacker Here<br />
 If you want Fix Problem Website &amp;#8230; !<br />
 Contact Me via Gmail : darinsniper007@ gmail.com<br />
 Contact Me Via Facebook : https://www.facebook.com
/balasniper007 </p>
```

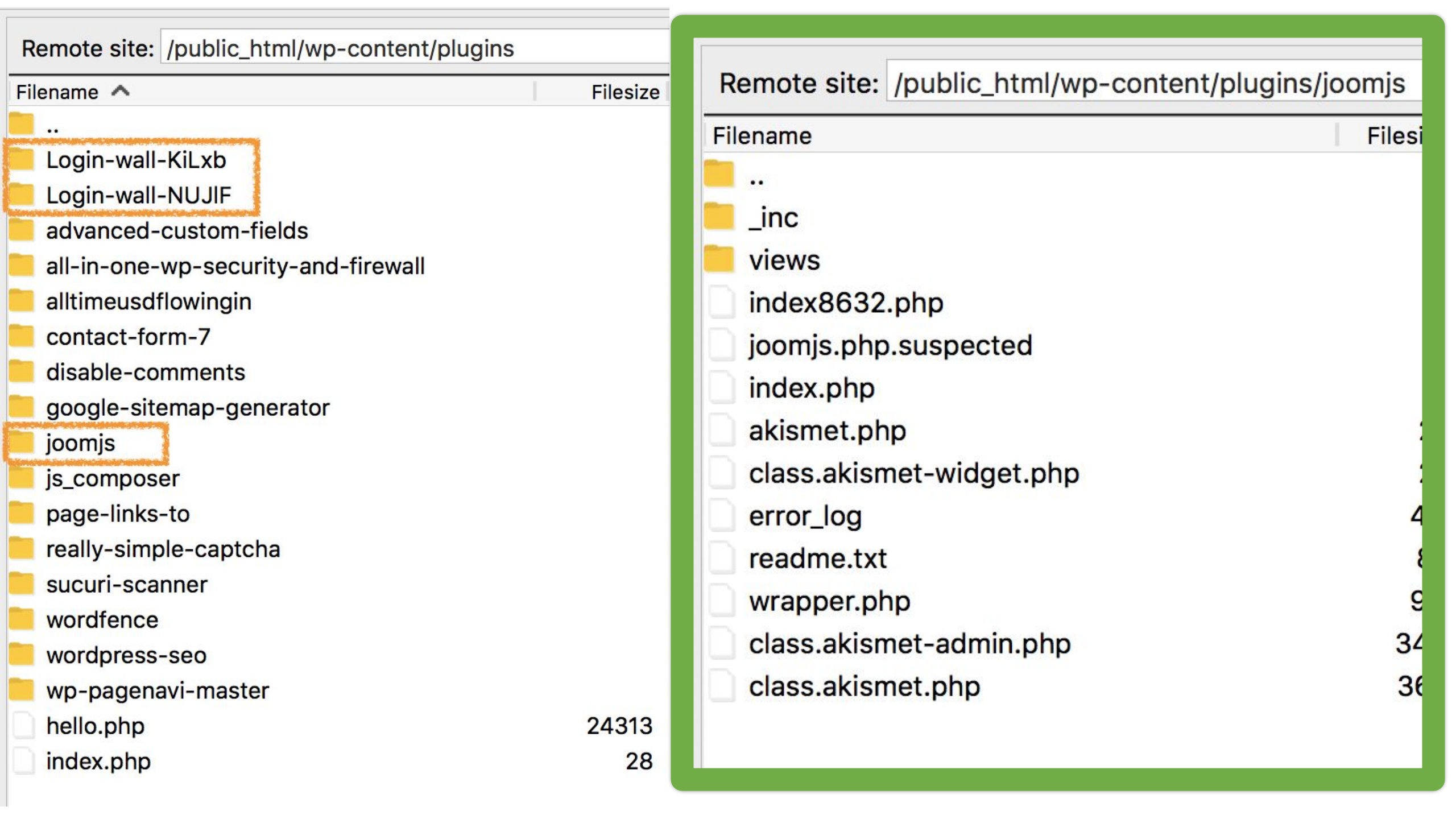
```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2> </font></p><img
border='0' src='http://www.officialpsds.com/images/thumbs
/Baby-Devil-Toon-psd9848.png'><br><br><br><b>Greetz :
Kuroi'SH, RxR, ~ </b><br><br></FOOTER><b><code>
<h1>\!/Just for Fun ~Hacked By GeNErAL\!/</code>
</b></b><p align='center'><font color='red' /><font
size='5' color='#FF0000'>Hacked By
GeNErAL! !</font></font></p>
```

Tus post cambian…

Aparece una portada ”ligeramente” diferente…



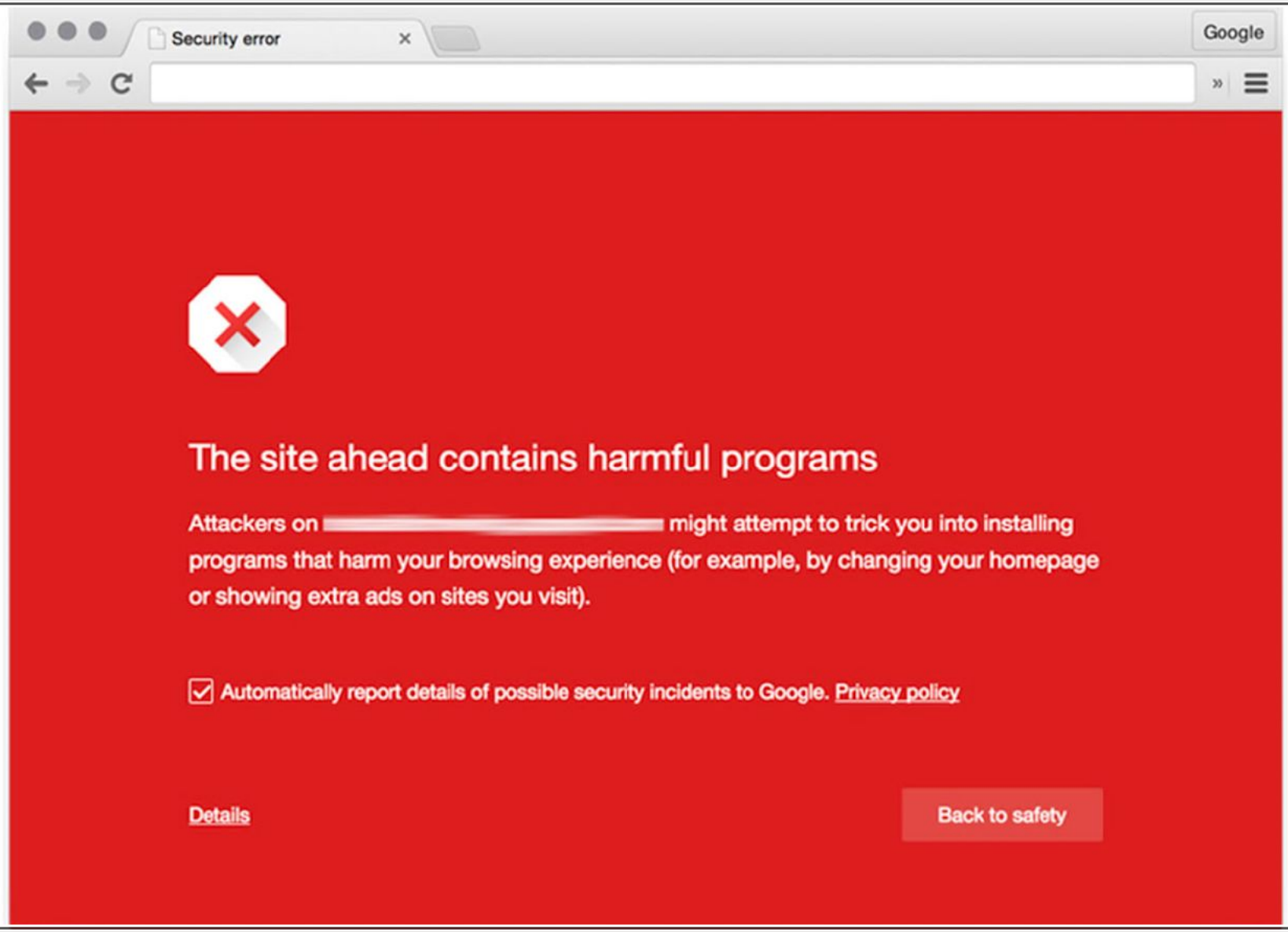
Venta de viagra y similares …

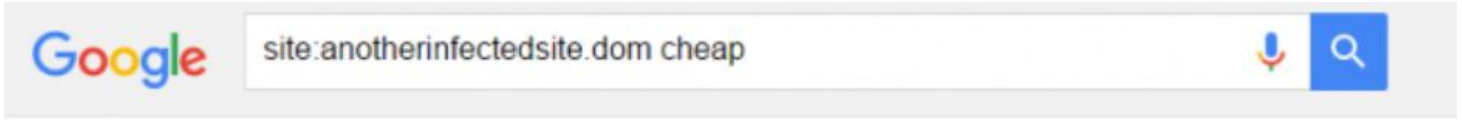

Remote site: /public_html/wp-content/plugins
Filename
Filesize
..
Login-wall-KiLxb
Login-wall-NUJlF
advanced-custom-fields
all-in-one-wp-security-and-firewall
alltimeusdflowingin
contact-form-7
disable-comments
google-sitemap-generator
joomjs
js_composer
page-links-to
really-simple-captcha
sucuri-scanner
wordfence
wordpress-seo
wp-pagenavi-master
hello.php
24313
index.php
28
Remote site: /public_html/wp-content/plugins/joomjs
Filename
Filesi
..
_inc
views
index8632.php
joomjs.php.suspected
index.php
akismet.php
class.akismet-widget.php
error_log
readme.txt
wrapper.php
class.akismet-admin.php
class.akismet.php

Account Suspended

This Account has been suspended.

Contact your hosting provider for more information.


Security error
Google
The site ahead contains harmful programs
Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).
Automatically report details of possible security incidents to Google. Privacy policy
Details
Back to safety

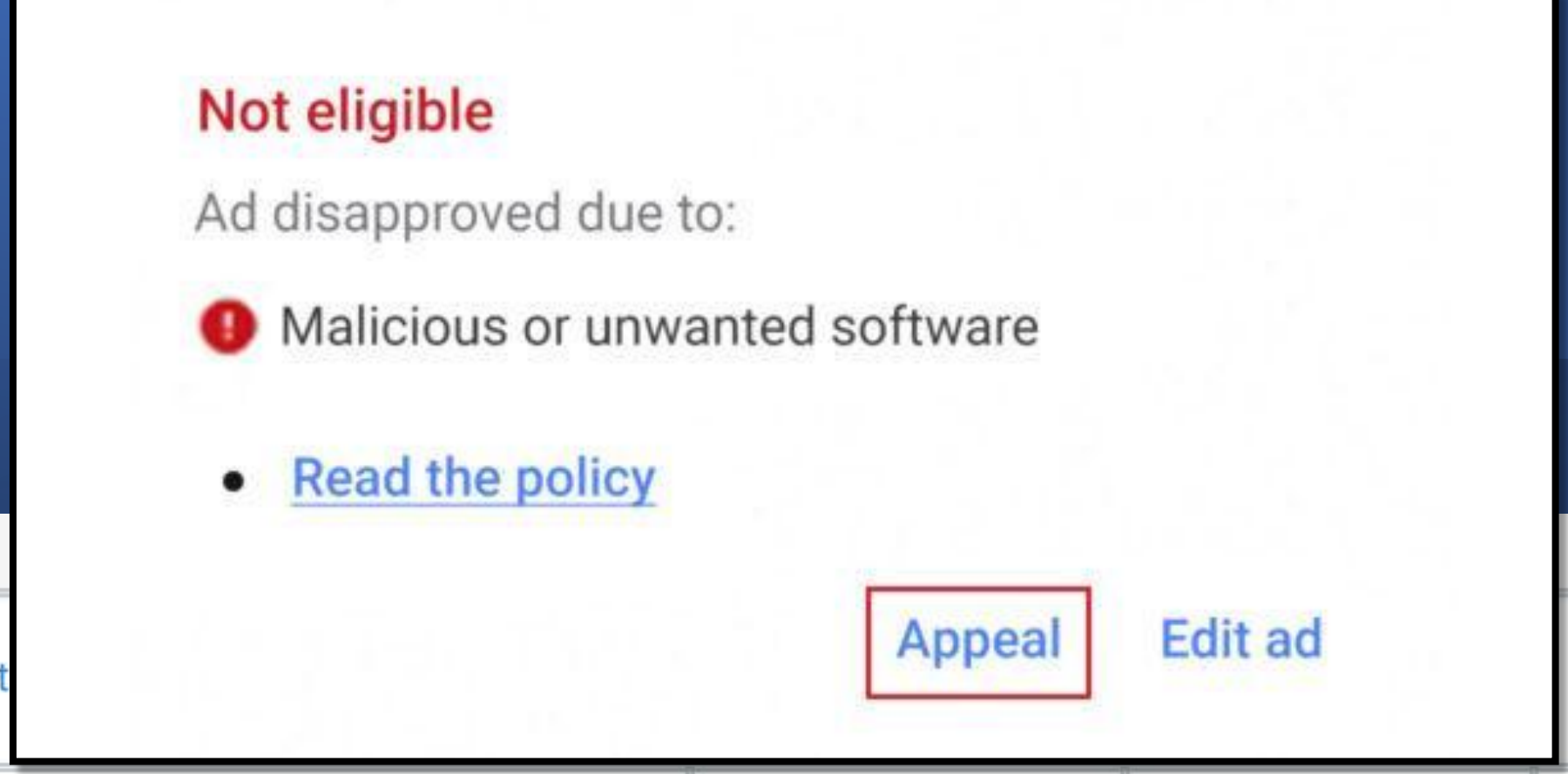


About 91,300 results (0.31 seconds)

Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...
anotherinfectedsite.dom/page/IvUxxxp1D
cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online now for great prices.Boys' toddler nike air max 90 premium running shoes.

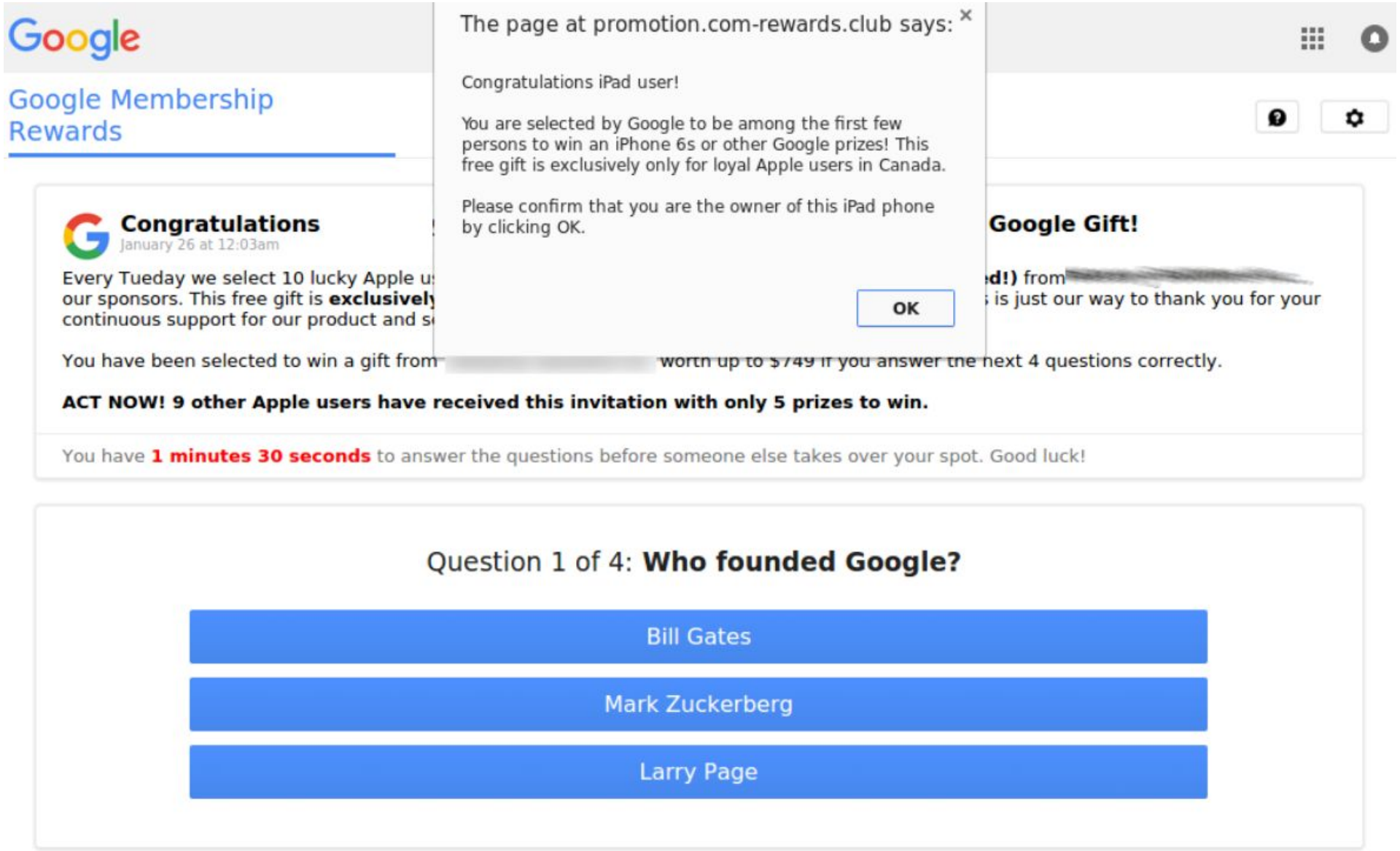
Air Yeezy Shoes Cheap Real Air Yeezy Shoes - Natural ...
anotherinfectedsite.dom/page/IpNxxxxx58vuK
Results great but cheap air yeezy shoe,cheap shoes,men's casual shoes,women's casual shoes,men's flats,as well as cheap and more online get.Size 6 nike air ...

Cheap Jordan Sneakers Wholesale Cheap Jordan Website ...
anotherinfectedsite.dom/page/Iv1CxxxxxIQVH
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...



Ad stat

Ad	Campaign	Ad group	Status
Your Website Ad | Advertising for Revenue example.com Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna.	Example Campaign	Example Ad Group	Disapproved Malicious or unwanted software


Google
Google Membership Rewards
The page at promotion.com-rewards.club says:
Congratulations iPad user!
You are selected by Google to be among the first few persons to win an iPhone 6s or other Google prizes! This free gift is exclusively only for loyal Apple users in Canada.
Please confirm that you are the owner of this iPad phone by clicking OK.
OK
Congratulations
January 26 at 12:03am
Google Gift!
Every Tueday we select 10 lucky Apple u
our sponsors. This free gift is exclusively
continuous support for our product and s
d!) from
is just our way to thank you for your
You have been selected to win a gift from
worth up to $749 if you answer the next 4 questions correctly.
ACT NOW! 9 other Apple users have received this invitation with only 5 prizes to win.
You have 1 minutes 30 seconds to answer the questions before someone else takes over your spot. Good luck!
Question 1 of 4: Who founded Google?
Bill Gates
Mark Zuckerberg
Larry Page

https://newsfile.club/?p=mezdezjtmi5gi3bpgu2de&sub1=fehgot#

Paused

Apps

DDecode - PHP D...

managedssl.int.go...

AutoDash

Blacklist Review T...

Sucuri Decoder

MSSL Invalid Sale...

newsfile.club wants to

Show notifications

Block

Allow

Haga clic en "Permitir" para confirmar que no es un robot

CONCLUSIÓN

- E-commerce con uso normal:
  - **Beneficios**: 50.000€ - 100.000€
- Hackeado
  - **Pérdidas**: - (270.000€ - 300.000€)

- **Coste de medidas de seguridad** -> 500€ - 1.000€


BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

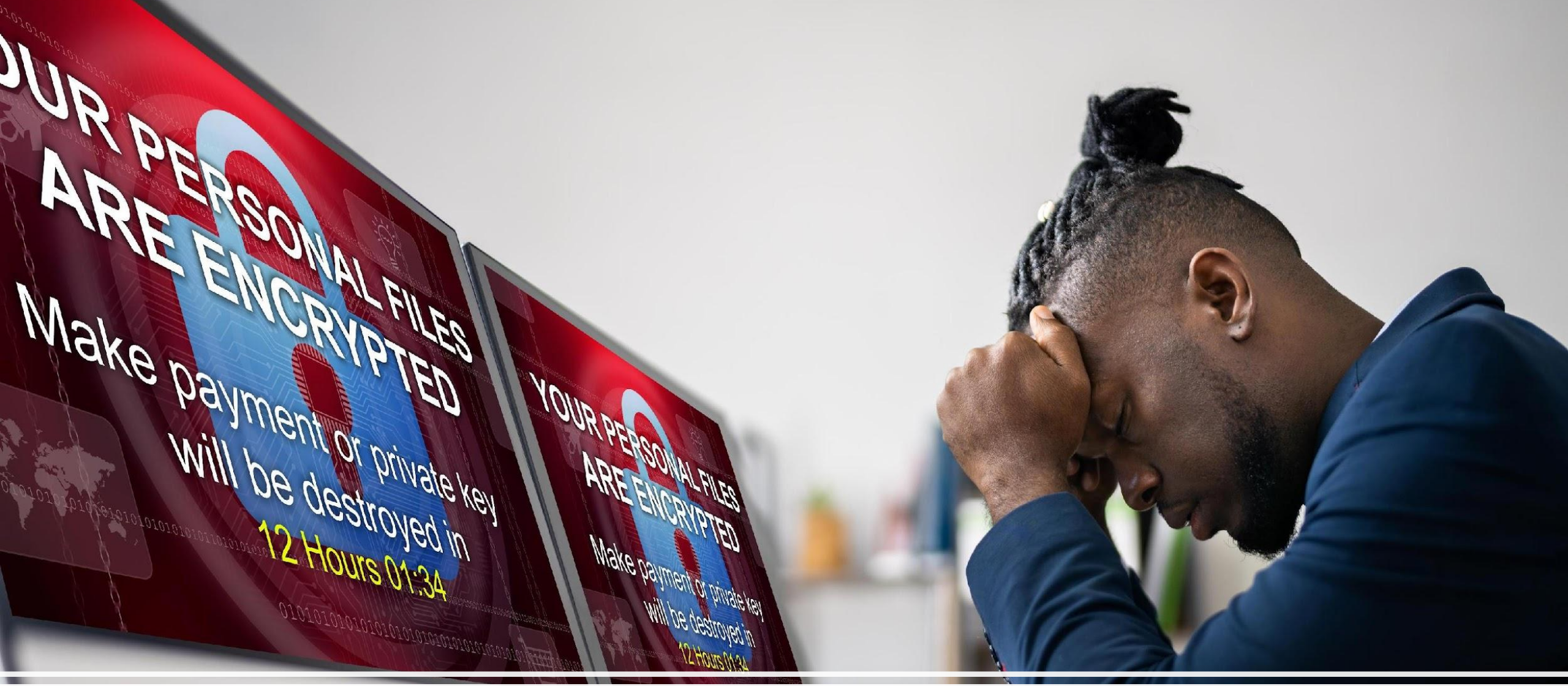
La Policía en tu casa....

HackedÃ,Â ByÃ,Â Jak

kanã,â beraniã,â matiã,â |ã,â indonesianã

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacl
Jiwa Kegelapan Team

OHMMMMMM

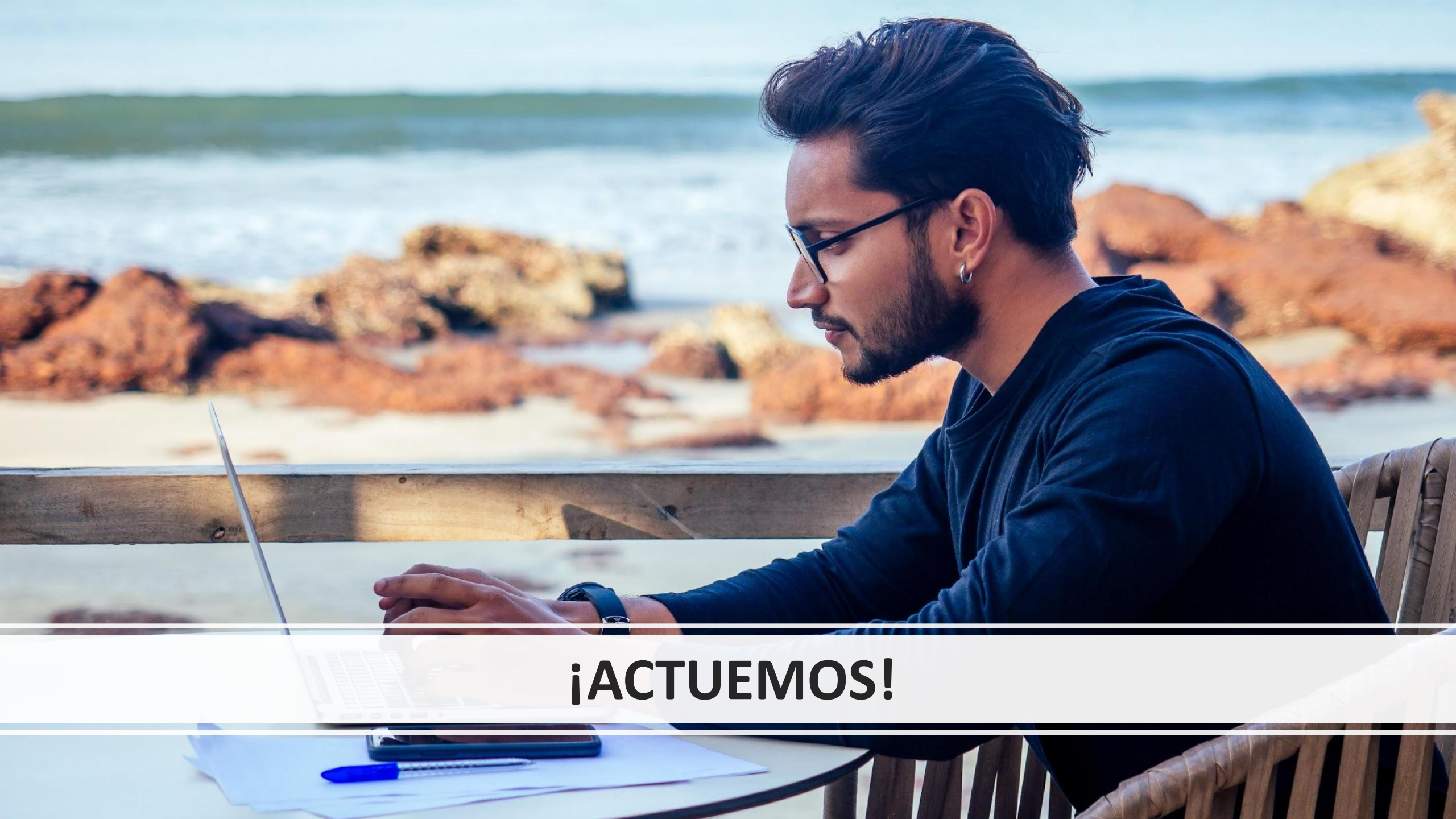

YOUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34

Si, lo sé …

¡GRITEMOS!

Es aceptable sentirse hecho polvo…

Pero después de todo esto …

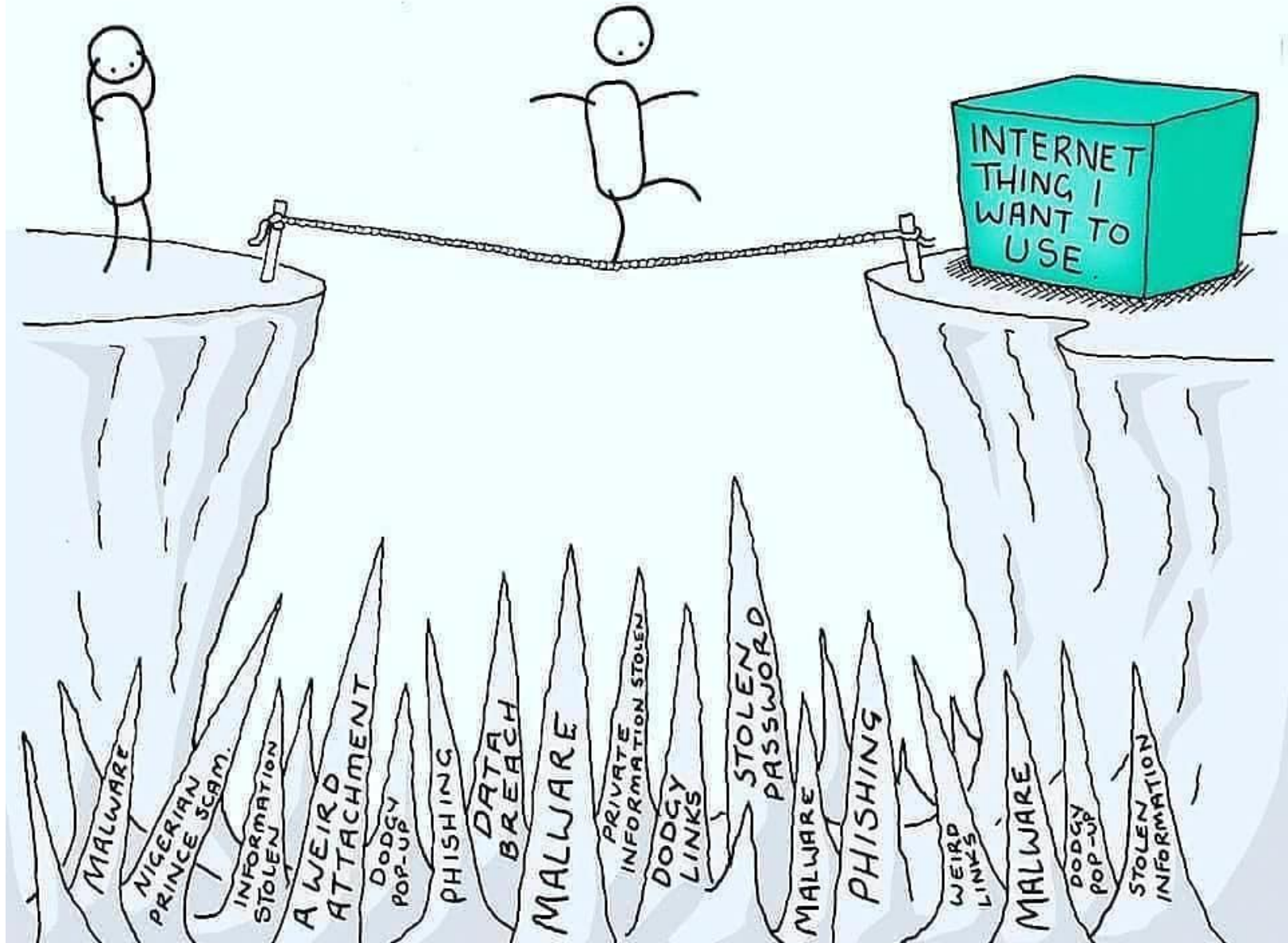


¡ACTUEMOS!

Primero… **Conceptos**


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

DEALING WITH CYBER STRESS




PHISHING
BOTNET
SPAM
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Hackers vs **Ciberterrorista**

Hacker

- **Persona curiosa** que disfruta yendo más allá de los límites y convenciones.

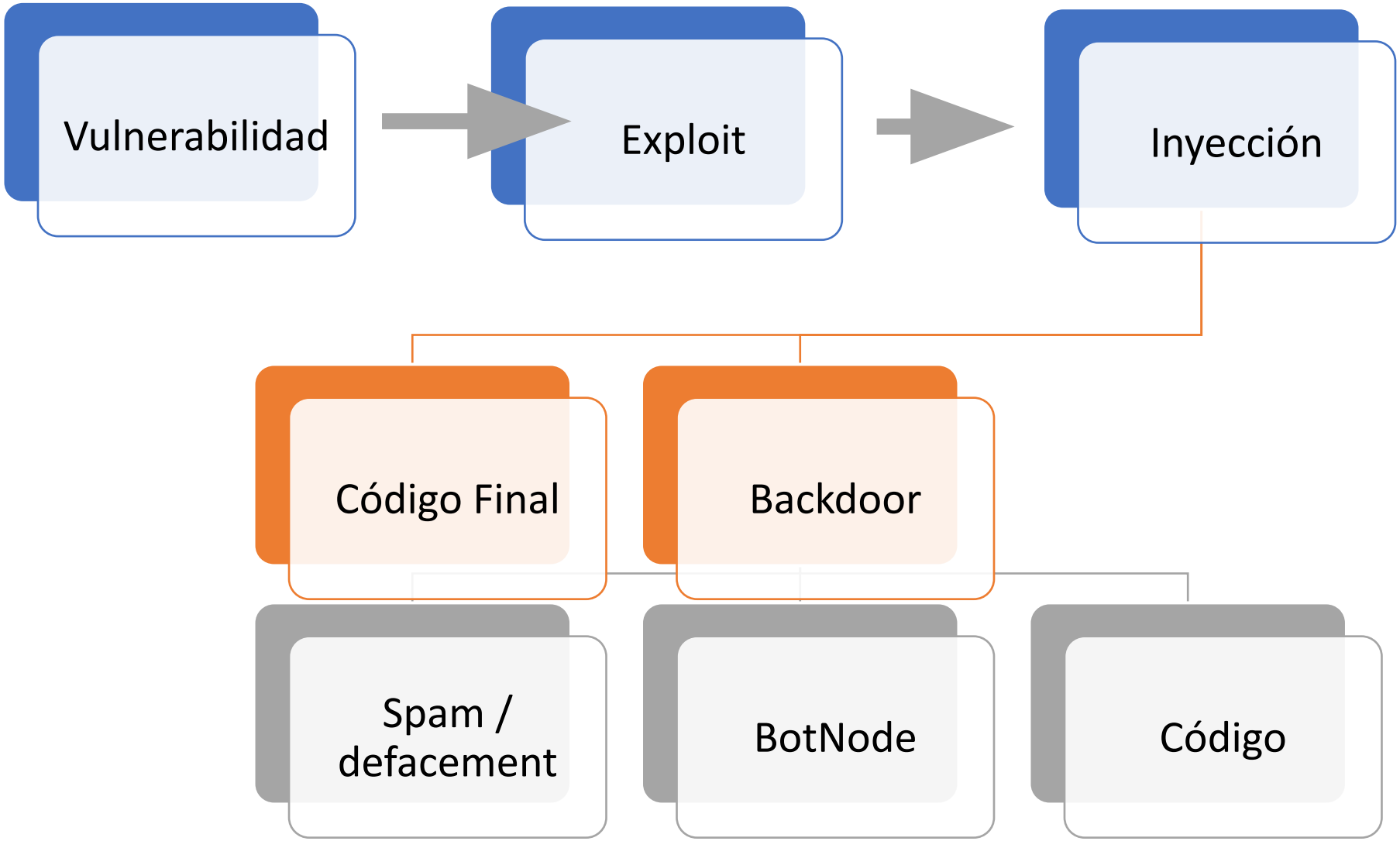
Ciberterrorista

- **Hacker informático**, cuyo objetivo es enriquecerse.
- **El malo.**

Seguridad: **Modelo de capas simplificado**

Capa	Protección

Cómo se **infecta** un sitio **WordPress**:



Hechos

Un hackeo **casi nunca está orientado** a un cliente

(98% of cases)

Casi siempre se debe a **mal mantenimiento** o **mal control**.

Un certificado **SSL** no es un **escudo anti- hacking**

Los parches de seguridad aparecen después de identificar los exploits

Errare Humanum Est
(El Ser Humano falla)

La **seguridad no es 100% efectiva**

(Y NUNCA lo será)

Agentes (si algo sale mal)

Tú

- Dueños / Admins
- Developer, Designer
- **Usuarios / clientes (¿GDPR o similar?)**

Soporte Hosting

- Agentes / C3
- Soporte y Copias de seguridad

Experto de Seguridad

- Departmento de seguridad
- Servicios externos

Agentes (si algo sale mal)

Tú

- Dueños / Admins
- Developer, Designer
- **Usuarios / clientes (¿GDPR o similar?)**

Soporte Hosting

- Agentes / C3
- Soporte y Copias de seguridad

Experto de Seguridad

- Departmento de seguridad
- Servicios externos

Medidas:

REACTIVAS

Cuando las cosas malas **ya han pasado**

Mitigación de **Daños**

INCIDENT RESPONSE

PROACTIVAS

Antes de que pase nada malo

Mitigación de **Riesgo**

ANÁLISIS Y MONITOREO

Segundo, la RESPUESTA A INCIDENTES

Incident response (IR) is **the effort to quickly identify an attack, minimize its effects, contain damage**, and remediate the cause to reduce the risk of future incidents.

(vmware.com)

Medidas **reactivas** (AKA Incident Response)

1) ESCANEA tu sitio

Front-end: **sitecheck.sucuri.net**

Escáner gratis en plugin: WordFence, etc.

2) ACTUALIZA

TODO

Incluyendo el software del servidor.

3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas …

- webpagetest.org

O restaurar **BACKUP Y** Volver a 1)

Posible pérdida de información

Posible re-instalación de malware

(PRIMERO) **ESCANEA** tu sitio

- Intentemos primero **entender que ha pasado.**
- FrontEnd análisis: **sitecheck.sucuri.net**
- Usar escáner gratuito (i.e. WordFence)
- Si tienes acceso al server, ejecuta un antivirus (i.e. Clam AV)

Warning: Malware Detected

Infected with malware. Immediate action is required

Request Cleanup

58
URLs Scanned

Pages scanned: 37
Javascript files scanned: 21
Other files: 0

System running on: LiteSpeed, Powered by: PHP/5.4.45
IP address:
More Details

Low | Medium | **Critical Security Risk**

Malware Found

http://www. /wp-includes/js/jquery/jquery.js?ver=1.12.4 (More details)

Definition

rogueads.unwanted_ads?9.5

Malware Found

http://www. /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 (More details)

Definition

rogueads.unwanted_ads?9.5

(SEGUNDO) **ACTUALIZA**

Actualiza todo, incluidos plugins, temas y el propio WordPress.

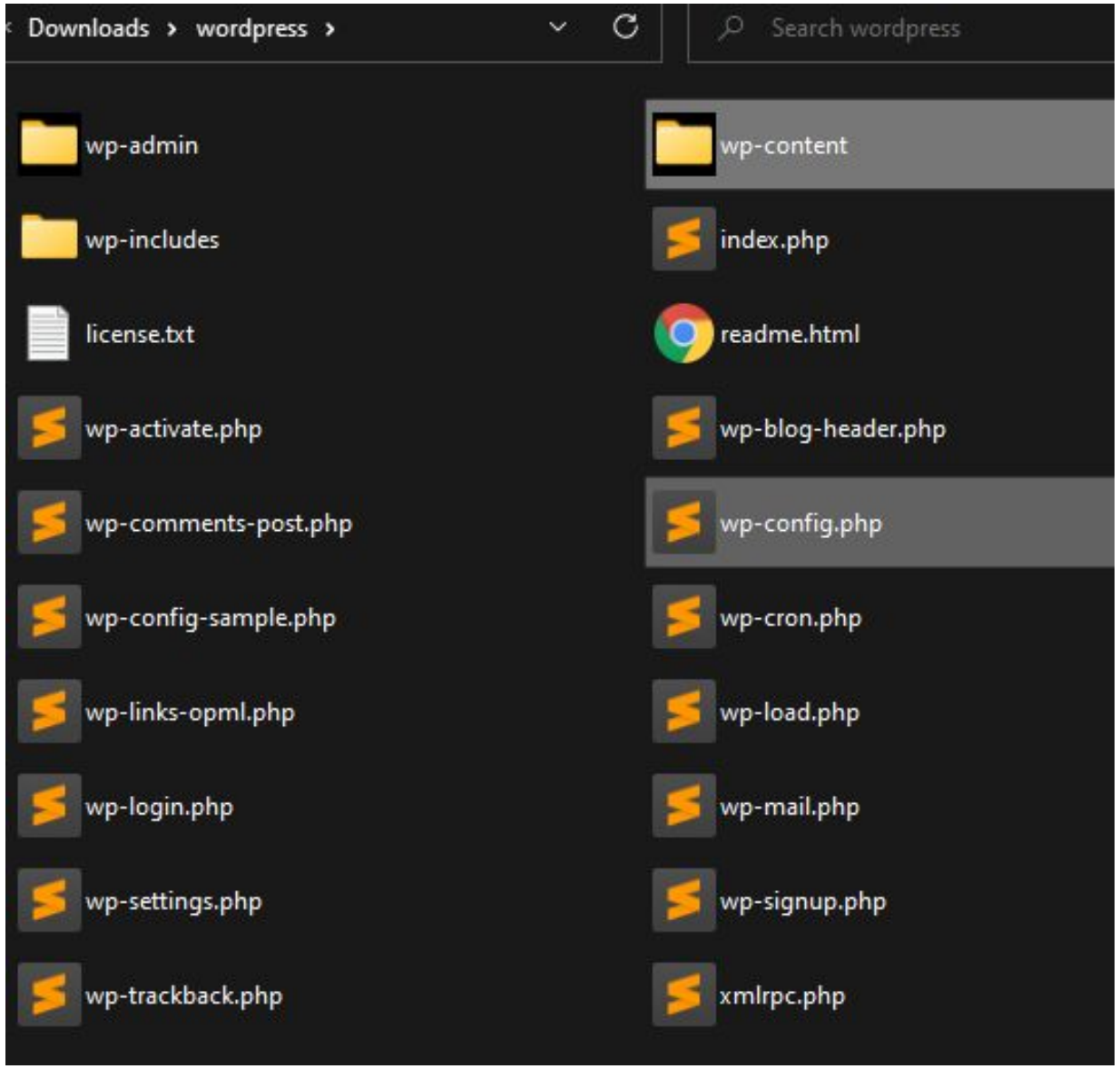
Esto hará que tapemos agujeros de seguridad, evitando una possible infección.

También, **sobreescribirá código comprometido/corrupto con código confiable** del repositorio oficial.

ACTUALIZA

PLUGINS	TEMAS	CORE	PHP
APACHE / NGINX	SERVIDOR	CPANEL / PLESK	…

¡SECRETO!


Downloads › wordpress ›
Search wordpress
wp-admin
wp-content
wp-includes
index.php
license.txt
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config-sample.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php

(TERCERO) **CRC**:
Check, remove and change

Check & Remove

- Admins innecesarios
- Plugins y temas que no sean estrictamente necesarios
- Copias de seguridad
- Sitios de test/en desarrollo en el servidor de producción.

Change Contraseñas

- Connexiones (cPanel, FTP, SSH, …)
- Base de datos (recuerda actualizar luego el **wp-config.php**)
- Panel admin (**wp-admin**)
- Acceso al proveedor de hosting.

Atención: Se perderá cualquier personalización que hayas hecho a los archivos del

Actualizar temas

Seleccionar todos

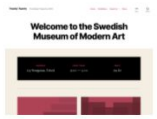
Twenty Fifteen
Tienes la versión 2.5. Actualiza a la 2.6.

Twenty Fourteen
Tienes la versión 2.7. Actualiza a la 2.8.

Twenty Nineteen
Tienes la versión 1.4. Actualiza a la 1.5.

Twenty Seventeen
Tienes la versión 2.2. Actualiza a la 2.3.

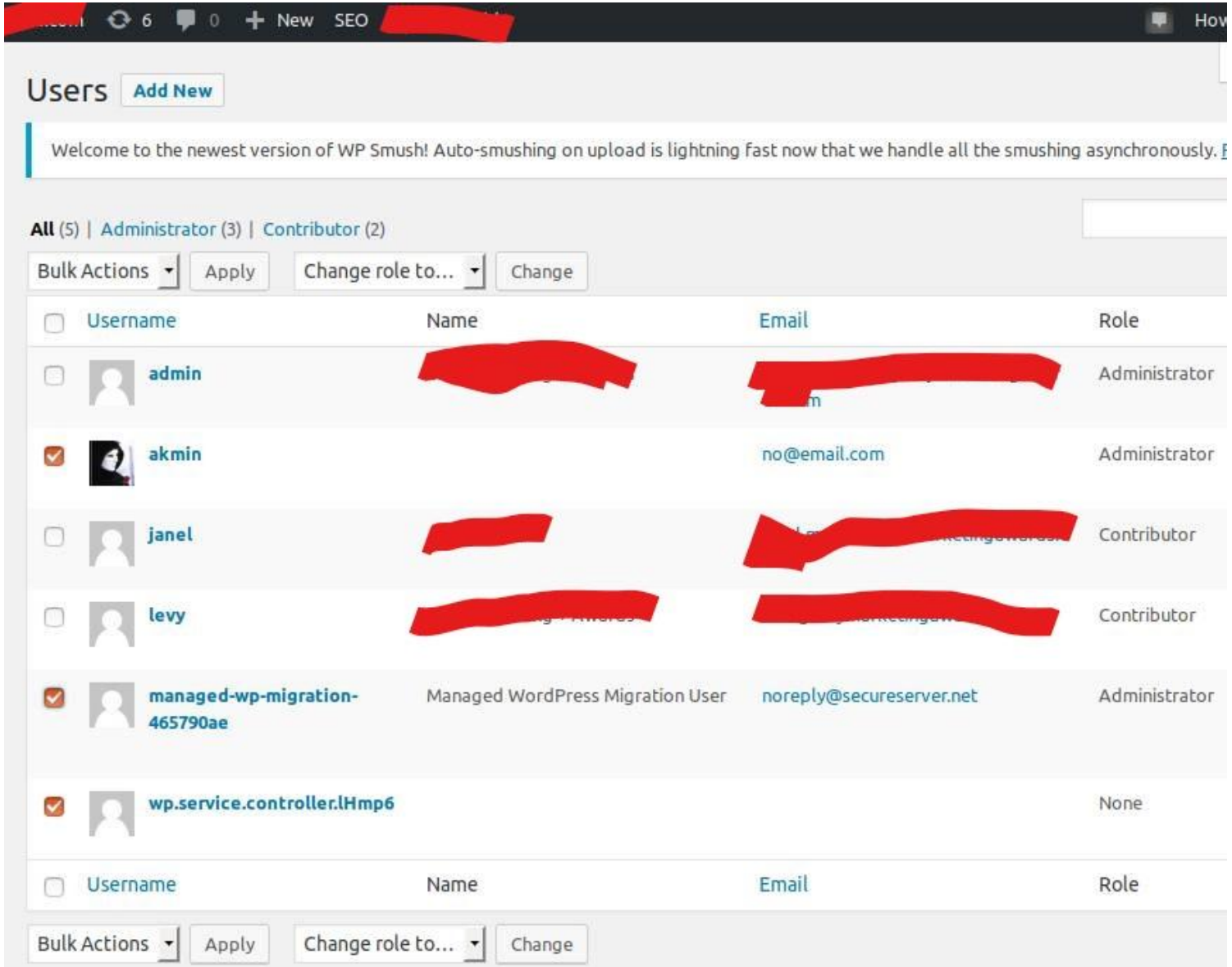
Twenty Thirteen
Tienes la versión 2.9. Actualiza a la 3.0.



Twenty Twenty
Tienes la versión 1.1. Actualiza a la 1.2.

Seleccionar todos

Actualizar temas



(ÚLTIMA OPCIÓN) Restaurar una **Copia de Seguridad**

- Puedes perder información
- No sabemos a ciencia cierta cuándo comenzó la infección

COPIAS DE SEGURIDAD

Ten una buena **estrategia**

Nunca las almacenes en tu servidor de producción

Una copia **FUNCIONAL** puede ser **tu mejor amiga** un mal día

¡RECUERDA! Medidas **reactivas**

1) ESCANEA tu sitio

Front-end: **sitecheck.sucuri.net**

Escáner gratis en plugin: WordFence, etc.

2) ACTUALIZA

TODO

Incluyendo el software del servidor.

3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas …

- webpagetest.org

O restaurar **BACKUP Y** Volver a 1)

Posible pérdida de información

Posible re-instalación de malware

Ahora, **la Reputación**

Bots, Motores de Búsueda y Blocklists

INTERNET ESTÁ CONSTANTEMENTE RASTREADO POR **BOTS**

LOS MOTORES DE BÚSQUEDA Y EMPRESAS DE SEGURIDAD TIENEN **BLOCKLISTS**

BLOCKLISTS -> REPUTACIÓN

MIENTRAS MÁS FAMOSA SEA LA BLOCKLIST MÁS ACEPTADA.

Algunos hechos

No es un proceso inmediato

- La inclusion en blocklists toma su tiempo
- Salir también

Normalmente, no dan información de por qué

Las RRSS tienen en cuenta las blocklists

Las empresas de Ads bloquean campañas

Los motores de búsqueda eliminant el sitio de las SERP

- Algunos eliminan completamente to rankeo de SEO

Un cosa (importante) más …

Algunas **leyes de protección de datos** pueden requerir que se reporte cualquier brecha de seguridad con pérdida de datos sensibles a las autoridades competentes

En el caso de que que **afecte a un ciudadano Euroeo**, la **GDPR da 72h** tras la detección de la brecha para notificarla.

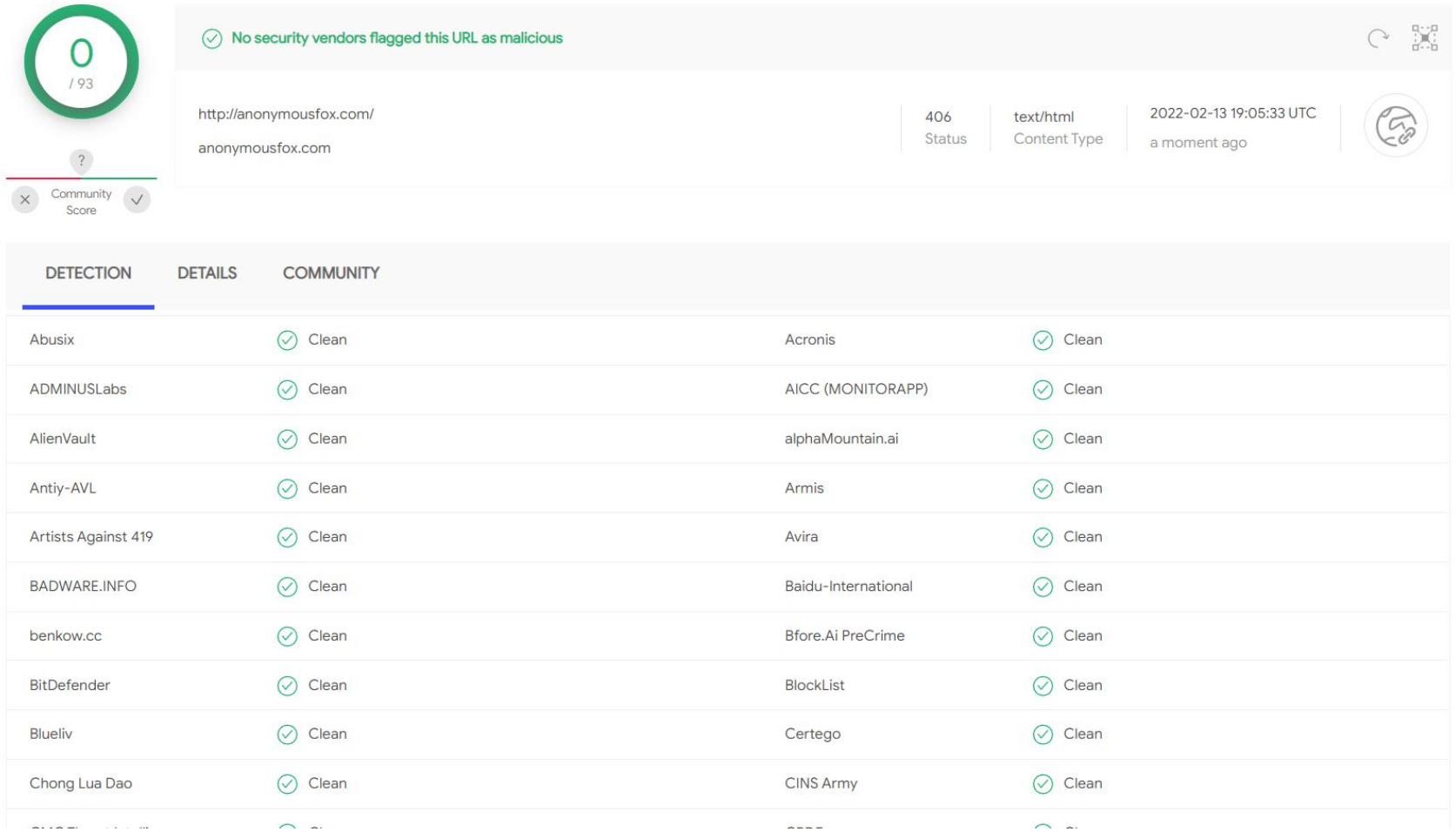
Comprueba las leyes aplicables, depende de país en el que operes y la nacionalidad de los clients.

Solución a las blocklists

1. **UNA VEZ LIMPIA**, comprueba las blocklists:

   Virustotal.com

2. **Procede a solicitar** una reconsideración por cada empresa en las blocklists, individualmente.



Informe Post-Mortem

Es **duro**, requiere servicios **forenses** y **expone** tu gestión.

Un informe claro **de lo que pasó** tras el ataque exitoso:

- Cómo y cuándo ocurrió
- Cómo y cuándo fue descubierto
- Qué se hizo para mitigar el daño y recuperar la situación normal
- Lecciones aprendidas

Ayuda a **aprender** para futuras situaciones

Ayuda a recuperar la **confianza de los usuarios**

Muestra tu compañía alineada con los conceptos de **transparencia**.

Y para finalizar…
¡Paz Mental!

Medidas Proactivas

- ...gins y temas (LEAST PRIVILEGE RULE)
- ...s, cambiar periódicamente, 2FA + Fuertes
- (¡VALIDARLAS!)
- ...rches vienen DESPUÉS de los EXPLOITS)
- ...N.com, PatchStack & Integridad de Ficheros)
- WAF (Web Application Firewall)

¡Recuerden! **INVERTIR** en:

HOSTING

SEGURIDAD


Everybody needs a hacker

Ponente

¡GRACIAS!

WordCamp Torrelodones 2023

WordCamp Torrelodones 2023

#WCTorre