Active security

for Joomla! sites

version 5.0

What is site security?

Security is about...

making it harder

to hack a site, not

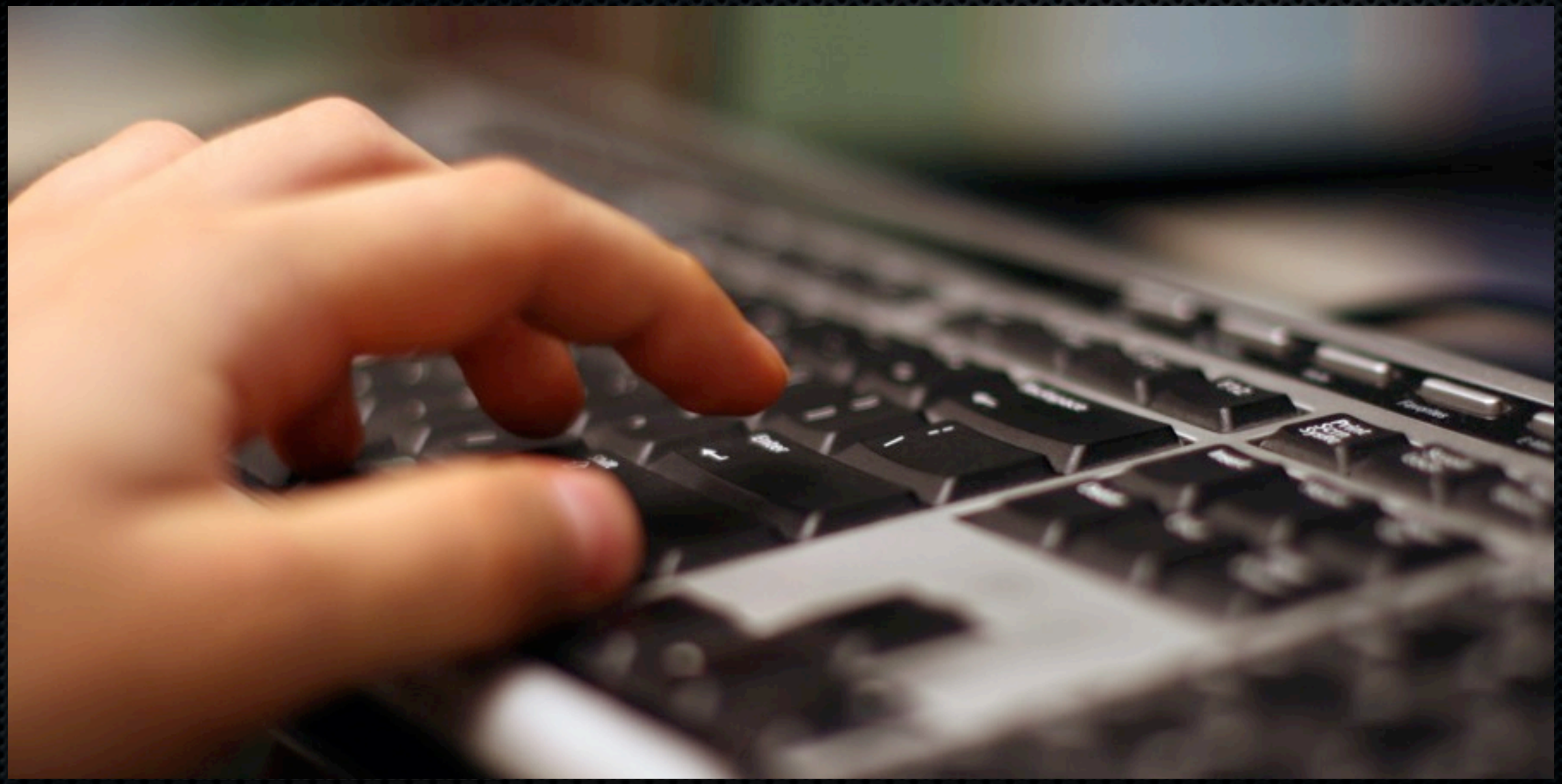
making it impossible

A site is like a building

- **Strong foundations**
- **Careful construction**
- **Active maintenance**

Strong foundations

Your server setup



Updated server software

PHP, MySQL, Apache, FTP Server...

Why?

- Old versions = bugs = security issues = you can get hacked
- Old versions = no support from third party software = old third party software versions = bugs = security issues = you can get hacked
- Ergo: **old versions = BAD IDEA™**

It’s simple

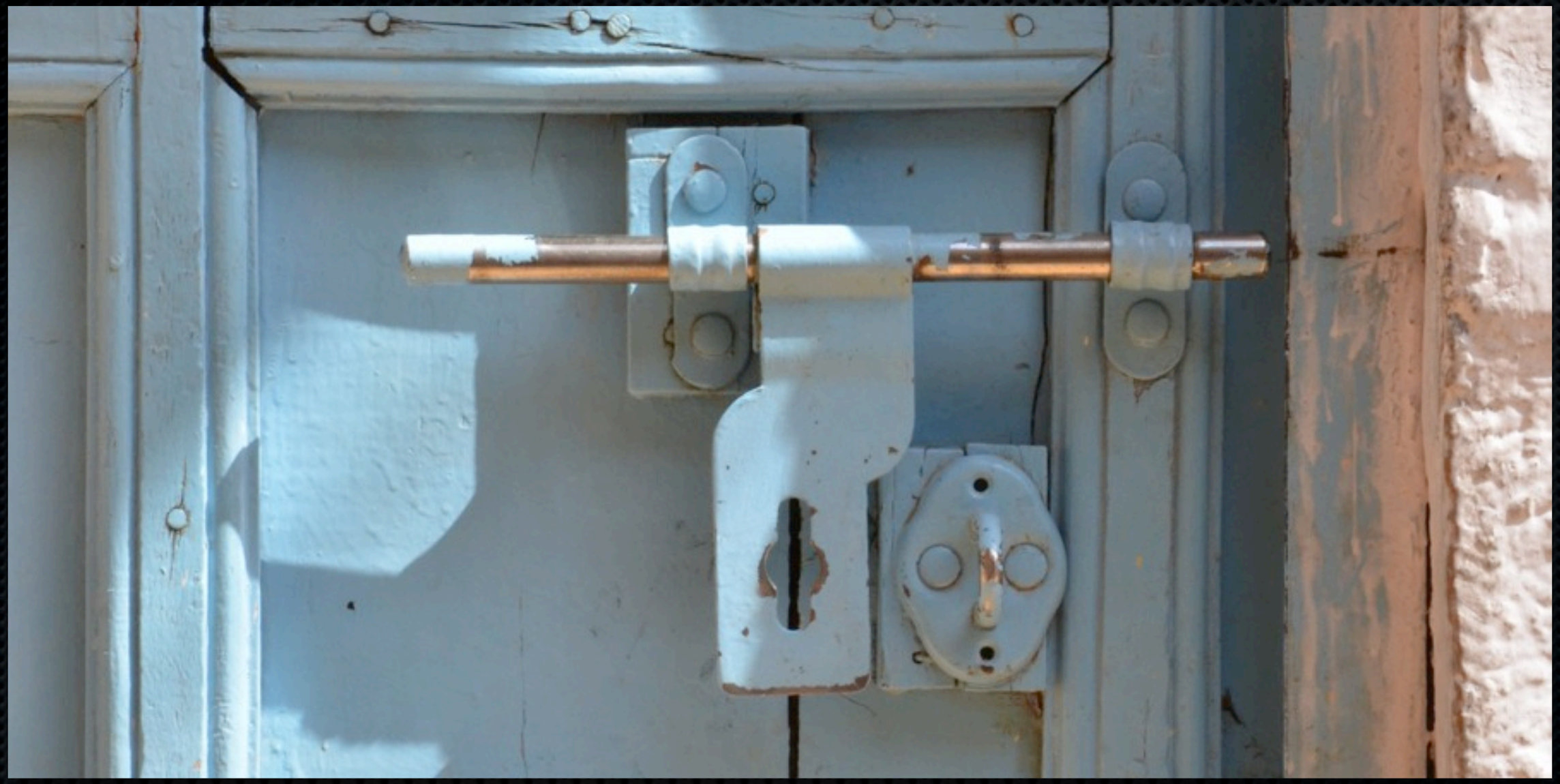
- Dedicated server with cPanel, Plesk etc can update automatically
- Self managed Ubuntu Server: apt-get update && apt-get upgrade
- Shared hosts & VPS: ask your host to upgrade

mod_security for Apache

Your server's security guard

You need some rules

- **Atomic (GotRoot) Rules:** http://www.atomicorp.com/wiki/index.php/Atomic_ModSecurity_Rules
- **OWASP Rules**: https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project



Permissions & ownership

Who can do what and where

What does ownership mean?

- Who owns the file?
- Who owns the web process?

What do permissions mean?

0 **6** **4** **4**

(forget this) | Owner | Group | World

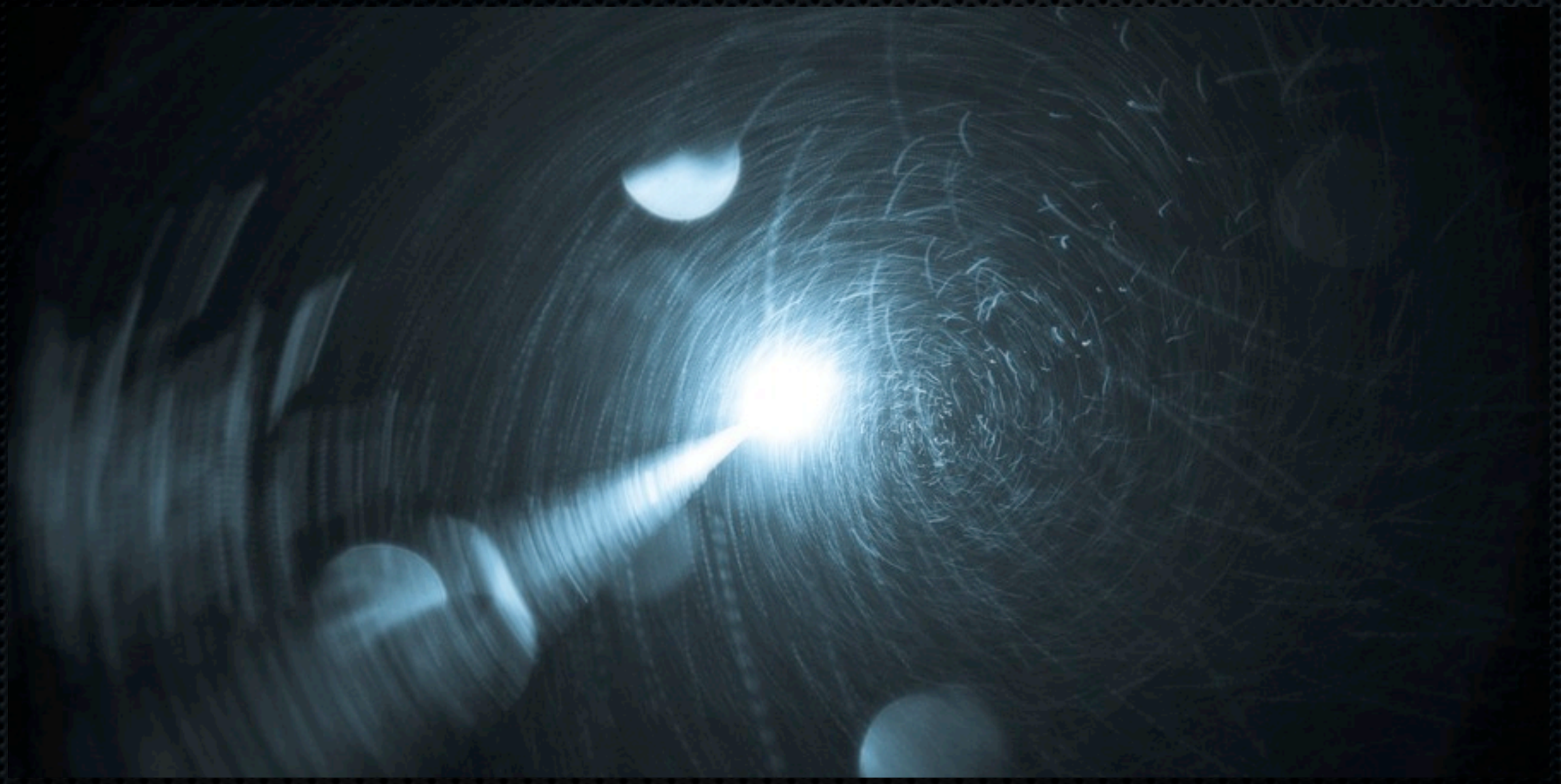
1 = Execute / Browse
2 = Write
4 = Read

Sane ownership & permissions

- All files and folders owned by the FTP user
- Folders: 0755 permissions
- Files: 0644 permissions
- Use Joomla!’s FTP mode on shared hosts
- Better yet, use suPHP or FastCGI

Too much to remember?

- **Akeeba Backup User's Guide, Security Information**
  https://www.akeebabackup.com/documentation/akeeba-backup-documentation/security-info.html
- **777: The number of the beast (in French)**
  http://www.dionysopoulos.me/blog/777-le-numero-du-demon



Make it all happen

The magic script

```
 19   CHARSET=
 20   SSHPORT=
 21   IGNOREIP=
22   USER=
3   ADMINEMAIL=
    PUBLICKEY="ssh-rsa ... foo@bar.com"
  # ================================================================== #
  #                        End system specific details                 #
 # ================================================================== #
#
echo
cho "System updates and basic setup"
ho "================================================================="
o
o

"First things first, let's make sure we have the latest updates."
-----------------------------------------------------------"
```

https://github.com/betweenbrain/ubuntu-web-server-build-script

written by Matt Thomas (@betweenbrain)

Careful construction

Your site setup

Update, yesterday

Joomla! & extensions

Think before installing

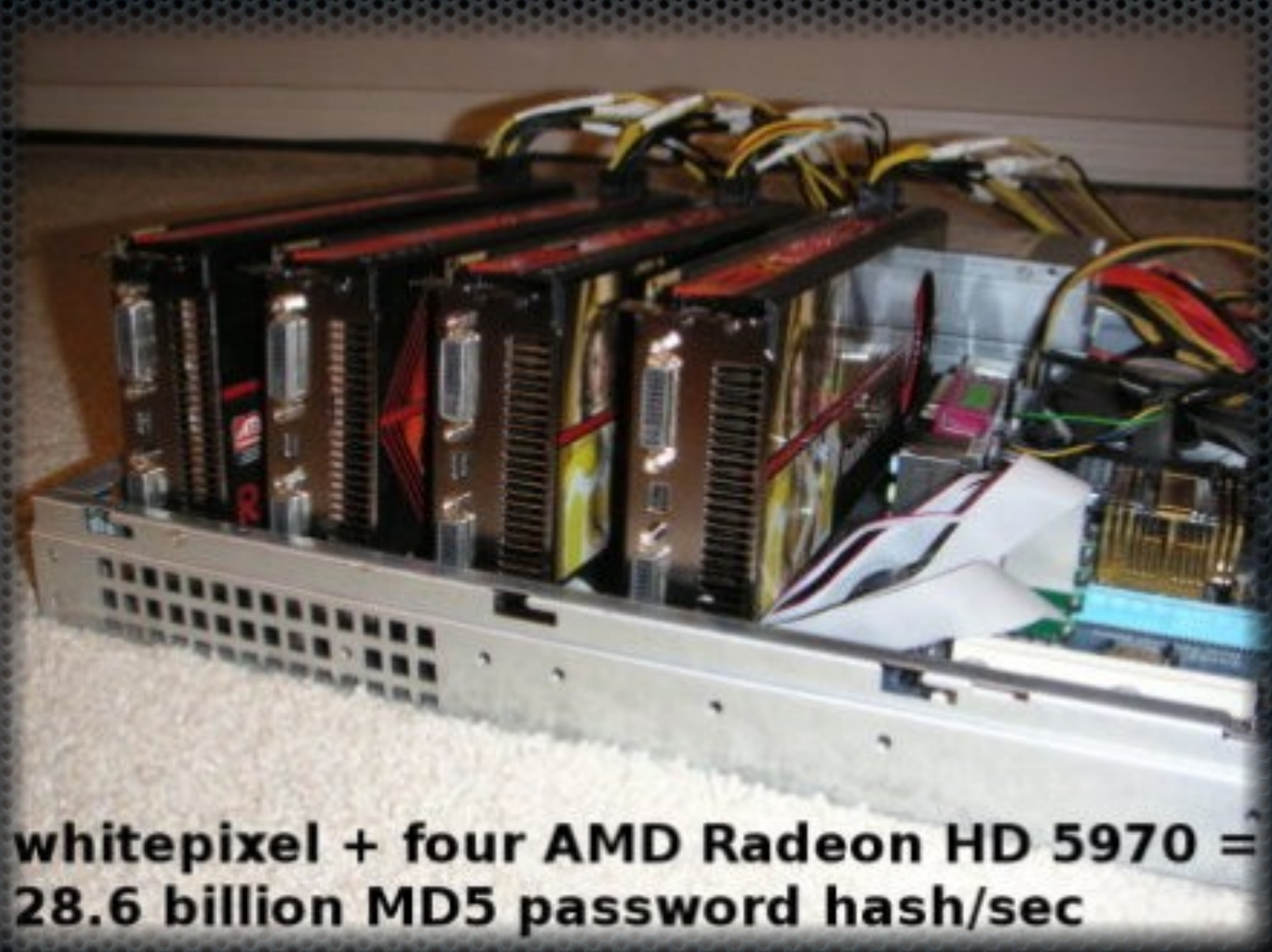
Don’t be the mouse in the trap!

Length matters

I’m talking about your password…

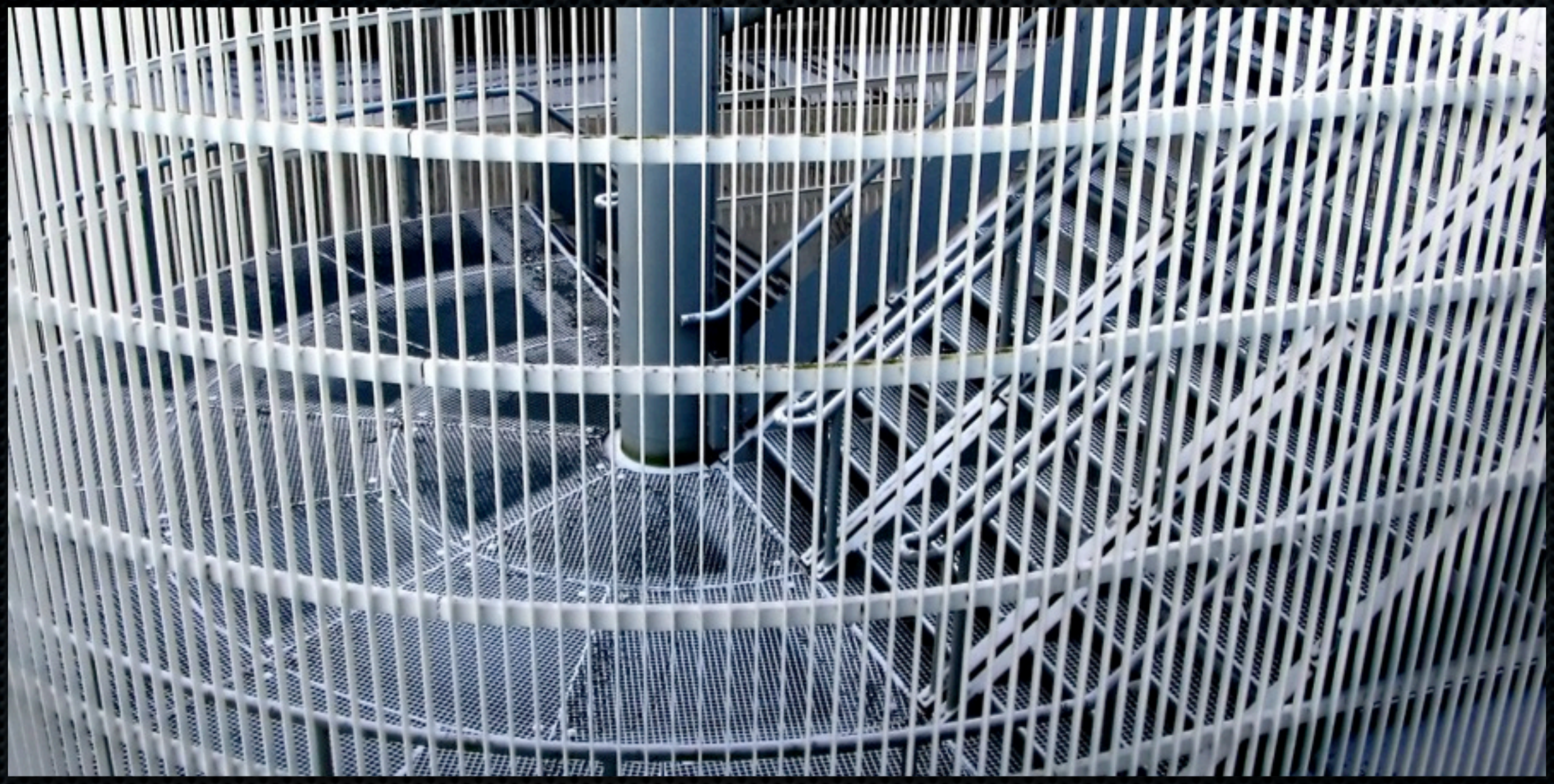
A terrifying thought

Password hacking super-computer: 2,700 USD



How safe is your password?

Password	Bits	Iterations	Time to crack
15082005	13,6	12416	0.00038 msec
admin	15,9	61147	0.00185 msec
ortrtaortftaaidbt	67,7	2,39e+20	228.95 years
0rtrTA0rtfTa&idbT	88,2	3,55e+26	340 *million* years
horse correct battery stapler	107,2	1,86e+32	178179 **billion** years



Lock it down

Nothing on my site runs unless I say so

.htaccess Rules

- **My Master .htaccess**
  http://akeeba.assembla.com/code/master-htaccess/git/nodes/htaccess.txt
- **Admin Tools Professional (20 Euros)**
  https://www.akeebabackup.com/products/46-software/855-admintools.html

Armor up

Protect your site

Active maintenance

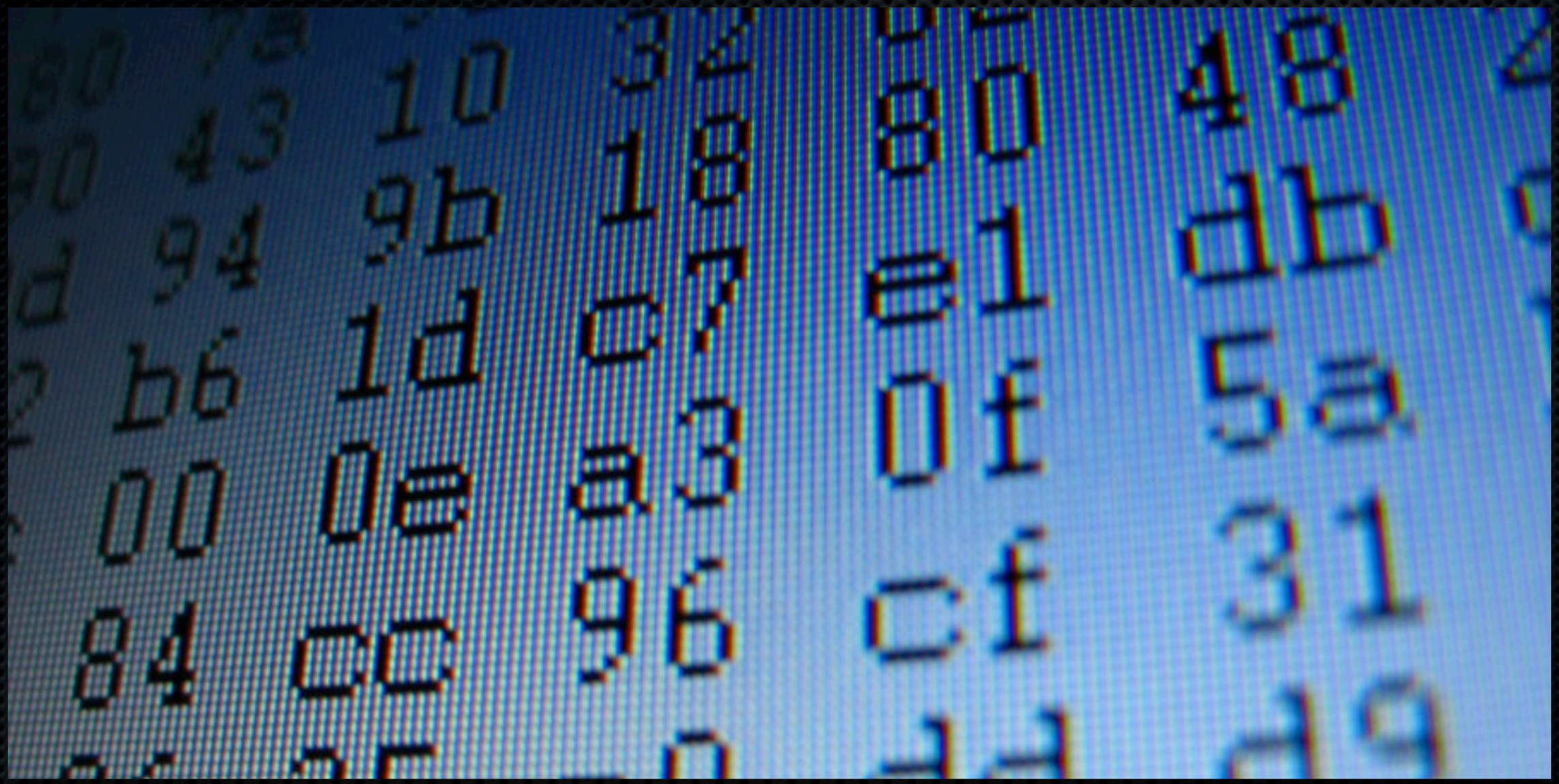
Staying on top of it all

Backups

Frequent, automated, off-site backups

Monitor file changes

A changed file is usually a bad thing



Monitor it

Keep an eye on the logs

In spite of it all...

Earthquake! Disaster!

You got hacked, now what?

DON'T

PANIC

We’ve got instructions

- **Unhacking your site**
  https://www.akeebabackup.com/documentation/walkthroughs/item/1124-unhacking-your-site.html
- You *do* have backups, right?
- Make sure you read the instructions before getting hacked.

Questions?

Download this presentation

www.slideshare.net/AkeebaBackup

Thank you for listening!

Image credits: sxc.hu; istockphoto.com