WordFest.

Big Orange Heart.

Breath IN... Breath OUT...

The **Checklist&Guide**

to recover **your**

Site&Reputation

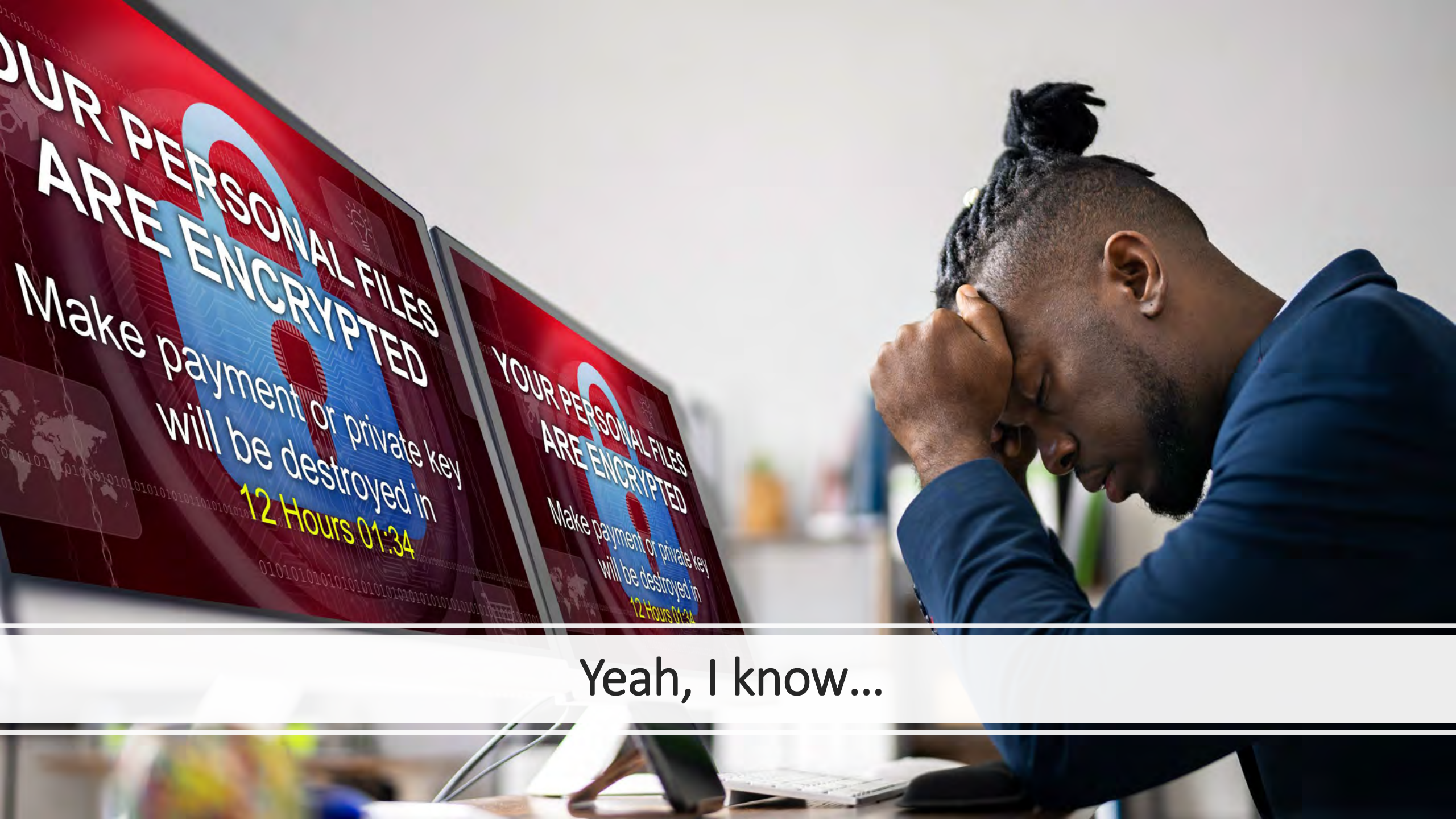
after a hack

by **Nestor Angulo**

HackedÃ,Â ByÃ,Â JakRa

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

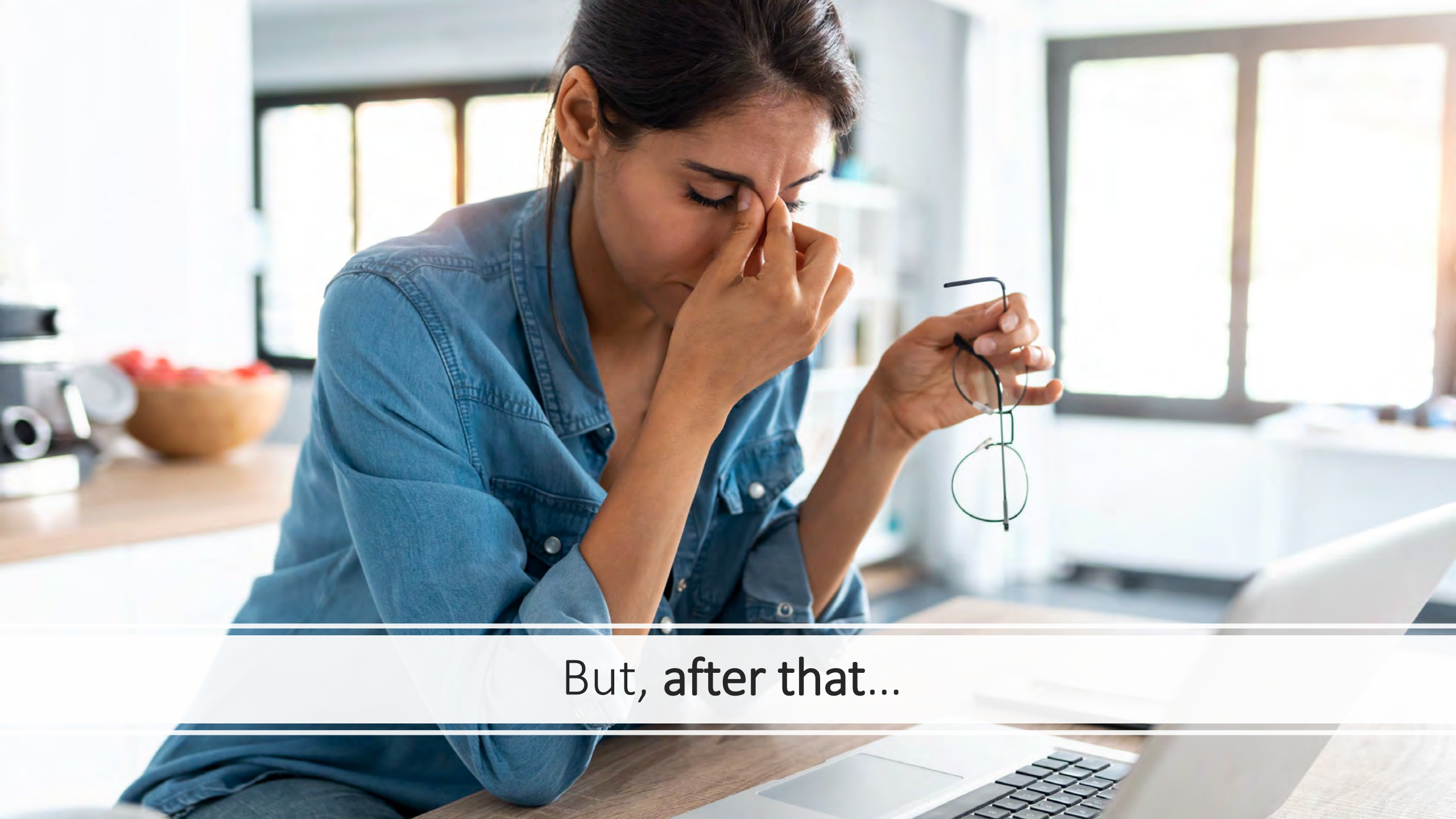
Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team


OUR 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

Yeah, I know...


So, let’s SCREAM!

It is acceptable to be down too…



But, **after that**…

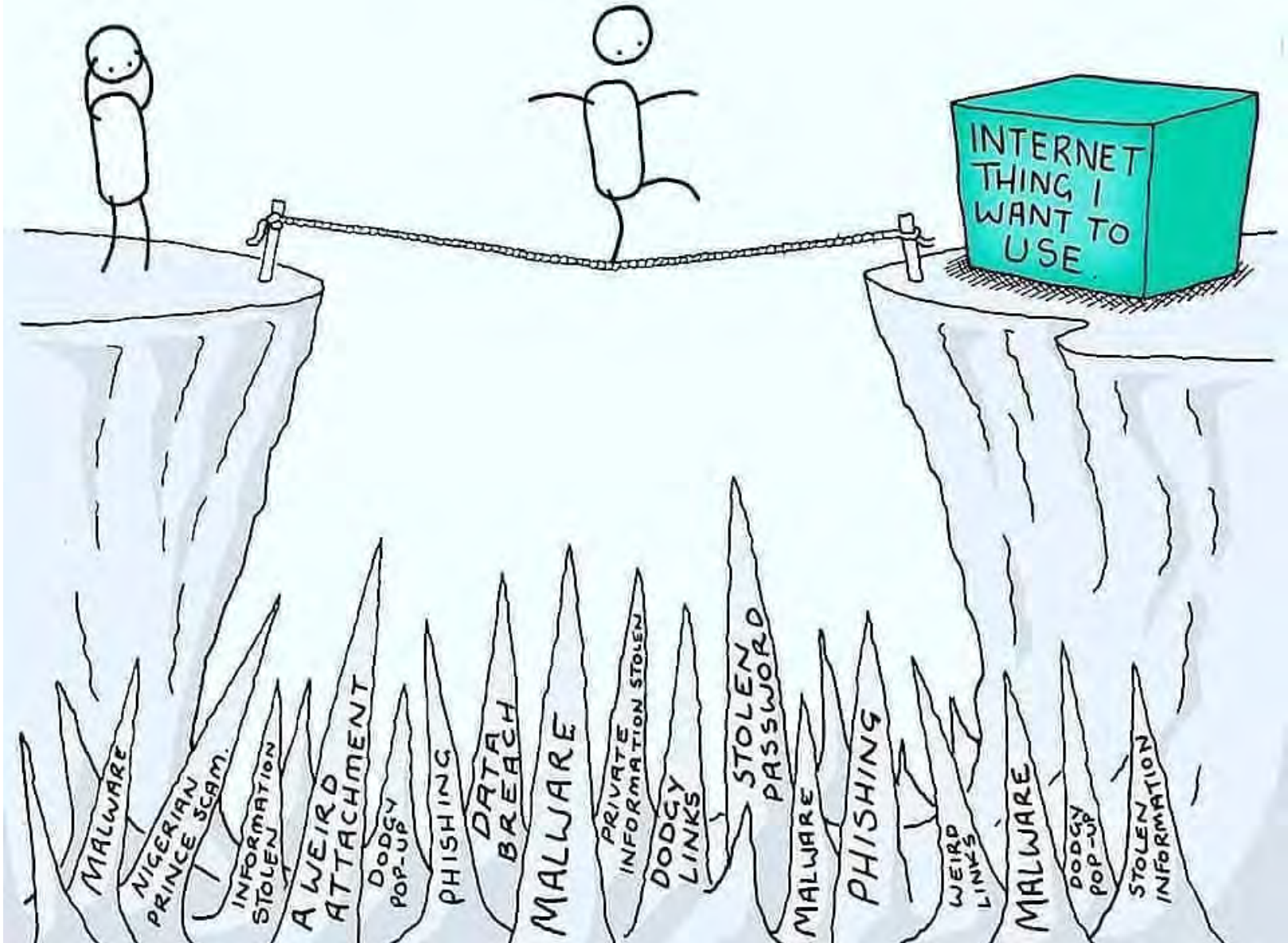
Let's **ACT**...

First of all… **Concepts**

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




BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Hackers vs Cyberterrorists

Hacker

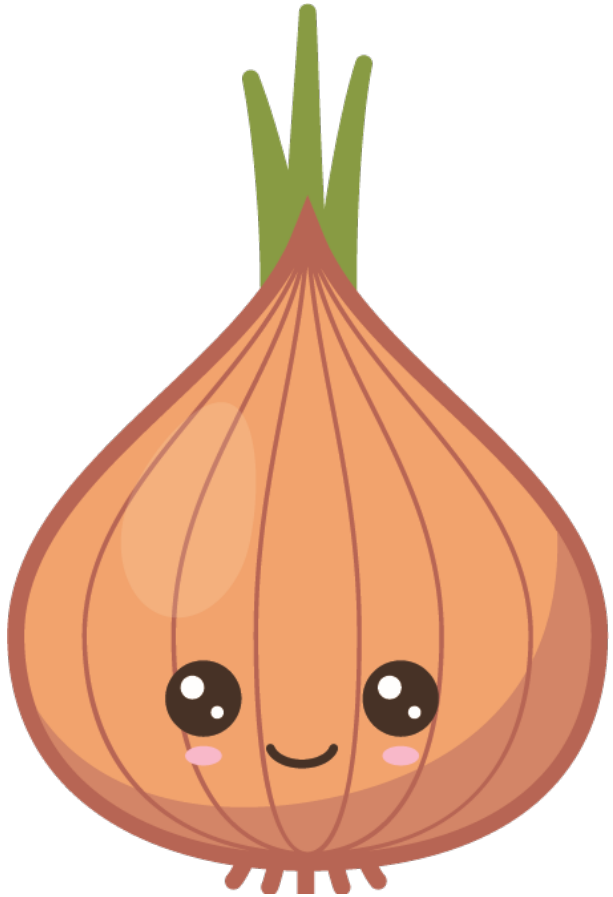
- **Curious person** who loves to go beyond limits or conventions.

Cyberterrorist

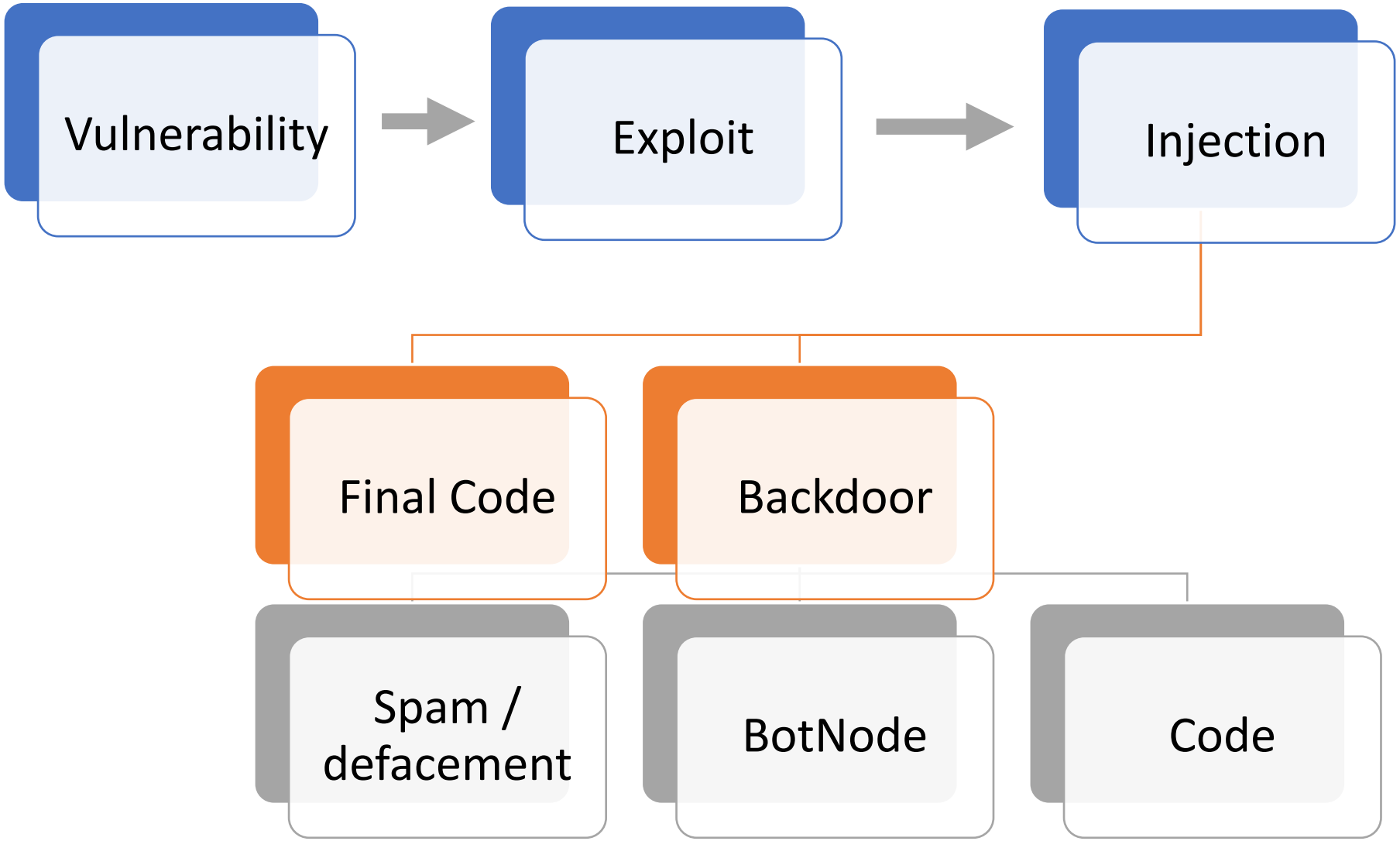
- **Computer Hacker**, aligned to enrich himself in a zero-sum game situation.
- **The bad guy**

Security: **Simplified Layer Model**

Layer	Protection
You, the weakest layer	Knowledge
Your **Device**	Antivirus
Your **Connection**	SSL
Your **Website Traffic**	WAF
Your **Credentials**	Strong passwords, 2FA
Website Security	monitor, plugins, updates
Server Security	monitor, sysadmin, updates
Database	monitor, sysadmin
Maintenance	



How a **WordPress** site is **infected**:



FACTS

Site hacking **almost never** is client-oriented (98% of cases)

Almost always happens due to a **deficient monitoring / maintenance**

A **SSL** certificate **is not** an antihacking shield

Patches & security updates appear almost always after hacking exploits

Errare Humanum Est (Human being fails)

Security **never is (nor will be)** 100% effective

Agents involved (if something bad happens)

You

- Owner / Admins
- Developer & Designer
- **Users/clients**
  (GDPR or similar?)

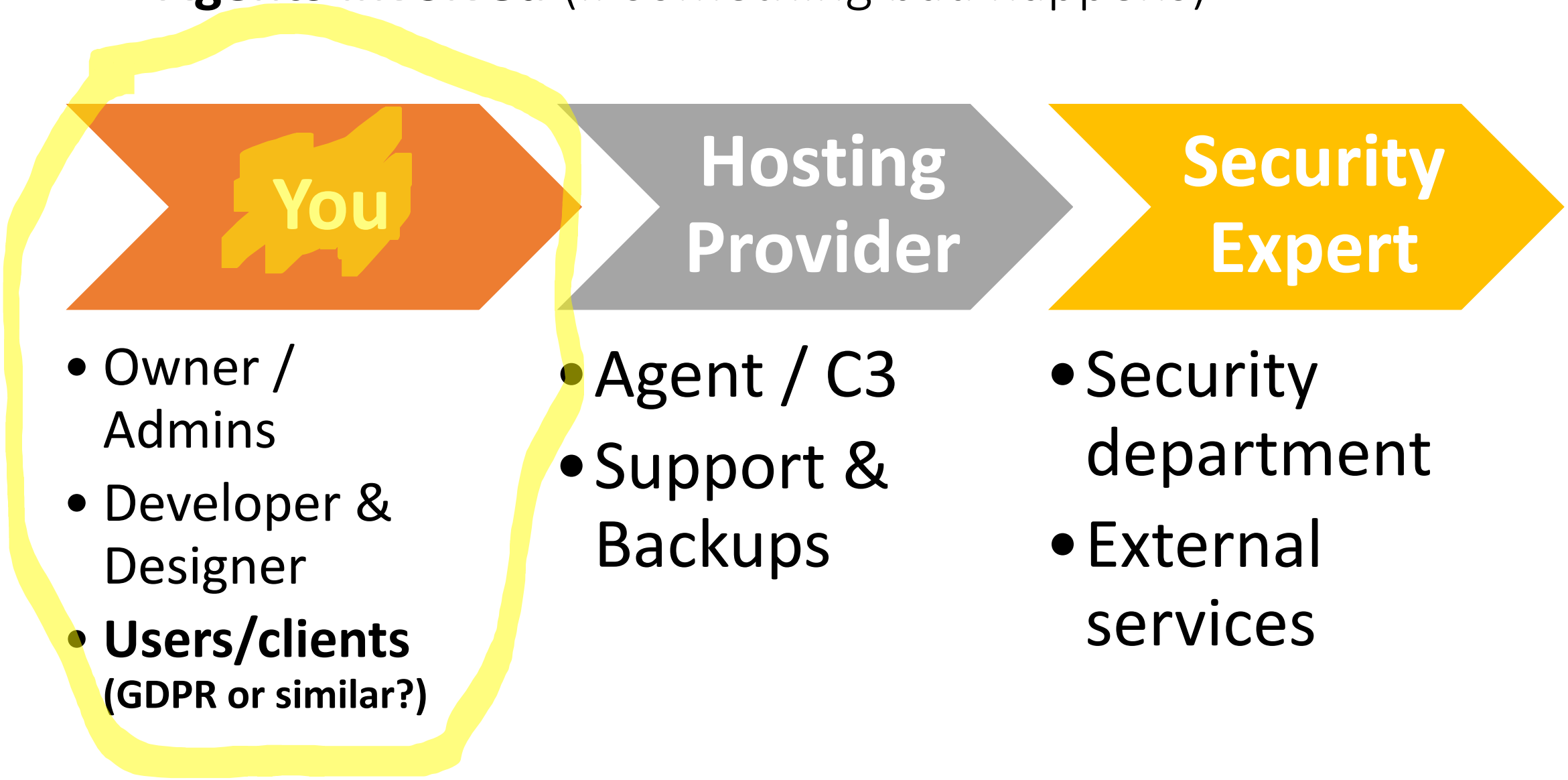
Hosting Provider

- Agent / C3
- Support & Backups

Security Expert

- Security department
- External services

Agents involved (if something bad happens)



Measures:

REACTIVE

When bad things have **already happened**

Pain mitigation

INCIDENT RESPONSE

PROACTIVE

Before anything bad happens

Risk mitigation

ANALYSIS & MONITORING

Secondly, the **Incident Response**

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)

Reactive measures (AKA Incident Response)

1) SCAN your site

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

Free tier plugin scanner: WordFence, etc.

2) UPDATE

EVERYTHING
Including server software

3) CRC: Check, Remove and Change

Admins, plugins, themes, Passwords …

- webpagetest.org

OR Restore a **BACKUP** & back to (1)

Possible lose of information

Possible re-installation of malware

(FIRST) **SCAN** your site

- Let's try to figure out **WHAT** happened
- FrontEnd Snapshot analysis: **sitecheck.sucuri.net**
- Use any free tier plugin scanner (i.e. WordFence)
- If you have access to the server, you can use a server 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

(SECOND) **UPDATE**

UPDATE ALL, including plugins, themes and WordPress itself.

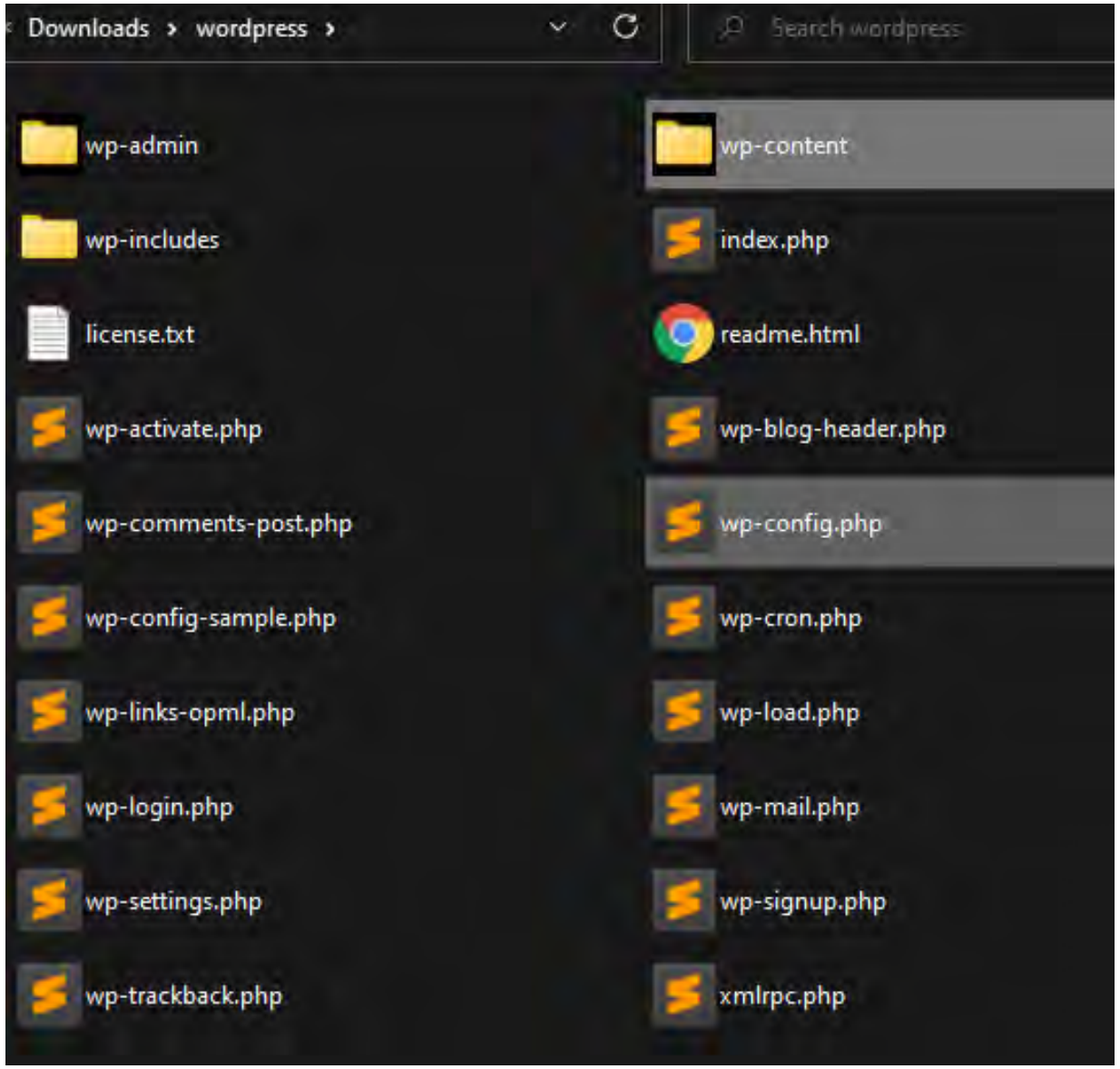
This patches security vulnerabilities

ALSO, this action **overwrites compromised/corrupted code** with trustworthy code from official repositories.

UPDATE

PLUGINS	THEMES	CORE	PHP
APACHE / NGINX	SERVER	CPANEL / PLESK	…

SECRET!


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

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

Check and Remove

- Unneeded admin users
- Plugins and themes which are strictly not in use
- Outdated backups
- DEV/TEST sites in your production server

Change Passwords

- Connections (cPanel, FTP, SSH, …)
- Database (remember to update your **wp-config.php**)
- Dashboard (**wp-admin**)
- Hosting provider

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

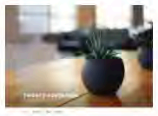
Actualizar temas

Seleccionar todos

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

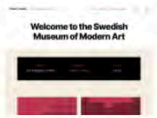
Twenty Fourteen
Tienes la versión 2.7. Actualiza a la 2.8.

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



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

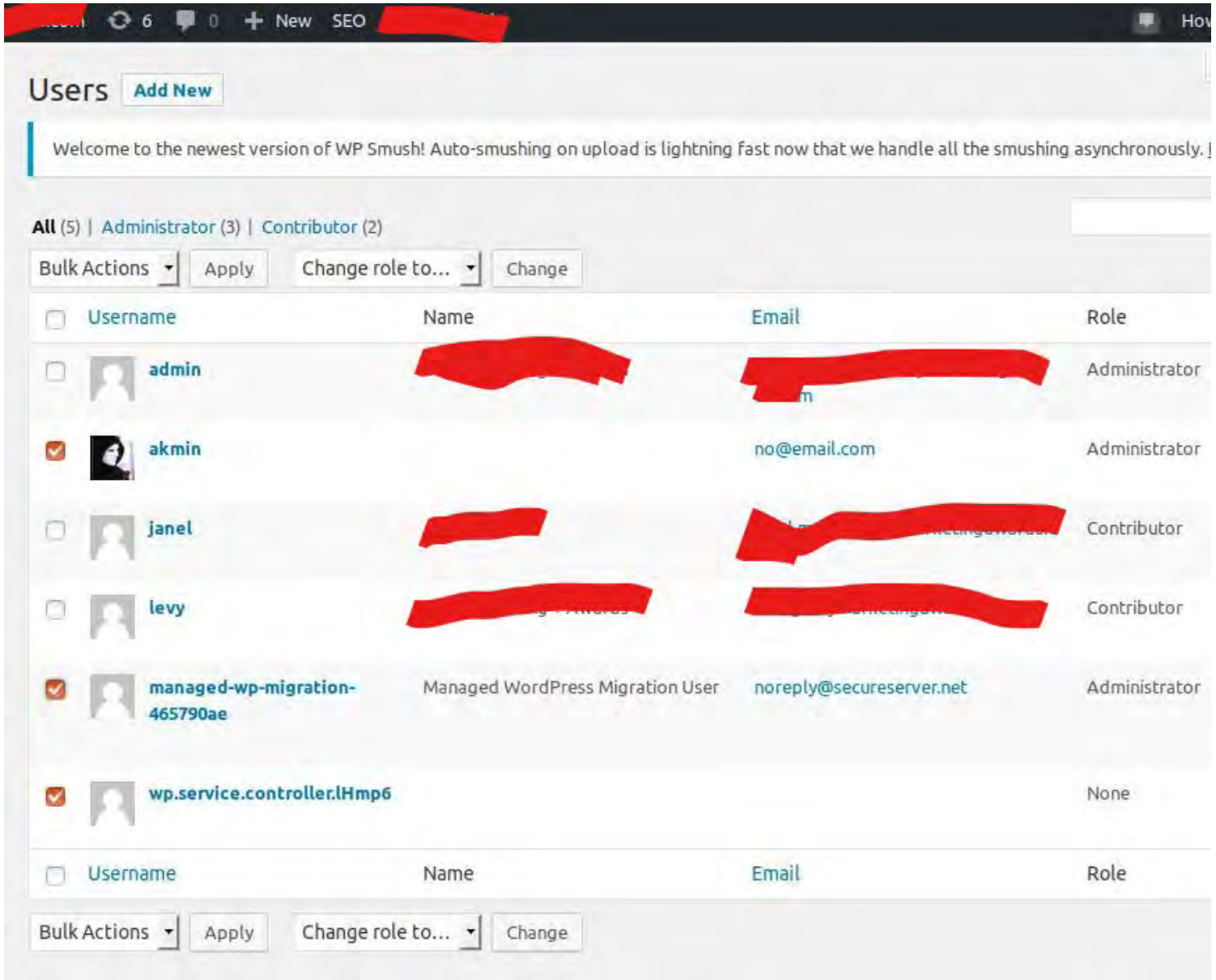
Twenty Thirteen
Tienes la versión 2.9. Actualiza a la 3.0.



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

Seleccionar todos

Actualizar temas



(LAST OPTION) Restore a **BACKUP**

- You can lose information
- We don’t always know when the infection begun

BACKUPS

Have a backups **strategy**

NEVER store the backups in your **production server**

A **FUNCTIONAL backup** will be your **best friend** a bad day

BACKUPS

Have a backups **strategy**

r

A FUNCTIONAL **backup** will be your **best friend** a bad day

REMEMBER: Reactive measures

1) SCAN your site

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

Free tier plugin scanner: WordFence, etc.

2) UPDATE

EVERYTHING
Including server software

3) CRC: Check, Remove and Change

Admins, plugins, themes, Passwords …

- webpagetest.org

OR Restore a **BACKUP** & back to (1)

Possible lose of information

Possible re-installation of malware

Then, the **Reputation**

Bots, Search Engines and Blocklists

INTERNET IS CONSTANTLY BEING CRAWLED BY **BOTS**

SEARCH ENGINES AND SECURITY VENDORS HAVE **BLOCKLISTS**

BLOCKLISTS -> REPUTATION

THE MORE FAMOUS THE BLOCKLIST THE MORE WIDELY ACCEPTED.

Some Facts

This is not an immediate process

- Inclusion takes time
- Delist takes time

Normally, there isn’t any info about **why**

SNS block or warn about posts

Ads companies block/hold campaigns

Search Engines remove your site from SERPs

- Some of them remove completely your SEO rank

One (important) more …

According to some Data Protection laws it might be **mandatory to report any personal data breach to supervisory authorities**.

In the case of **affecting any European citizen**, the **GDPR gives 72h** after the breach is detected to report about it.

Check the applicable law, depending on the country you are operating from and the nationality of the affected person.

In Asia there are several laws that may apply some restrictions or obligations in this case. For instance:

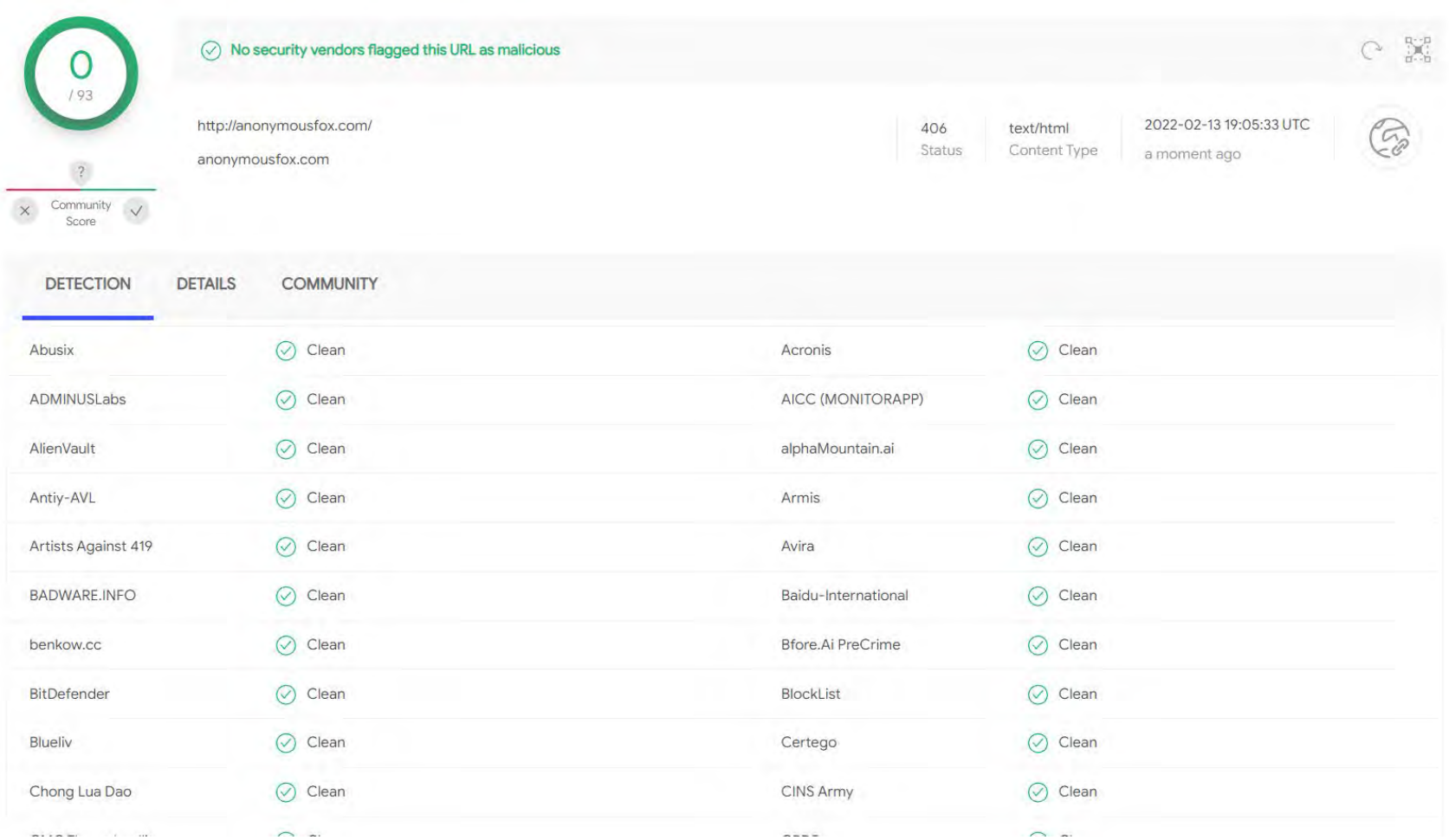
- New Zealand: Privacy Act 2020
- Japan: APPI
- South Korea: PIPA
- Thailand: PDPA

Troubleshooting

1. **ONCE THE SITE IS CLEAN**, check blocklists:

   Virustotal.com

2. **Submit** for reconsideration to all the blocklists vendors **individually**



Post-Mortem report

It is **hard**, requires **forensic** services and **exposes** your management

A report of **what happened**, after a successfully hacking attempt

- How and when it happened
- How and when it was discovered
- What did you do to mitigate the situation and to recover the normal situation
- Lessons learnt

Helps to **learn** for future situations

Helps to recover **user's trust**

Shows your company as **transparency advocated**

Lastly, **never again**!

Proactive measures


Reduce admins, plugins and themes (LEAST PRIVILEGE RULE)


Use a Passwords Manager, change periodically, strong ones


Backups (VALIDATE THEM)


Updates (REMEMBER: PATCHES COMES AFTER EXPLOITS)


Monitor your site (WPSCAN.com & files integrity scanner)


WAF (Web Application Firewall)

Remember to **Invest** in

HOSTING

SECURITY


Everybody needs a hacker

WordFest.

THANKS! 

QUESTIONS!