Law and Order
Telco Victims Unit (TVU)

Dan Burwitz
IT Security Specialist
Vantage Point Solutions
2211 N. Minnesota St.
Mitchell, SD 57301

(605) 995-1835
dan.burwitz@vantagepnt.com

VantagePoint
EMPLOYEE OWNED

VantagePoint EMPLOYEE OWNED

Today's Speaker

Dan Burwitz

IT Security Specialist

Vantage Point Solutions

About Me

- Graduate of Dakota State University, Bachelors Degrees in Cyber-Operations (Information Security)
- Loves understanding cryptography and how the internet connects securely

“Knowing your enemy enables you to take the offensive, knowing yourself enables you to stand on the defensive.”

— Sun Tzu, The Art of War

Actual Red-Team Results

Names have been changed to protect those involved

Dan Burwitz
IT Security Specialist
Vantage Point Solutions
2211 N. Minnesota St.
Mitchell, SD 57301

(605) 995-1777
FAX: (605) 995-1778
Dan.burwitz@vantagepnt.com

The Heist

Goals:

Money Money Money
External Government
Angry Customer
Kids bored at school

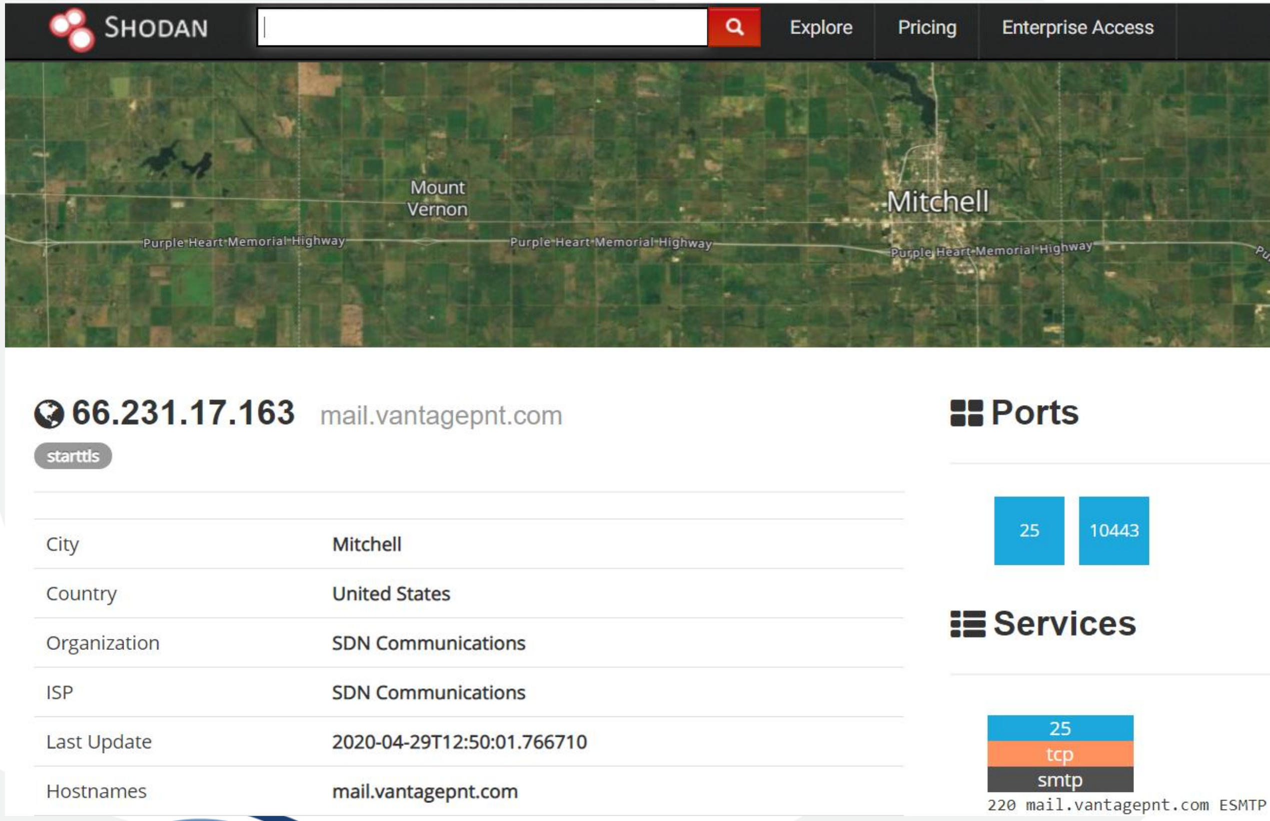
VantagePoint EMPLOYEE OWNED

Starting from the Ground up

Passive Reconnaissance

- Shodan.io
- theHarvester (Kali Linux)
- Exploit-db (Google Hacking)
- ARIN

(American Registry for Internet Numbers)


SHODAN
Explore
Pricing
Enterprise Access
Mount Vernon
Mitchell
Purple Heart Memorial Highway
Purple Heart Memorial Highway
Purple Heart Memorial Highway
starttls
Ports
25
10443
Services

66.231.17.163 mail.vantagepnt.com

City	Mitchell
Country	United States
Organization	SDN Communications
ISP	SDN Communications
Last Update	2020-04-29T12:50:01.766710
Hostnames	mail.vantagepnt.com

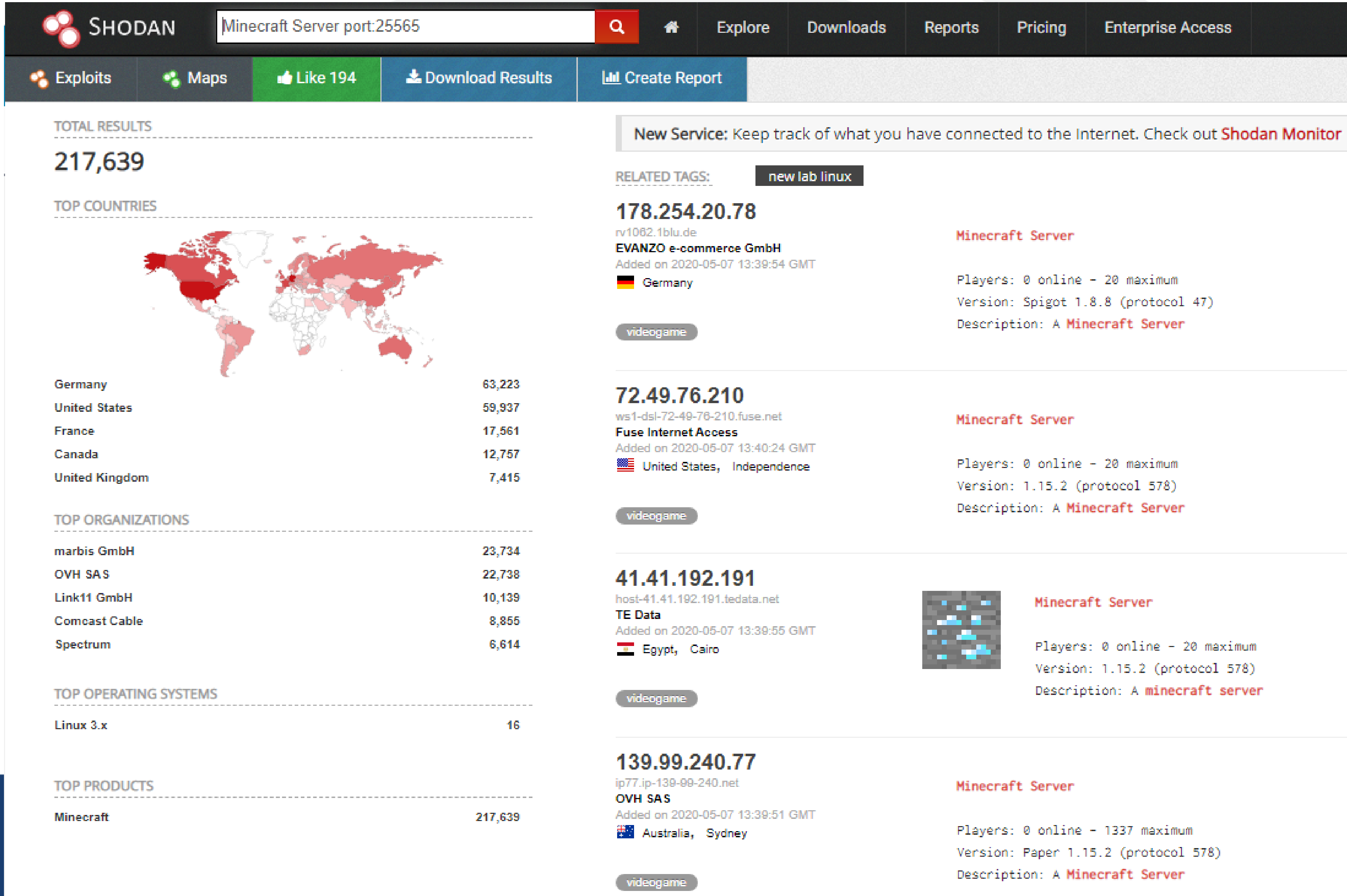
25
tcp
smtp

```
220 mail.vantagepnt.com ESMTP
```

VantagePoint
EMPLOYEE OWNED

Shodan.io

Minecraft: 217,639 servers Germany & US lead the way



TOTAL RESULTS

217,639

TOP COUNTRIES

Germany	63,223
United States	59,937
France	17,561
Canada	12,757
United Kingdom	7,415

TOP ORGANIZATIONS

marbis GmbH	23,734
OVH SAS	22,738
Link11 GmbH	10,139
Comcast Cable	8,855
Spectrum	6,614

TOP OPERATING SYSTEMS

Linux 3.x	16

TOP PRODUCTS

Minecraft	217,639

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: new lab linux

178.254.20.78
rv1062.1blu.de
EVANZO e-commerce GmbH
Added on 2020-05-07 13:39:54 GMT
Germany
videogame

```
Minecraft Server

Players: 0 online - 20 maximum
Version: Spigot 1.8.8 (protocol 47)
Description: A Minecraft Server
```

72.49.76.210
ws1-dsl-72-49-76-210.fuse.net
Fuse Internet Access
Added on 2020-05-07 13:40:24 GMT
United States, Independence
videogame

```
Minecraft Server

Players: 0 online - 20 maximum
Version: 1.15.2 (protocol 578)
Description: A Minecraft Server
```

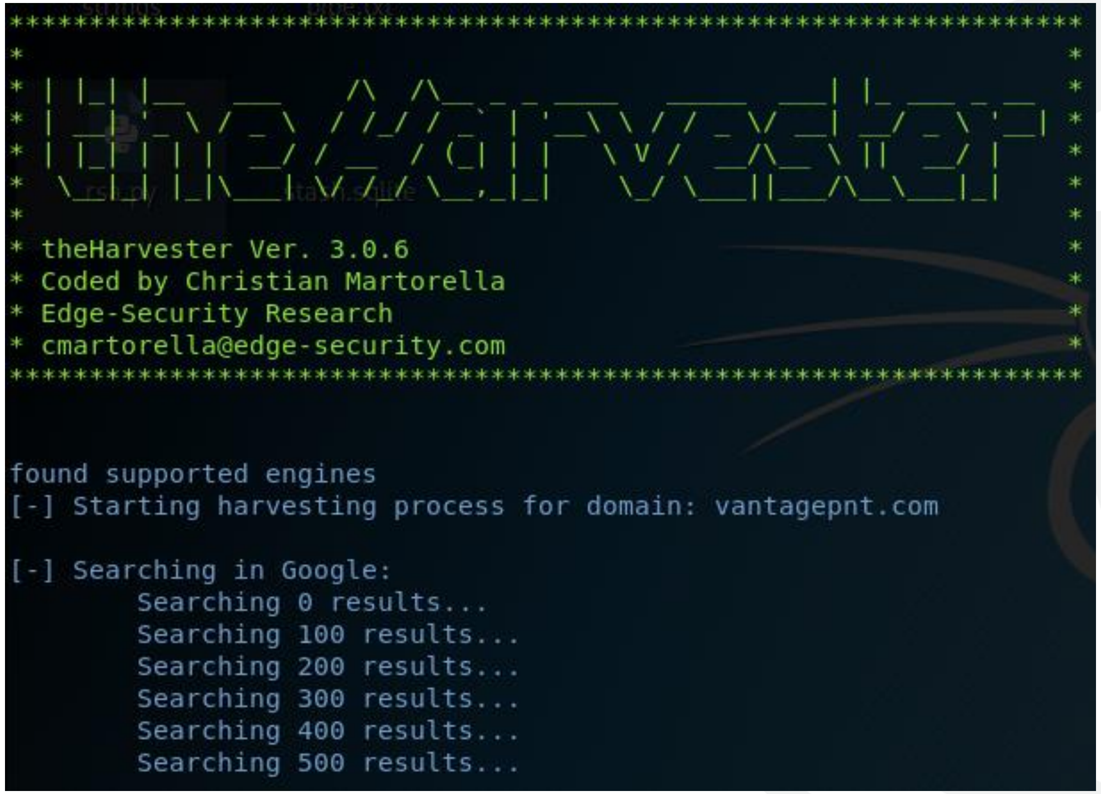
41.41.192.191
host-41.41.192.191.tedata.net
TE Data
Added on 2020-05-07 13:39:55 GMT
Egypt, Cairo
videogame

```
Minecraft Server

Players: 0 online - 20 maximum
Version: 1.15.2 (protocol 578)
Description: A minecraft server
```

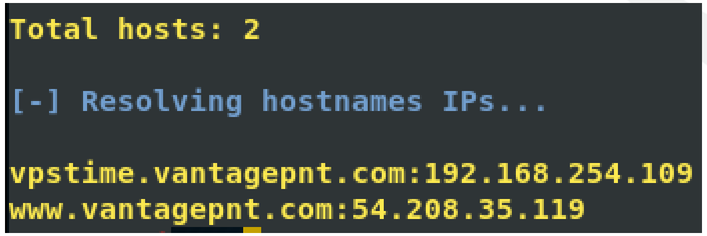
139.99.240.77
ip77.ip-139-99-240.net
OVH SAS
Added on 2020-05-07 13:39:51 GMT
Australia, Sydney
videogame

```
Minecraft Server

Players: 0 online - 1337 maximum
Version: Paper 1.15.2 (protocol 578)
Description: A Minecraft Server
```

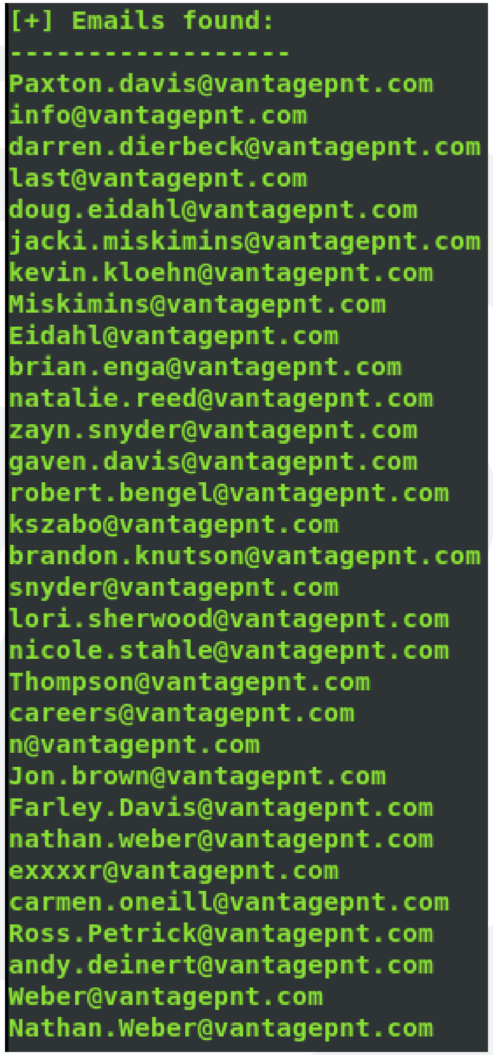
The Harvester



```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester Ver. 3.0.6                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


found supported engines
[-] Starting harvesting process for domain: vantagepnt.com

[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...
```

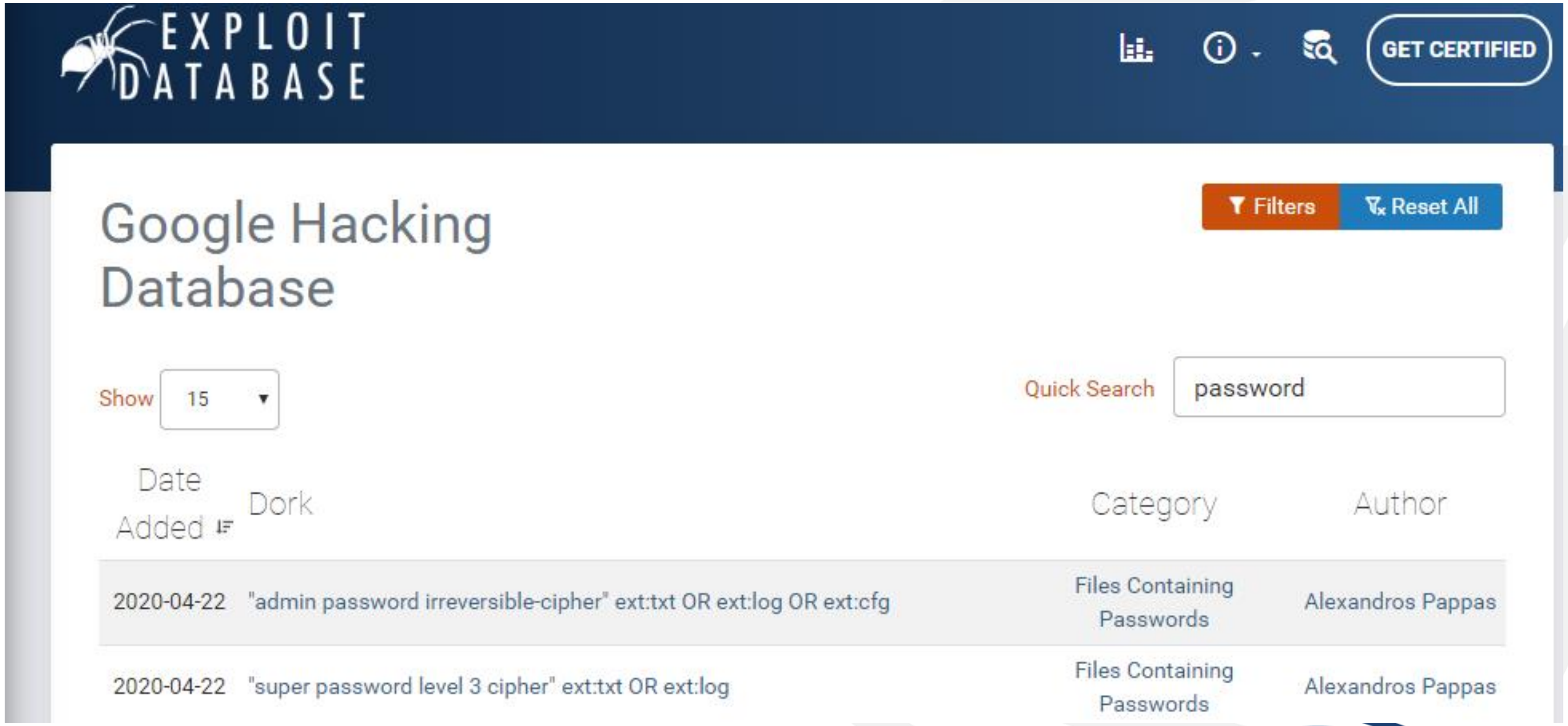


```
Total hosts: 2

[-] Resolving hostnames IPs...

vpstime.vantagepnt.com:192.168.254.109
www.vantagepnt.com:54.208.35.119
```



```
[+] Emails found:
------------------
Paxton.davis@vantagepnt.com
info@vantagepnt.com
darren.dierbeck@vantagepnt.com
last@vantagepnt.com
doug.eidahl@vantagepnt.com
jacki.miskimins@vantagepnt.com
kevin.kloehn@vantagepnt.com
Miskimins@vantagepnt.com
Eidahl@vantagepnt.com
brian.enga@vantagepnt.com
natalie.reed@vantagepnt.com
zayn.snyder@vantagepnt.com
gaven.davis@vantagepnt.com
robert.bengel@vantagepnt.com
kszabo@vantagepnt.com
brandon.knutson@vantagepnt.com
snyder@vantagepnt.com
lori.sherwood@vantagepnt.com
nicole.stahle@vantagepnt.com
Thompson@vantagepnt.com
careers@vantagepnt.com
n@vantagepnt.com
Jon.brown@vantagepnt.com
Farley.Davis@vantagepnt.com
nathan.weber@vantagepnt.com
exxxxr@vantagepnt.com
carmen.oneill@vantagepnt.com
Ross.Petrick@vantagepnt.com
andy.deinert@vantagepnt.com
Weber@vantagepnt.com
Nathan.Weber@vantagepnt.com
```

Exploit Database Google Hacking

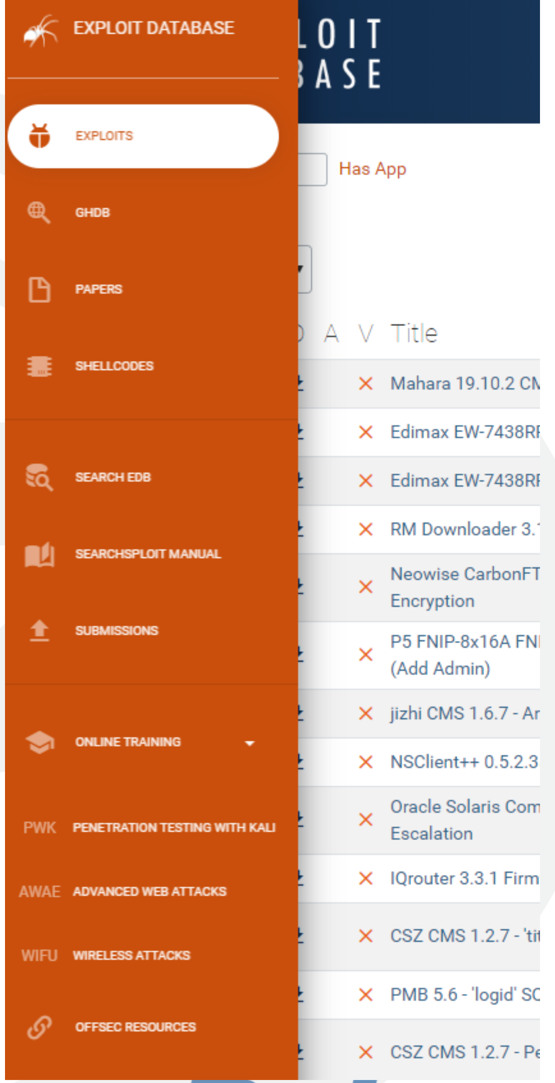


Google Hacking Database

Show 15

Quick Search password

Date Added	Dork	Category	Author
2020-04-22	"admin password irreversible-cipher" ext:txt OR ext:log OR ext:cfg	Files Containing Passwords	Alexandros Pappas
2020-04-22	"super password level 3 cipher" ext:txt OR ext:log	Files Containing Passwords	Alexandros Pappas



Title
Mahara 19.10.2 CM
Edimax EW-7438RF
Edimax EW-7438RF
RM Downloader 3.1
Neowise CarbonFT Encryption
P5 FNIP-8x16A FNI (Add Admin)
jizhi CMS 1.6.7 - Ar
NSClient++ 0.5.2.3
Oracle Solaris Com Escalation
IQrouter 3.3.1 Firm
CSZ CMS 1.2.7 - 'ti
PMB 5.6 - 'logid' SC
CSZ CMS 1.2.7 - Pe

VantagePoint EMPLOYEE OWNED

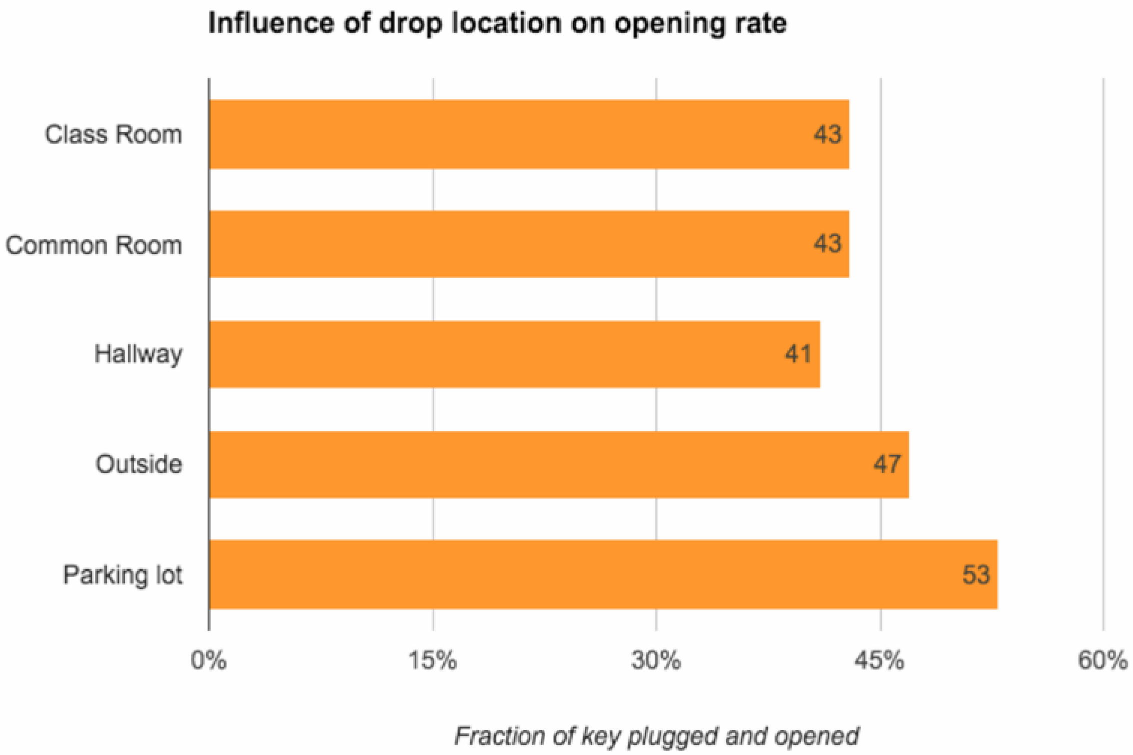
Layout 101

- **Google Maps**
- **Social Media**
- Dress Code / Badges

VantagePoint
EMPLOYEE OWNED

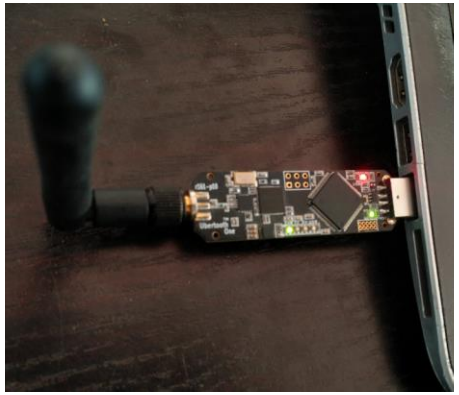
Tools

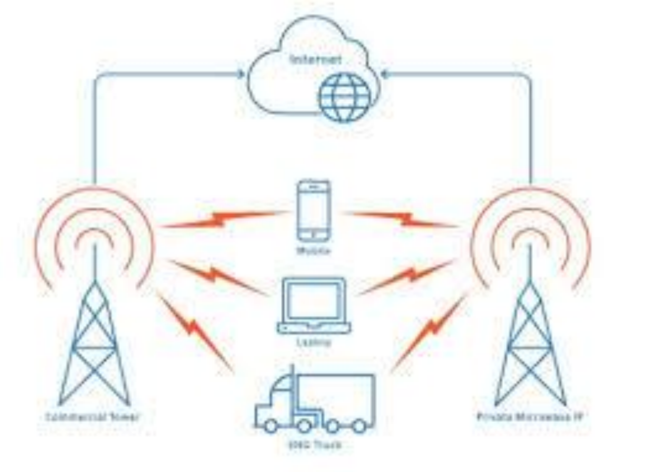
Packet Squirr
HAK5GEAR
FREEBUF
PacketSquirrel.com
Bash Bunny

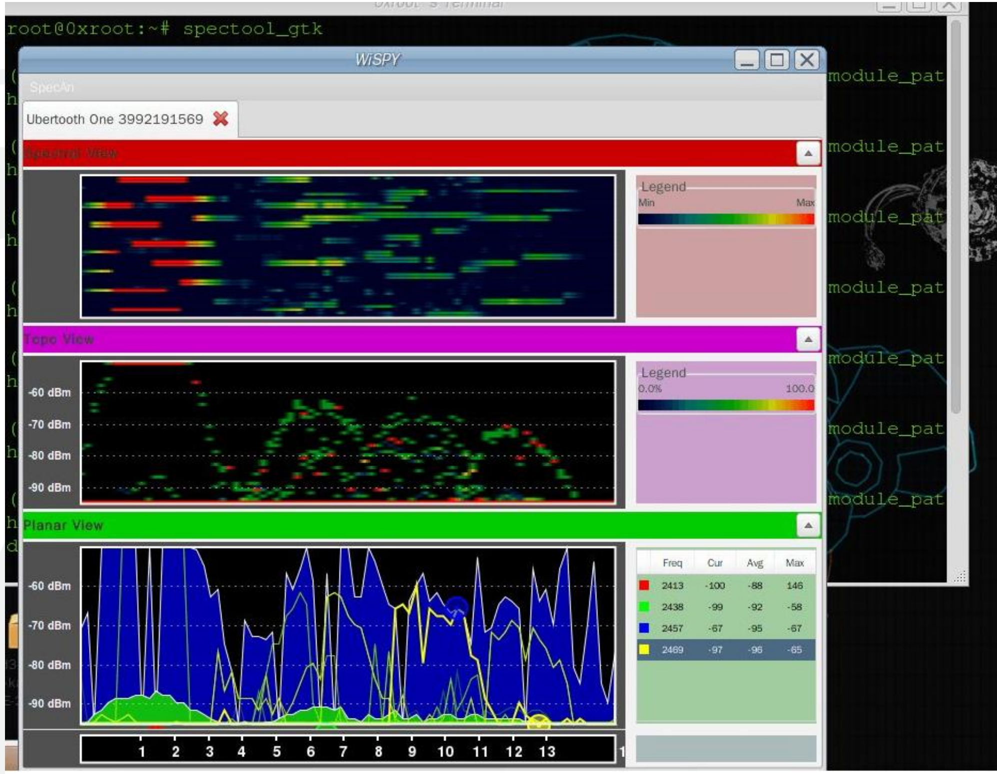


LAYOFF NOTICE

The Final Plan







```
root@0xroot:~# spectool_gtk
```

	Freq	Cur	Avg	Max
🟥	2413	-100	-88	146
🟩	2438	-99	-92	-58
🟦	2457	-67	-95	-67
🟨	2469	-97	-96	-65

- Acquire Caffeine
- Check Wireless & plant the seed
- Attempt to gain access without being noticed
- Social engineer my way in

VP VantagePoint
EMPLOYEE OWNED

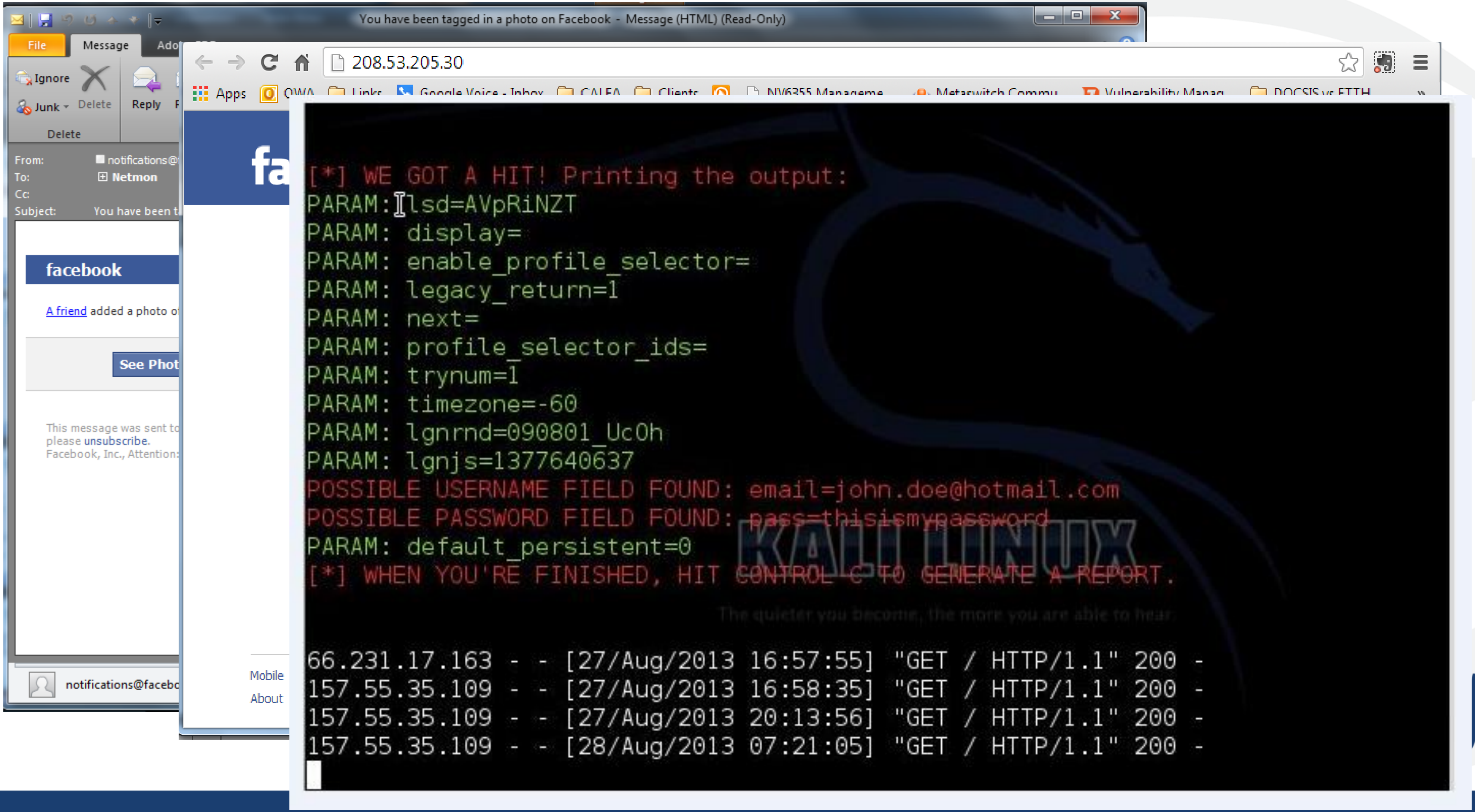
Social Engineering

- Attackers can obtain extremely sensitive data just by asking for it (in creative ways)
  - Common stories for larger organizations is to impersonate internal IT staff
  - On most occasions, we gain control of 2 machines out of 10 (only takes one)
- By far THE most dangerous of all attacks for all industries

Phishing Vishing Impersonation

VantagePoint EMPLOYEE OWNED

You have been tagged…



From: notifications@

To: Netmon

Cc:

Subject: You have been t

facebook

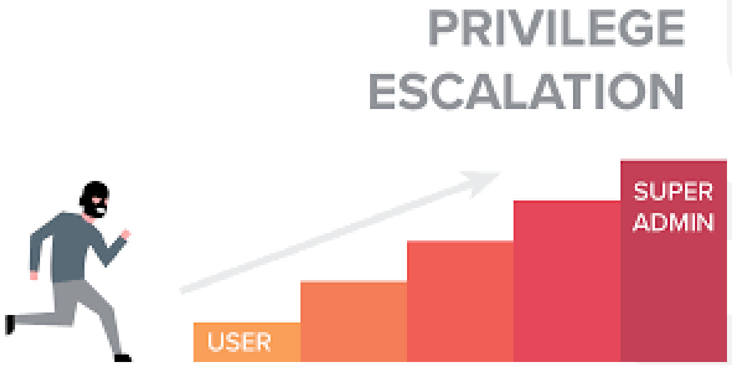
A friend added a photo o

See Phot

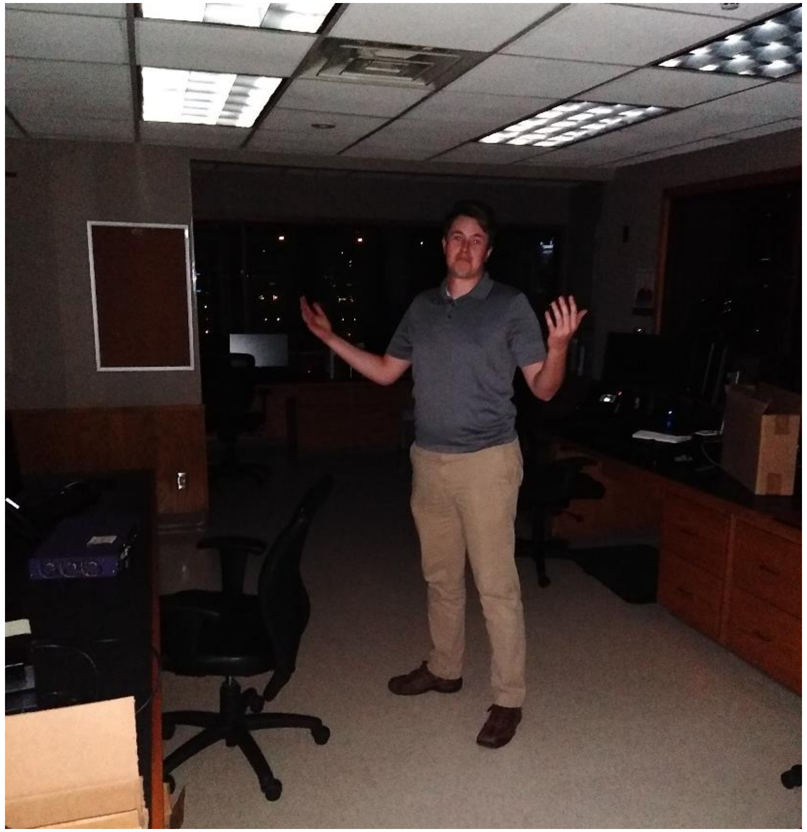
This message was sent t
please unsubscribe.
Facebook, Inc., Attention:

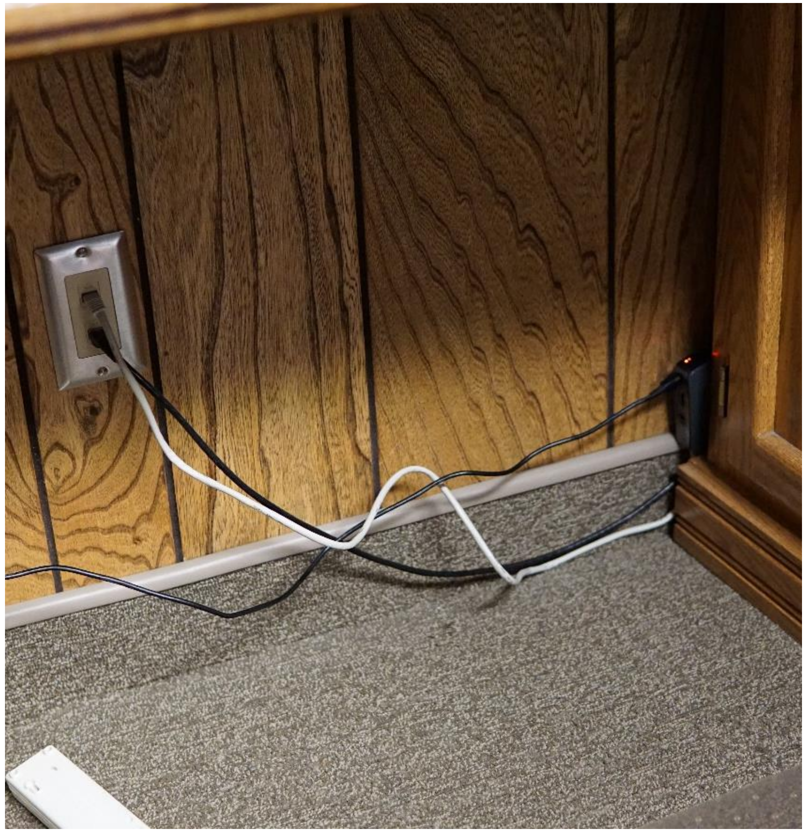
notifications@facebo

```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVpRiNZT
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-60
PARAM: lgnrnd=090801_UcOh
PARAM: lgnjs=1377640637
POSSIBLE USERNAME FIELD FOUND: email=john.doe@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=thisismypassword
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


66.231.17.163 - - [27/Aug/2013 16:57:55] "GET / HTTP/1.1" 200 -
157.55.35.109 - - [27/Aug/2013 16:58:35] "GET / HTTP/1.1" 200 -
157.55.35.109 - - [27/Aug/2013 20:13:56] "GET / HTTP/1.1" 200 -
157.55.35.109 - - [28/Aug/2013 07:21:05] "GET / HTTP/1.1" 200 -
```



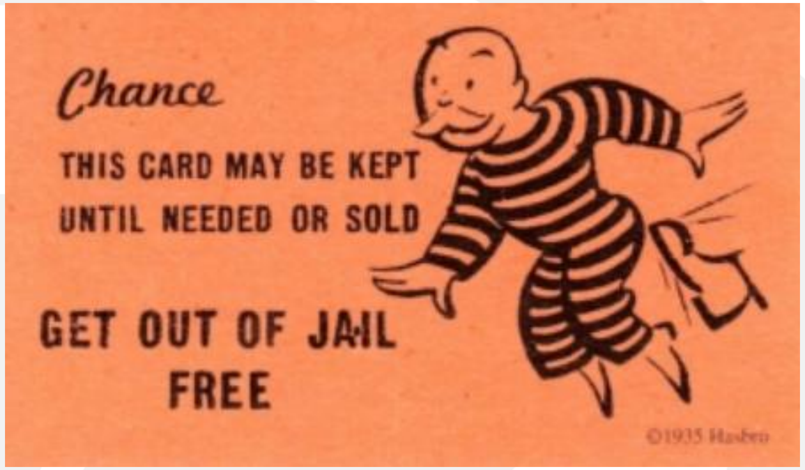
VantagePoint
EMPLOYEE OWNED





Success

Failure



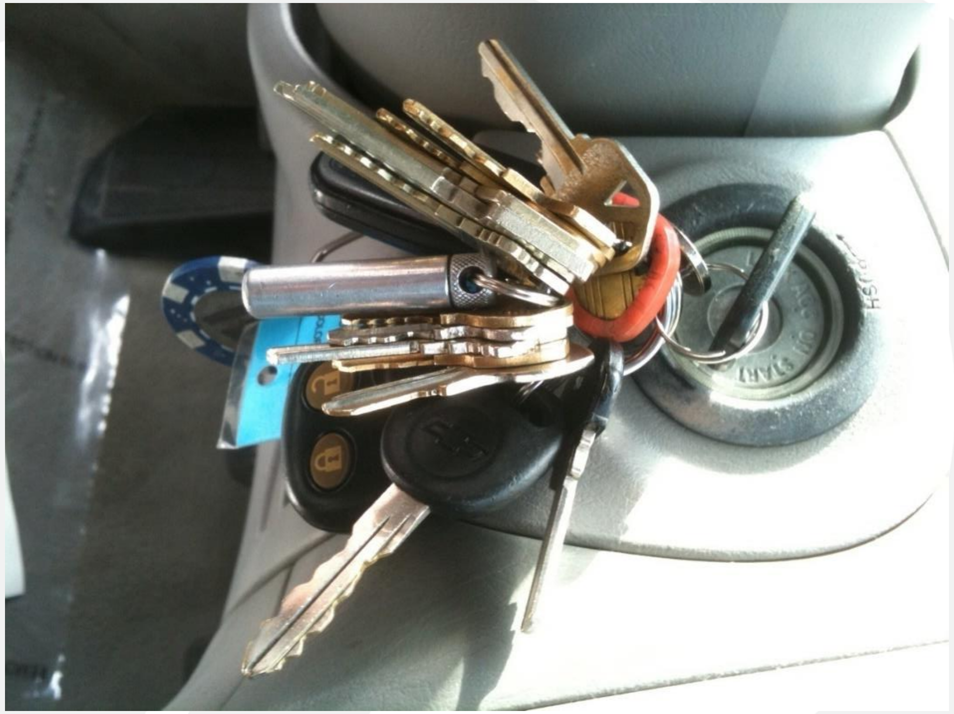
Chance

THIS CARD MAY BE KEPT UNTIL NEEDED OR SOLD

GET OUT OF JAIL FREE

©1935 Hasbro

Unattended Cars



Why is it so easy for Hackers?

- Time
- Motivation
- Only need to find one issue

Let’s Be Honest…

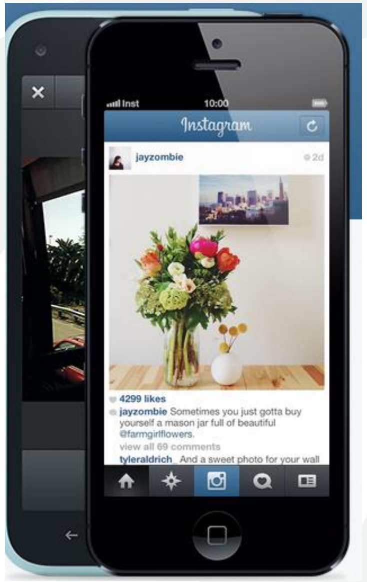
- We really have no clue how secure our apps are
- Have they been breached?
    - Was our information included?

- Apps all tie together more than you realize
    - Google Anything, Facebook, etc.

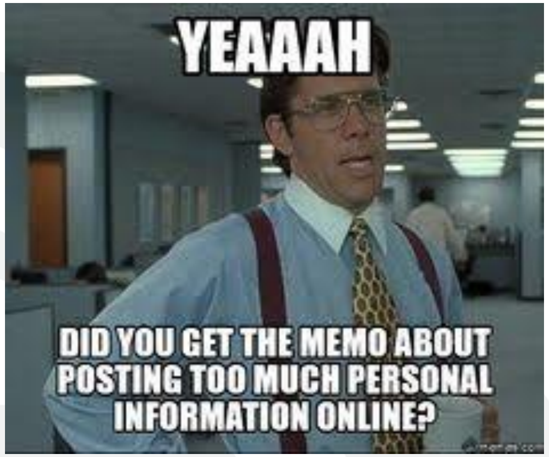
VantagePoint
EMPLOYEE OWNED

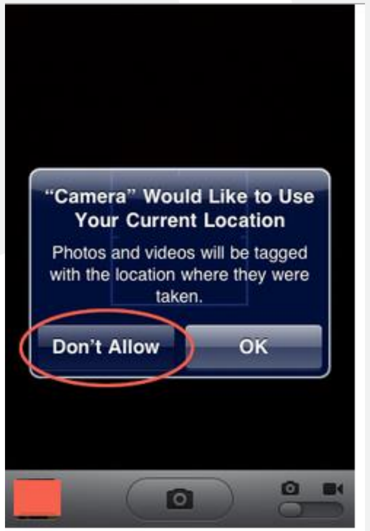
Are We Too Social?

- Twitter
- Instagram
- Facebook
- Instant Messenger
- Skype
- Ask.fm
- Blogger
- Google+


Instagram
10:00
jayzombie
2d
4299 likes
jayzombie Sometimes you just gotta buy yourself a mason jar full of beautiful @farmgirlflowers.
view all 69 comments
tyleraldrich And a sweet photo for your wall

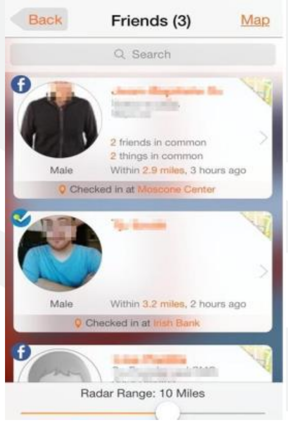
Tweet
Red Bull Stratos
@RedBullStratos
"Start the cameras, and our guardian angel will take care of you." Joe Kittinger


YEAAAH
DID YOU GET THE MEMO ABOUT POSTING TOO MUCH PERSONAL INFORMATION ONLINE?


"Camera" Would Like to Use Your Current Location

Photos and videos will be tagged with the location where they were taken.

Don't Allow | OK


Back | Friends (3) | Map

Search

[redacted]

2 friends in common

2 things in common

Male | Within 2.9 miles, 3 hours ago

Checked in at Moscone Center

[redacted]

Male | Within 3.2 miles, 2 hours ago

Checked in at Irish Bank

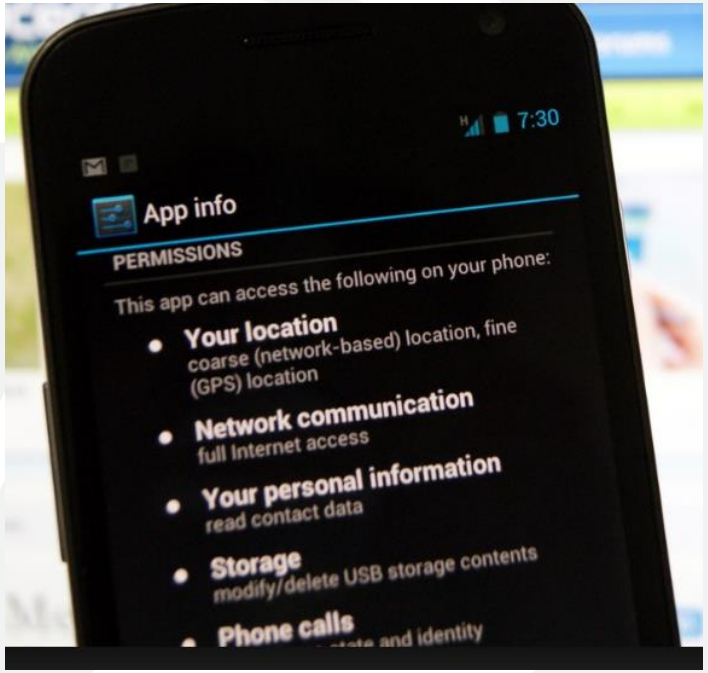
[redacted]

Radar Range: 10 Miles

VP VantagePoint EMPLOYEE OWNED

But Are We REALLY Qualified?

- Do you ever actually understand what your phone is asking for permissions when you install an app?
- Mobile Device Permissions
  - User-granted Permissions
  - Restricted Permissions
  - Developer-Driven Permissions
  - App Permissions
  - GPS location
  - Full Network Access



App info

PERMISSIONS

This app can access the following on your phone:

- **Your location**
  coarse (network-based) location, fine (GPS) location
- **Network communication**
  full Internet access
- **Your personal information**
  read contact data
- **Storage**
  modify/delete USB storage contents
- **Phone calls**
  state and identity

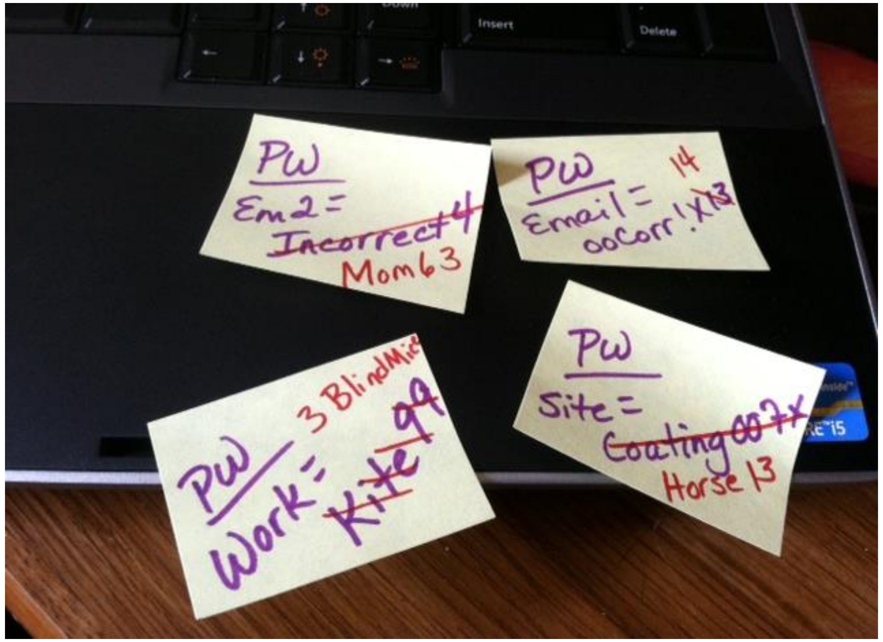
VantagePoint
EMPLOYEE OWNED

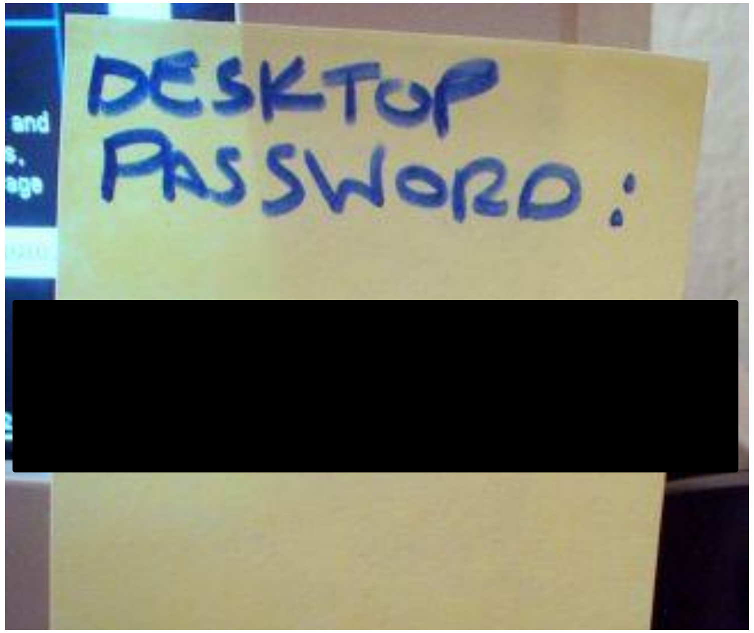
You have been endorsed….

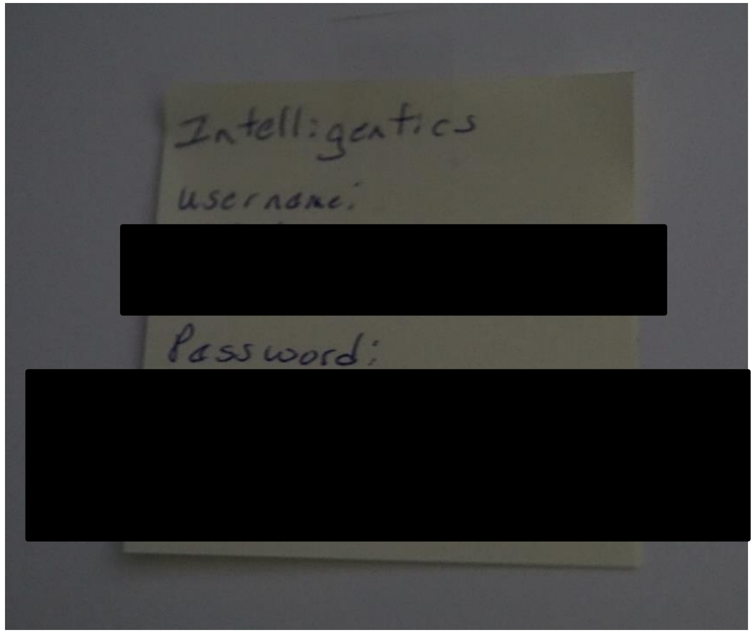
- There are currently 1.62 million active users for Facebook
- How many people using Facebook actually read and understood the disclaimer?
- How many people even knew there was a disclaimer?
  - The **Facebook disclaimer is currently 9110 words** and requires at least a sophomore in college level of education to understand
- I would like you to join my network… **LinkedIn**
  - **7895 words** on their disclaimers
- Clearly there are some risks if they need THAT much CYA.

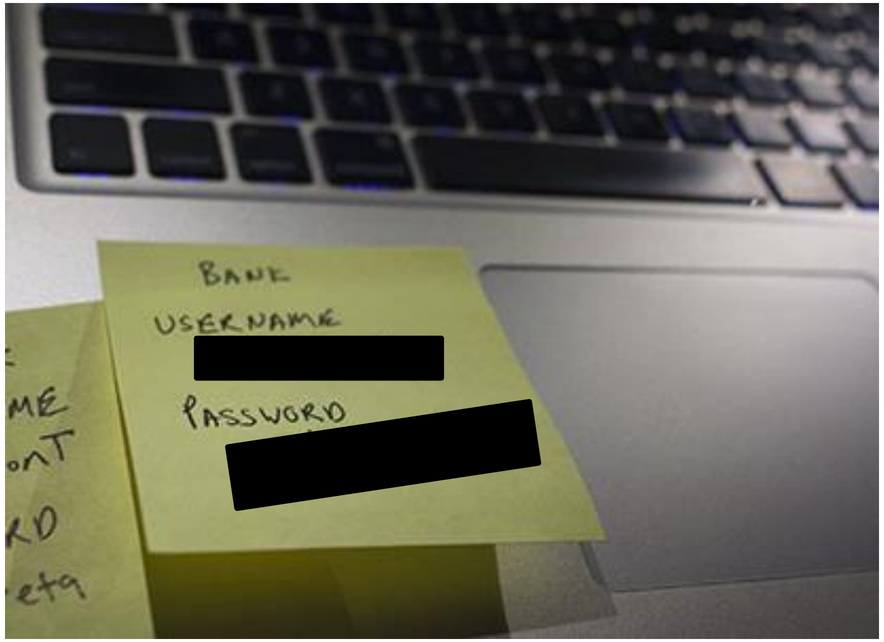
So…Now What?

VantagePoint
EMPLOYEE OWNED









Don’t Make it Easy

Clean your desk of ALL passwords & sensitive information

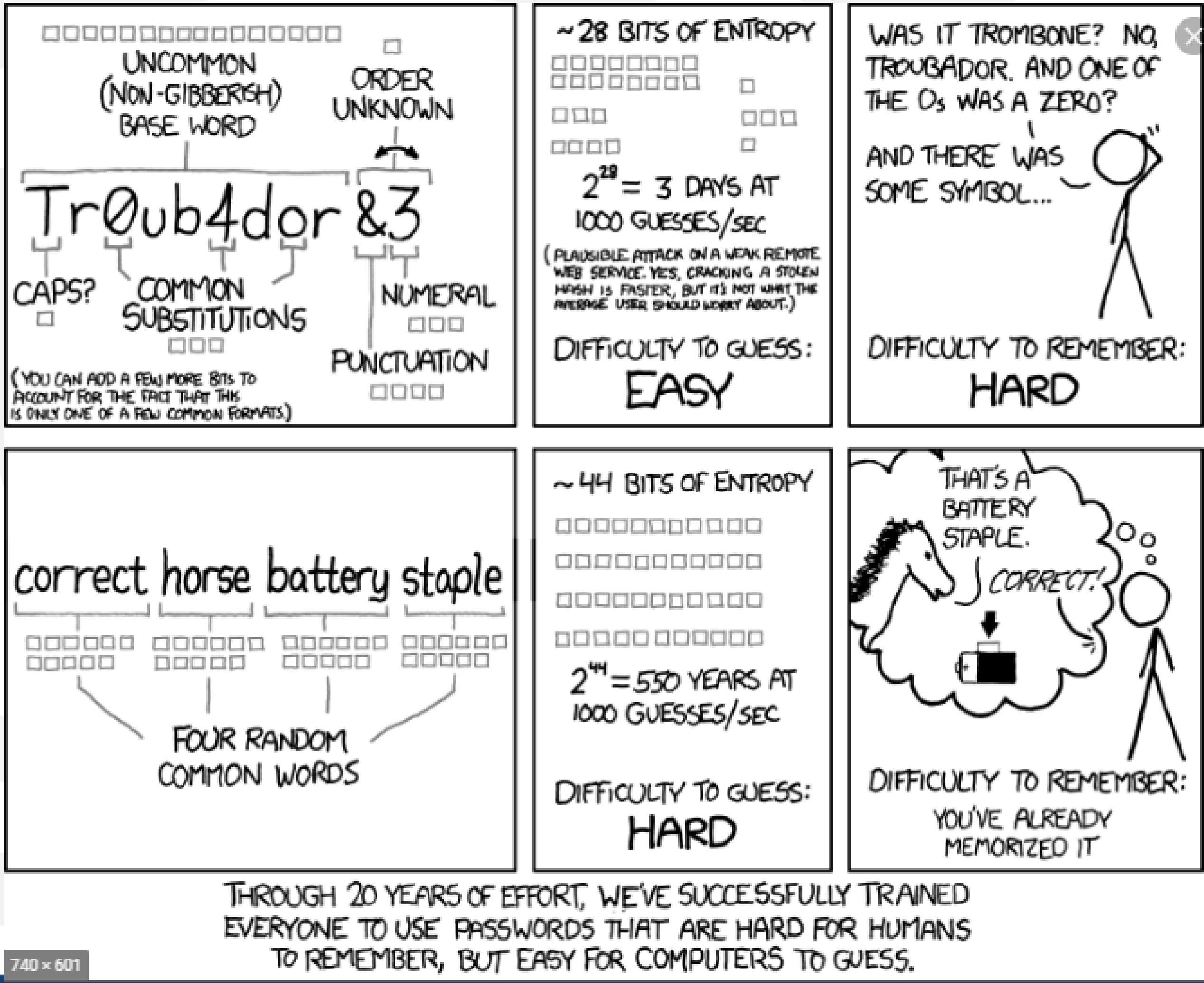
Passphrase & 2FA

Two Factor Authentication

These are normally 90 second unique time codes that are required after the correct username and password has logged in

Authenticators:

- Google
- LastPass
- Microsoft
- Authy
- Titan
- Yubikey


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.
740 × 601

Disable Unneeded Settings

- Remember who you friend - Your friends have access to whatever you post, so make sure they are people you trust.

- Limit access to your location - A lot of services and devices have GPS capabilities which let you share where you are. Disable these functions and only give people you trust information about your whereabouts.

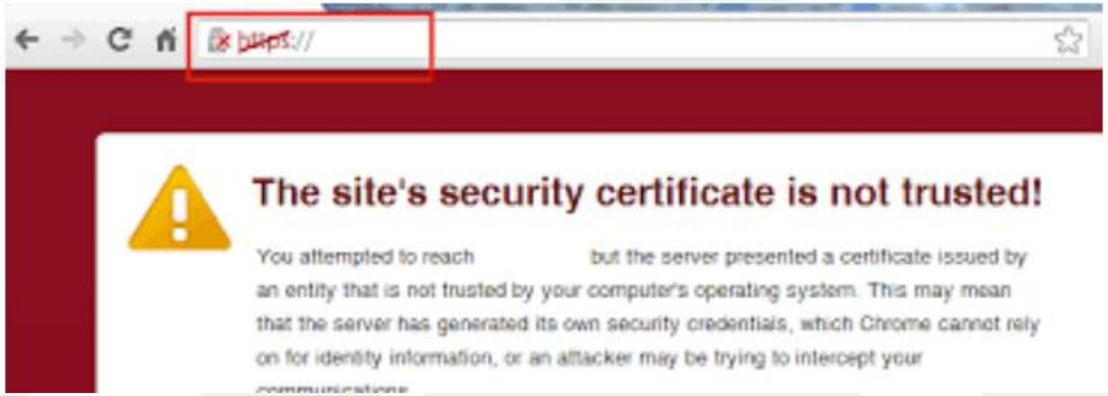
VantagePoint EMPLOYEE OWNED

What more can you do?

- ALWAYS look for a lock symbol or “https” in the address bar of websites that ask for financial information.

- Don’t share others’ personal information, for example, sharing a friend’s cell phone number online.

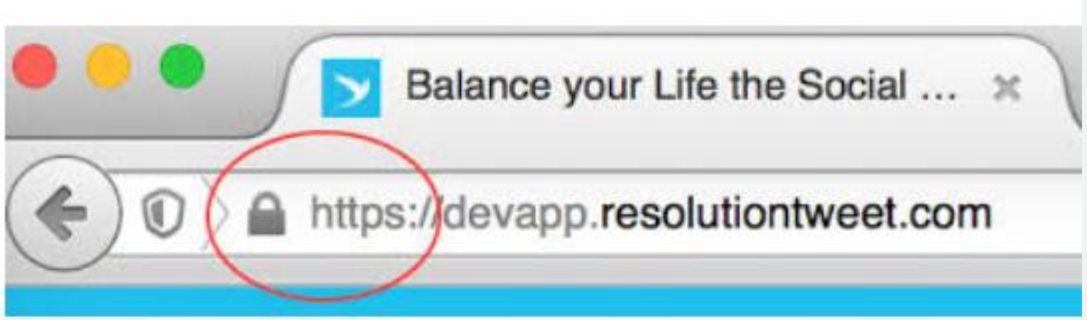
- NEVER Click a Link on an email



~~https~~://

The site's security certificate is not trusted!

You attempted to reach but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications



Balance your Life the Social ...

https://devapp.resolutiontweet.com

VantagePoint EMPLOYEE OWNED

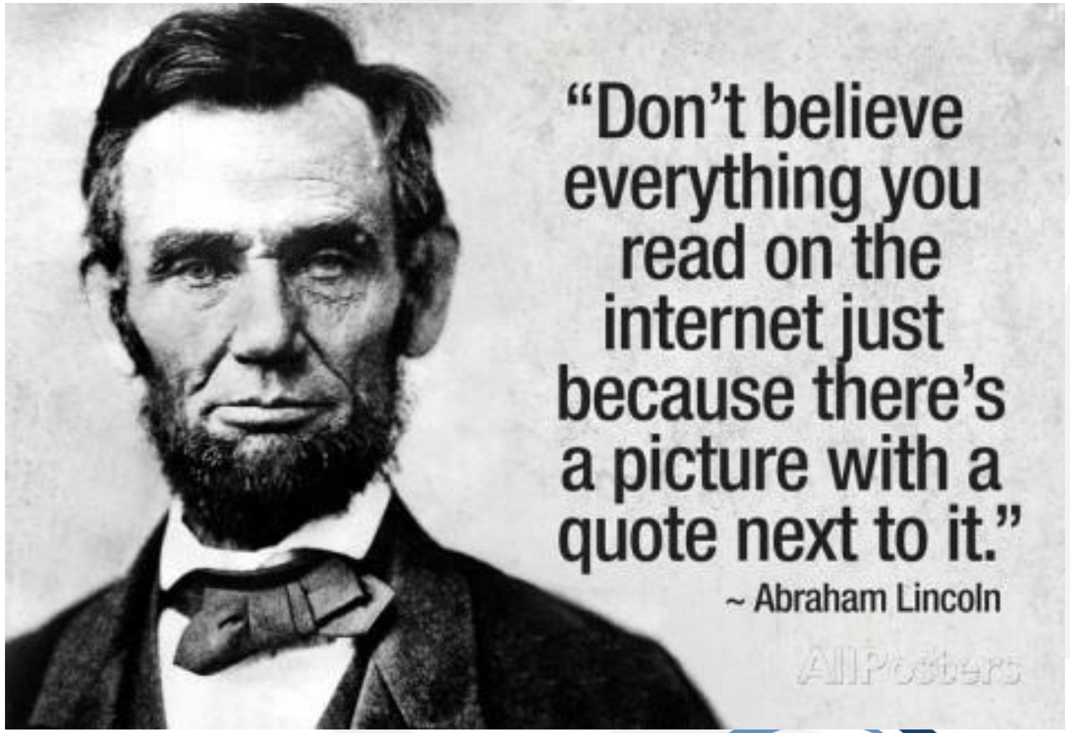
What more can you do?

- "INVEST" in Cybersecurity
- Get a third-party Assessment
- NEVER Click a Link on an email
- Never skip TRANING

TRAINING TRAINING TRAINING

VantagePoint
EMPLOYEE OWNED

Thank You



"Don't believe everything you read on the internet just because there's a picture with a quote next to it."

~ Abraham Lincoln

VantagePoint

EMPLOYEE OWNED