Tales from the Trenches – Learning from the Misery of Others.

*Confessions of a Sh*tty SysAdmin*

Andy Thompson, CISSP, GPEN
CyberArk

whoami – Andy Thompson

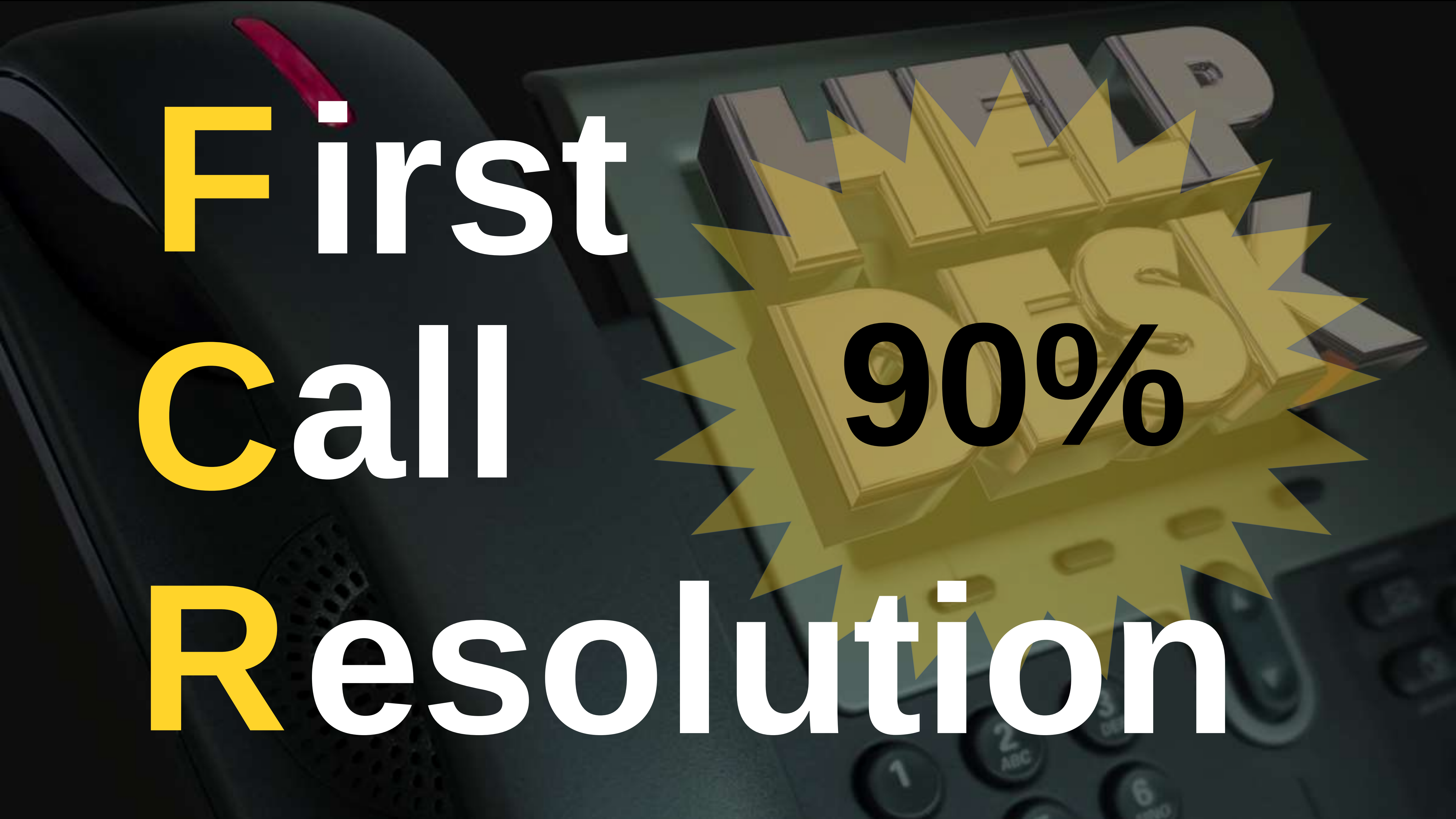
- Programs Office - Customer Success ¯_(ツ)_/¯
- B.S. MIS – Univ of Texas at Arlington
- Credentials:
  - COMPTIA A+ & Sec+
  - (ISC)2 SSCP & CISSP
  - GIAC – Certified Penetration Tester (GPEN)
- DC214 / DHA / ISSA / NTXCSG +++
- Travel-Hacker
- Shitty SysAdmin 💩

📞 💩 💻

WARNING!

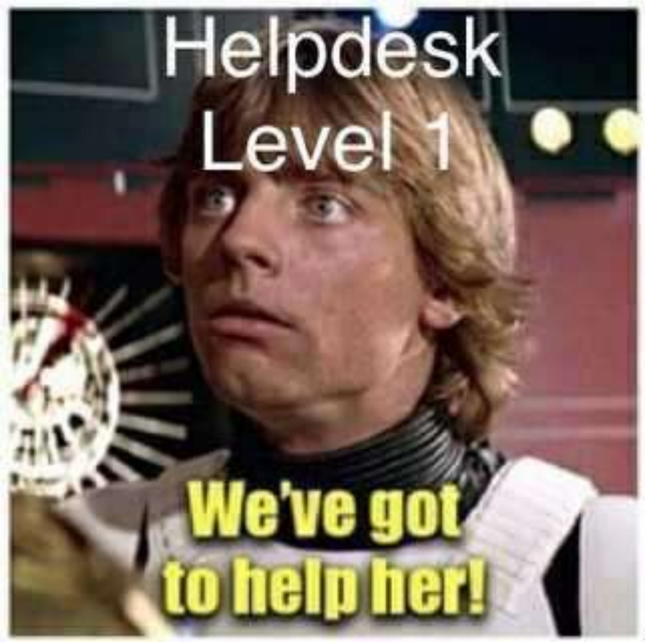
- Lots of TLA’s ahead.
- Take notes.
- Quiz later.

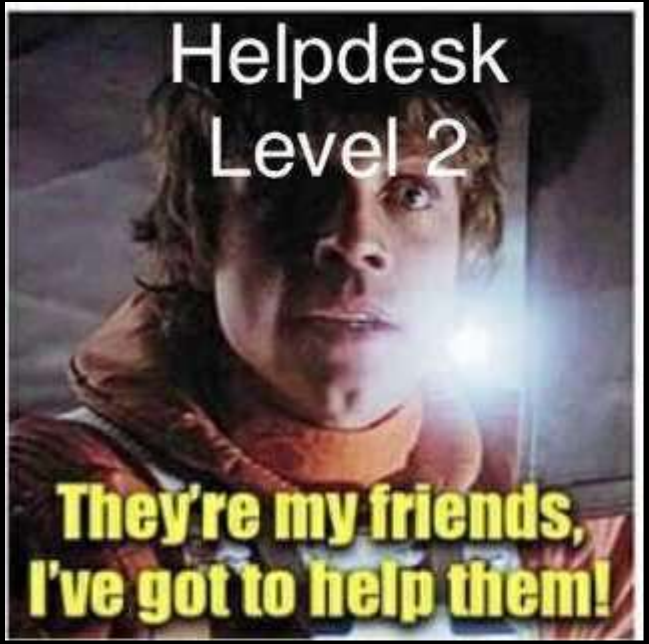
Service Level Agreement



First
Call
Resolution

90%



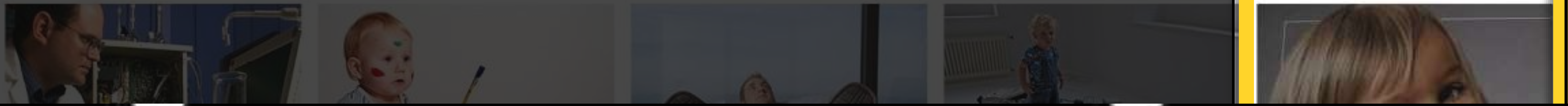


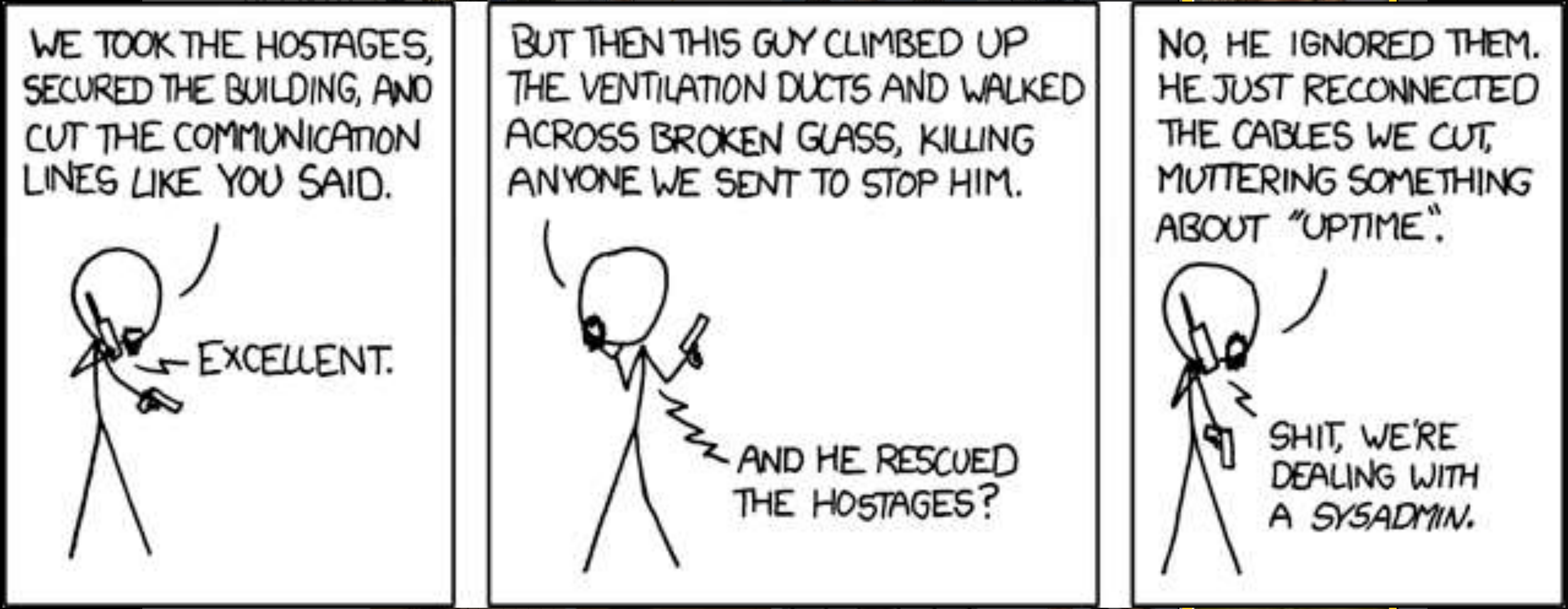
SYSTEM ADMINS

I AM THE KEYMASTER
OpenDNS
I LOVE
FASTER SAFER
MORE SECURE
BETTER DNS
SysAdmin
ARE YOU THE GATEKEEPER?

DEVELOPERS | DESIGNERS | PROJECT MANAGERS | QA | SYSADMINS

SEEN BY




WE TOOK THE HOSTAGES, SECURED THE BUILDING, AND CUT THE COMMUNICATION LINES LIKE YOU SAID.
EXCELLENT.
BUT THEN THIS GUY CLIMBED UP THE VENTILATION DUCTS AND WALKED ACROSS BROKEN GLASS, KILLING ANYONE WE SENT TO STOP HIM.
AND HE RESCUED THE HOSTAGES?
NO, HE IGNORED THEM. HE JUST RECONNECTED THE CABLES WE CUT, MUTTERING SOMETHING ABOUT "UPTIME".
SHIT, WE'RE DEALING WITH A *SYSADMIN*.

SEEN BY
SYSADMINS

Confidentality

Integrity

Availability

Availability
Availability
Availability

Systems Administrator

What my friends think I do

What society thinks I do

What my boss thinks I do

What my users think I do

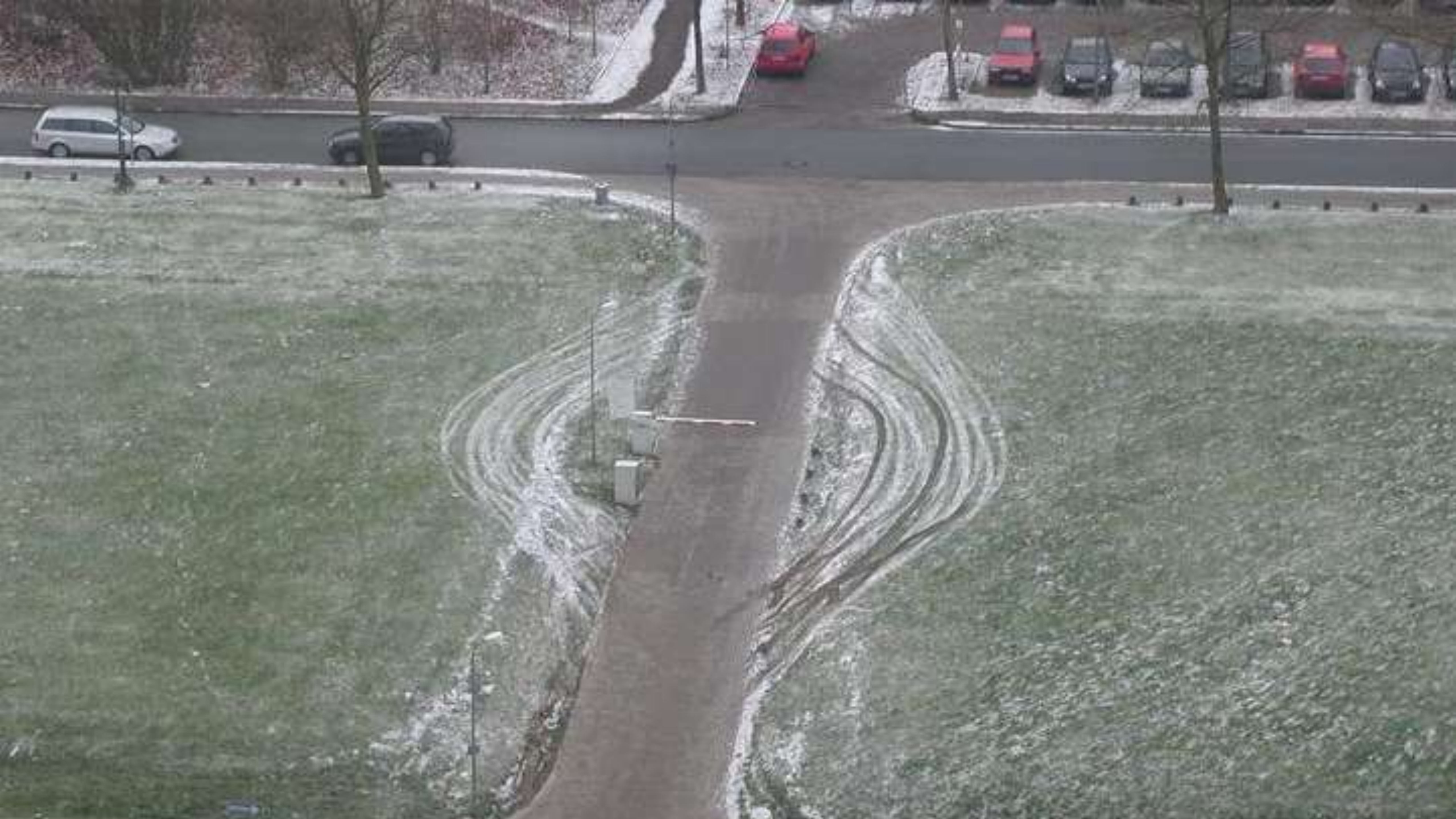
What I think I do

What I actually do

How I took the name Rainmaker?

¯_(ツ)_/¯

FREE WIFI



MFA

*****

Compliance!

YOU'RE BAD
AND YOU SHOULD FEEL BAD

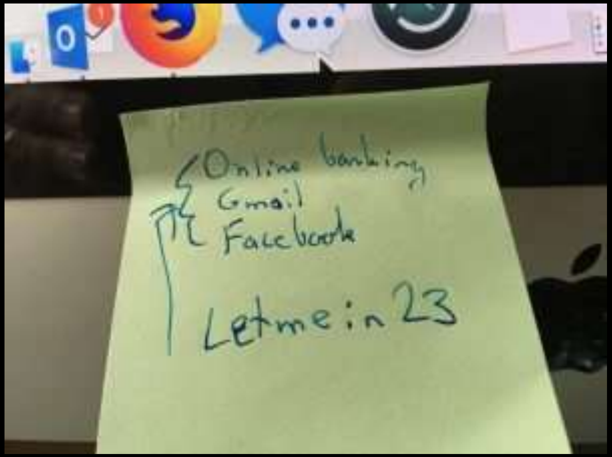
i've seen things...
terrible things...

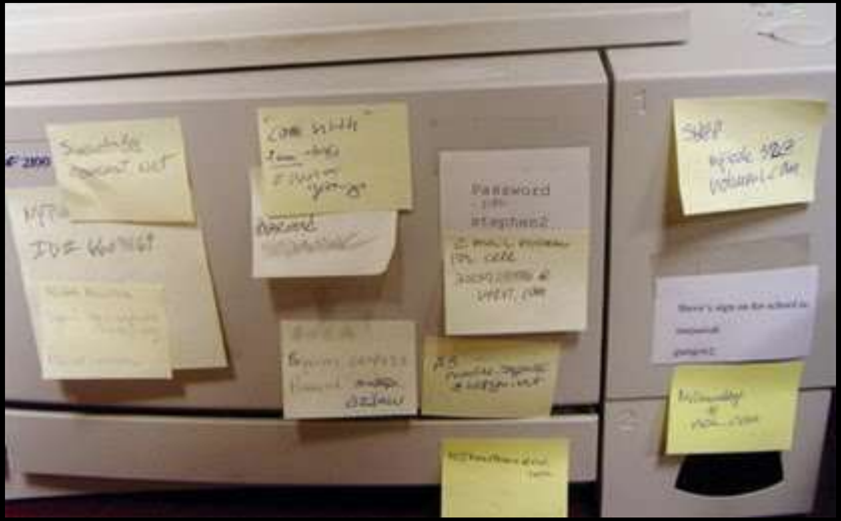
Exposed Passwords

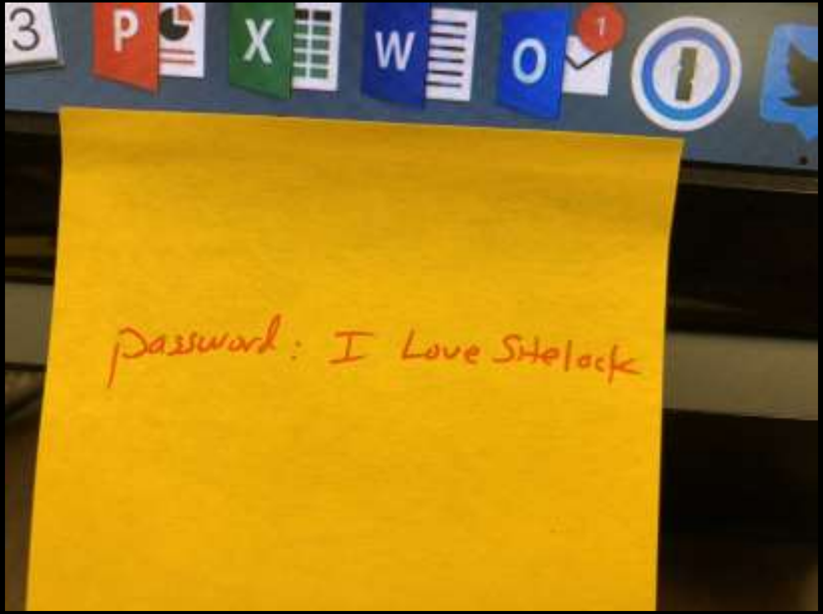
If you're dumb enough to leave your login on a PostIt on your desk, it’s not a hack. It’s barely social engineering. It’s more like natural selection.

- *Gilfoyle*

DESKTOP PASSWORD:
r4ewo1ss89

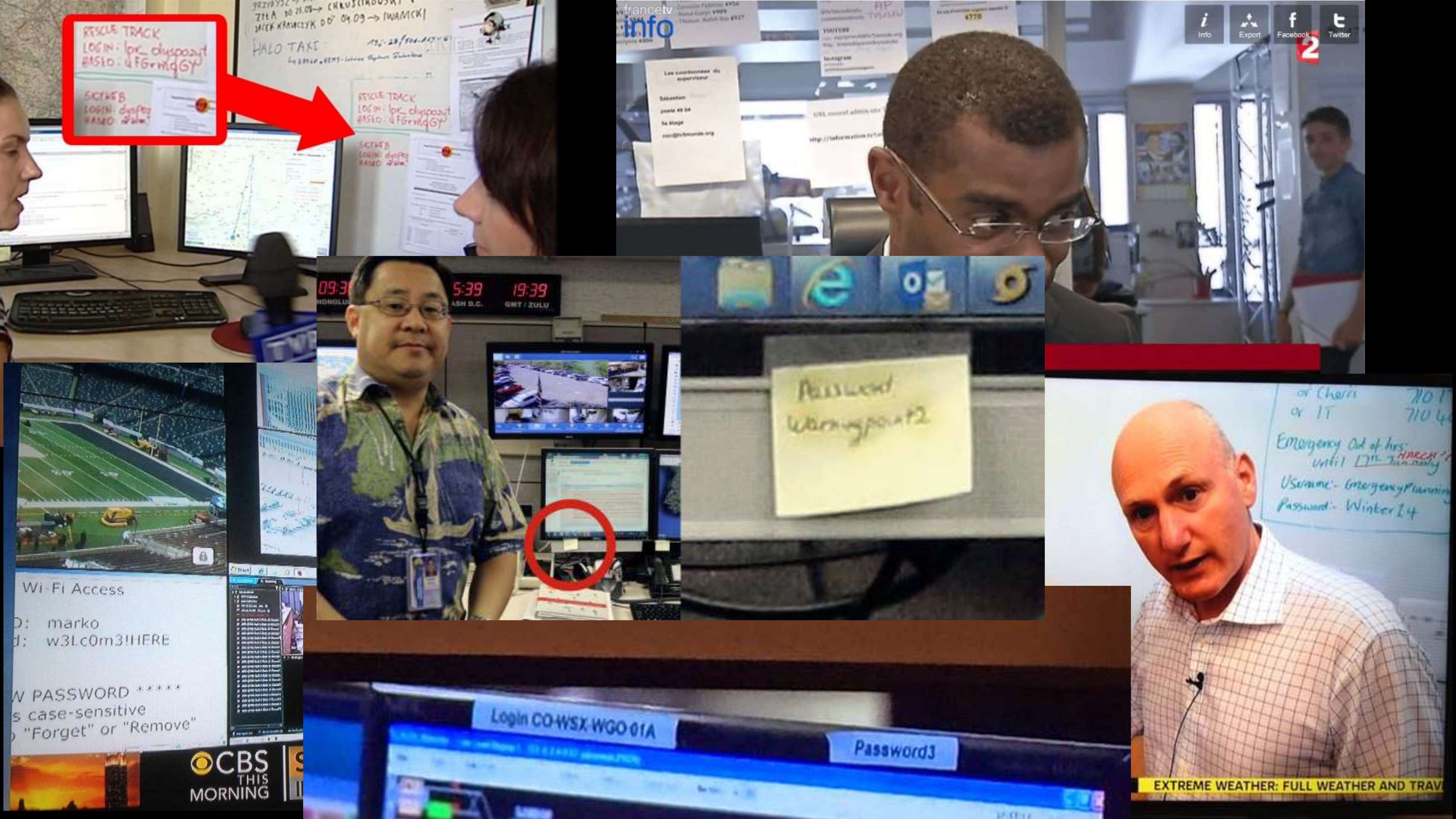

Online banking
Gmail
Facebook
Letmein23


Password
#Stephen2


password: I Love Sitelock

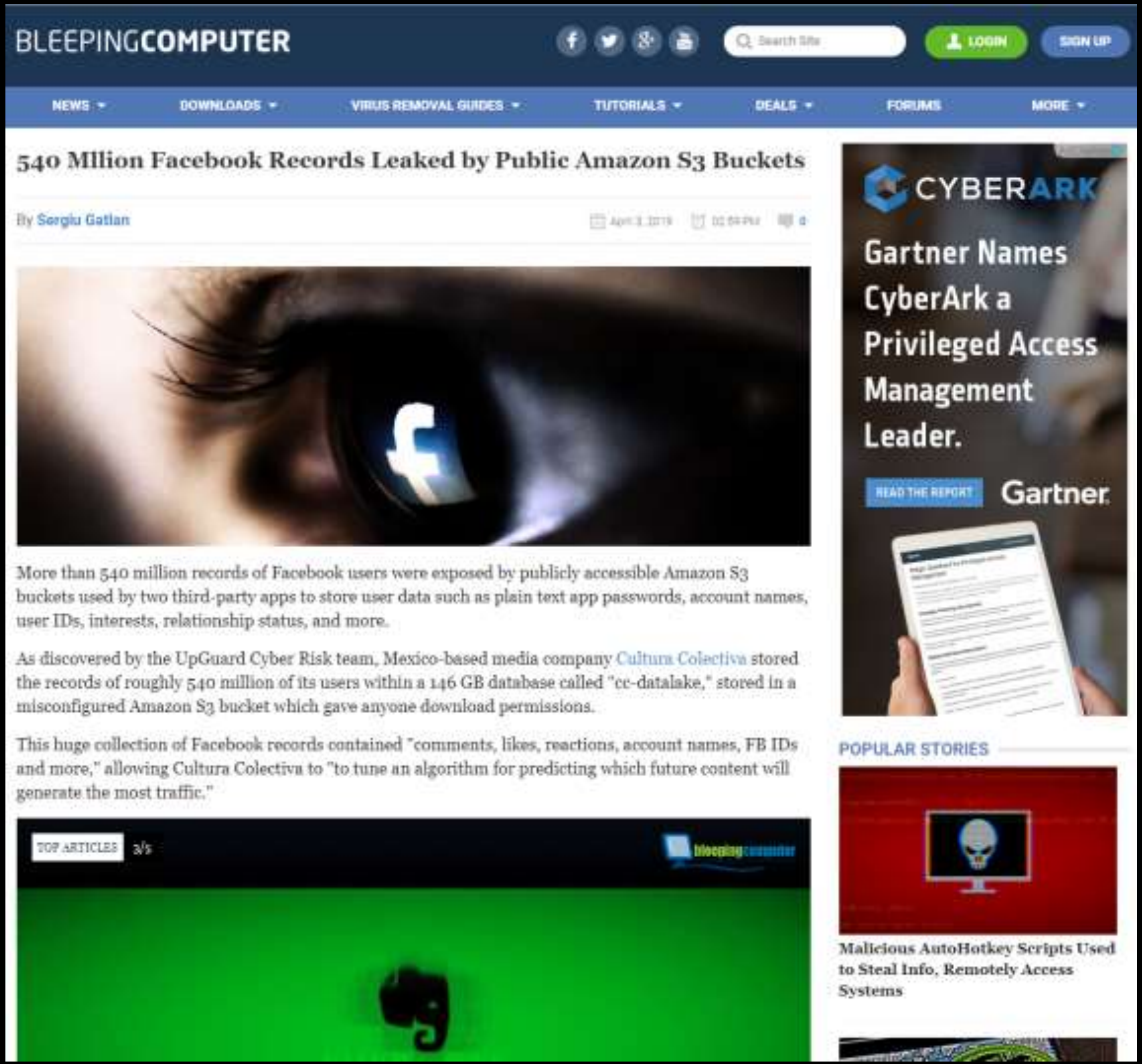
Bank pswd:
lucky 77
yahoo: mary 7916
pswd: eric 3132004
AMD Turion X2

MAKE A
GREAT A


RESCUE TRACK
LOGIN: lpr_dyspozyt
HASŁO: uFGrmqGY
SKYHEB
LOGIN: dyspoz
ZIĘA DO 25.09 → CHRUŚCIKOWSKI
JACEK KRAWCZYK DO 04.09 → IWAMCKI
HALO TAXE
franceTV info
Info
Export
Facebook
Twitter
Les coordonnées du superviseur
Sébastien
09:3
5:39
19:39
HONOLU
ASH D.C.
GMT / ZULU
Password
Warningpoint2
or Chem
or IT
710
710 4
Emergency Out of hrs:
until 17th MARCH
Username:- EmergencyPlanning
Password:- Winter14
EXTREME WEATHER: FULL WEATHER AND TRAV
Wi-Fi Access
D: marko
d: w3Lc0m3!HERE
W PASSWORD *****
s case-sensitive
"Forget" or "Remove"
CBS THIS MORNING
Login CO-WSX-WGO 01A
Password3

Misconfiguration in the news.

According to Gartner, through 2023 at least 99% of cloud security failures will be the customer’s fault.



540 Mllion Facebook Records Leaked by Public Amazon S3 Buckets

By Sergiu Gatlan · April 3, 2019 · 02:04 PM · 0

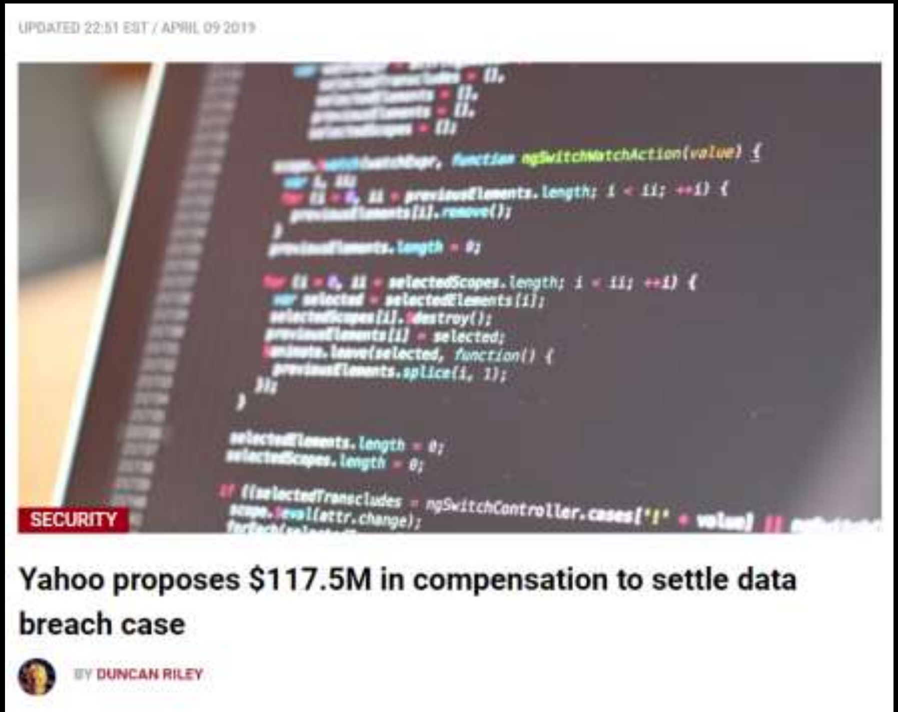
More than 540 million records of Facebook users were exposed by publicly accessible Amazon S3 buckets used by two third-party apps to store user data such as plain text app passwords, account names, user IDs, interests, relationship status, and more.

As discovered by the UpGuard Cyber Risk team, Mexico-based media company Cultura Colectiva stored the records of roughly 540 million of its users within a 146 GB database called "cc-datalake," stored in a misconfigured Amazon S3 bucket which gave anyone download permissions.

This huge collection of Facebook records contained "comments, likes, reactions, account names, FB IDs and more," allowing Cultura Colectiva to "to tune an algorithm for predicting which future content will generate the most traffic."

POPULAR STORIES

Malicious AutoHotkey Scripts Used to Steal Info, Remotely Access Systems



UPDATED 22:51 EST / APRIL 09 2019

Yahoo proposes $117.5M in compensation to settle data breach case

BY DUNCAN RILEY

Misconfiguration Leads to Major Health Data Breach

UW Medicine Notifying Nearly 1 Million Patients of Data Exposure

Marianne Kolbasuk McGee (HealthInfoSec) • February 21, 2019

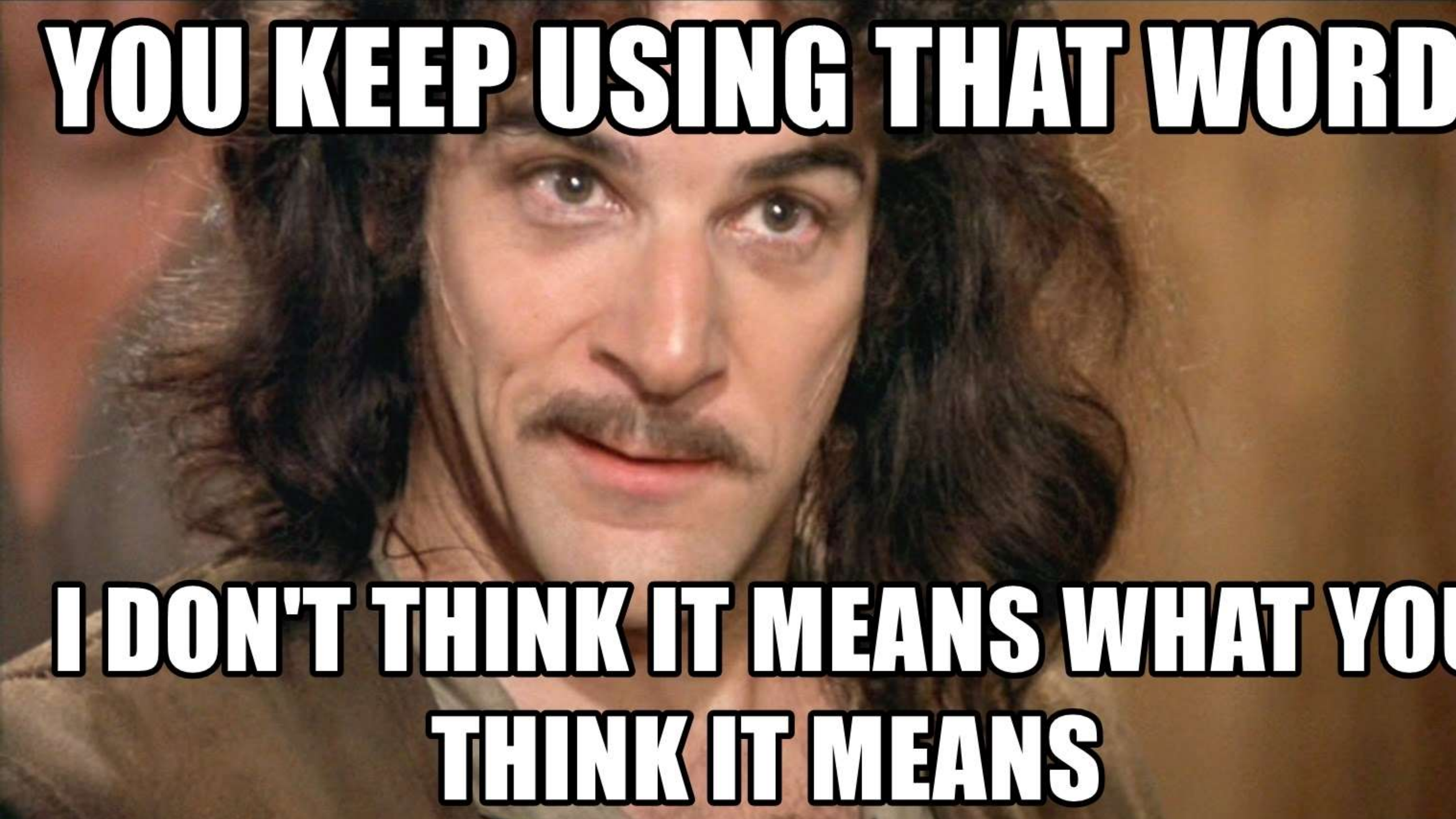
https://www.fugue.co/blog/the-human-factor-in-cloud-misconfiguration

PROFI
TRUFFLEHOG

IT'S APRIL
FOOLS!

18+

FOR ADULTS ONLY


YOU KEEP USING THAT WORD
I DON'T THINK IT MEANS WHAT YOU
THINK IT MEANS

PING

TO BE HONEST...

BURNING THE SHIPS

BRAND-JACKING

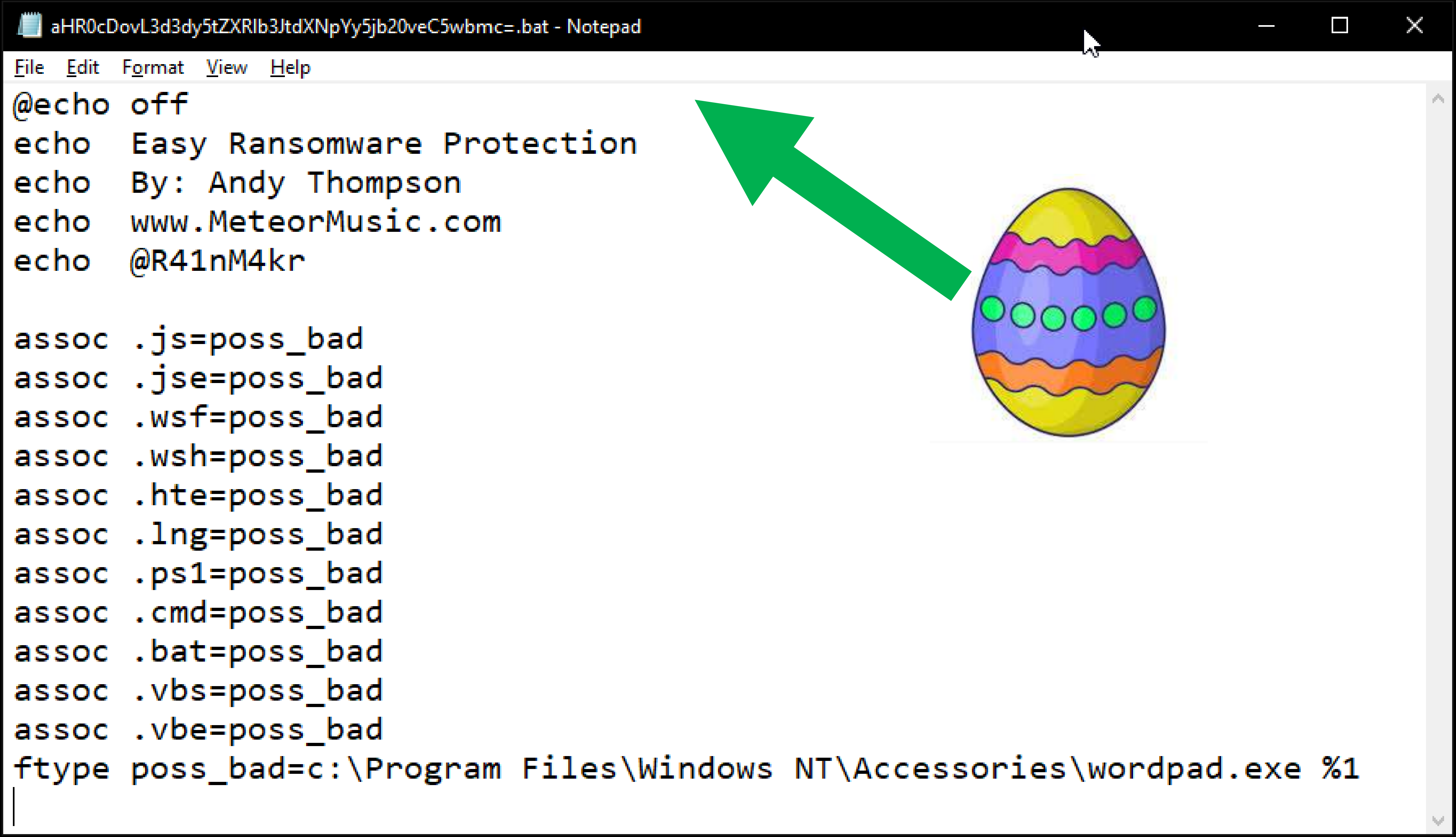
OPEN THE KIMONO

HACKING

IS NOT A CRIME

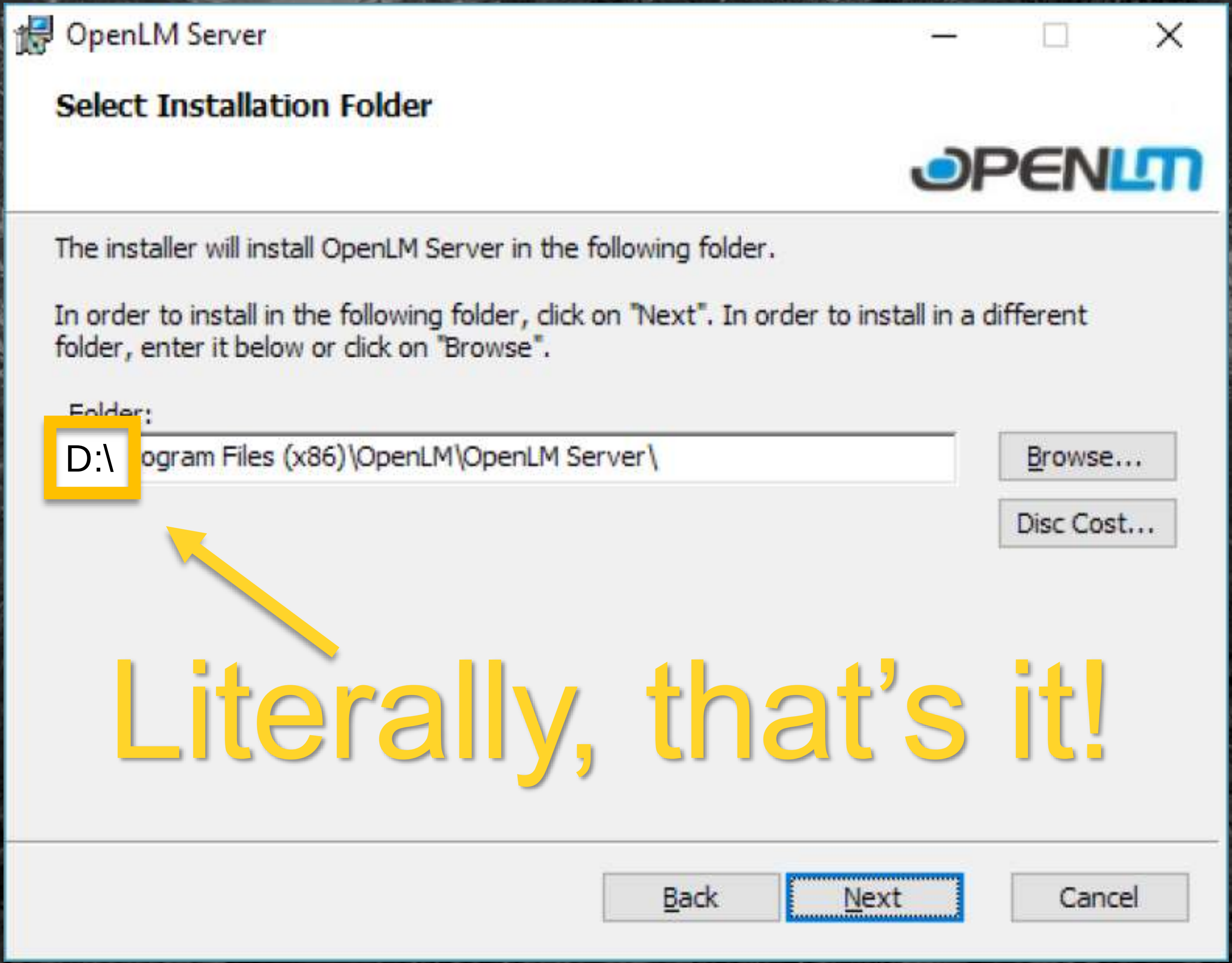
HACKING

I’ve seen some good things too…



```
@echo off
echo  Easy Ransomware Protection
echo  By: Andy Thompson
echo  www.MeteorMusic.com
echo  @R41nM4kr

assoc .js=poss_bad
assoc .jse=poss_bad
assoc .wsf=poss_bad
assoc .wsh=poss_bad
assoc .hte=poss_bad
assoc .lng=poss_bad
assoc .ps1=poss_bad
assoc .cmd=poss_bad
assoc .bat=poss_bad
assoc .vbs=poss_bad
assoc .vbe=poss_bad
ftype poss_bad=c:\Program Files\Windows NT\Accessories\wordpad.exe %1
```



Select Installation Folder

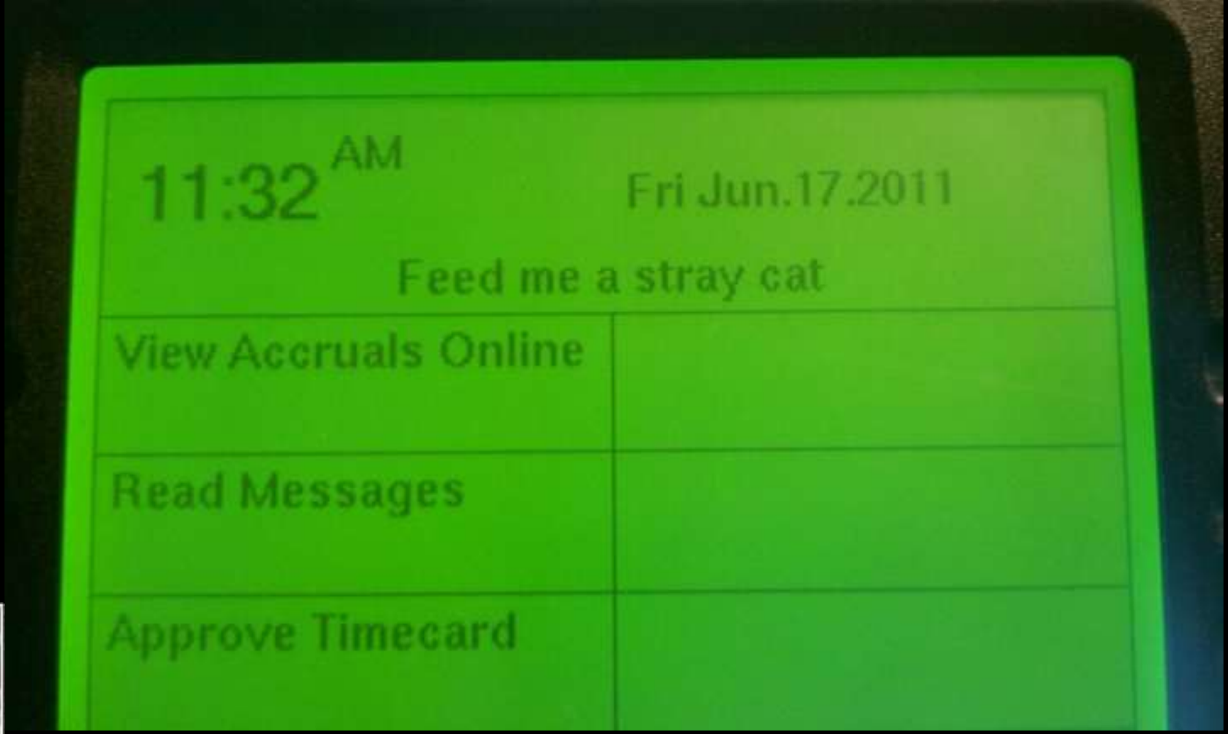
The installer will install OpenLM Server in the following folder.

In order to install in the following folder, click on "Next". In order to install in a different folder, enter it below or click on "Browse".

Folder:

D:\ ogram Files (x86)\OpenLM\OpenLM Server\

Literally, that’s it!



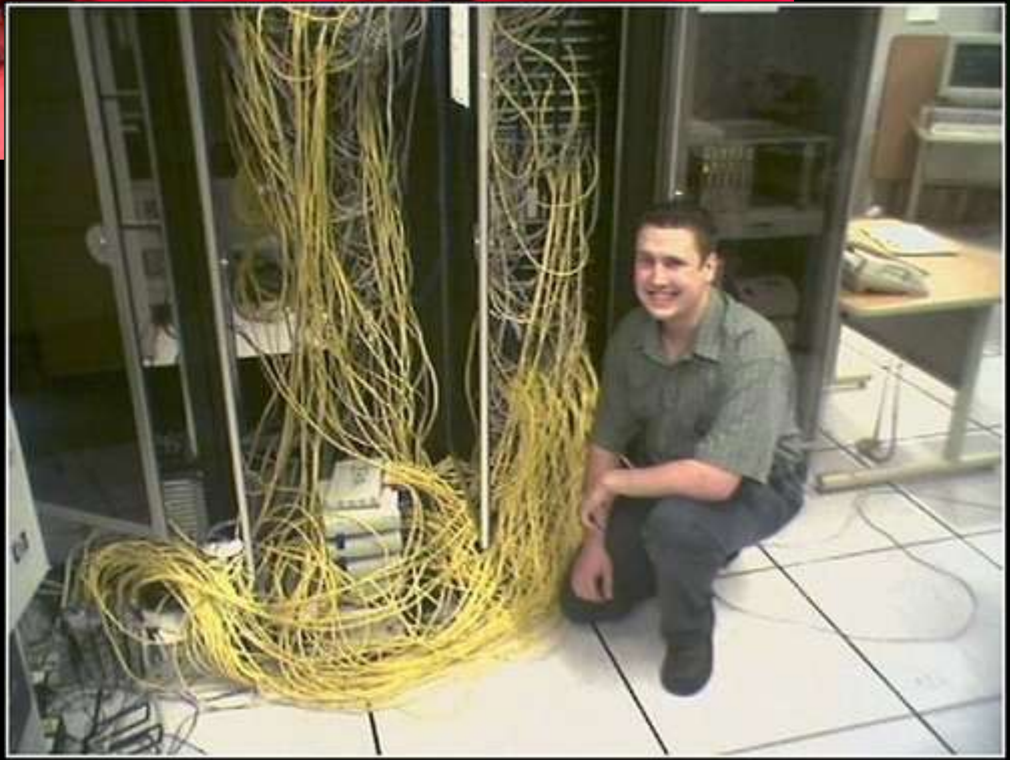
11:32 AM Fri Jun.17.2011

Feed me a stray cat

View Accruals Online

Read Messages

Approve Timecard



LOOK
TEL

Experience vs. Certification

VISA

CompTIA A+

CompTIA Security+

SSCP®

CISSP®

CCSP®

HCISPP®

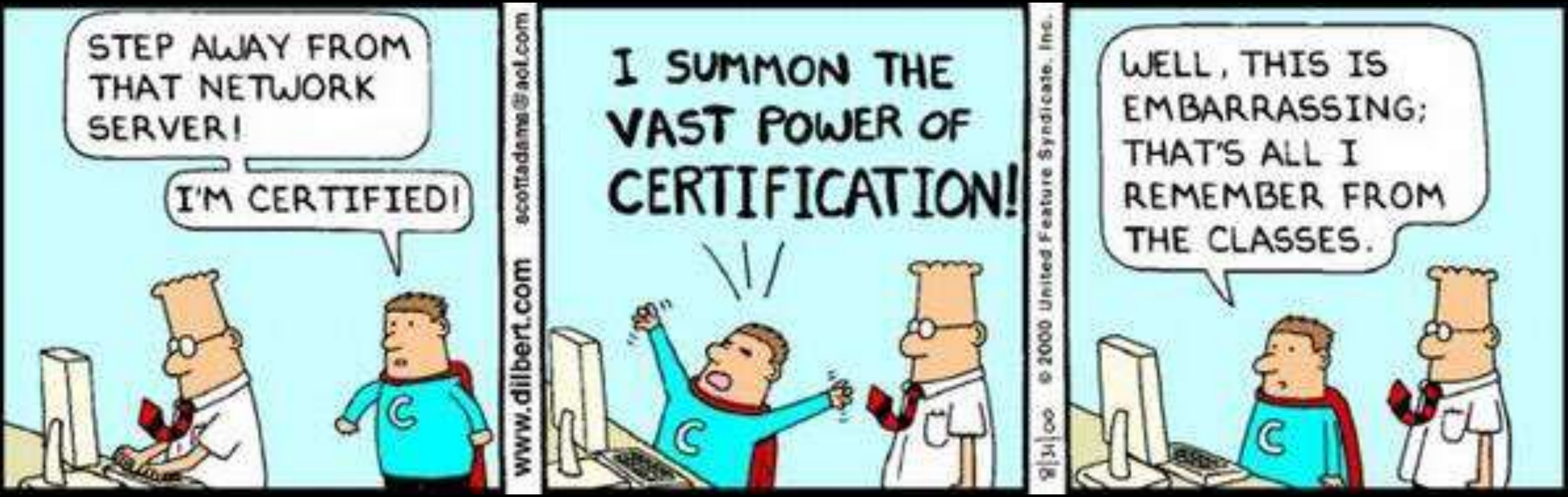
C|EH
CERTIFIED
ETHICAL HACKER

GIAC CERTIFIED PENETRATION TESTER
GPEN

OFFENSIVE® security
OSCP

OFFENSIVE® security
OSCE

???

STEP AWAY FROM THAT NETWORK SERVER!
I'M CERTIFIED!
scottadams@aol.com
www.dilbert.com
I SUMMON THE VAST POWER OF CERTIFICATION!
9|14|00 © 2000 United Feature Syndicate, Inc.
WELL, THIS IS EMBARRASSING; THAT'S ALL I REMEMBER FROM THE CLASSES.

SafePlace SM

Dragnet video here

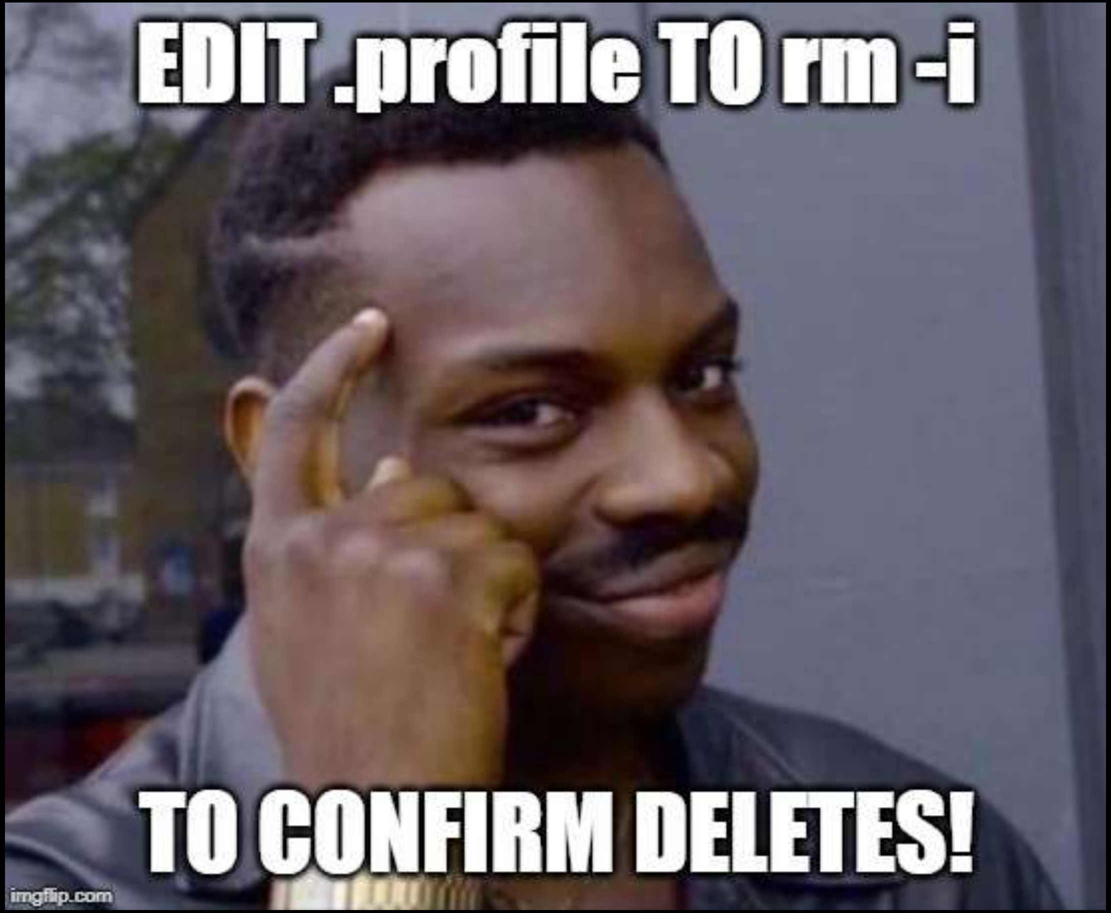
```
uname -s
```

Checks machine name properties of remote server

```
uname -s
```

RENAMES HOST

rm –rf /



+

Welcome to GeoCities
Your Home On The Web!

What does this symbol mean?

Today's Cool Home Page

[illegible]

Enter Here!

Tell us what you think!
Take the first GeoCities User Survey!

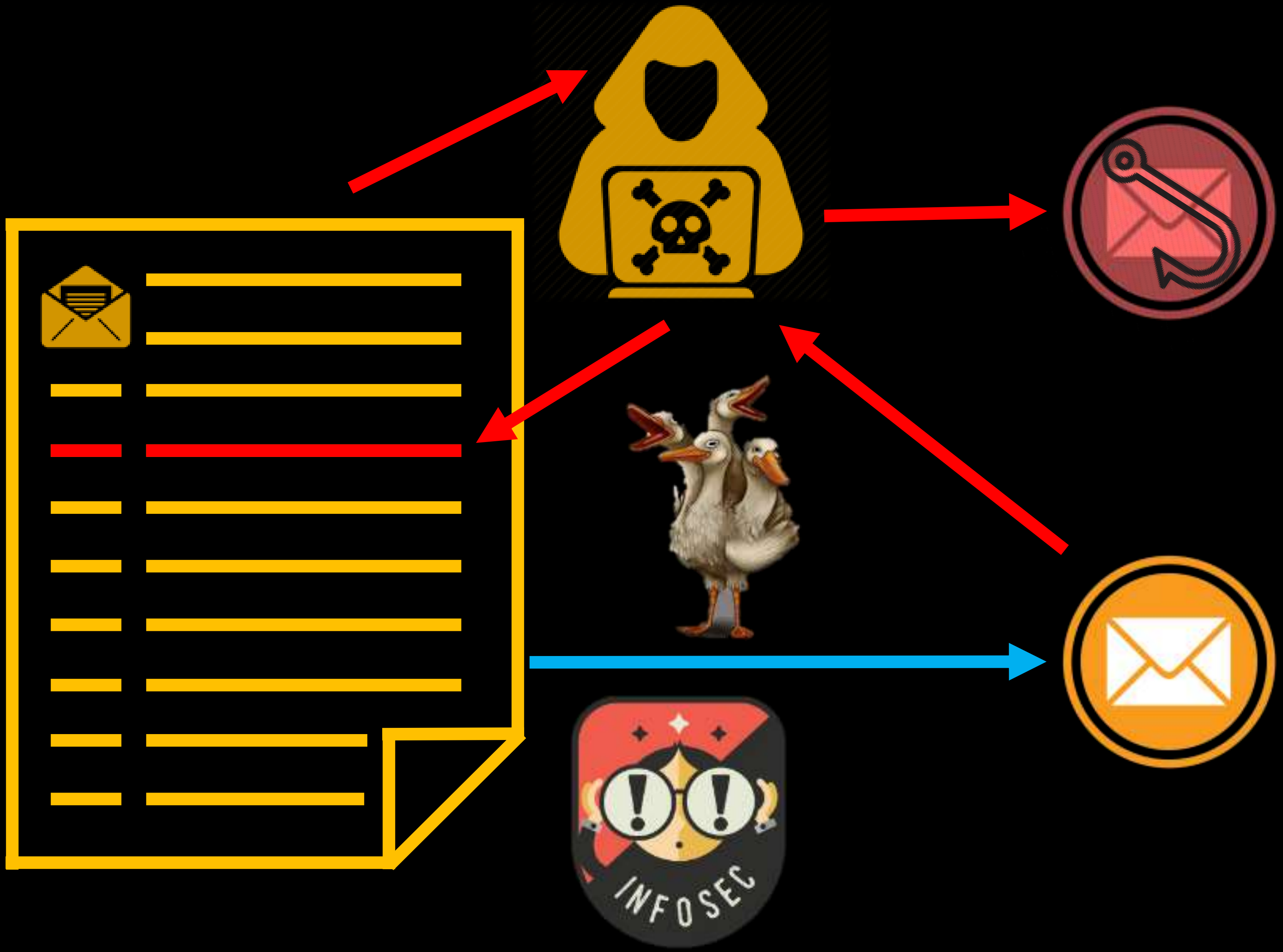
TAKE STOCK!

[illegible]

[illegible]

+

WayBackMachine


INFOSEC

SysAdmin Quiz

• SLA	Service Level Agreement
• FCR	First Call Resolution
• CIA	Confidentiality Integrity Availability
• AAA	Availability^3
• WTFBBQ	Shrug

Key Takeaways

- Prioritize Security.
- Don’t cut corners.
- Watch the Watchers
- Systems are more vulnerable to misconfiguration vs traditional exploits.
- SysAdmins are people too.

WARNING!

- Risk is EVERYWHERE.
- Learn from these mistakes.
- Don’t let this happen to you.

Parting Advice

- Blame the previous sysadmin.
- Blame the vendor.
- Prepare 3 envelopes.

Thank You!

Andy@MeteorMusic.com
@R41nM4kr
www.MeteorMusic.com