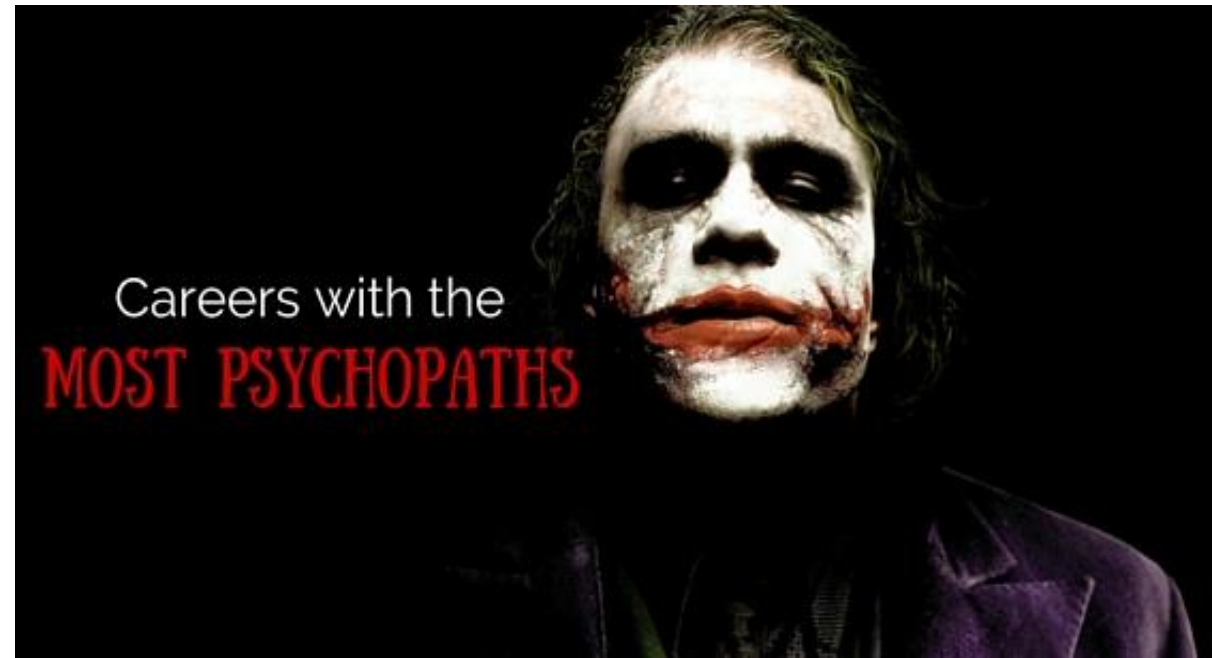# You Fail in SE If You Make Those Mistakes
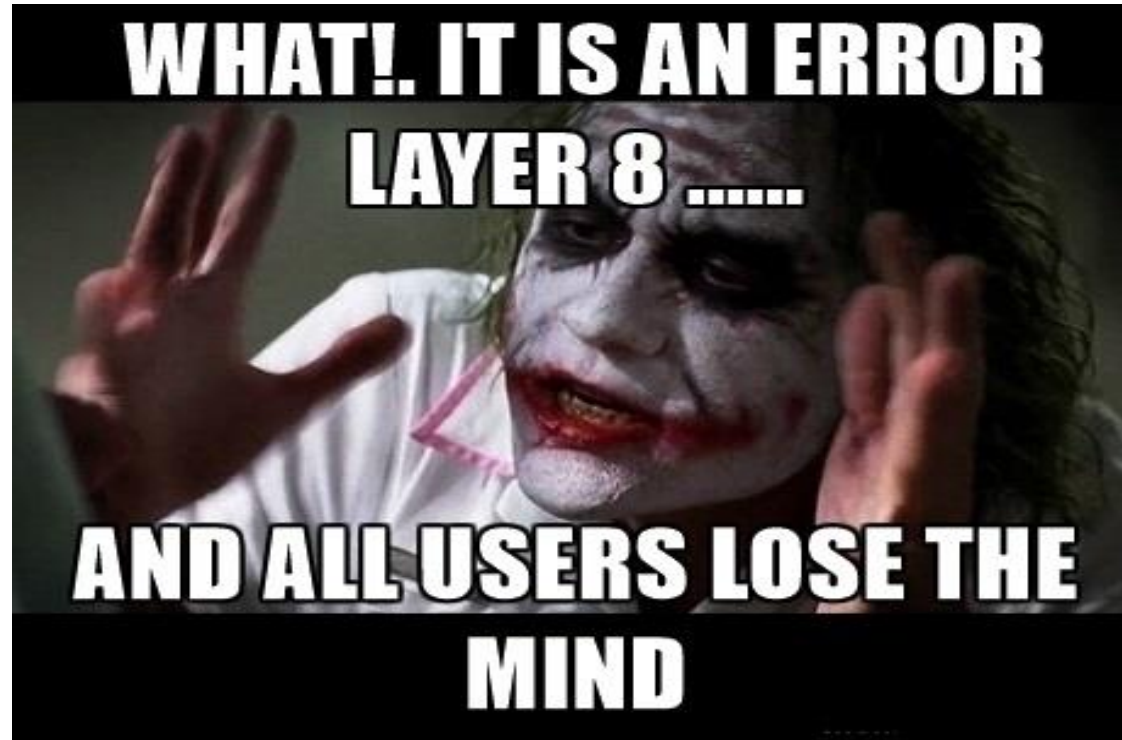
Yehia Mamdouh

The Famous Who Am I Today?!

* Penetration Tester Specialist and Security Researcher @ DTS-Solution – 8+ years in VAPT - Physical & Social Engineering Assessments)

* Author of XSSYA-V-1,2 and BetWorm

* Keynote-Speaker (Qubit 2016 – DefCamp 2016 – Middle East Security Summit)

* I mainly focus on Social engineer and Physical Assessments

Yehia-@dts-solution.com
@Yehia1mamdouh

Careers with the
MOST PSYCHOPATHS

We Know!!

WHAT!. IT IS AN ERROR LAYER 8 ...... AND ALL USERS LOSE THE MIND

Our nervous system was designed for being attacked or attacking Animals Only - but now we are nervous all time because - we feel dangerous all the time

What This Talk about?

Definitions & Facts

SE Mistakes

Break In Mistakes

Reporting Mistakes
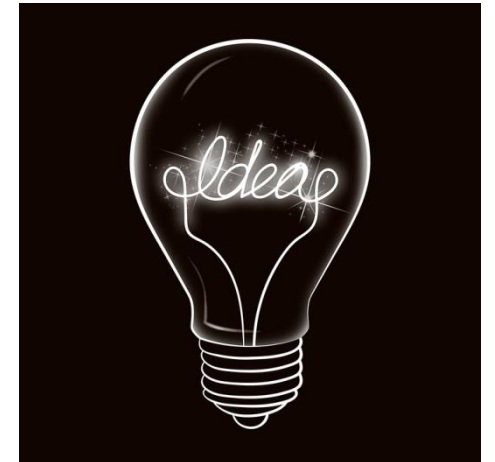
Story Time

Mitigation Gaps

Disclaimer

[0] I am Not:
Philosopher or phycologist but I do lot of Research

[0] My Talk Based on:
Science – Personal Experience and my examples

[0] This presentation is for Informational and educational purpose only

Definitions & Facts

* Psychological Manipulation of people behavior → in order to gain information

* Social Engineer being used from the existence of humans

* Now Days Social Engineer combined with Technology & have methodologies

* Human Minds has Gaps by default

* An intelligent person can be ignorant.- A stupid person can be knowledgeable.

* Is there something called Stupid ?

SE Mistakes - Reconnaissance

Employees

Internet activity – Hopes – Experience – Certifications – Pervious Companies

Company

Policy – News – Location - Signature - Market - Customers

Social Media

Activities – Families – Friends - Places they visit

SE Mistakes - Reconnaissance

Before We start Reconnaissance:

* We should identify Organization type – Sector
* Create scenarios first or do reconnaissance first ?

While we do Reconnaissance:

* knowledge of a company lingo, corporate structure
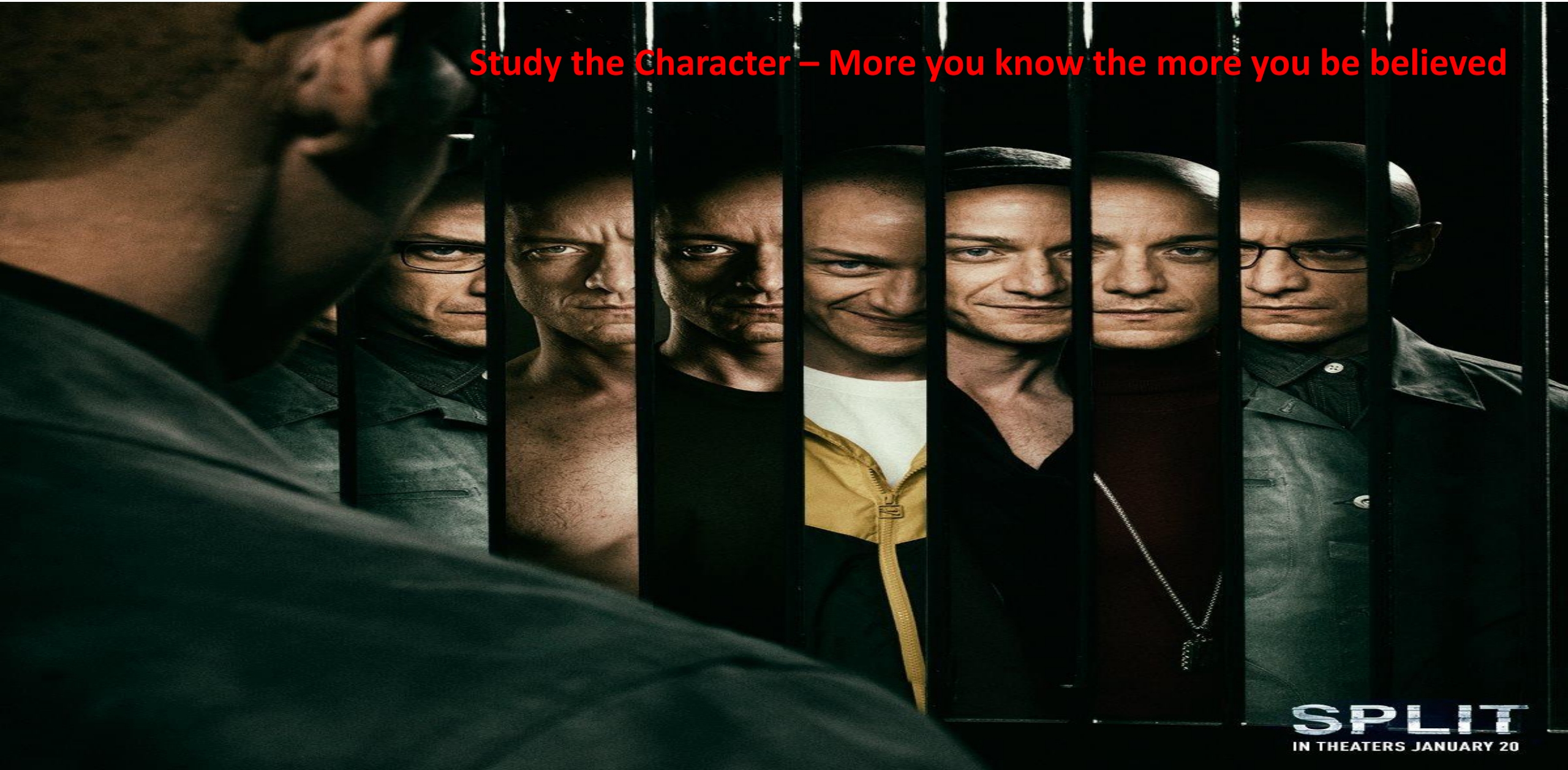* Society affect social engineer
* Stop your EGO
* Continue using OSNIT

IT'S THE NEW MANAGEMENT STRUCTURE, THE WORKER'S THE ONE AT THE BOTTOM...
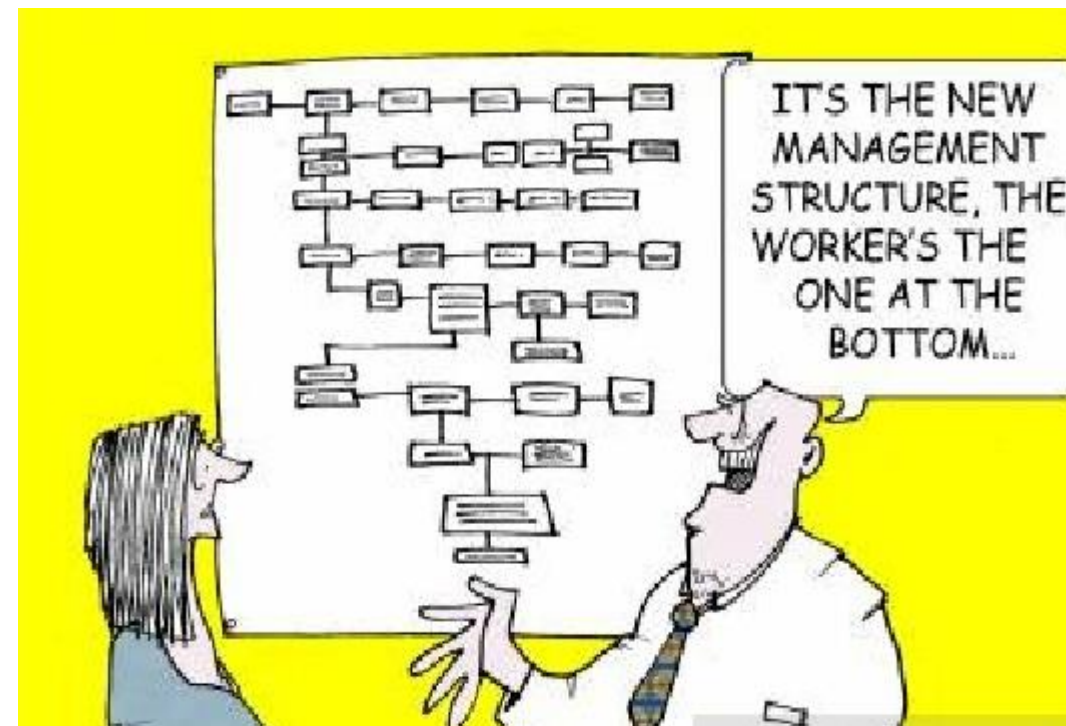
SE Mistakes - Preparations

SE Mistakes - Preparations

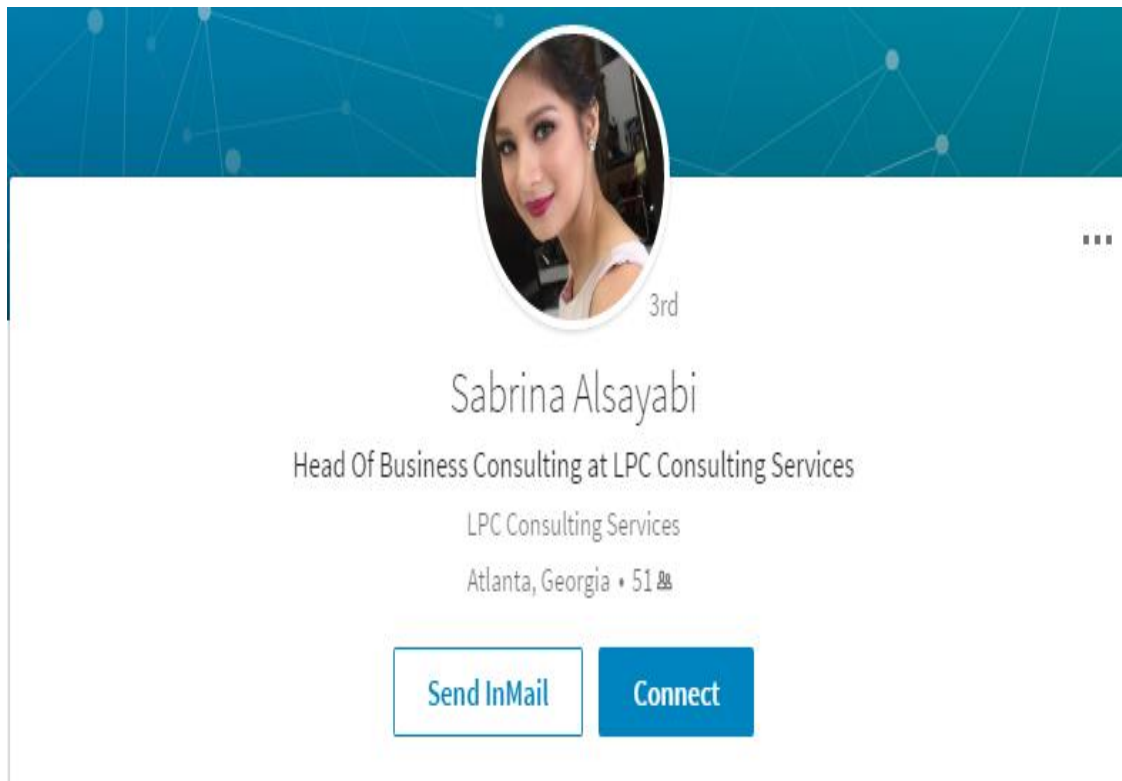**Study the Character – More you know the more you be believed**

SE Mistakes - Preparations

Social Networks: Facebook – twitter – Instagram – LinkedIn ..etc.
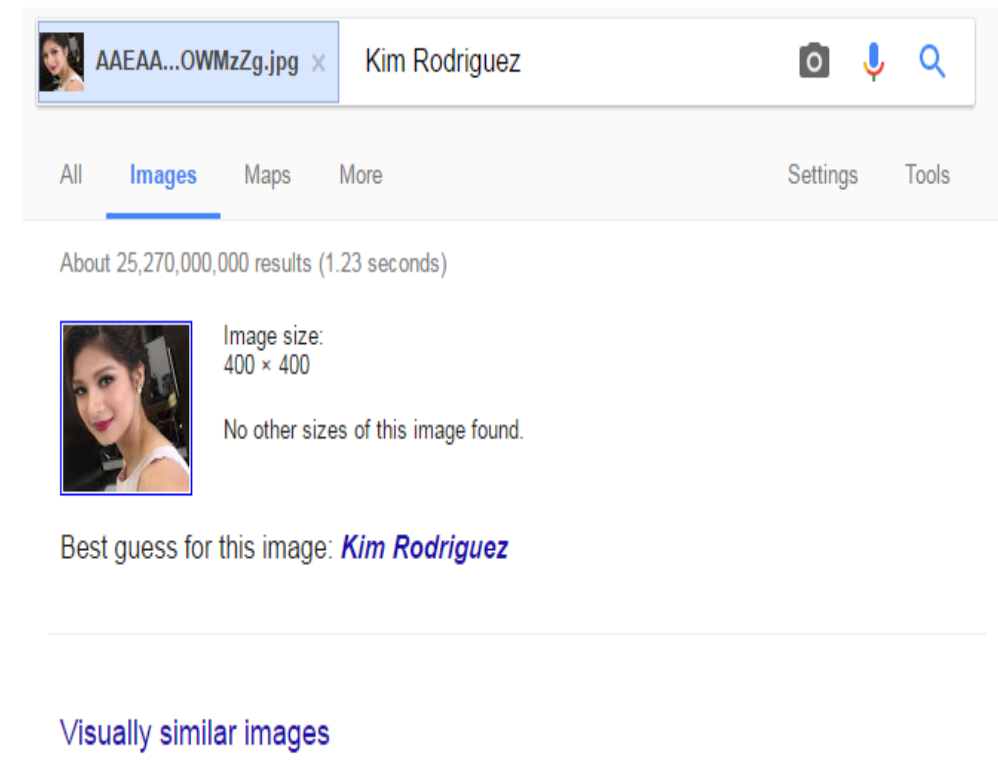* A Fake …. LinkedIn profile !!

SE Mistakes - Preparations

Social Networks: Facebook – twitter – Instagram – LinkedIn ..etc.

Before you create legitimate profile you Must:

*   Study the character (Man or Woman)
*   Read about the new job (Everything)
*   Avoid Random – (Add – Accept) friends !
*   Watch every detail
*   Have Schizophrenia !
*   Keep Alive

SE Mistakes - Preparations

Social Networks: Facebook – twitter – Instagram – LinkedIn ..etc.
* Think like End-User have basic awareness for social media threats

SE Mistakes - Preparations

If don't how to lie then learn How to Lie?

* Keep it Short and To the Point

* Keep it Reasonable

* Keep Calm

* Don't wait for interrogation

* Know your target

* Watch your Body Language

* Finally Practice

Break In - Mistakes

Vishing Mistakes

* Always Watch the Tone changes

* Never end the conversation after getting the key information.

* A Little Chat before you say goodbye

* Don't call number that already exposed to Public

Break In - Mistakes

We Know what human behaviors we target

* Social Engineer Target: (Trust – Helpfulness – False Assumptions – Curiosity – Fear – Ignorance – Sympathy)

* We know Social Engineers target What – We target who?

* We can not use Fear towards higher positions (Managers – CEO)

* As per psychology Woman's are more vulnerable to Helpfulness more than men

* As per psychology Woman's are more Sympathy than men (Niedenthal, Kruth-Gruber 2006) – (Baron-Cohen & Wheelwright, 2004)

*** Confirmed Hypothesis: men and women give their opposite gender a higher Trust rating than the same gender.
Institute of psychology 2016 - Chinese Academy of Sciences**

* Don't put borders around Helpfulness - Give Hope !

Break In - Mistakes

Before You Break In:

* Be careful of what you are wearing
* Remove all signs that can identify you!
* Before you know about people know yourself
* Practice on your Pretext
* Colors can very powerful (Subconscious Impact)

Energy, Passion, Action, Ambition and Determination	Confidence, Self-esteem, Extraversion, Emotional Strength, Friendliness.	Harmony, balance, refreshment, universal love, peace	Communication, Trust, efficiency, serenity, logic, coolness, reflection, calm
Glamour, security, emotional safety, efficiency, substance	Physical comfort, food, warmth, security, sensuality, passion, abundance, fun.	Physical tranquility, nurture, warmth, femininity, love, sexuality	Hygiene, sterility, clarity, purity, cleanness, simplicity, efficiency.

Break In - Mistakes

After You Break In:

* Observation not only (Clothes - Uniform type - Body type - Gender/Age – Ethnicity - Manners/Discipline Physical Markings – Smell – Teeth – Hands – Interaction - Pictures) (Observe the Security layers)

* Attacking old woman not the same as you attack a young man

* Don't run away from the Security Guard

Reporting - Mistakes

* Clear Scenarios

* Attach more NON technical POC

* Don't Mention Names - Faces

* Rise Business Risk

SPOOKY STORY TIME

Story Time

Target: Retail Company

1- Tailgating will not be effective (Open Place - Store Rooms are monitored by CCTV and controlled by employees

2- Steal sensitive documents or equipment's not effective (Sensors on the Entry – Many CCTV – Many Employees

The only Way is to be Legitimate and Authorized

Story Time

DIGITAL POINT OF SALE FOR RETAIL

ALPHA-POS allows you to make sales faster. Manage inventory like never before, create any point of sale report and make your business stronger and more efficient. Designed to make your retail network quick and easy and can be connected from Individual single terminal as much as 90 terminals or multiple stores, affiliates or branches. Alpha POS is a user-friendly POS software technology that stays ahead of industry demands.

With proven implementation tools and an intuitive user experience, the software can be up and running quickly-in the cloud or on your servers.

Letter of Authorization

Subject: Letter of Authorization Point of sale system [ERP] Check

▬▬▬ has authorized **Yehia Mamdouh** to conduct a point of sale system [ERP] check within its Headquarters office which is in Dubai. The checking is planned to be completed within 1 week starting from ▬▬ Aug-2017 and it covers the following sites:

- ▬▬▬▬
- ▬▬▬▬
- ▬▬▬▬
- ▬▬▬▬▬
- ▬▬▬▬▬

Branch Manager: ▬▬▬▬ is fully aware of this checking and approach which Yehia Mamdouh to complete the point of sale system checking, so assist him with any help he needs.

▬▬▬▬

SIGNATURE:

NAME: ▬▬▬▬
EMAIL: ▬▬▬▬
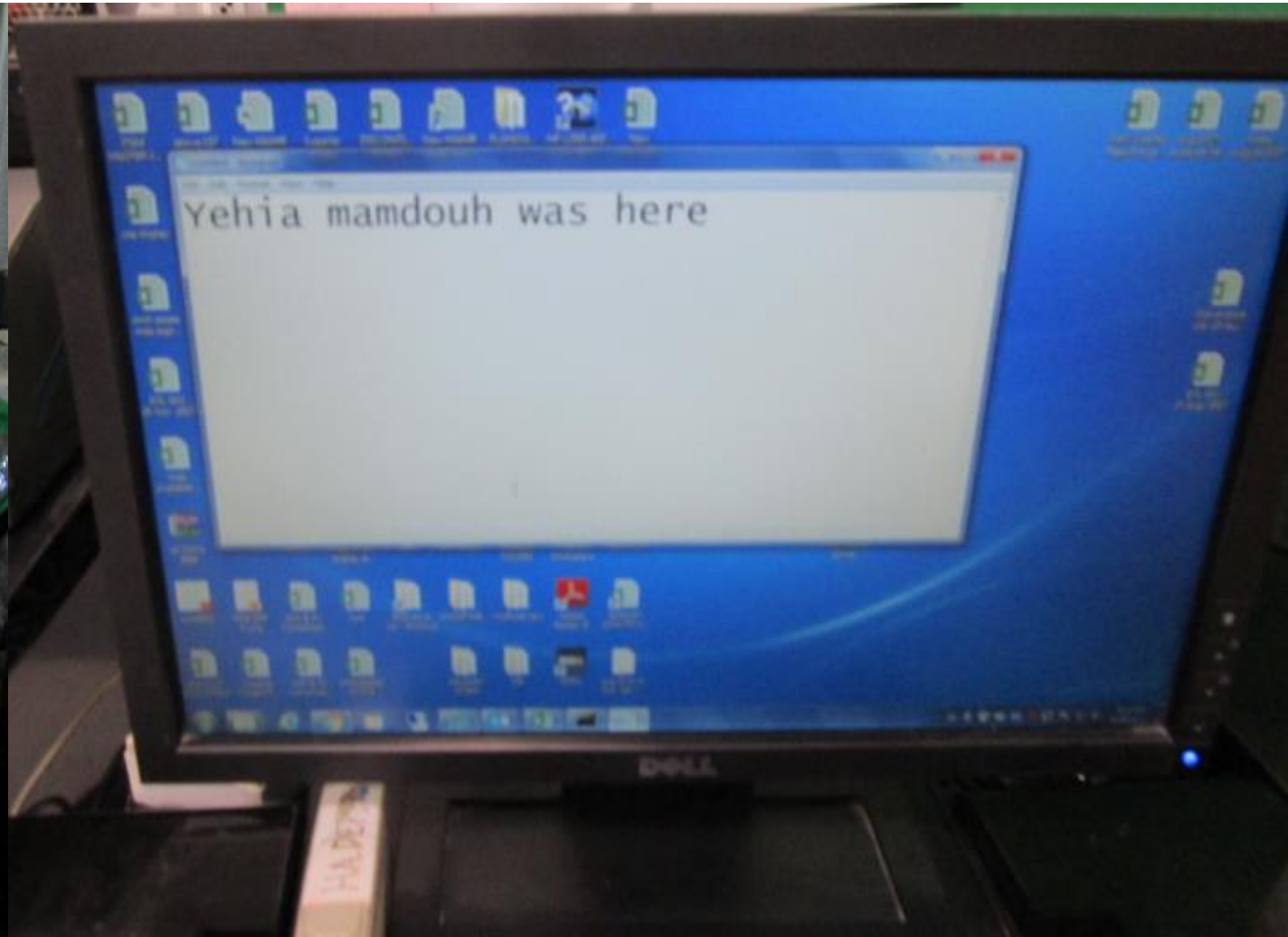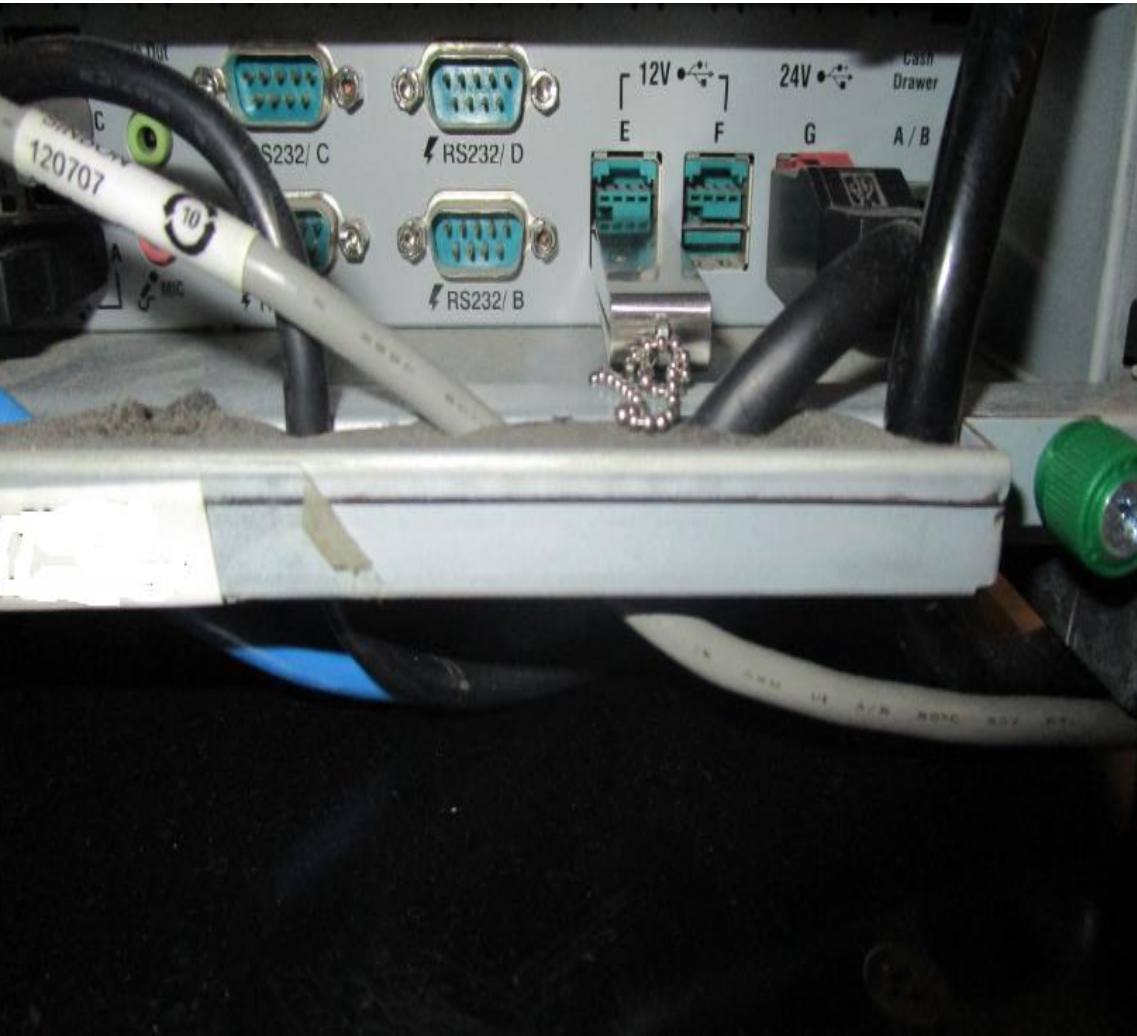DATE: ▬▬▬

Yehia Mamdouh
SIGNATURE:

NAME: Yehia Mamdouh
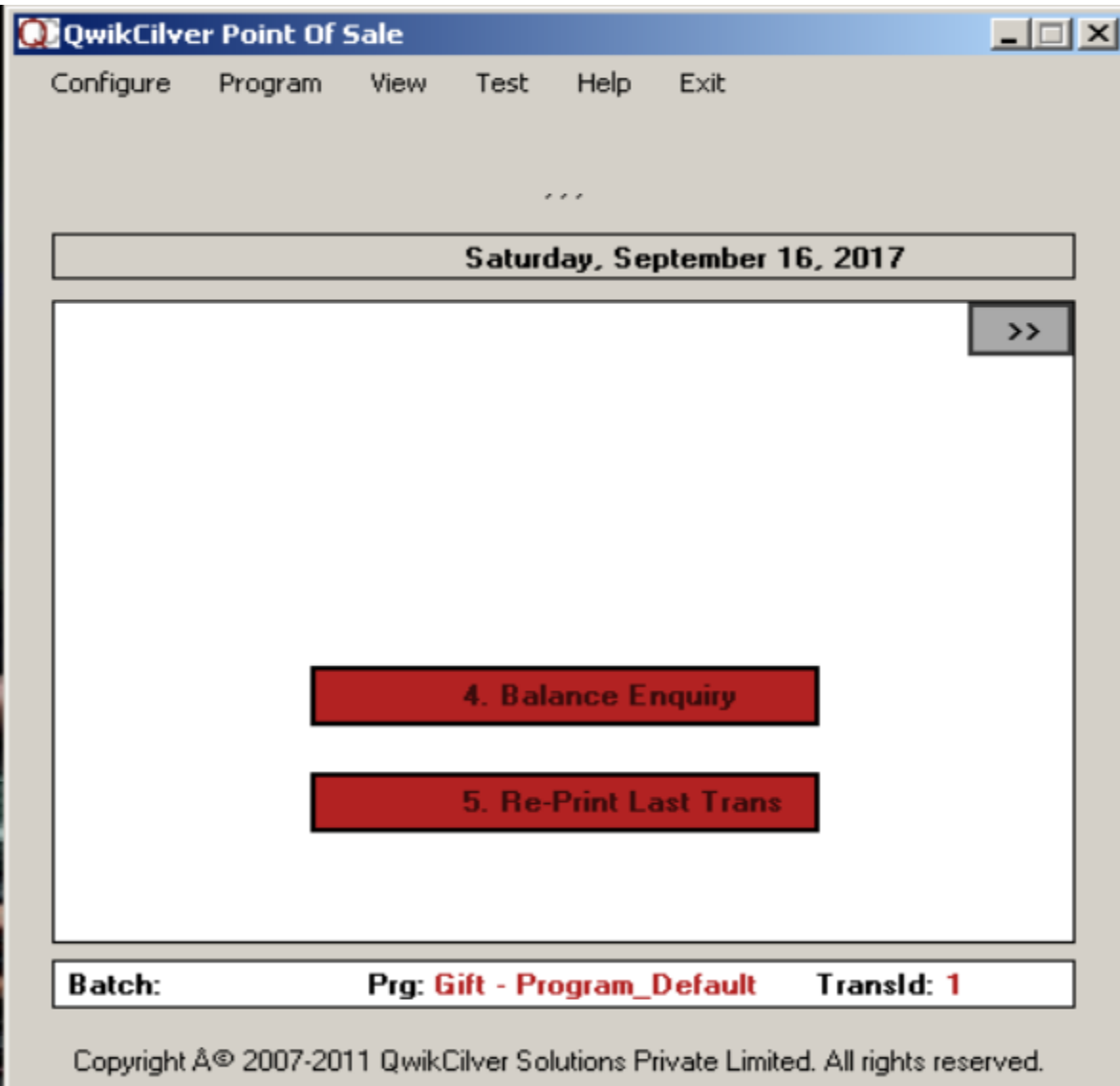EMAIL: it@alphauae.com
DATE: ▬▬▬

Story Time

Results

Story Time
Results

I take POC by That !!!!!!!!!

Mitigation Gaps

Mitigation Gaps

That what they have told you!!

* Basic Layer: Security Policy : No information is useless - information value is different from one to another
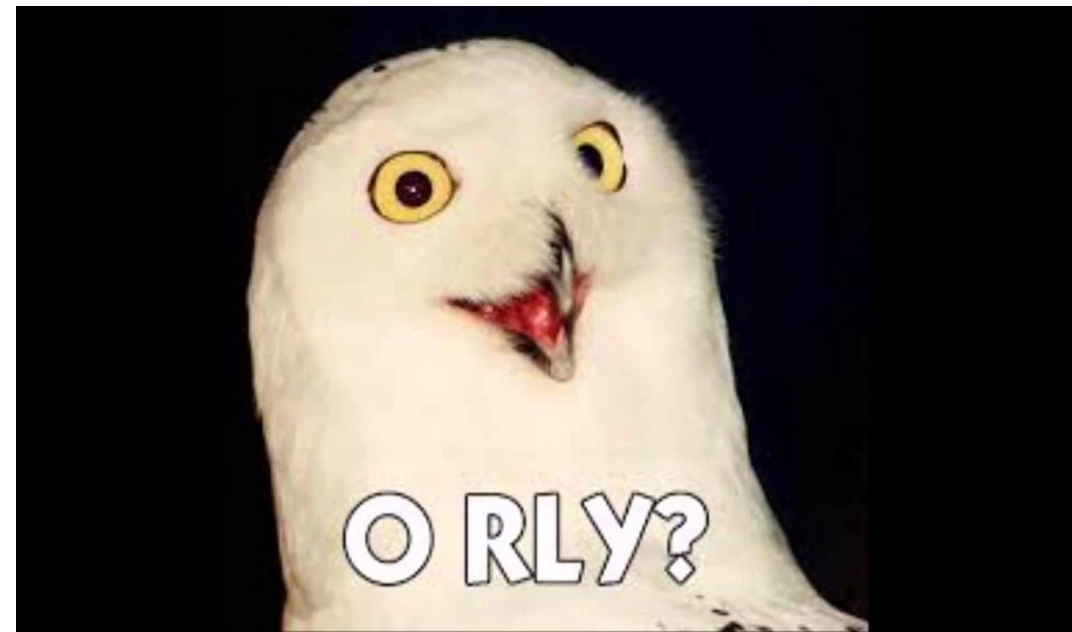
* Learning Layer: Security Awareness:
Friends are not friends: Social engineer he/she don't need to be your friend !
Passwords are Personal: passwords can be exposed by several ways
Uniforms are cheap: Social Engineer can be normal person !

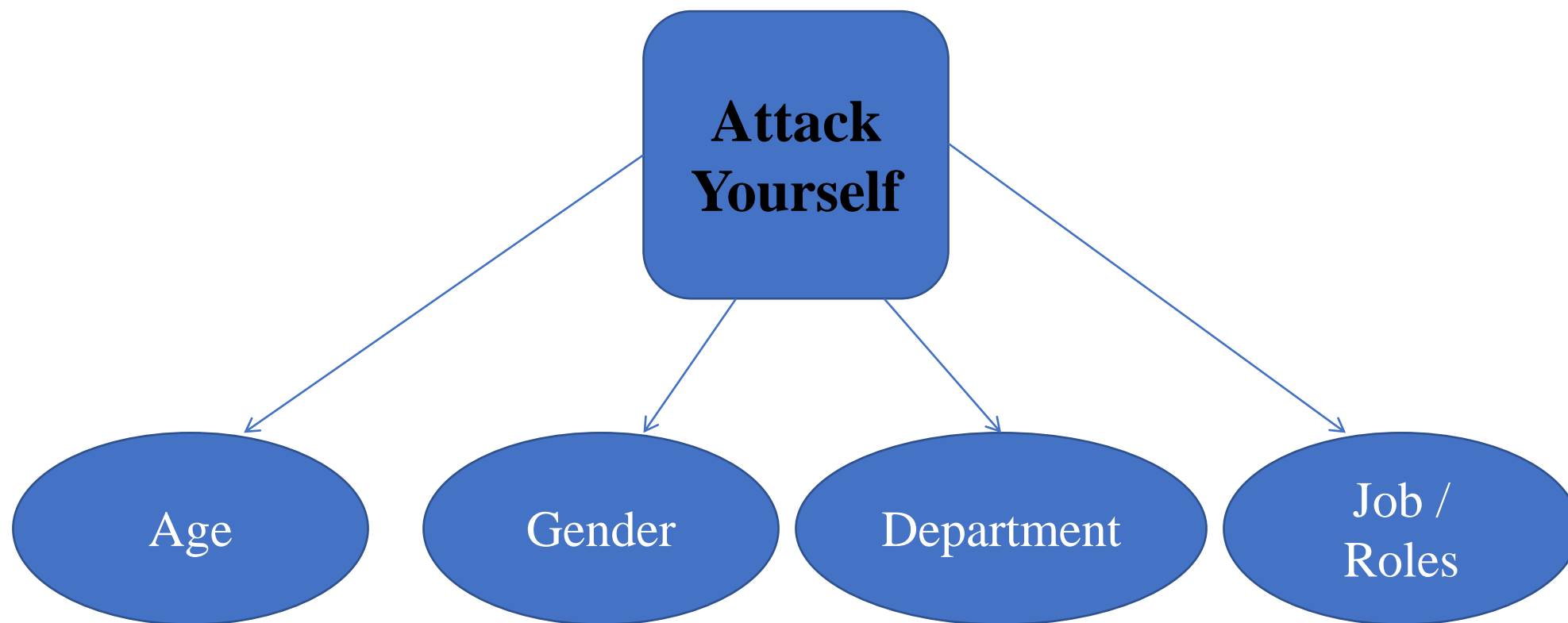* Do not click on malicious links
* Do not install malicious software

Mitigation Gaps

* Users will not make any rational choices
* Punish and Reward is not working anymore
* Don't fire any employee
* It's boring I know → Review Standards and Policies
* Acknowledge them about latest incidents

Mitigation Gaps

Forget about reminders & Emails – Show to them real threats

Mitigation Gaps

Phishing

Request   **Exploit**   **Credentials**

Mitigation Gaps

Method to Help You Decide If Someone's Lying

* Many effective ways to detect lies but only if you practice these skills
* No lie detection magic bullet
* There are many (False positive and False negatives)

Best Way to Detect Lies (**As per Psychologytoday**)

1- Begin ask a series of innocuous Questions and watch eye movement patterns

2- Start to ask the real questions that the person may or may not want to answer truthfully

(Dale Hartley 2017)

Mitigation Gaps

Security Awareness!

Mitigation Gaps

Security Awareness!

Mitigation Gaps

(Urgent Message) "Security Alert": Targeted phishing/email attack campaign on ▬▬▬▬▬▬▬▬
IT Security Team

This message was sent with High importance.

Sent:	Sunday, November 29, 2015 8:45 AM
To:	3 - ALL EMPLOYEES (Head Office); ▬▬▬▬▬▬▬▬▬▬▬
Attachments:	▬▬▬▬▬▬▬▬▬▬▬▬

Based on a report received from The ▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬, attached.

Kindly Note that a group known as "**Team C.L.I.M.A.T.**" is targeting the Oil and Energy Companies with targeted phishing email with pictu[res]
of destroyed landscapes. The group published a target list on the public internet including ▬▬▬▬▬and other oil companies around the worl[d]

Oops! You clicked on a phishing email.
Remember these three 'Rules To Stay Safe Online'

✓ **RULE NUMBER ONE:**
- Stop, Look, Think!
- Use that delete key.

✓ **RULE NUMBER TWO:**
- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium.

✓ **RULE NUMBER THREE:**
- "When in doubt, throw it out". There are a

Recommendations:

You are advised to do the following:
1.   Ensure that your security team is alerted in case of any suspicious mail is received.
2.   Monitor your emails for anomalies or suspicious behavior
3.   Ensure that awareness is raised by being vigilant and informing all employees of the following:
   - Avoid clicking on links in e-mails, especially any which are requesting your username and password
   - Do not open any email message from an unknown source.
   - Be wary of any unexpected e-mail attachments or links, even from people you know.
   - Avoid access to none business browsing categories and social networking.
   - Do not open attachment of certain extensions such as .exe .pac .vbs and password protected compressed files.

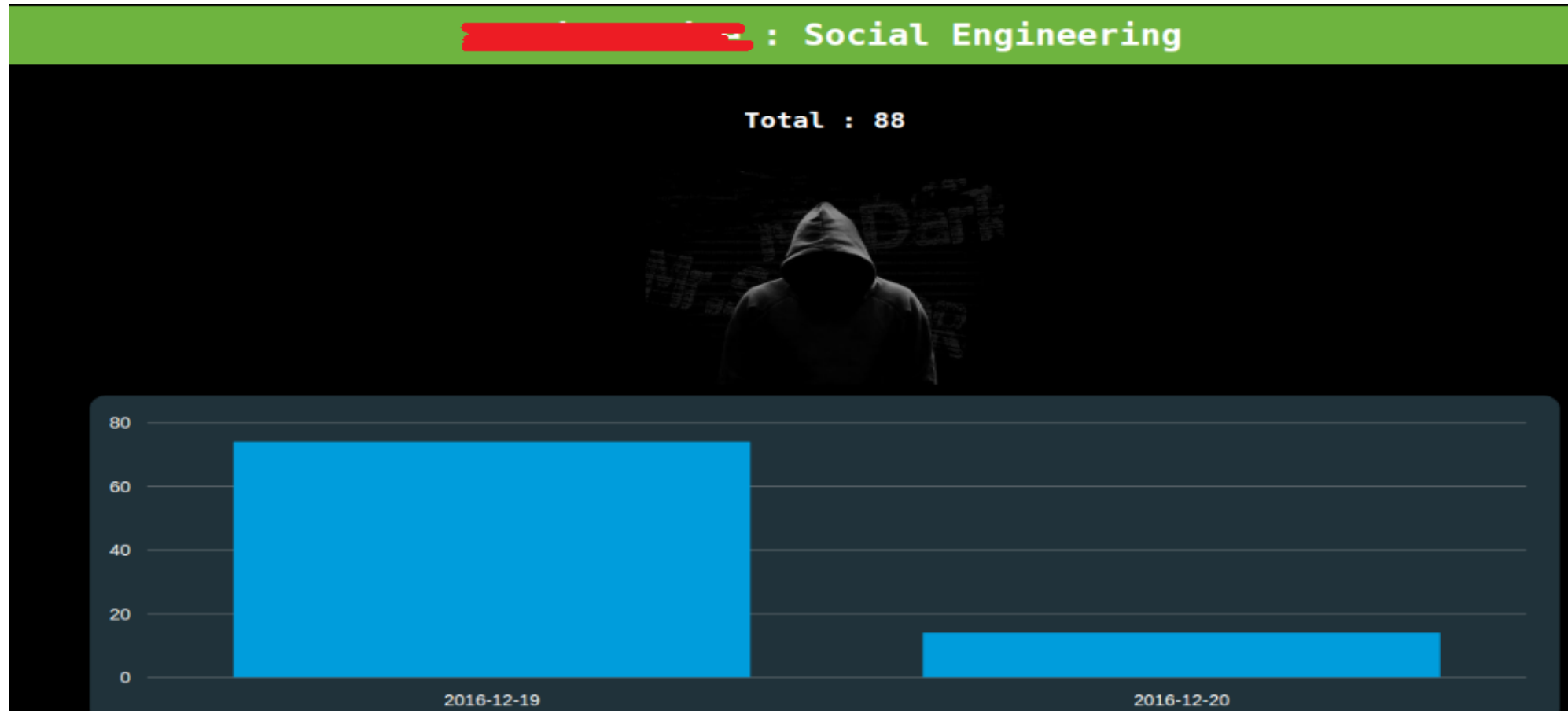You can contact your security team on ▬▬▬▬▬▬▬▬▬▬or call them on Ext: ▬▬▬▬▬▬

Mitigation Gaps

But this happen:
We send a convincing Phishing Mail

Mitigation Gaps

But This Happened

Mitigation Gaps

Mitigation Gaps

Access to one of Power Plants Regulation Login Page

Mitigation Gaps

**The Paranoid is never entirely mistaken
Sigmund Freud**

Mitigation Gaps

It's for you

Your Job is not only break in organization or hack into networks

"Create a touchable moments for who are vulnerable"

questions?