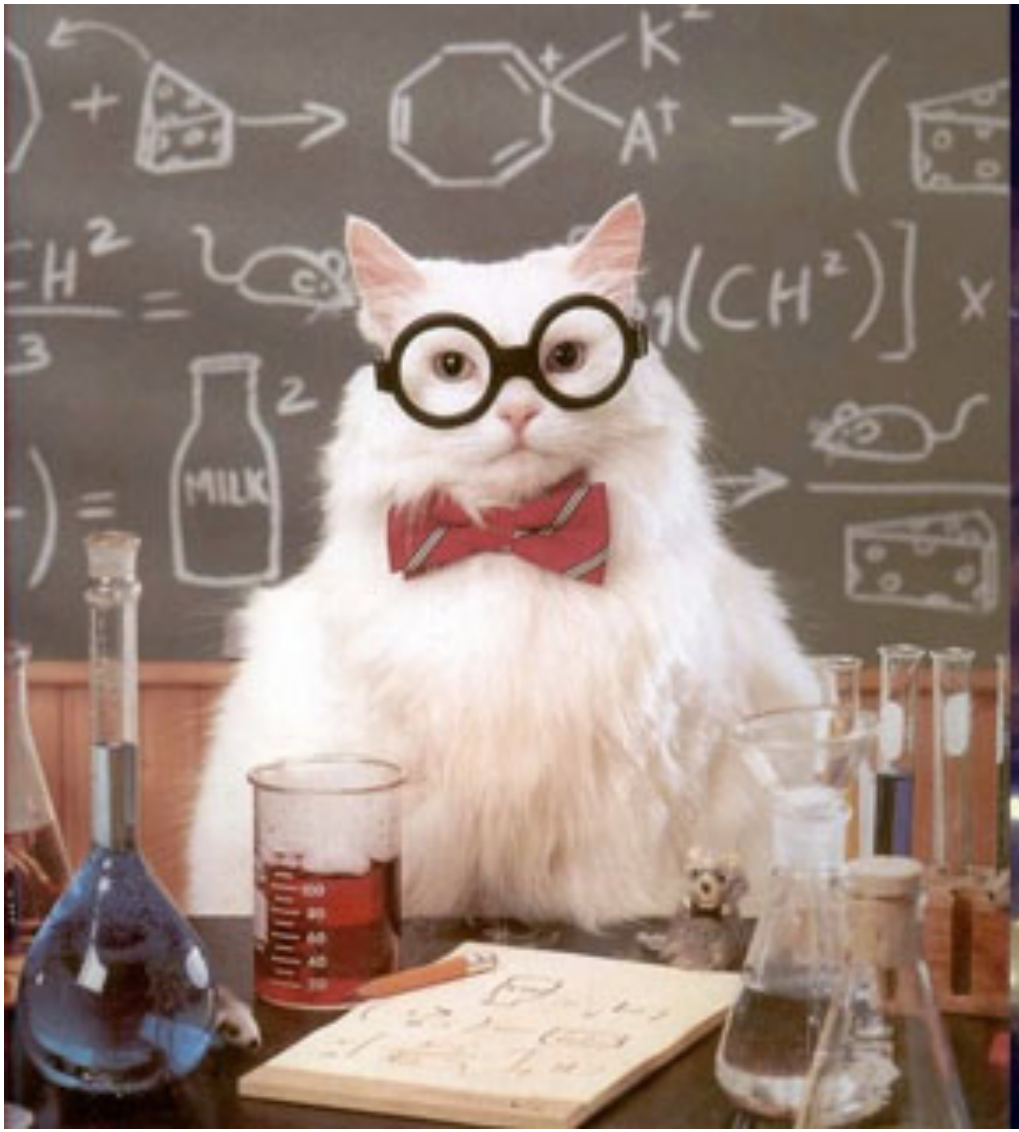

MILK

I'm the one who DOESN'T knock!

Who am I?

Twitter: @JaysonStreet

You keep using that word. I do not think it means what you think it means.

Everyone keeps repeating the term
Advance Persistent Threats like a broken record!

Why not throw some love to Basic Adorable Destruction?!?

We all know how easy it is to just be BAD!

The key indicators of a person doing BAD

1.RECON Mode is only about 2 hours of Google & Victims own website. (Though I've never used the full 2 hours yet)

2.SE Mode is usually walking into victims location and winging it (note sometimes without doing #1)

3.Pwnage Mode is basically plugging in a device to the victims computer or network (sometimes with their help)

4.????

5.Profit!?!

So let's break down the 3 best approaches I've used to be BAD

1. Tech, Repair Guy, Delivery, Job Applicant, Customer, Wanderer

2. Auditor, Executive, Policy Enforcement

3. Crazy Off The Wall Personalities (Not recommended but totally fun and usually work)

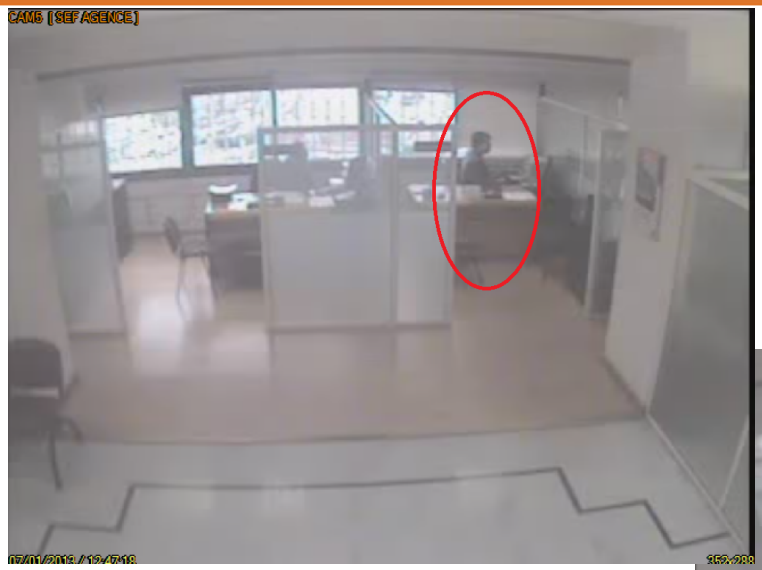
Story Time

The Beirut Bank Job!

@hackerstrip

http://hackerstrip.com

The Beirut Bank Job!



The Beirut Bank Job!

Time from 1st walk into door to full access to bank.
= 2 minutes & 22 seconds

The Beirut Bank Job!

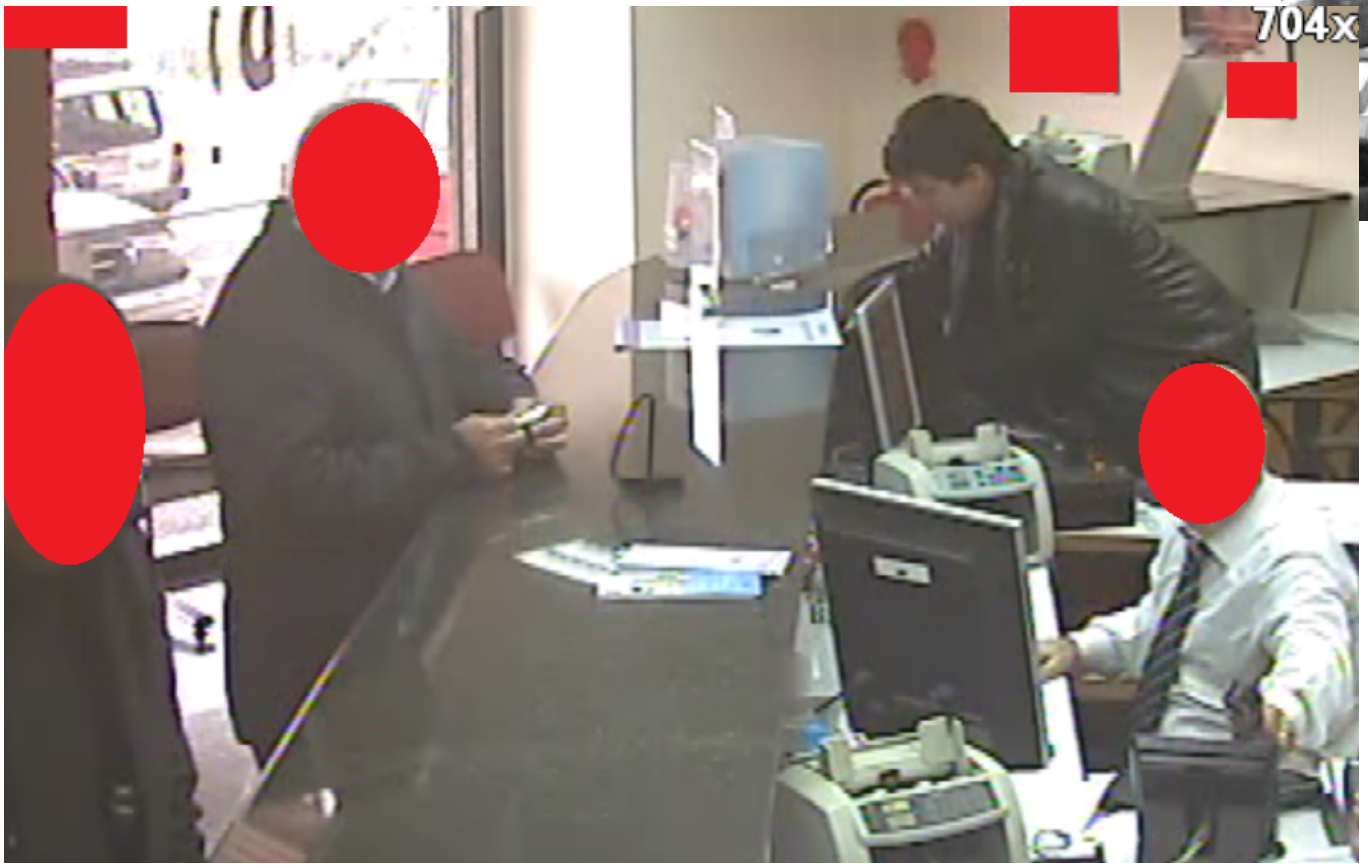
The Beirut Bank Job!

So I have the employee ID, password & smart card! Now I need their PC and Network access

I was there doing BAD things for over TWENTY MINUTES! WITHOUT BEING STOPPED!

The Beirut Bank Job!

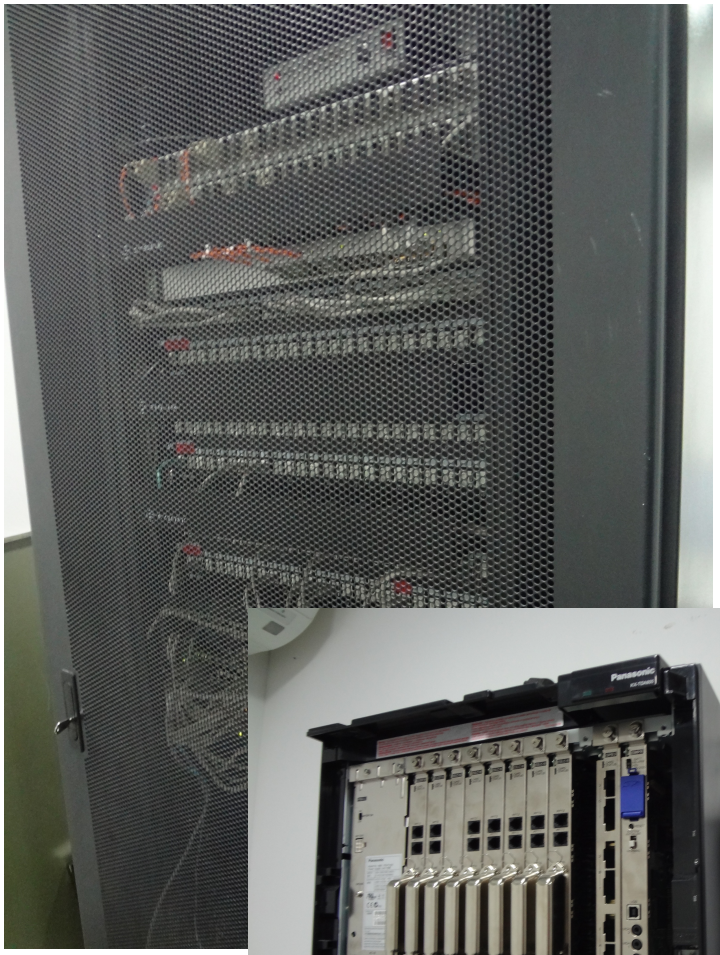
Well I needed a computer!



The Beirut Bank Job!

Well I got a computer!

The Beirut Bank Job!



Last I needed access to their internal network!..... OK DONE!

Sad State of Security at the State Treasury

Sad State of Security at the State Treasury

Rules of Engagement

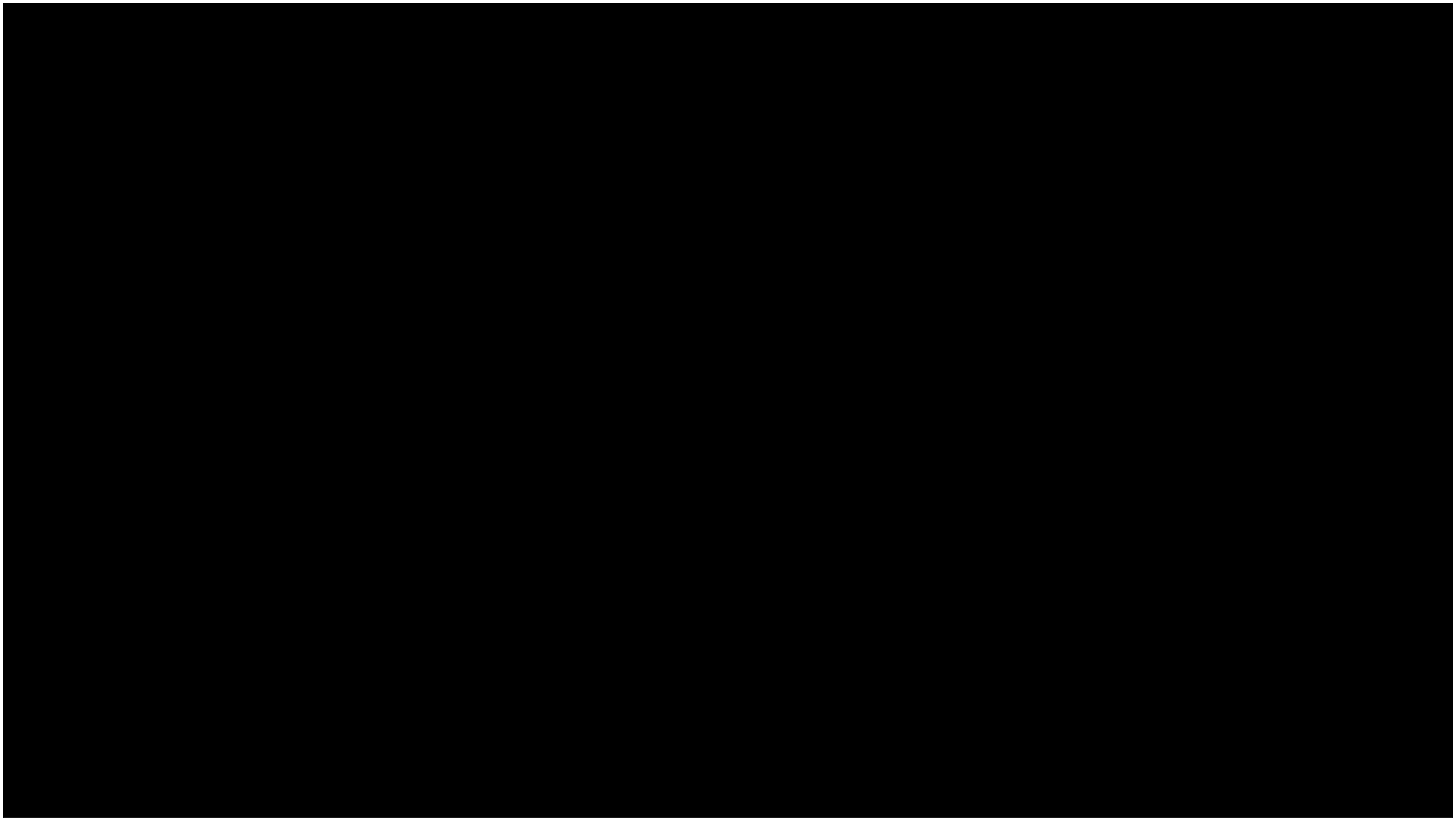
1.Talk to no one coming in or out of the building.

2. Only stay in the public areas if you do get in.

3. You can only talk to the cleaners but you are not allowed to lie to them!

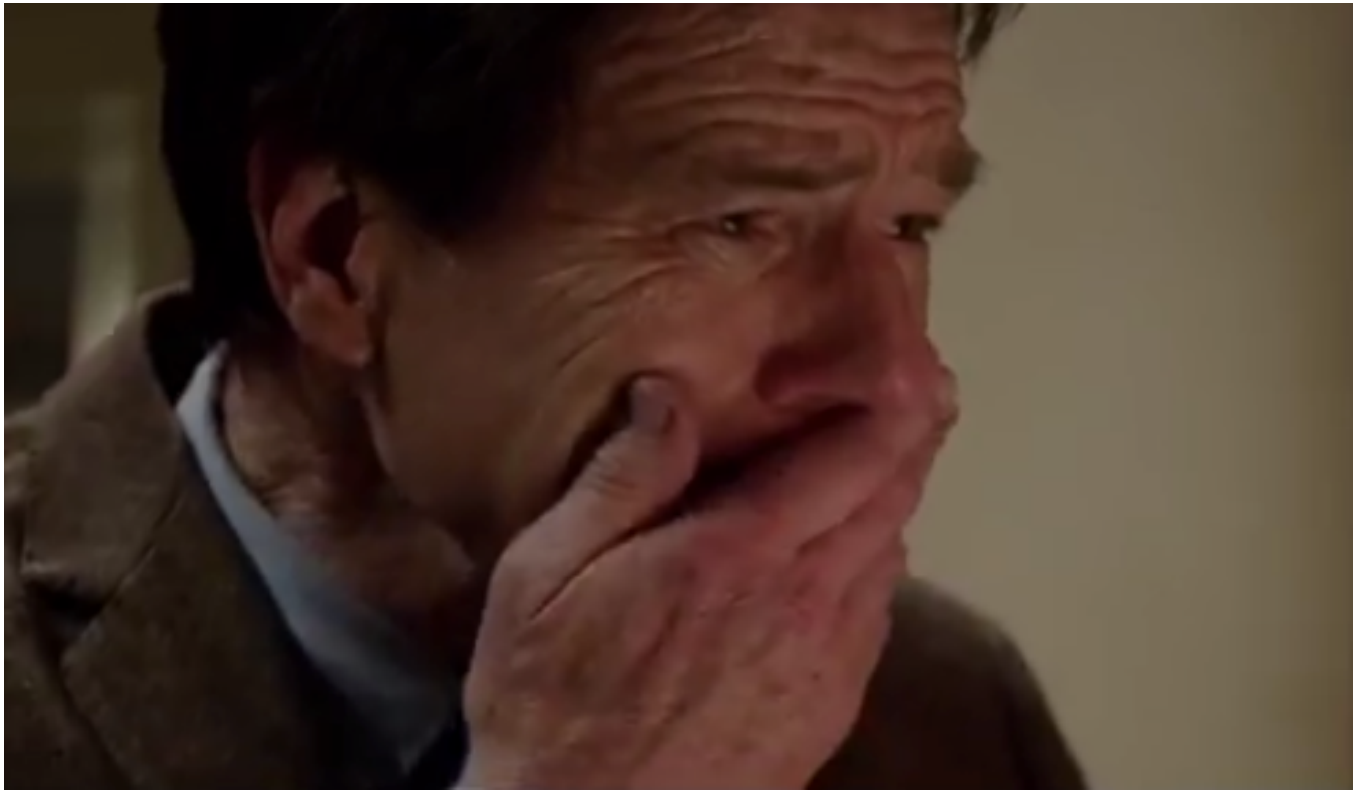
How did that work out for them?!?

How did that work out for them?!?



Seriously are you really buying this story?!?

Jayson and the Terrible, Horrible, No Good, Very Bad Social Engineering Engagement!



Target – Charity organization
(It was in scope they were on the same network I promise!)

Pretext – Visiting TV Producer from America doing a show on companies doing great works in their communities.

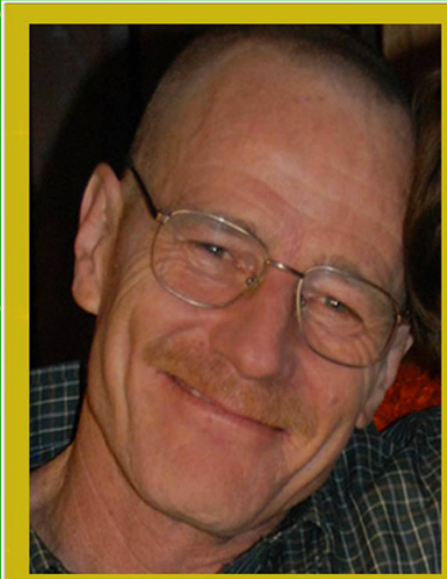
Outcome – Total compromise of the entire organization & target company!

Results – I felt really BAD PWNing them so harshly!

Summary

Walter White

Father, Husband & Teacher



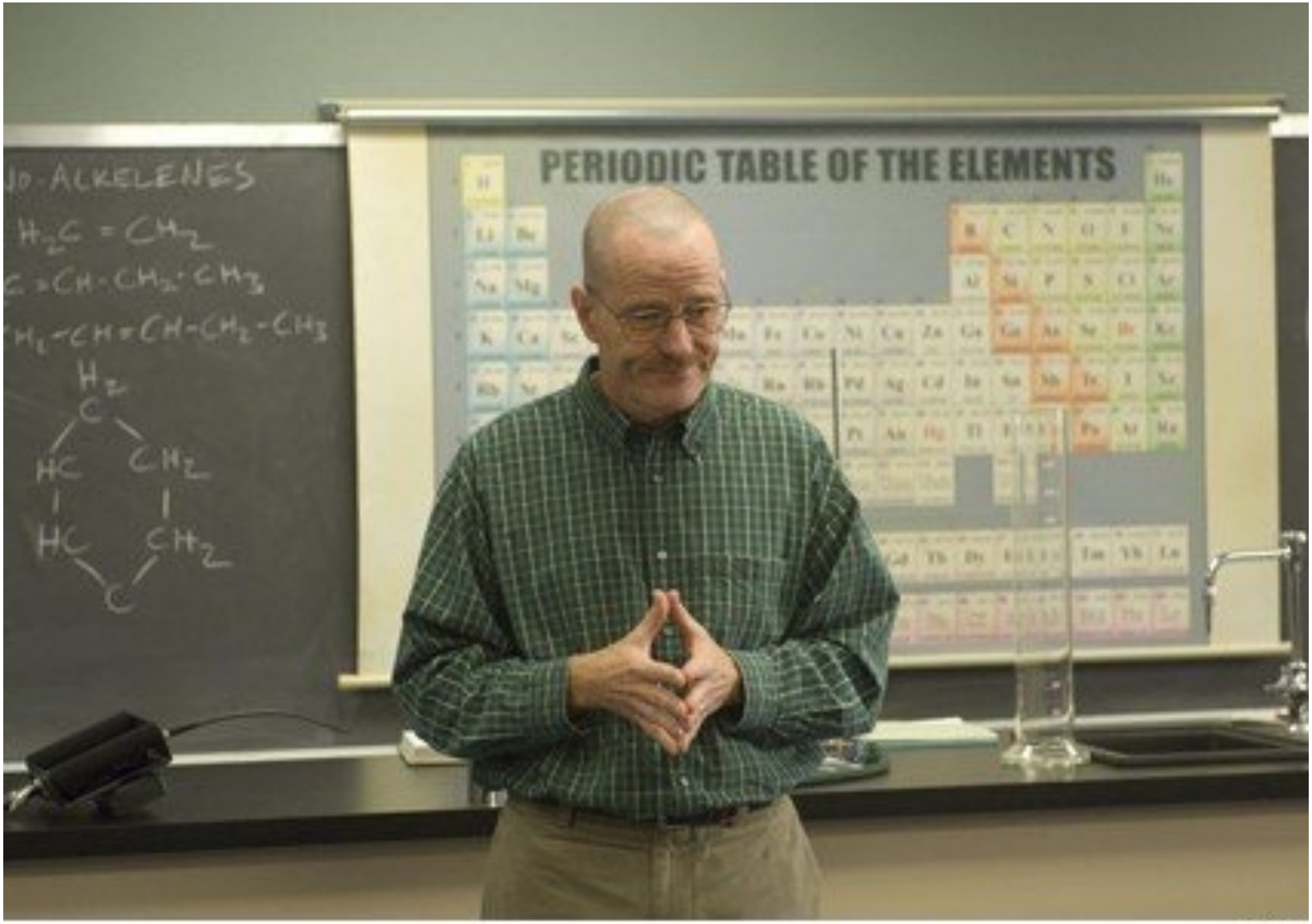
The Three E's

Educate

Empower

Enforce

Educate



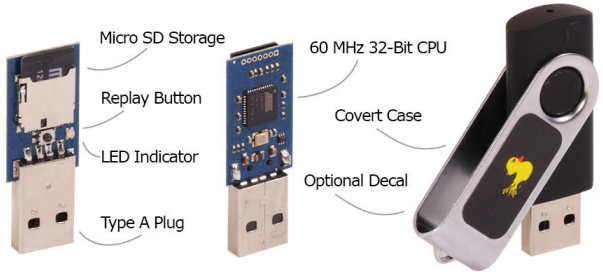
Educate

We have learned to be afraid of people with these!

(Well maybe not scared of these guys) ;-)

Educate

But not people with THESE!



Educate

OR THESE!!!!

Educate

I’m not saying these has malware on it…….YET!!! ☺

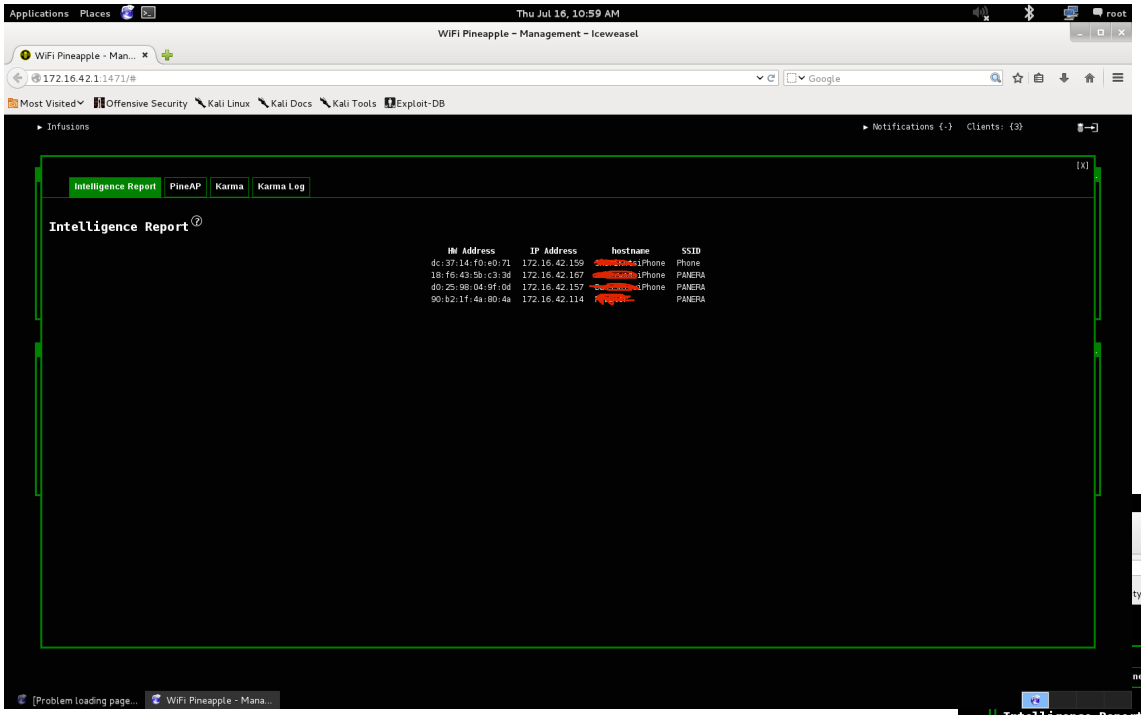
Educate

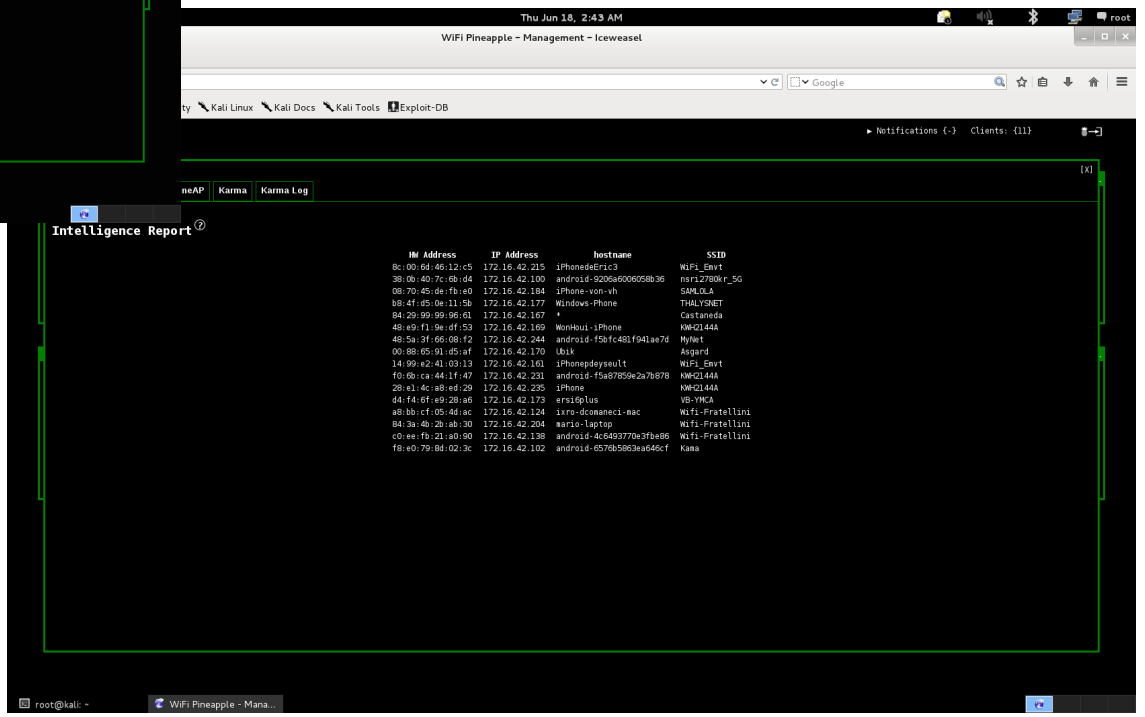
1. Teach employees common dangers they face not only at work but at home as well! Make them security conscious by default not by policy!

2. Drive home the fact that “Stranger Danger” is a good policy no matter how old you are!

3. Create teachable events year round not an annual exercise in futility!

Educate


Applications Places
Thu Jul 16, 10:59 AM
root
WiFi Pineapple – Management – Iceweasel
WiFi Pineapple - Man...
172.16.42.1:1471/#
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Infusions
Notifications {-}
Clients: {3}
Intelligence Report
PineAP
Karma
Karma Log
Intelligence Report
HW Address
IP Address
hostname
SSID
dc:37:14:f0:e0:71 172.16.42.159 iPhone Phone
18:f6:43:5b:c3:3d 172.16.42.167 iPhone PANERA
d0:25:98:04:9f:0d 172.16.42.157 iPhone PANERA
90:b2:1f:4a:80:4a 172.16.42.114 PANERA
[Problem loading page...
WiFi Pineapple - Mana...


Thu Jun 18, 2:43 AM
root
WiFi Pineapple – Management – Iceweasel
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Notifications {-}
Clients: {11}
Karma
Karma Log
Intelligence Report
HW Address
IP Address
hostname
SSID
8c:00:6d:46:12:c5 172.16.42.215 iPhonedeEric3 WiFi_Emvt
38:0b:40:7c:6b:d4 172.16.42.100 android-9206a6006058b36 nsri2780kr_5G
08:70:45:de:fb:e0 172.16.42.184 iPhone-von-vh SAMLOLA
b8:4f:d5:0e:11:5b 172.16.42.177 Windows-Phone THALYSNET
84:29:99:99:96:61 172.16.42.167 * Castaneda
48:e9:f1:9e:df:53 172.16.42.169 WonHoui-iPhone KWH2144A
48:5a:3f:66:08:f2 172.16.42.244 android-f5bfc481f941ae7d MyNet
00:88:65:91:d5:af 172.16.42.170 Ubik Asgard
14:99:e2:41:03:13 172.16.42.161 iPhonepdyseult WiFi_Emvt
f0:6b:ca:44:1f:47 172.16.42.231 android-f5a87859e2a7b878 KWH2144A
28:e1:4c:a8:ed:29 172.16.42.235 iPhone KWH2144A
d4:f4:6f:e9:28:a6 172.16.42.173 ersi6plus VB-YMCA
a8:bb:cf:05:4d:ac 172.16.42.124 ixro-dcomaneci-mac Wifi-Fratellini
84:3a:4b:2b:ab:30 172.16.42.204 mario-laptop Wifi-Fratellini
c0:ee:fb:21:a0:90 172.16.42.138 android-4c6493770e3fbe86 Wifi-Fratellini
f8:e0:79:8d:02:3c 172.16.42.102 android-6576b5863ea646cf Kama
root@kali: ~
WiFi Pineapple - Mana...

Educate

Empower

In the end you realize that the only person who can protect you is…
YOU!

Empower

1. Users are not your problem they are part of your solution!

1. Give your employees a way to be effective then let them KNOW about it!

2. Give them opportunities to do the right thing & reward them when they succeed & teach when they fail.

Enforce

Employees must feel valued &
Management must take security seriously

Enforce

1. Do employee see policy being enforced EVENLY throughout the enterprise?

2. Using positive reinforcement sometimes is more effective than the negative kind.

3. Visibility is sometimes all that is necessary!

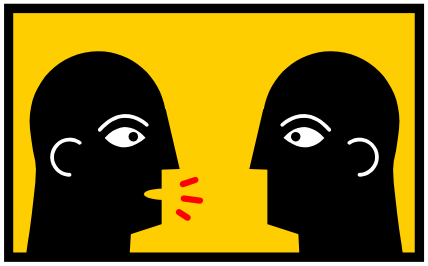
Summary

The only thing necessary for the triumph of evil is for good men to do nothing. ~Edmund Burke 1770 AD

Now let's learn from others

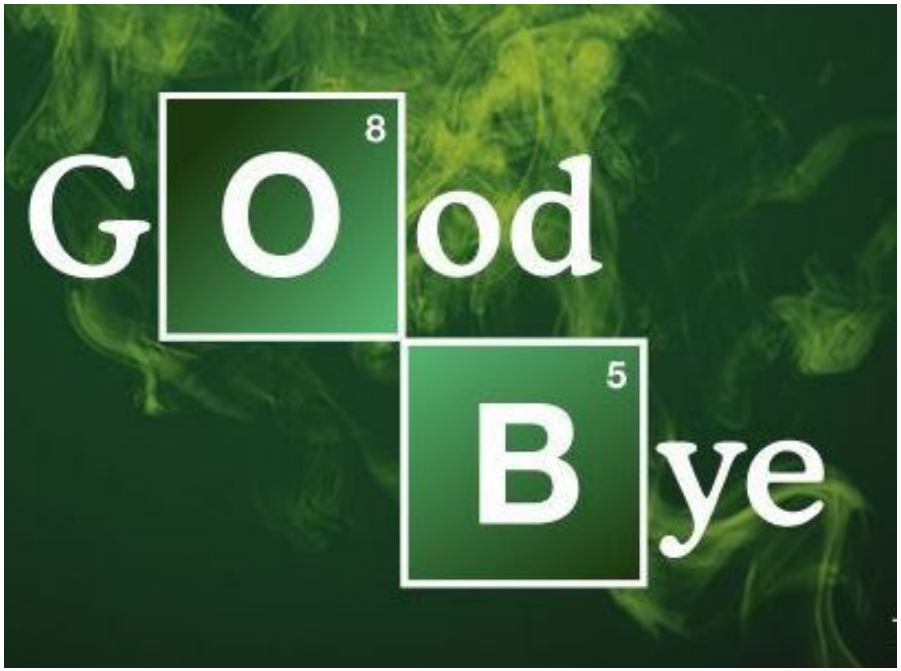
Discussion and Questions????

Or several minutes of uncomfortable silence it's your choice.



This concludes my presentation Thank You

LINKS as you LEAVE



http://pwnieexpress.com/jaysonstreet

Twitter @jaysonstreet

Shout outs to @sehnaoui, Sara Kantor, @Hak5Darren, @Pwnieexpress, @GreyBrimstone, @KentNabors

Company Info

pwn (pōn) ***v.* pwned** - tr. Slang. **1.** To own in the sense of defeat: *Don´t get pwned by network hackers.* **2.** To beat someone or something by a wide margin, usually in relation to a game.

Security Assessment for Remote Sites & Wireless

- Closes huge gap in security infrastructure
- Founded 2010
- Boston HQ & Vermont Research Lab
- Financing: $5.1 million Series A (July 2013)
- Over 1000 accounts globally, 600 Enterprises, & Partner Channel
- Recognition and Awards