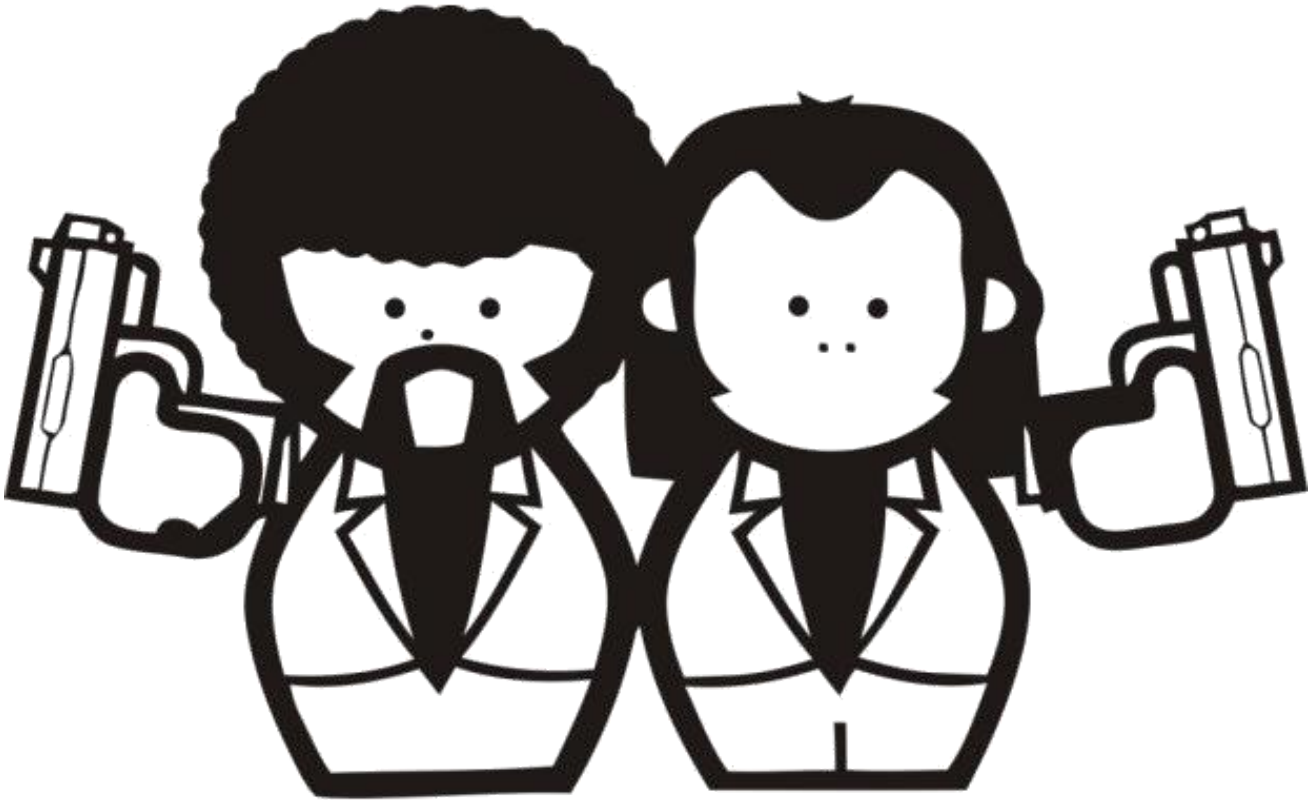
An innovative and comprehensive framework for Social Driven Vulnerability Assessment

20 November 2014

Who are we?



Enrico Frumento

(twitter: enricoff)

ICT Security Specialist @ CEFRIEL

Main Activities: unconventional security, phreak, tweak, psychohistorian, …

Roberto Puricelli

(twitter: robywankenoby)

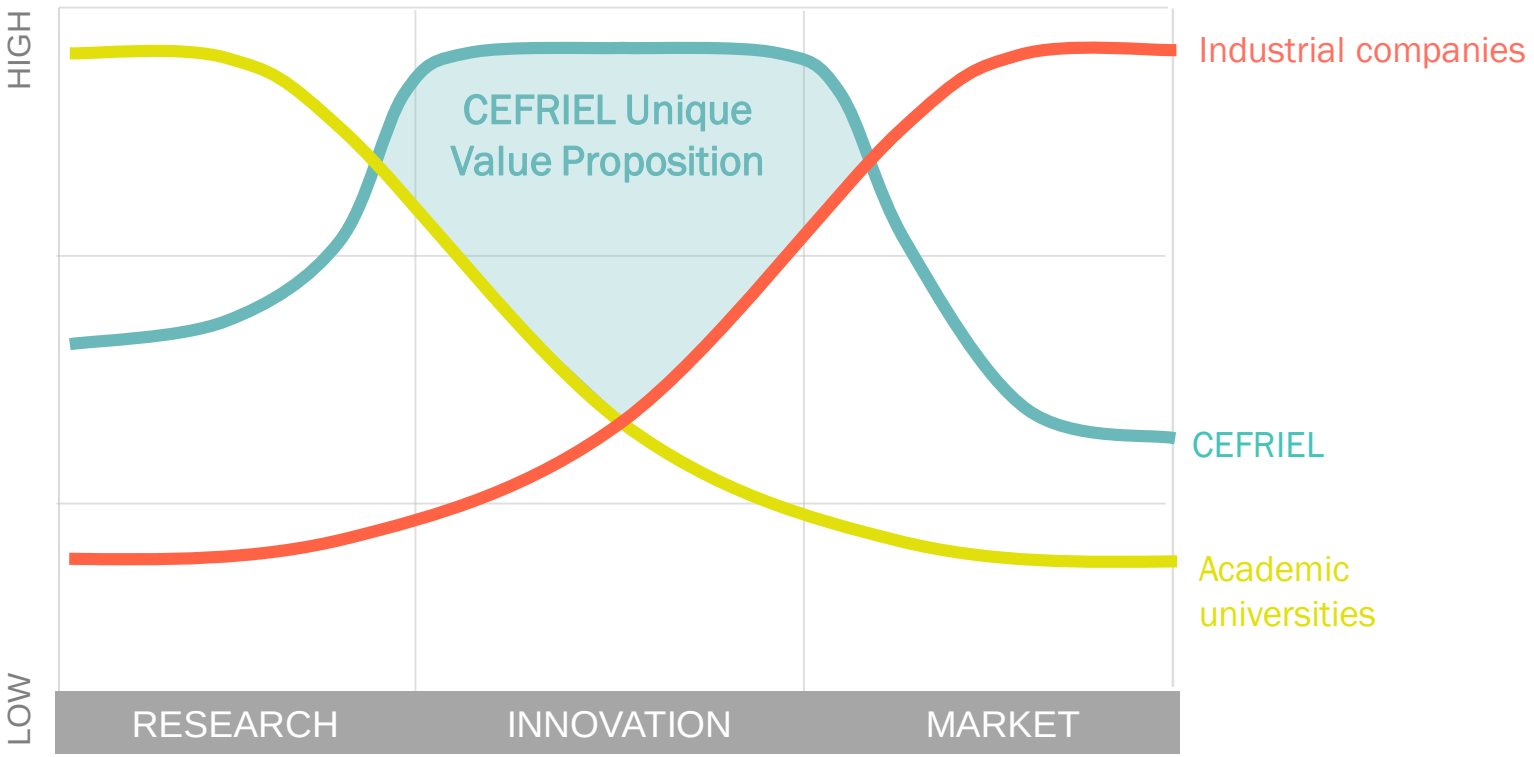
ICT Security Consultant @ CEFRIEL

Main Activities: Social-driven Vulnerability Assessment, Security research, passionate of technology…

Who is CEFRIEL?

Bridging the gap between **industries** and **academia** to

BOOST INNOVATION



What will you get?

What is SE today?

How companies react?

How vulnerable are?

Real numbers

…a lot of phun, but no beers

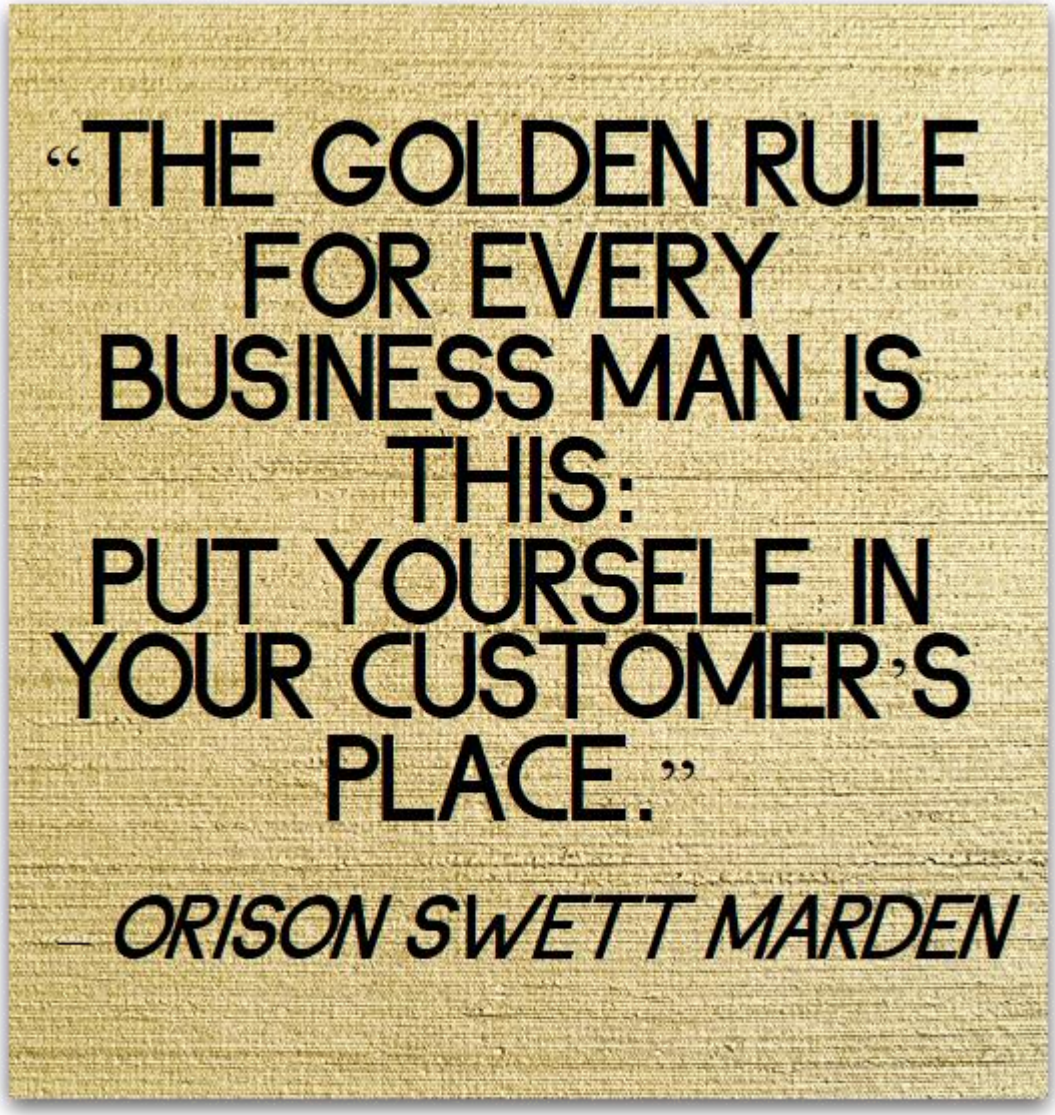
What’s cybercrime today?

From geek-driven to business-driven.

Selling is selling!

What do you need to sell cybercriminals products?

Who’s the customer?



What's cybercrime today?

BOTH TRIES TO ENTER, TWEAKING THE PERSON AT THE DOOR..

DOOR-2-DOOR SELLER

==

MODERN CYBERCRIMINAL-SELLER

What's cybersecurity today?

YES A TOTALLY DIFFERENT APPROACH, USING THE SAME TECHNIQUES OF MARKETING..

VIRAL,

GUERRILLA,

UNCONVENTIONAL,

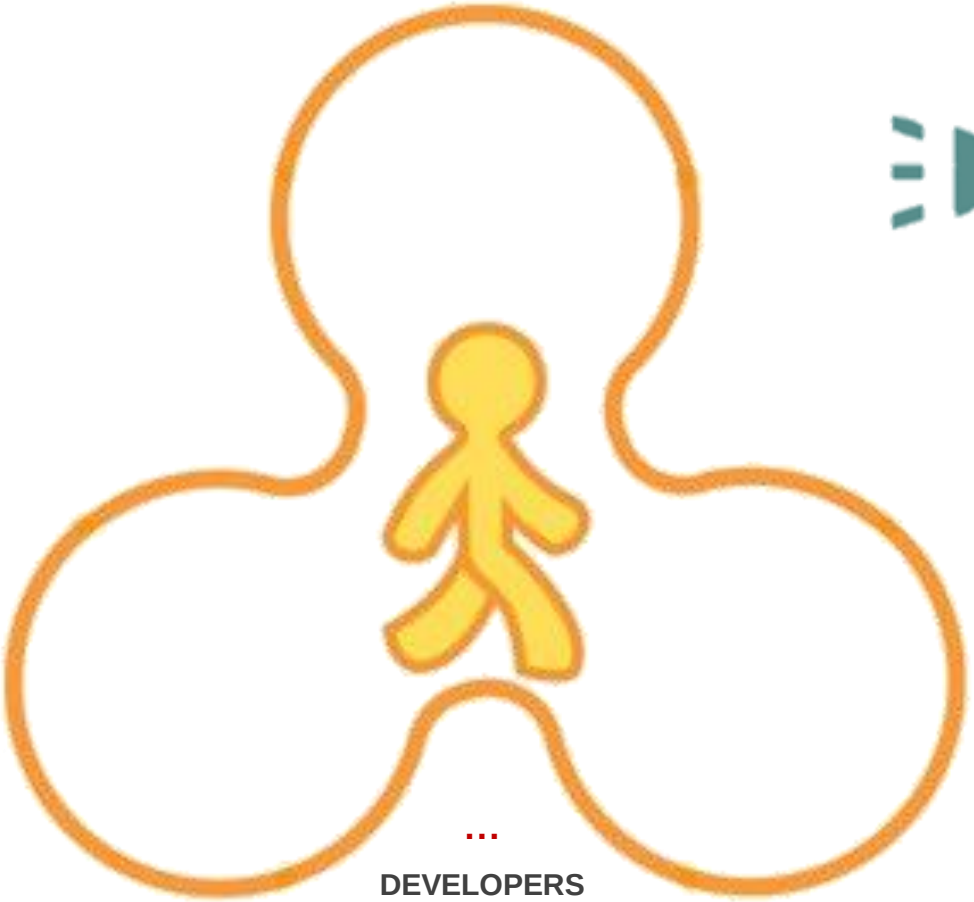
... AND OF COURSE SOCIAL ENGINEERING 2.0

SO WHAT? **ANYTHING NEW??**

What's cybercrime today?

"ADVERTISING"

ADVERTISING



...

DEVELOPERS

SOCIOLOGIST

HCI EXPERTS

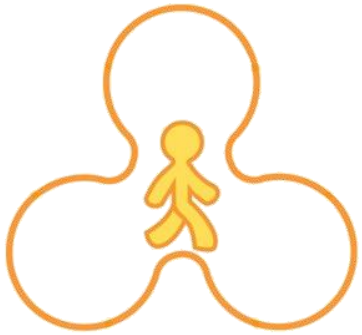
PSYCHOLOGIST

SELLERS

MARKETING EXPERTS

SN INFLUENCERS

What is the security team?

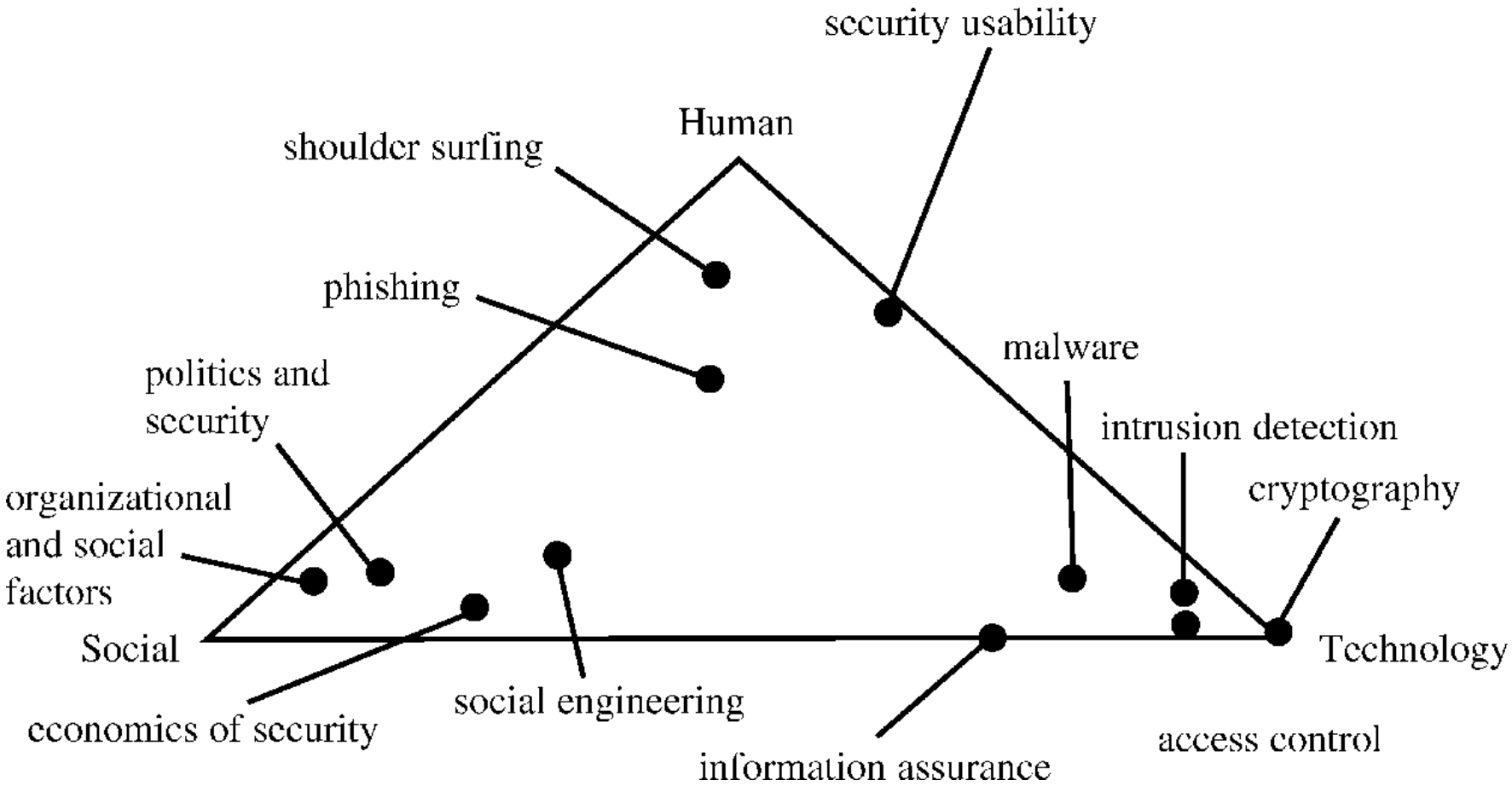


Our team includes several competences

- malware expert
- web designer
- web developer
- psychologist
- expert of HCI interaction
- marketing expert
- SN influencer
- legal advisor

SOCIAL ENGINEERING 2.0

The Role of the Human Factor in Hacker Attacks



Characteristics of SE 2.0

- Malware Ecosystem 2.0
- Automatic Social Engineering Attacks (ASE)
- (ab)use of linked-data
- Chat-bot
- (ab)use of psychology, personality profiling systems and cognitive science models
- Mail attack vector
- Economic Drivers

Malware Ecosystem 2.0

SE became an important part of the malware 2.0 and the main infection strategy

Automatic Social Engineering Attacks (ASE)

Automation of SE attacks through information collection and mining and through the **sentiment analysis** from Social Networks

(ab)use of linked-data

The public bodies and anyone are moving toward the free circulation of data, to the web 3.0.

This is the **Linked-Open-Data** or **web-of-data**.

(ab)using LOD will facilitate the collection of data to fully contextualize attacks to targets.

Chat-bot

Diffused use of chat-bot, as in **ASE** attacks to start and maintain conversations with other social networks users and to balance the lack of a real social engineer (**mass social engineering attacks**)

(Ab)use of Psychology and Cognitive Science

Professional use of **memetics** and **personality models** of the attacked users, especially of models coming from theories of **cognitive psychology**

Mail Attack Vector

Massive use of mails - if compared to other attack vectors - since it doesn't need **talented hackers** and it can reach lot of victims at a time (i.e. new forms of spam)

Economic Drivers

SE 2.0 is since the beginning an investment (no ways doing it for phun), all attacks have one common aim: **making money**.

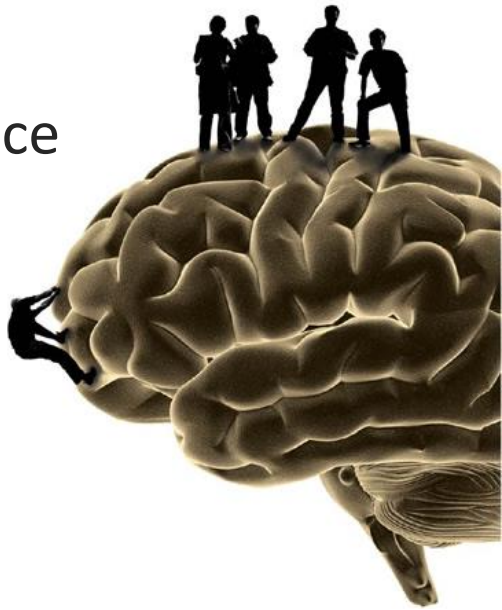
Characteristics of SE 2.0

USE

VS

(AB)USE

Characteristics of SE 2.0



(ab)use of psychology and models of cognitive science

Professional use of memetics and personality models of the attacked users, especially of models coming from theories of cognitive psychology

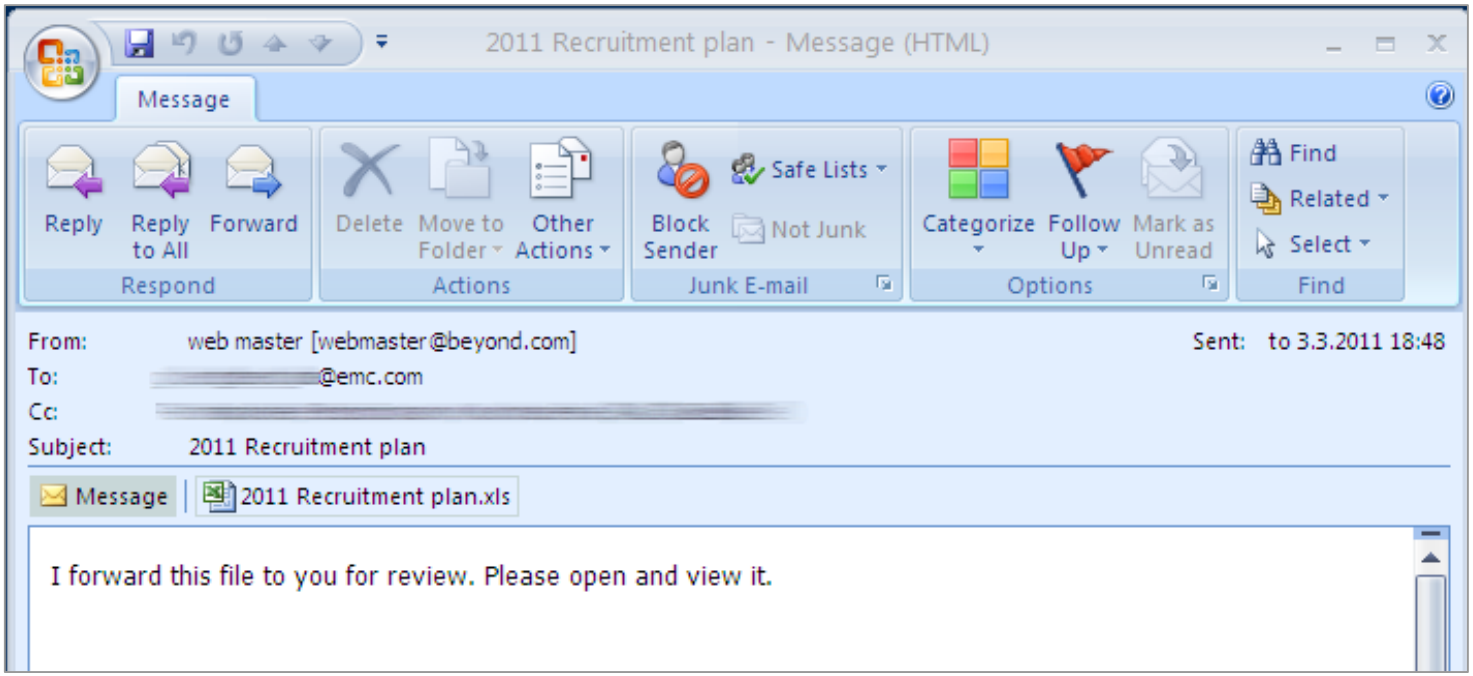
(ab)use of Social Networks

Social Networks are fantastic sources of information about victims, tastes, personalities, profiles, etc. The phase of information collection about the target in a crucial step for each attack.


It's advanced!
It's persistent!
It's a threat!

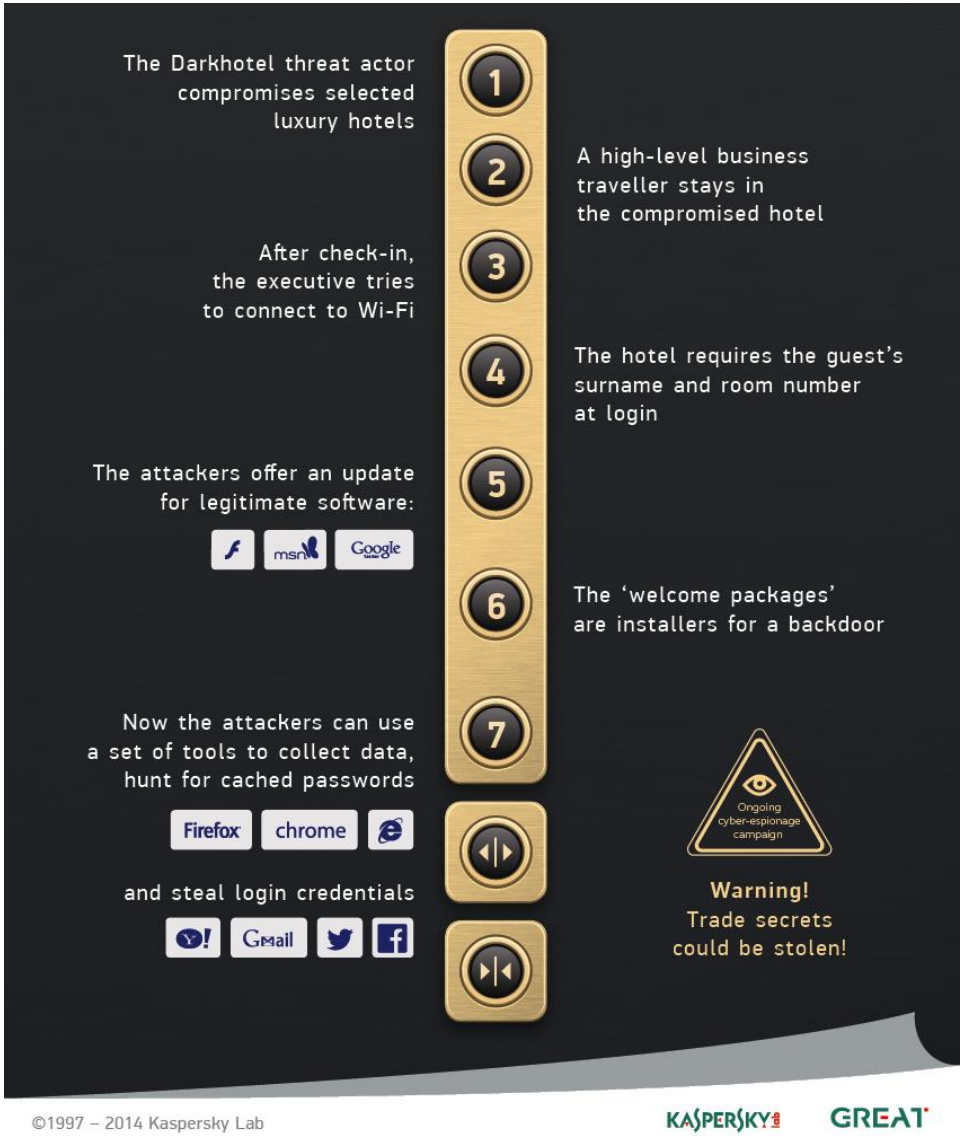
The first example… RSA

THE case study…



You probably know this email

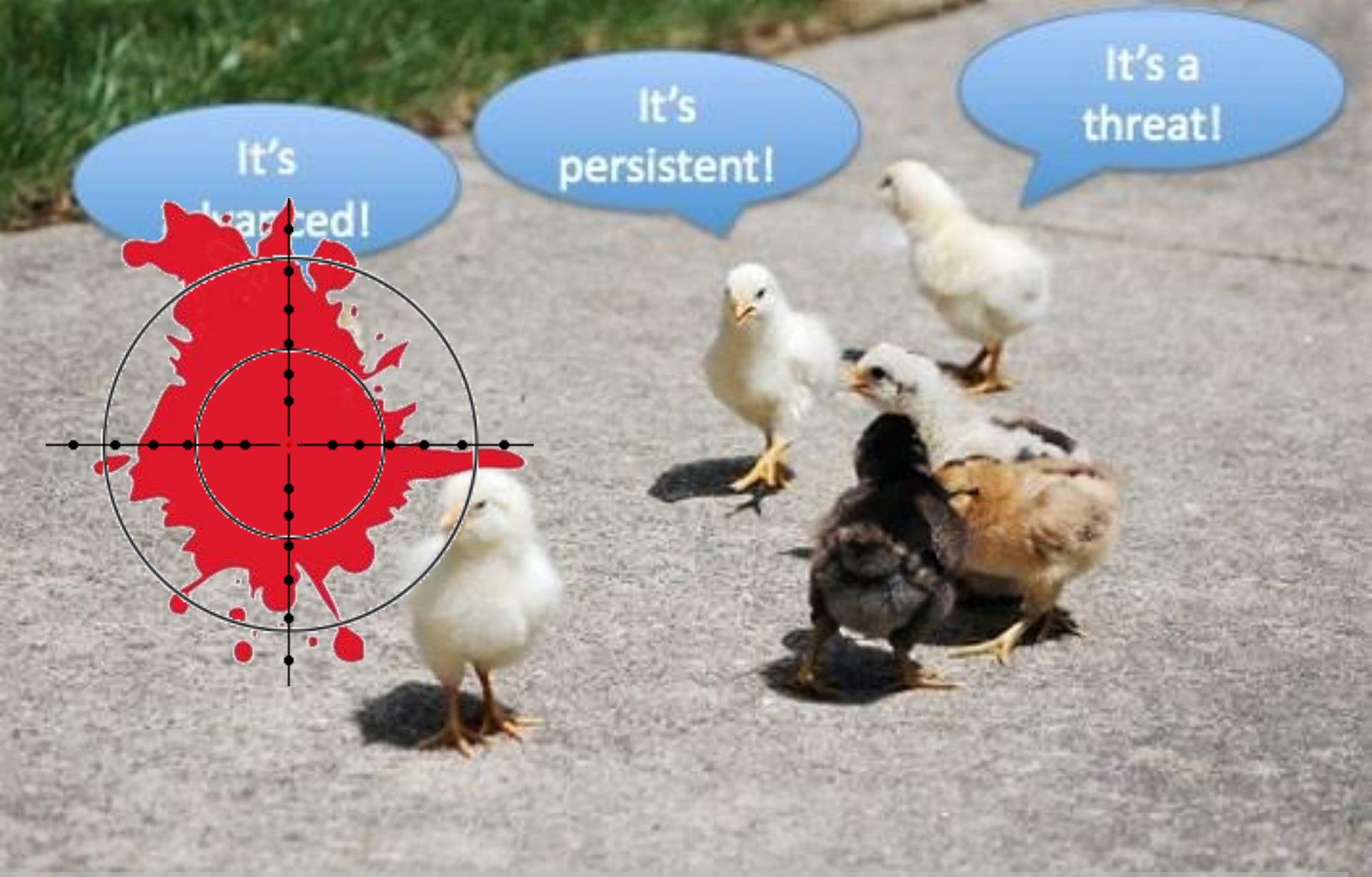
.. the latest one: Darkhotel attacks



- More than 7 years
- Target business executives
- Drive-by download attack
- Steal data and collect passwords

What's in common?

Social Engineering at the beginning



PROBLEM: IT'S NOT ANYMORE SO ADVANCED.

"ADVANCED" ONLY MEANS THAT THE ATTACKERS HAVE A (DEVILISH)BUSINESS PLAN

Advanced Persistent Threat Model

An APT often begins with a Social Engineering attack

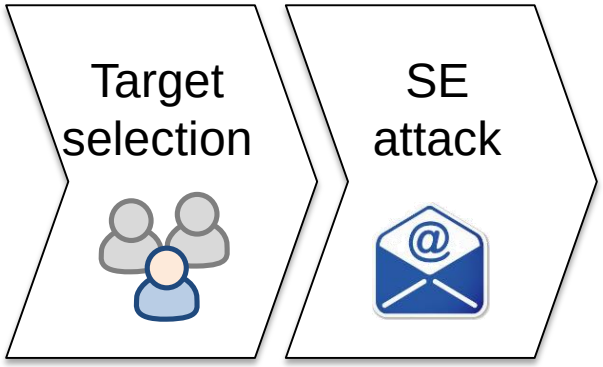
- Email is the most used attack vector

- How to build an effective attack?

Advanced Persistent Threat Model

Spear phishing is the new evil

- A contextualized email is more effective

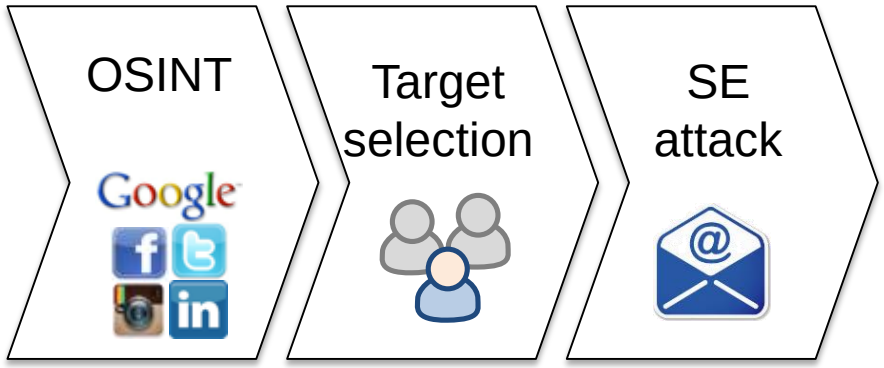


- How to gather information?

Advanced Persistent Threat Model

Internet and Social Network allow to retrieve lots of information

- Public information are already available
- Also “active” attacks

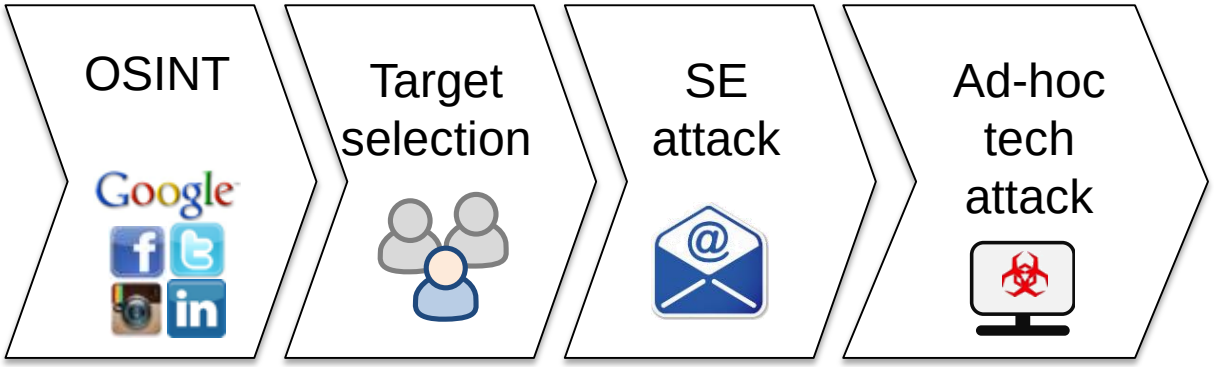


- What’s the result?

Advanced Persistent Threat Model

Technological attack can create a backdoor inside the company

- Known vulnerabilities or zero-day attacks



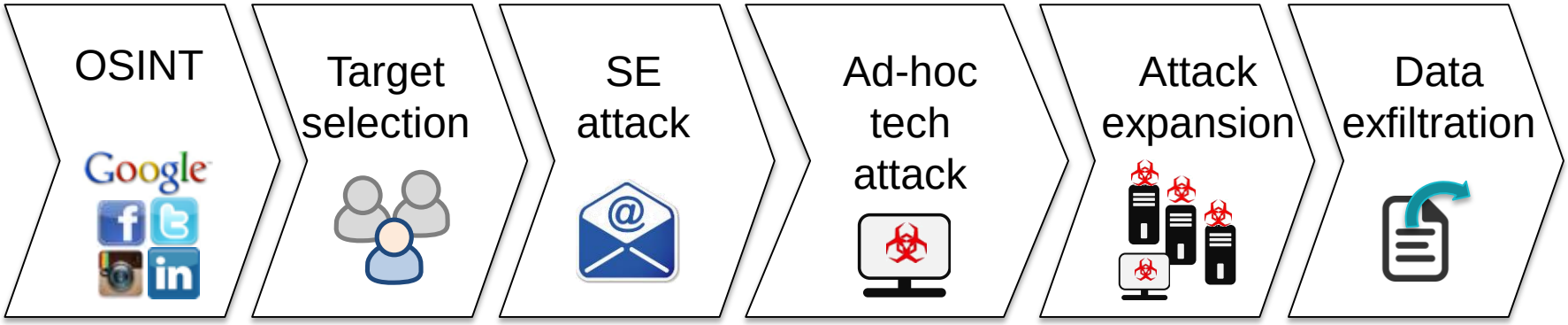
- What's next?

Advanced Persistent Threat Model

Inside the network, lateral movement

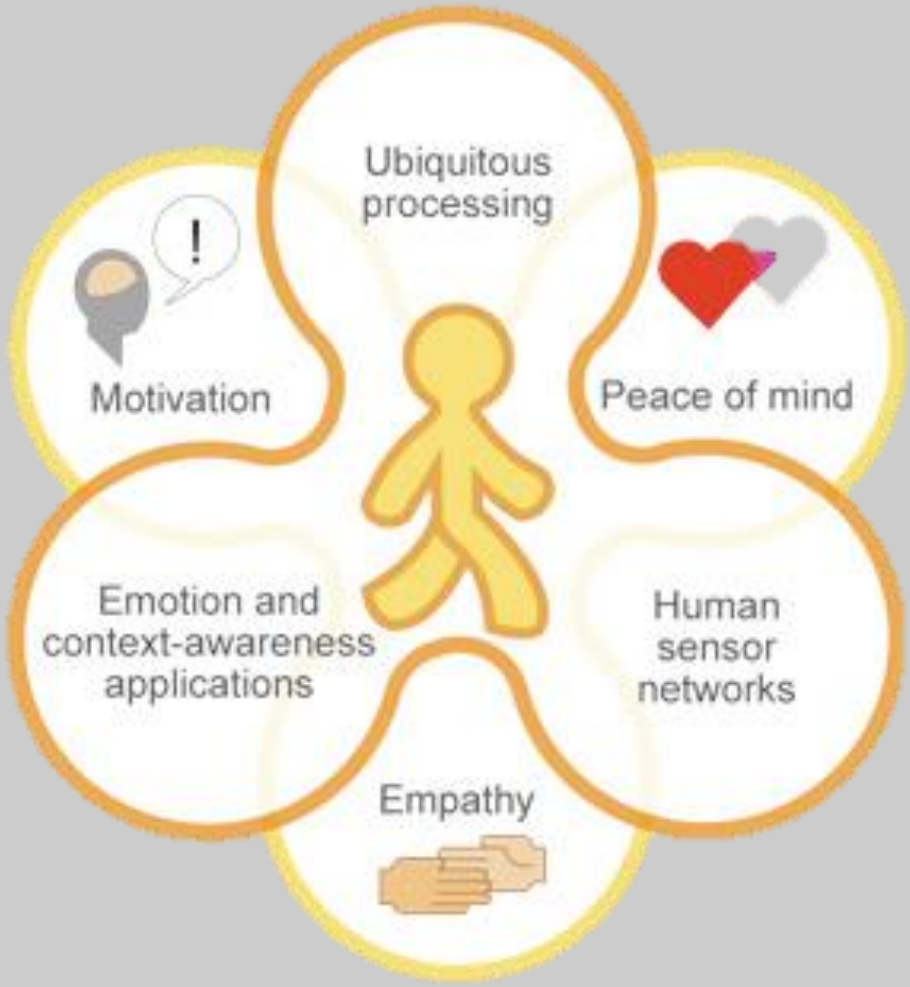
Difficult to detect slow and punctual attacks

Advanced Persistent Threat Model

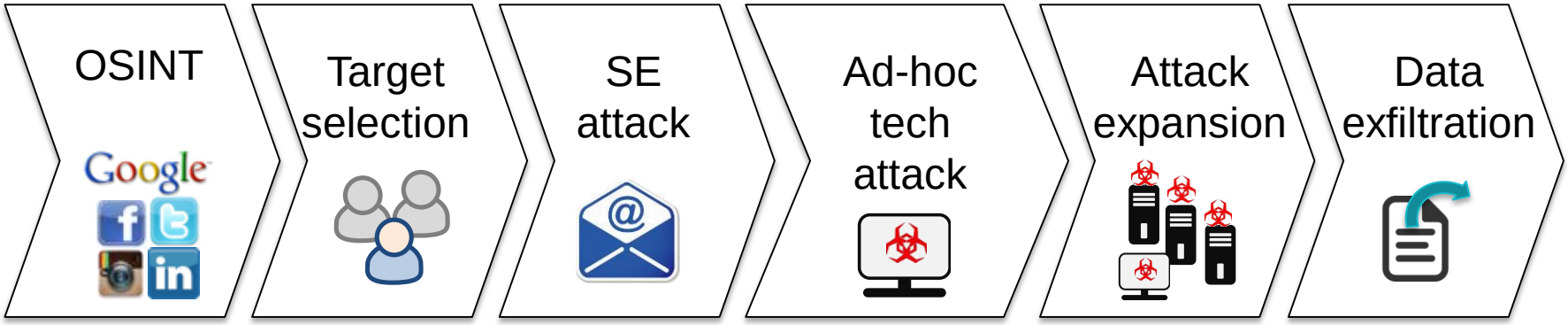


How can we measure that risk?

OUR FRAMEWORK



Our Framework

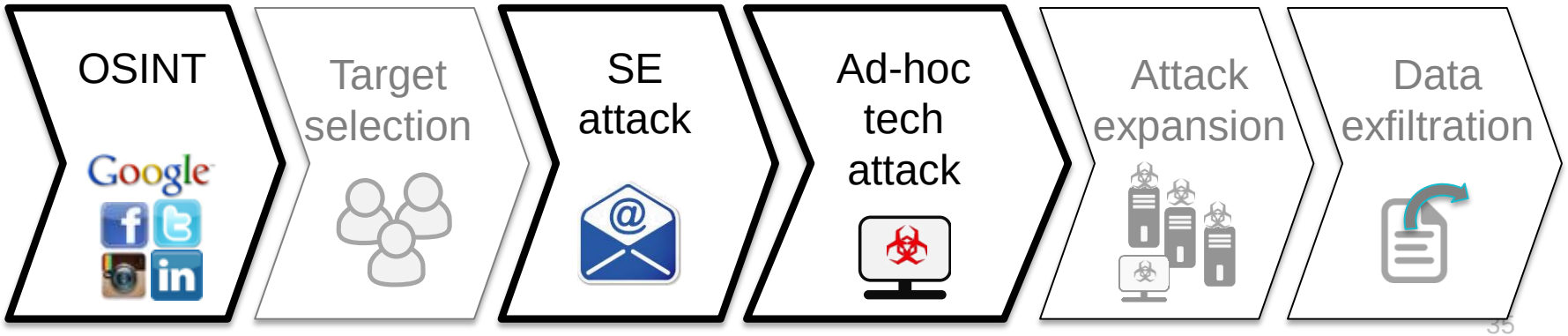


Our Framework

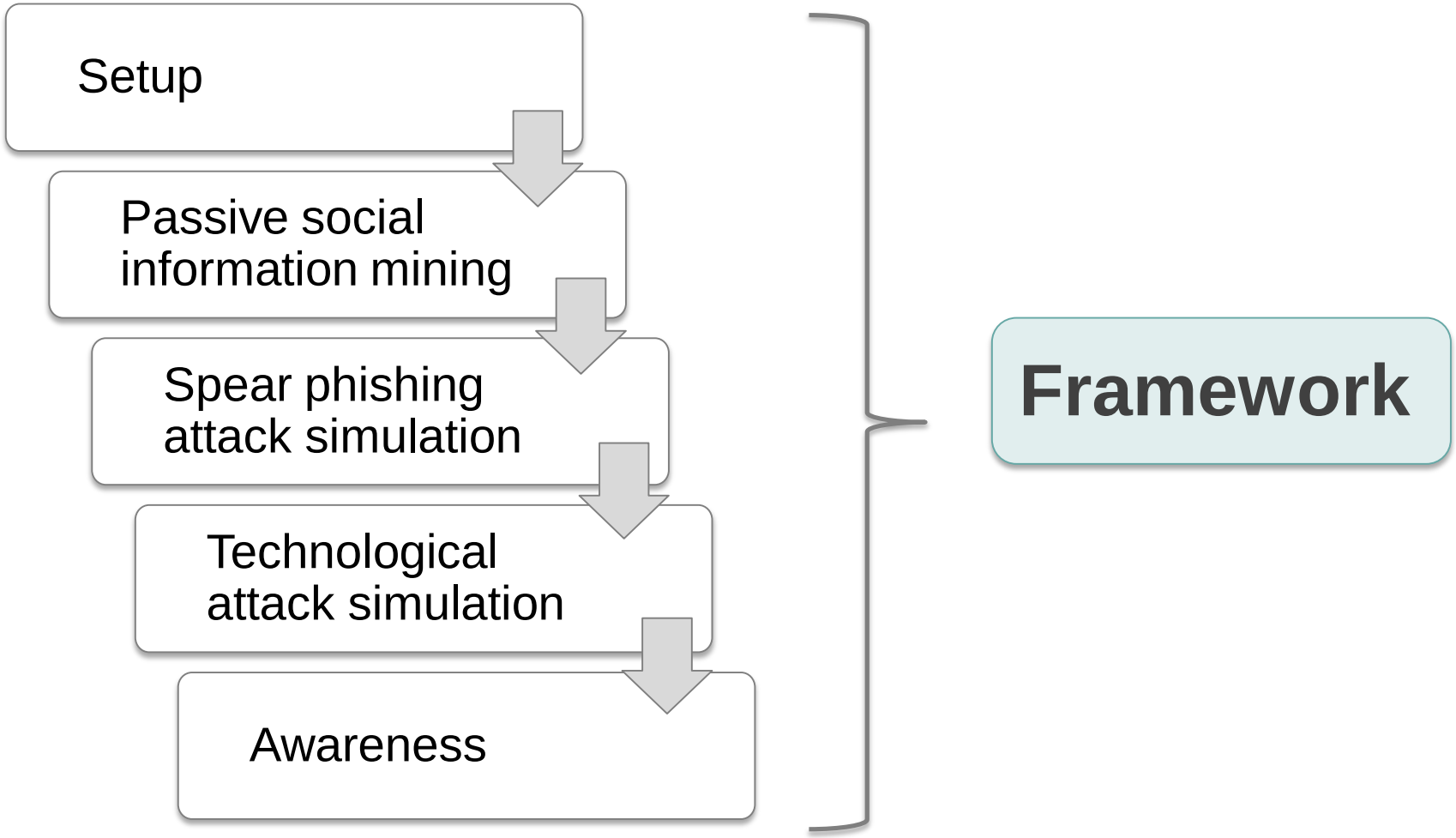
Passive social information mining

Spear phishing attack simulation

Technological attack simulation



Our Framework



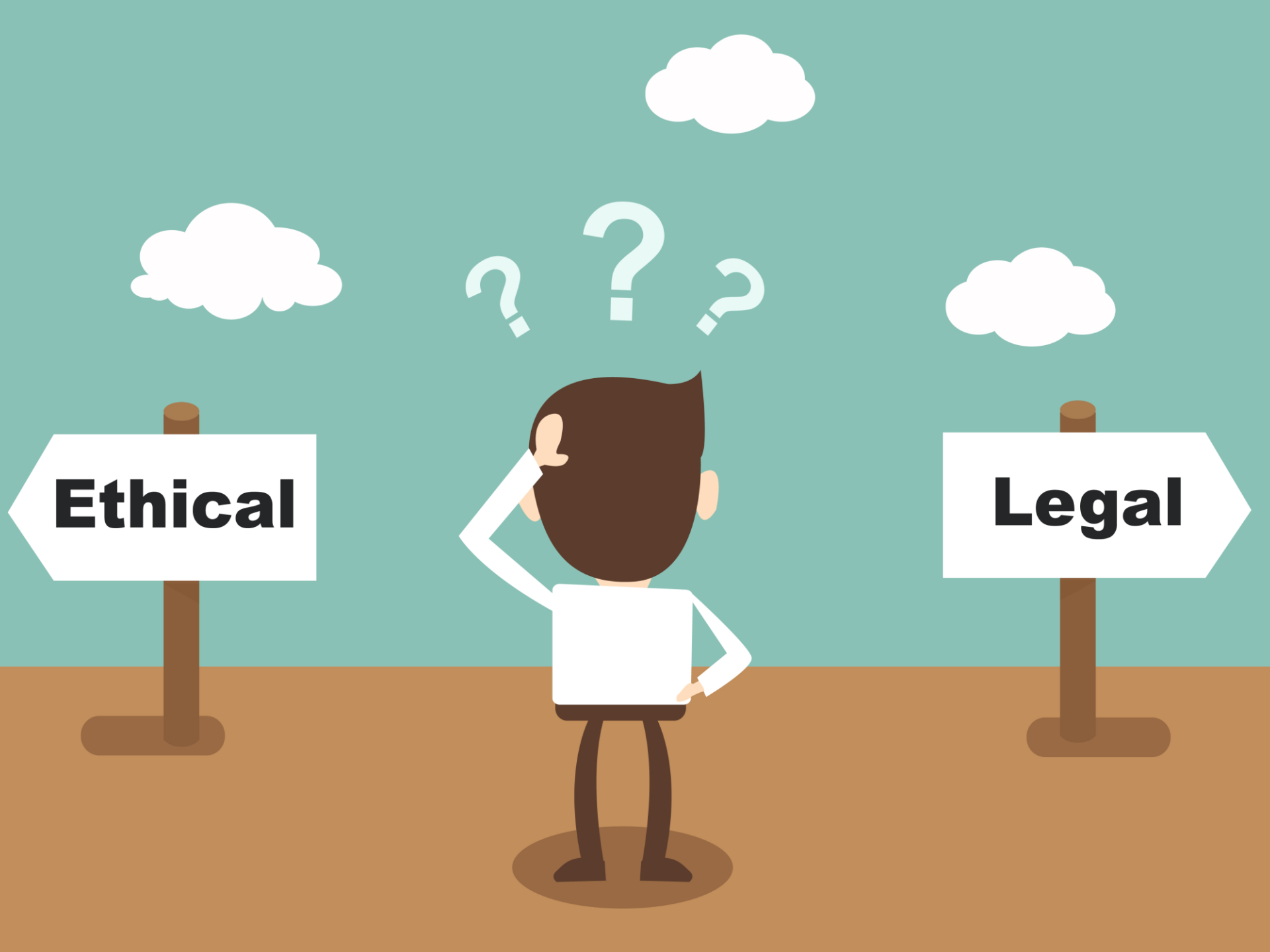
Setup

Prior to start the assessment, it is necessary to **provide a startup phase**

Since the activities is innovative stakeholders need to:

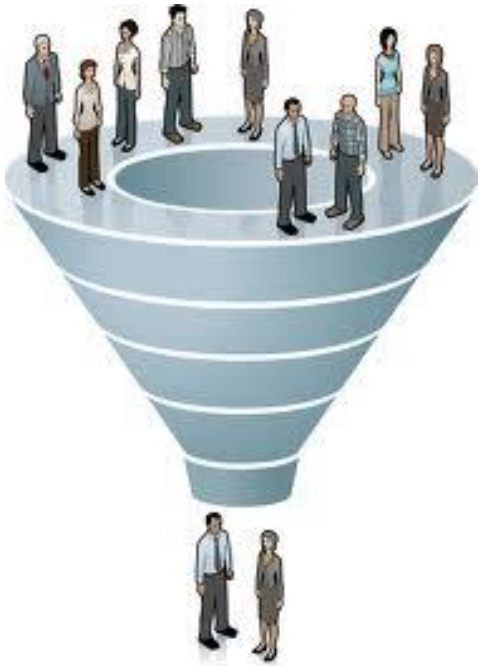
- share objectives
- define the boundaries

Stakeholders of the company


Ethical
Legal

Passive information mining

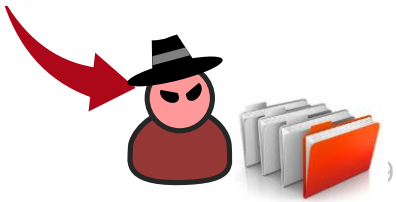
The purpose is to find some evidence regarding the **feasibility of the social engineering attack**



Focus on the company, not on the user

Even if the source are public, lot of information retrieved…

..and it's just the tip of the iceberg



WEAPONS OF

MASS DISTRACTION

Source2
123
mail

Source3
11 mail

Source1
633 mail

Source4
103 mail

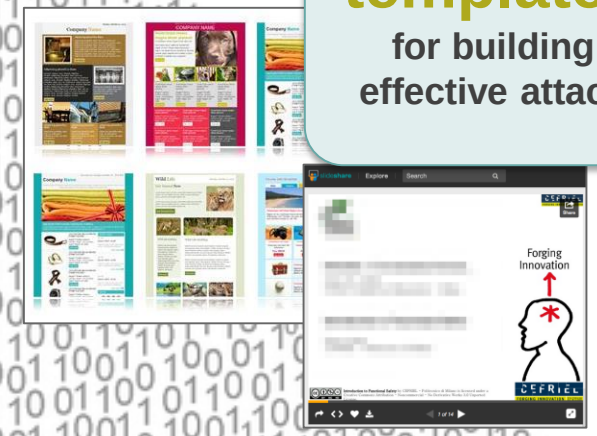
Source5
91 mail

emails
of employees
possibily attacked

initiatives
related to
company or
employees

templates
for building
effective attack

evidence
related to specific
risks



Spear Phishing Attack Simulation

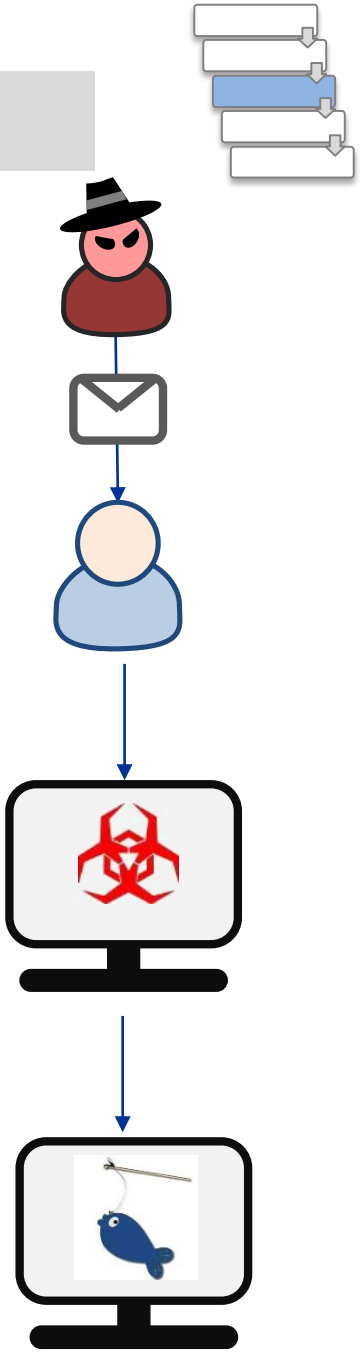
The purpose is to **test the user behavior** when stimulated with social engineering attack

It begins with emails sent to employees

Target is a sample of employees

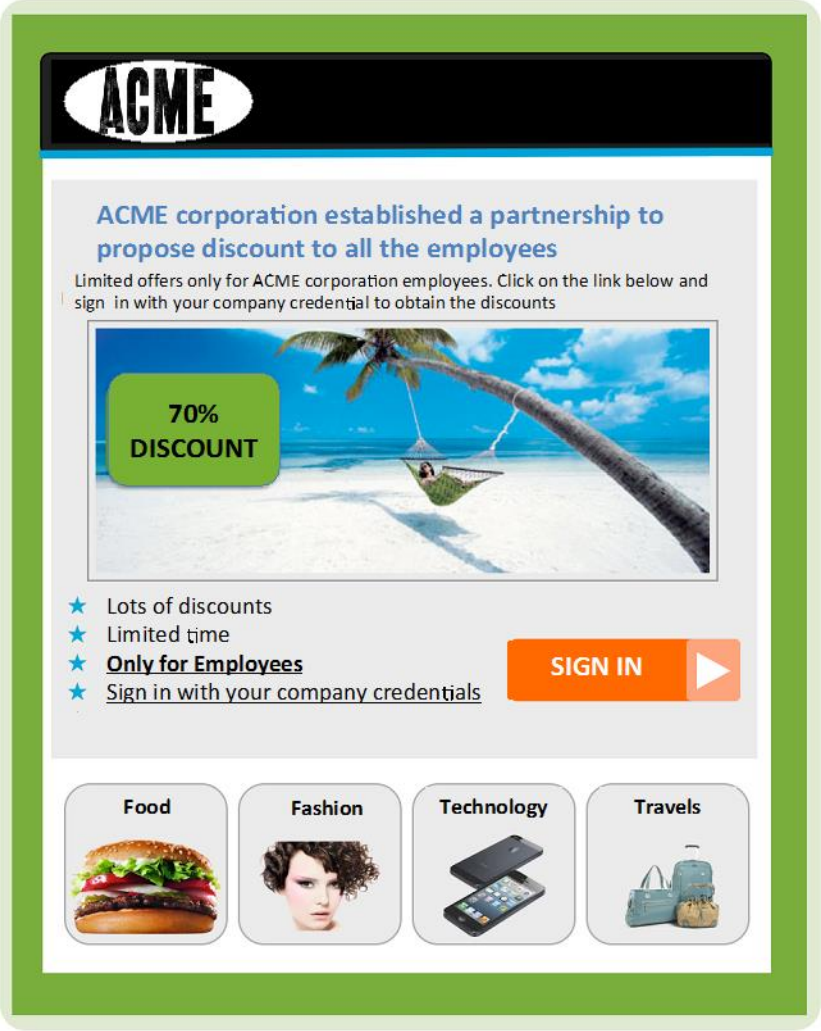
We evaluate two different type of risks:

1. The user click on the email
   - Expose to drive by-infection
2. The user also provides the requested credentials
   - Lose of a critical company asset



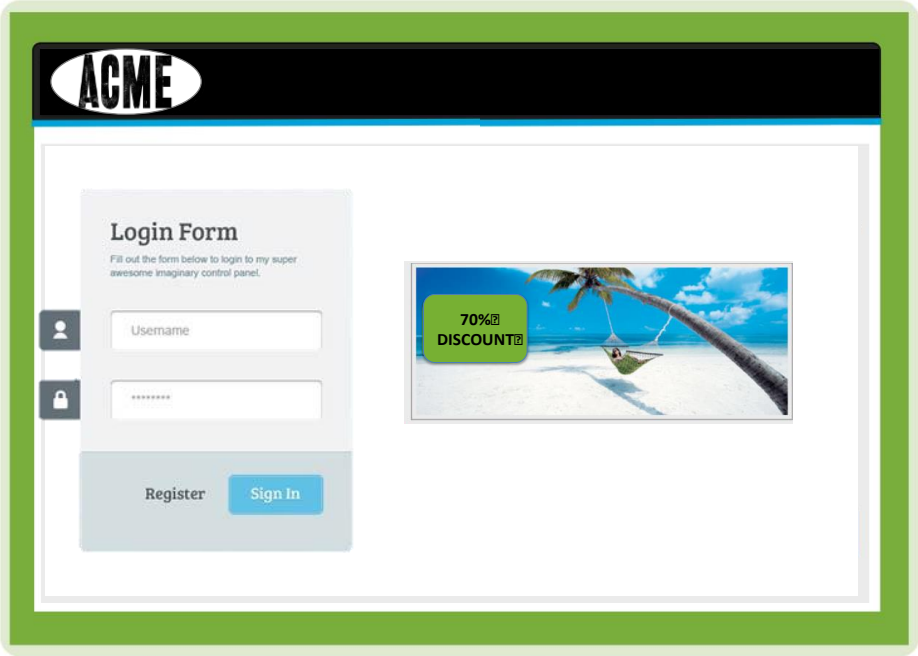
Type of phishing: A SDVA Example

An example of email for a SDVA test



Type of phishing – Example of a website

An example of the related phishing website



Refers to the phishing campaign

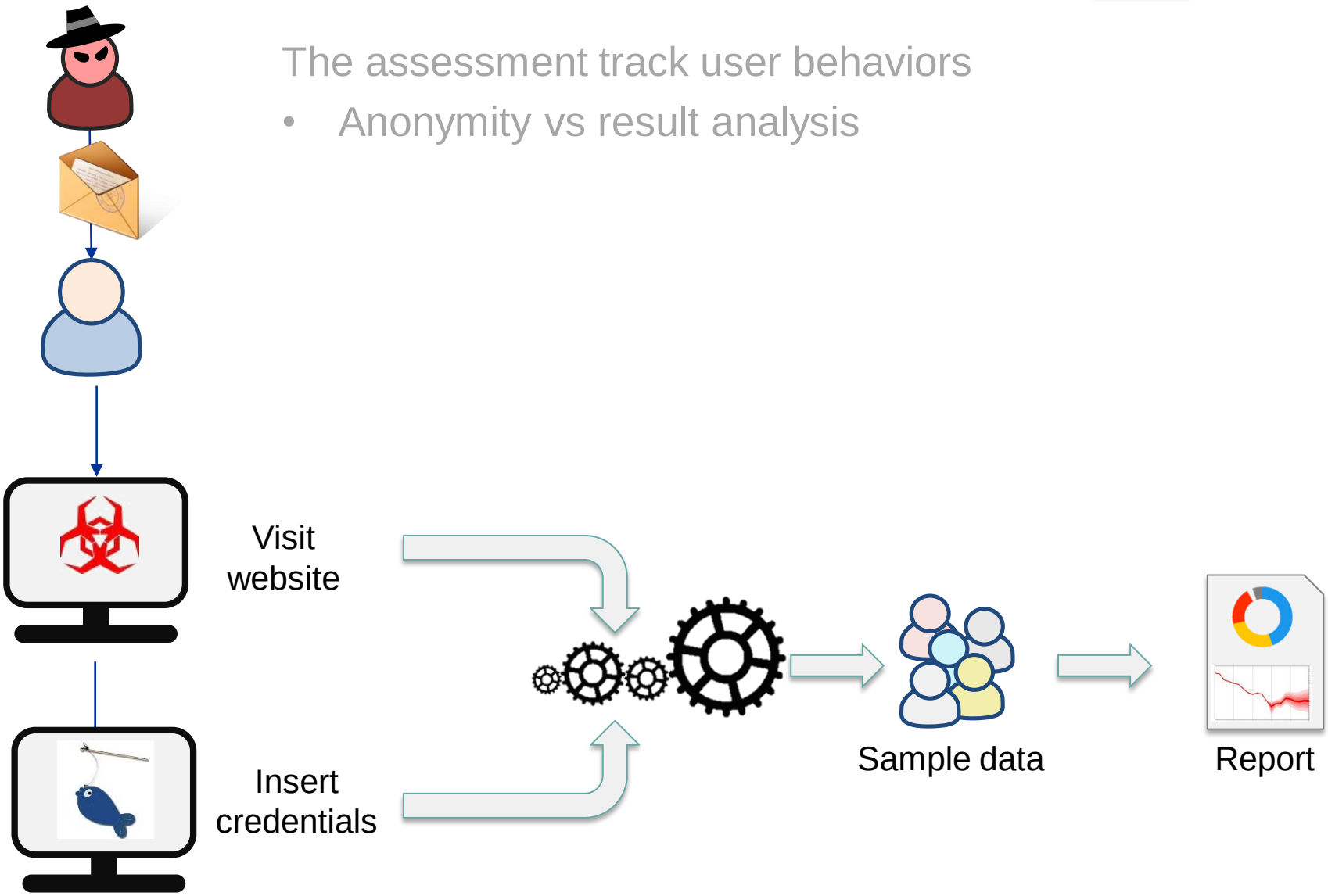
Company asset requested (credential)

Both email and website contains clues that allow to identify the risk

Collected information

The assessment track user behaviors

- Anonymity vs result analysis



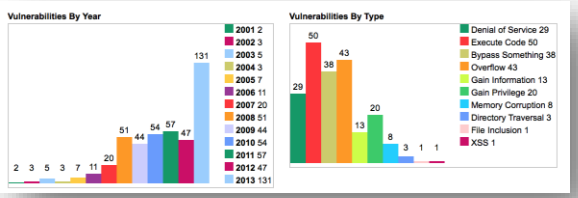

People often have potentially dangerous behaviors
Most part of Workstation analyzed include
Obsolete or Unpatched Software

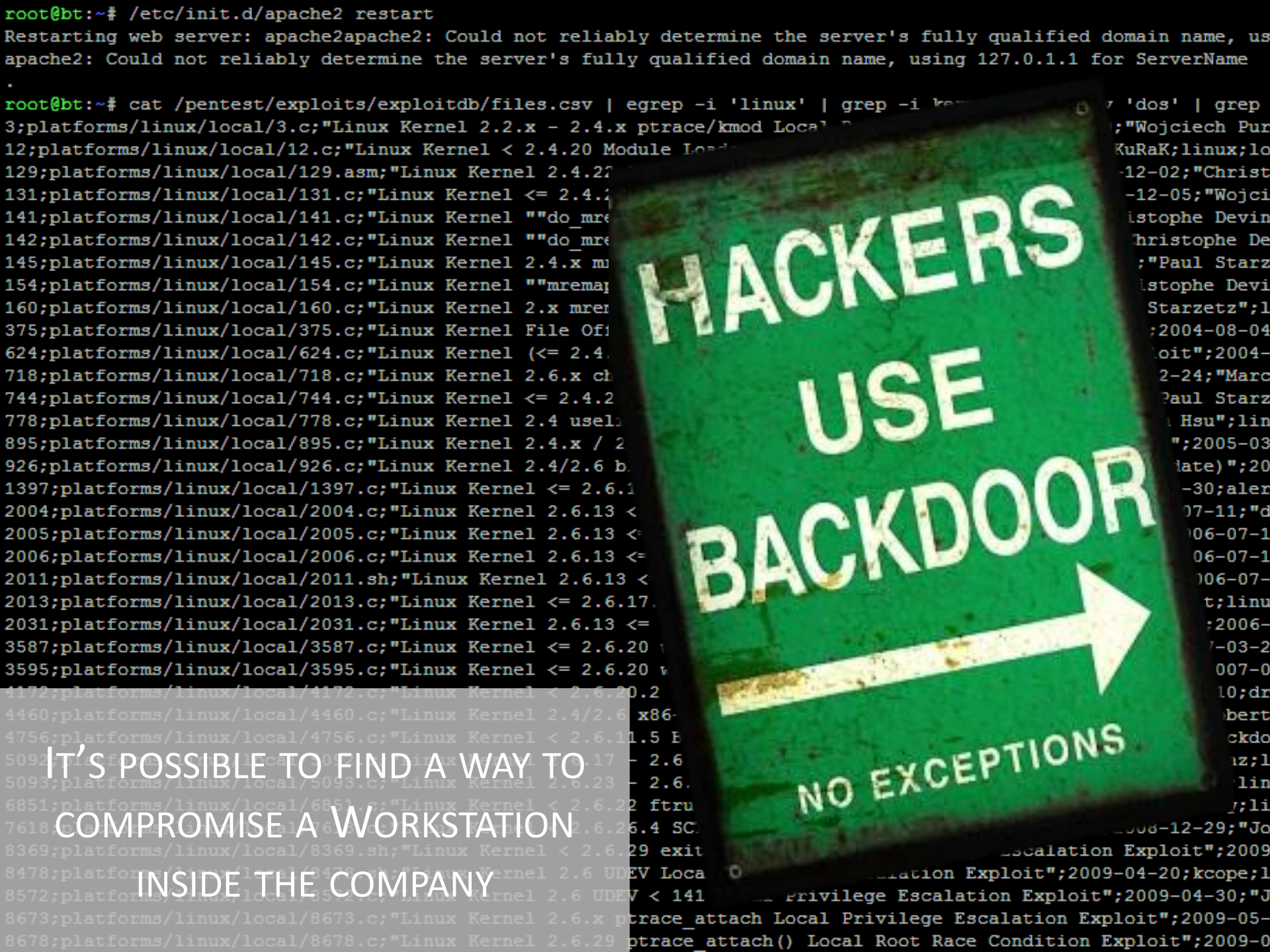
Technological attack simulation

The aim is to **demonstrate the possibility to compromise the company laptop**, knowing its configuration

Usually through a proof-of-Concept

- Analyze software configuration
- Correlate with vulnerabilities
- Create a custom exploit payload





It's possible to find a way to compromise a Workstation inside the company

Awareness

The assessment should help to **raise awareness inside the company against these threats**

People is the weak point

- Management need to be aware
- Employees need to know

Training and awareness is the only (nowadays) effective countermeasure

..but need to be properly done.

Video
Raise awareness through visual information

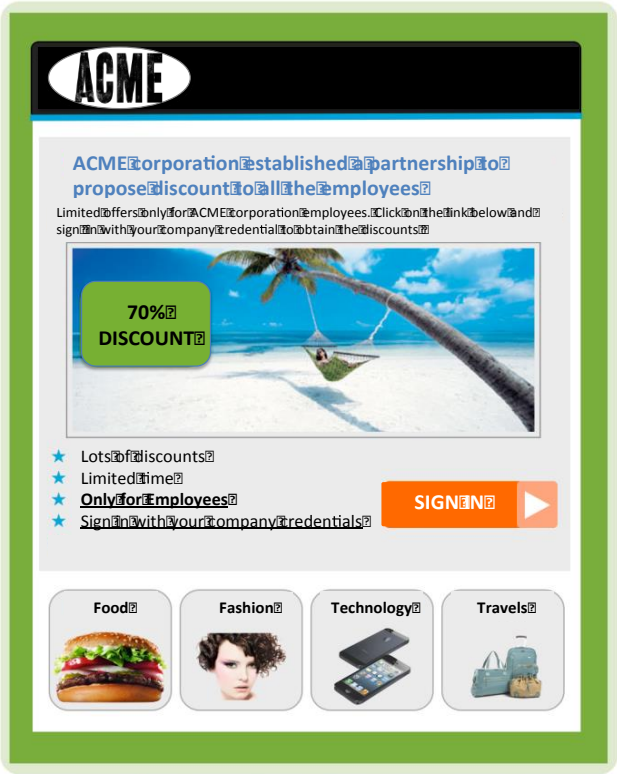
Pills
describe correct behaviour

Gamification
Stimulate users to enhance learning

RESULTS

Our experience

In the last five years we performed about **15 SDVA** in big enterprises with thousands of employees, involving about **12000 users**

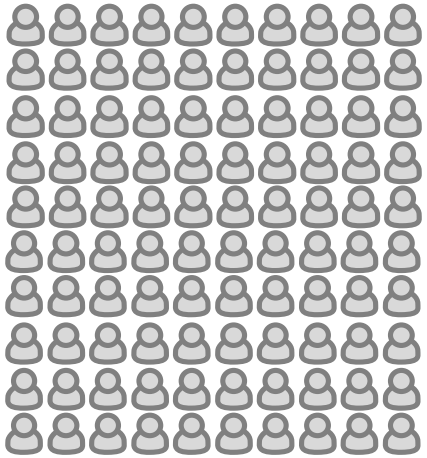


Given an example of a possibile test email

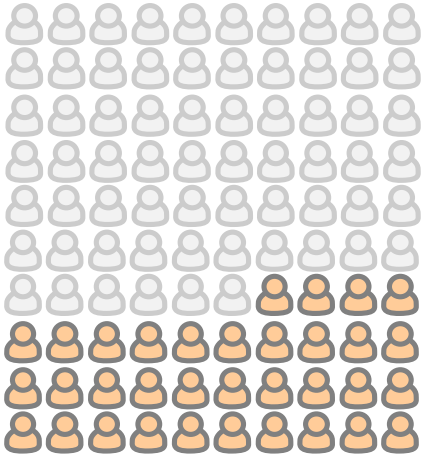
In your opinion, what are the results ?

Overall results

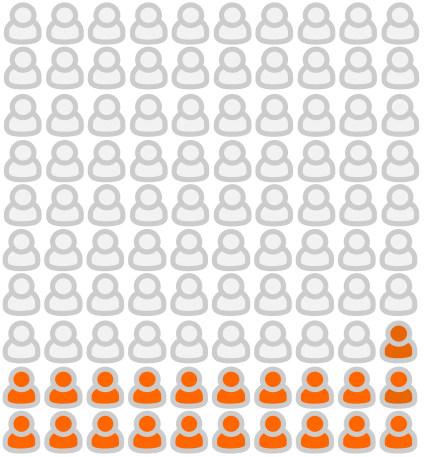
Employees receive the email



34% visit the website



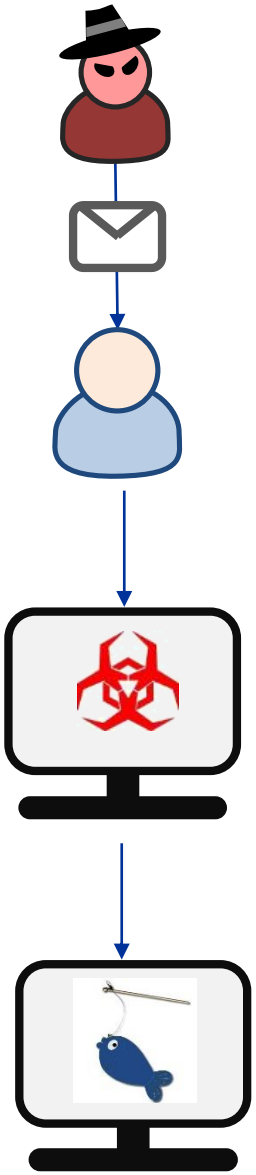
21% also insert the credentials



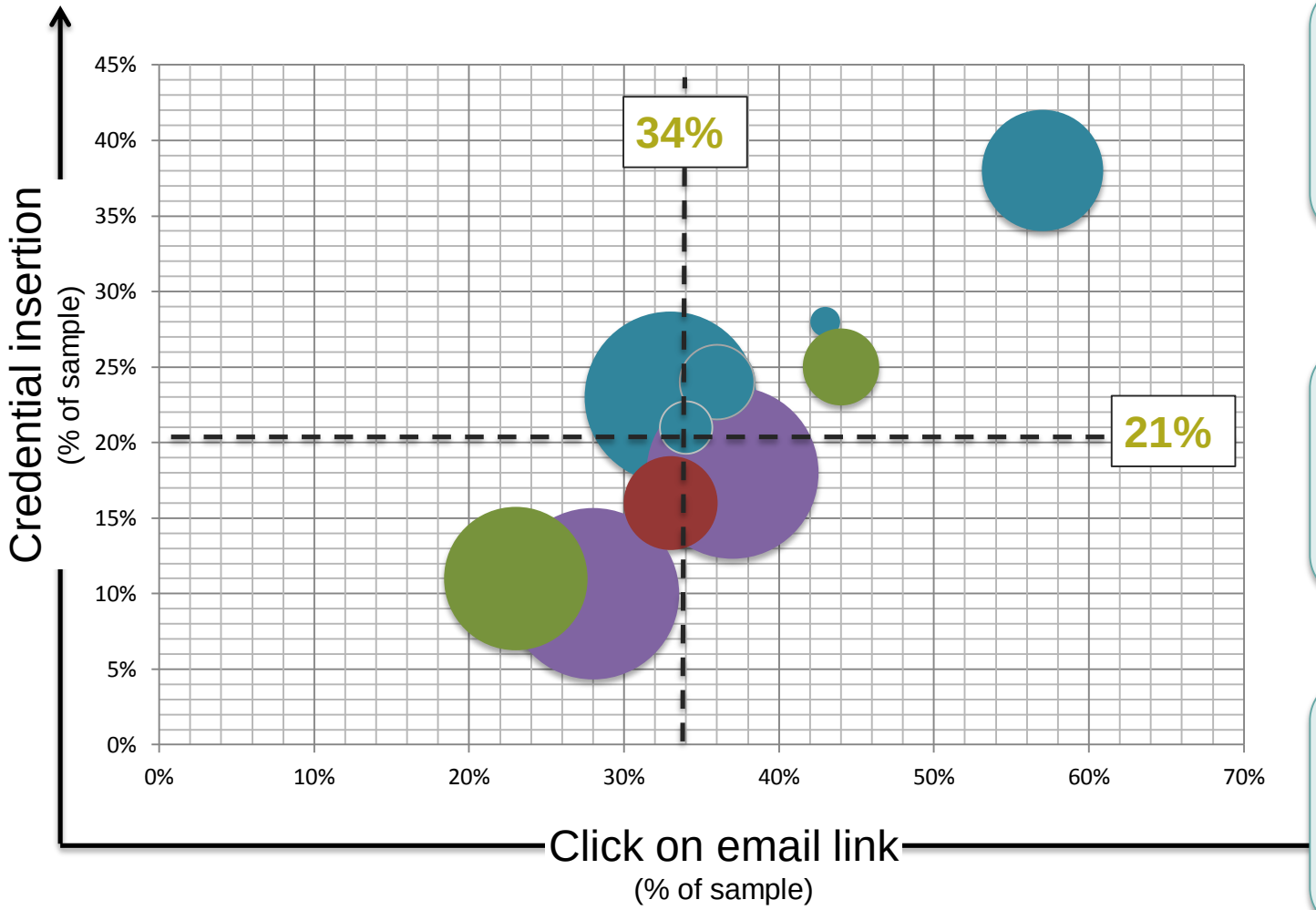
Benchmarking

Credential insertion
(% of sample)

Click on email link
(% of sample)



Benchmarking

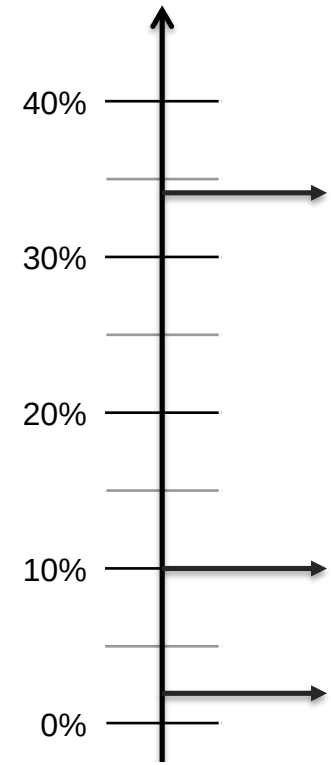


3 emails
to obtain one click

5 emails
to obtain a valid credential

58%
conversion rate
click/insertion

Comparison with other studies



Success ratio
(% of overall success)

34% Average click rate in our research

10% Average click rate in modern phishing

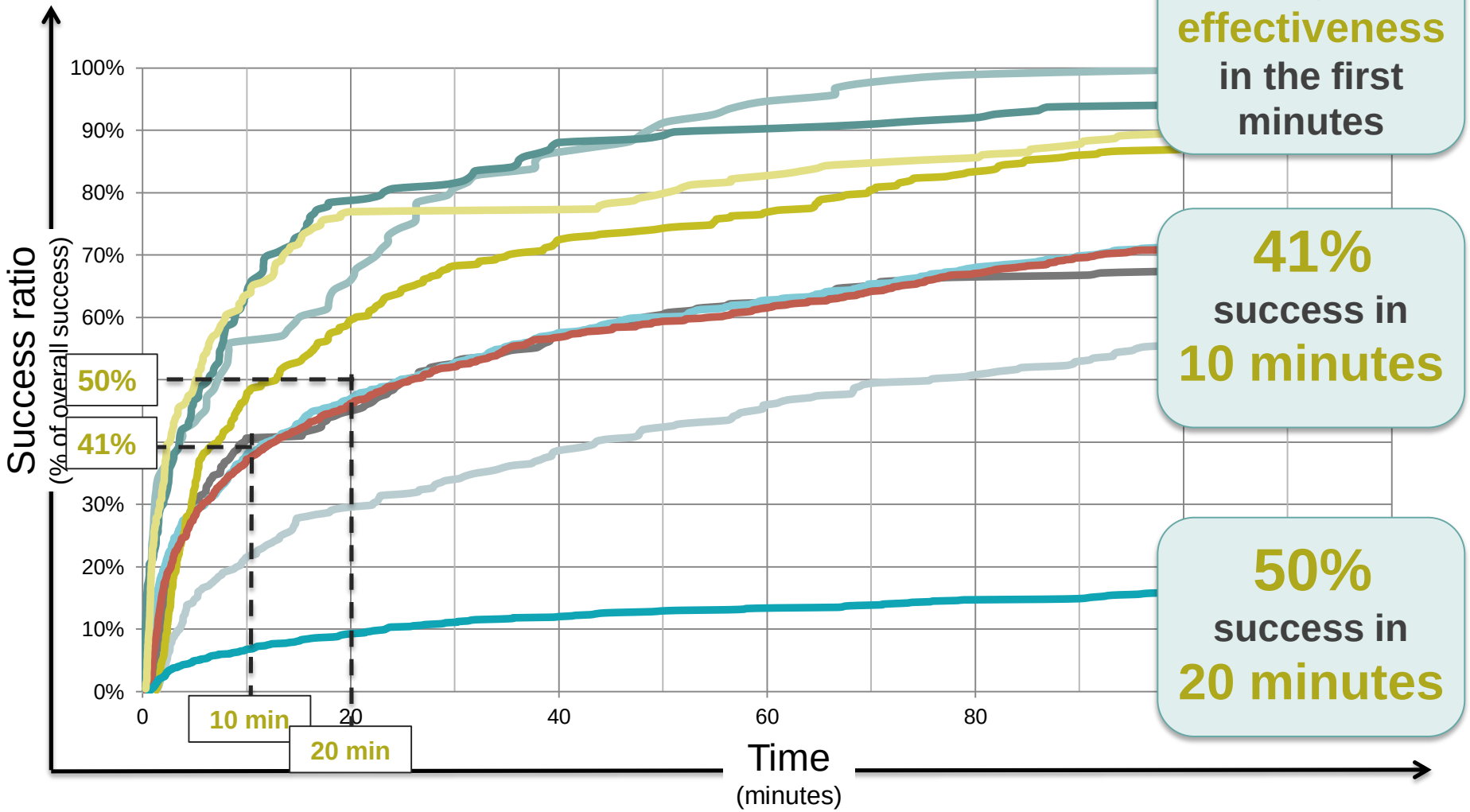
2% Average click rate in Marketing

0,01% Average success in “traditional” phishing

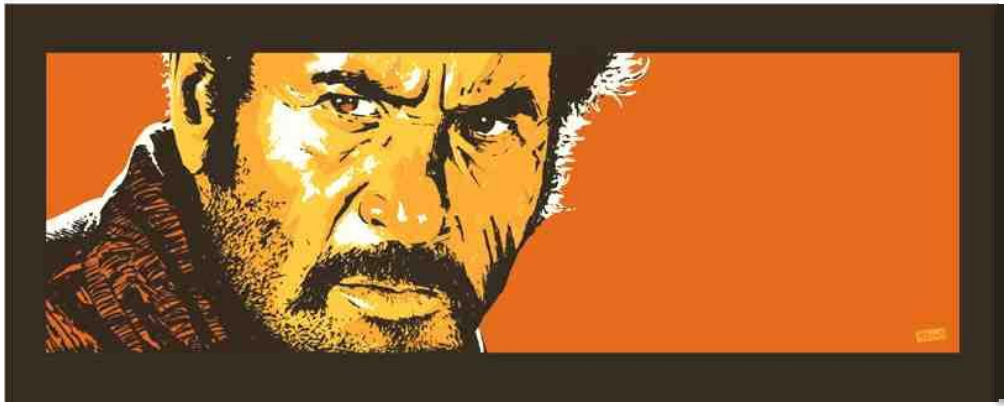
Source: www.proofpoint.com

Time analysis - Visits

We measure relative effectiveness per campaign



User reactions



The FOOL

“I inserted the credential, but I don’t receive a confirm”

“I inserted the credential, but I think it’s phishing and I change the password”

The GUILTY

The GOOD

“This is definitely phishing. Please do something!”

User reactions

1% of employess
signal the phishing

6 minutes
fastest email to antiphishing

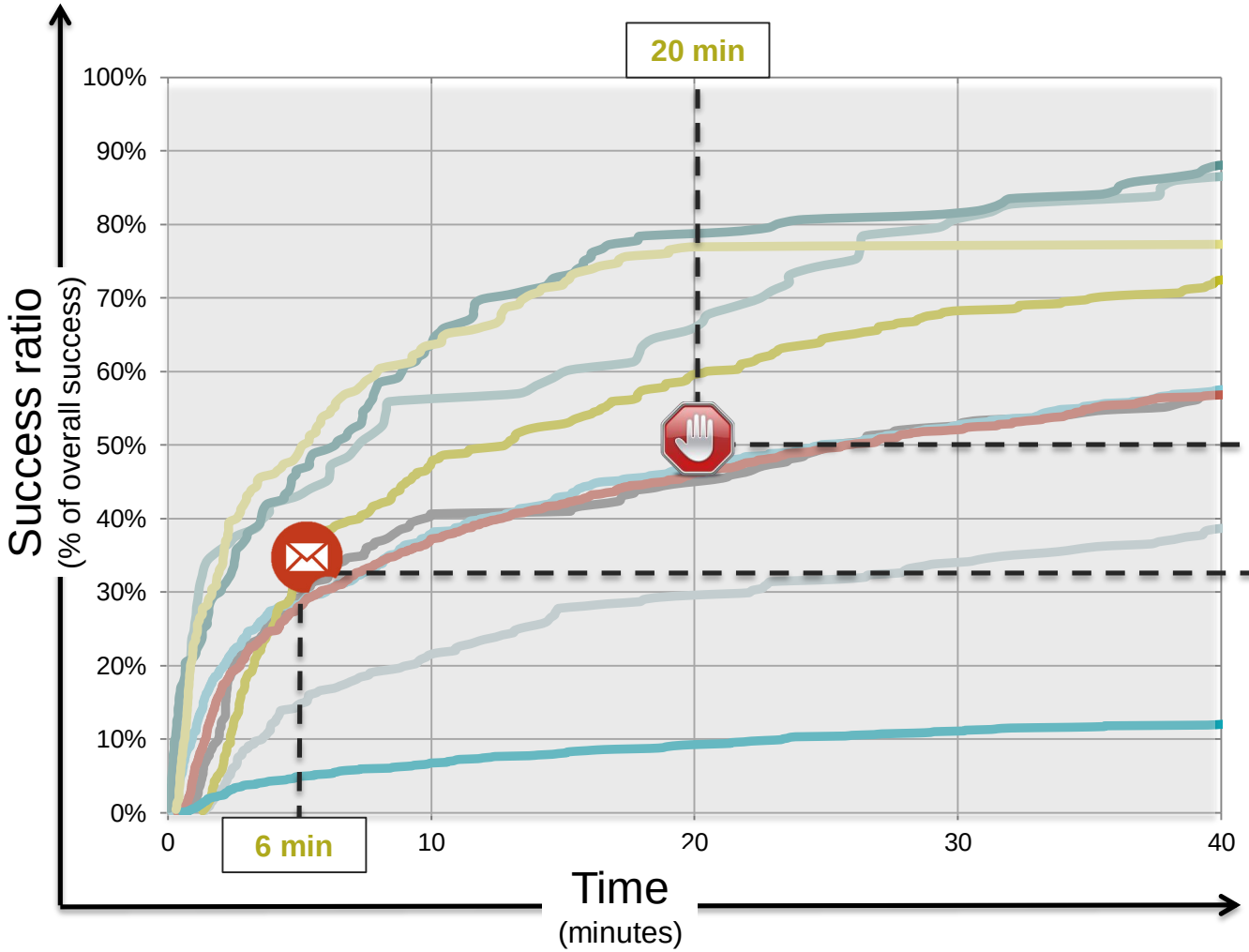
20 minutes
record on block website

The GOOD

> This is definitely phishing. Please do something!

Time analysis - Visits

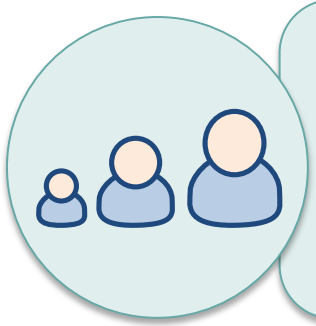
We measure relative effectiveness per campaign

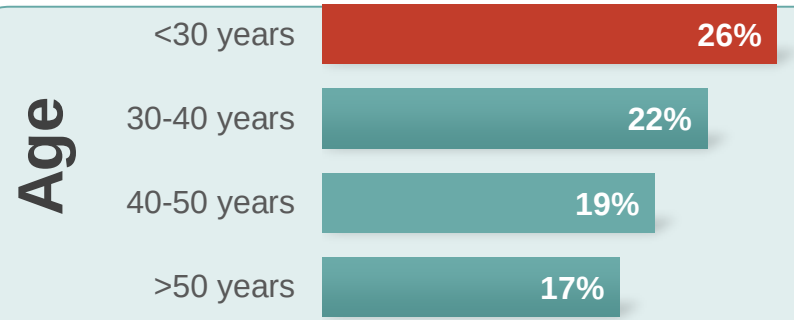


Already 50% success before block website

32% Success before first report email

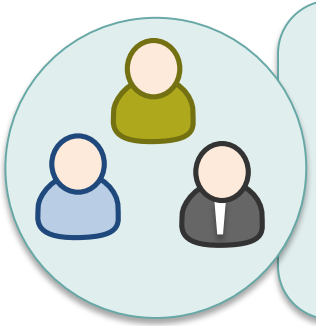
User characterization

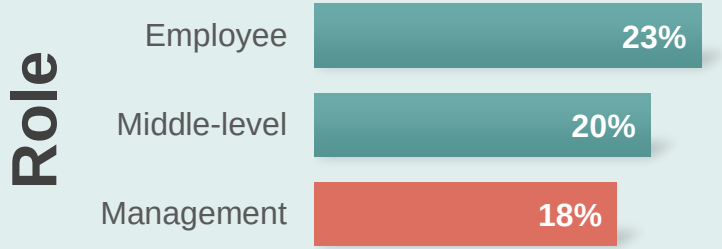




Younger employees are more exposed

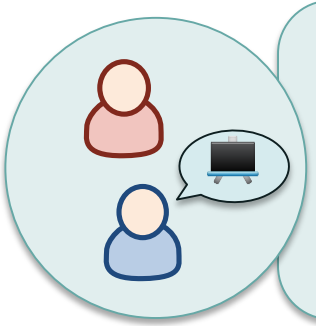
Habits of new generation?

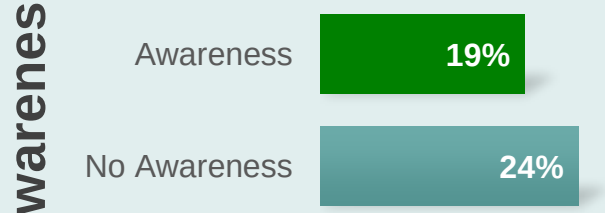




Also managers are vulnerable

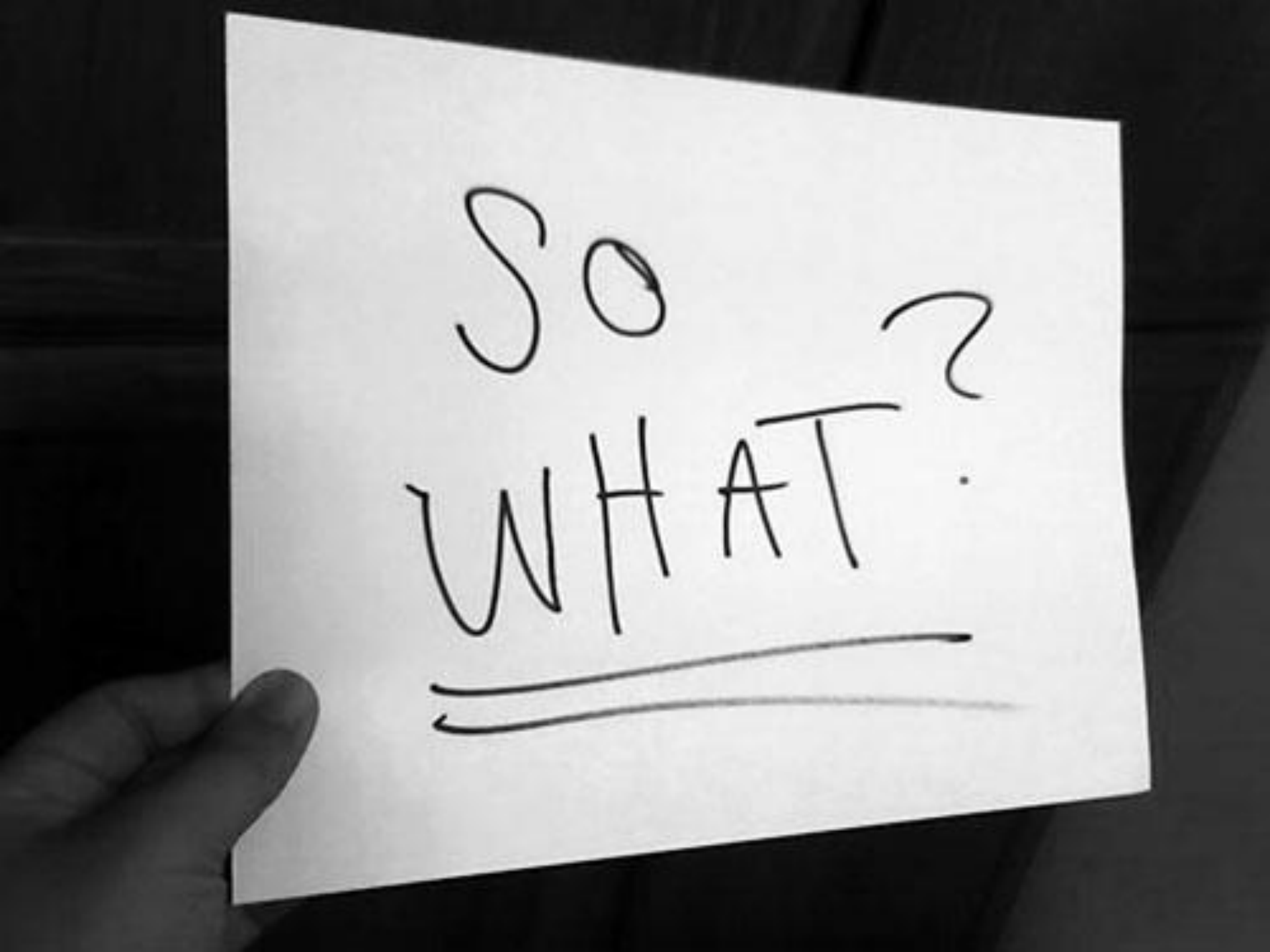
Risk is (not enough) lower



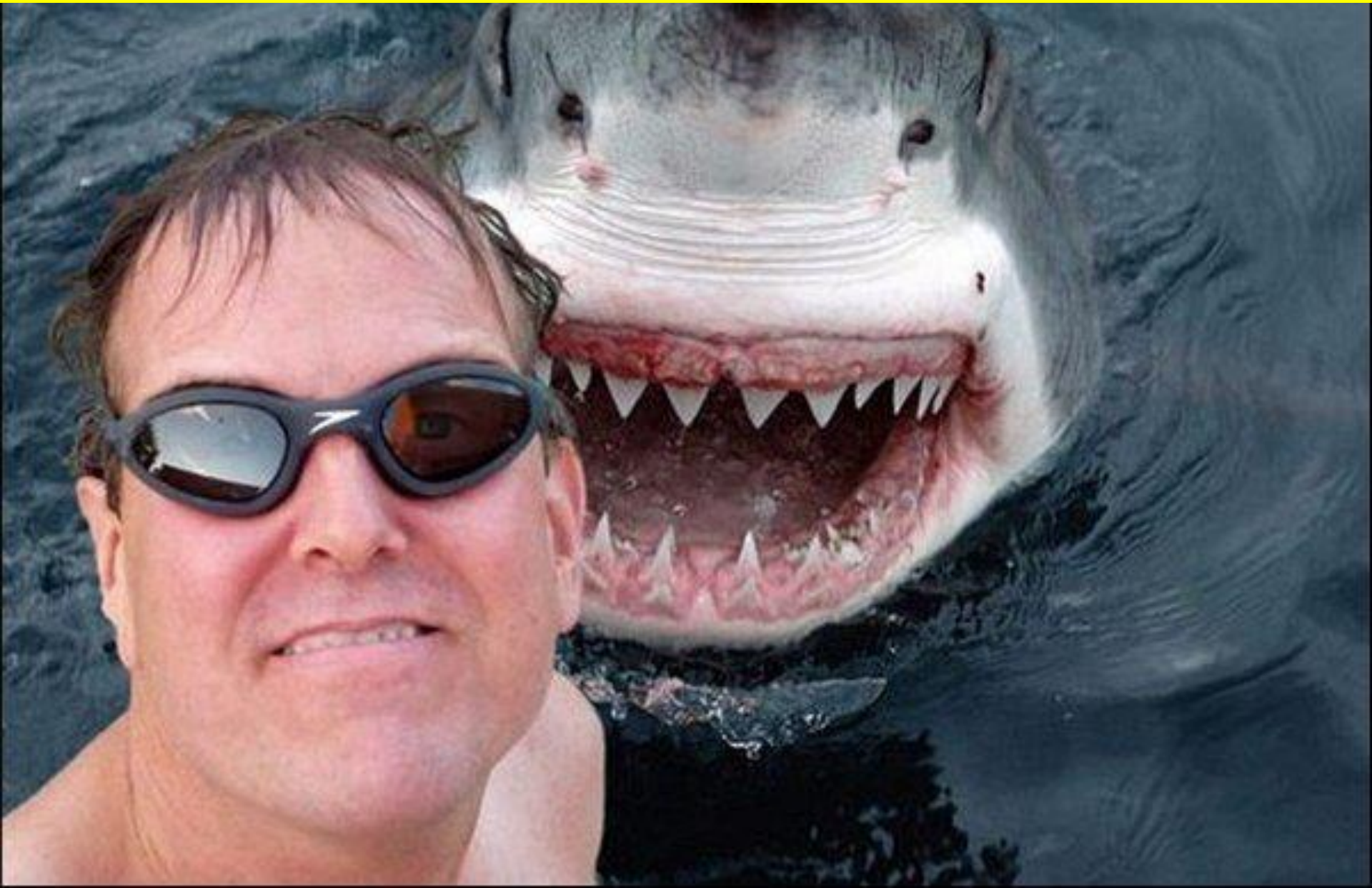


Targeted training mitigate the risk

Behaviour is impacted by awareness


SO
WHAT?

PEOPLE DON'T KNOW THAT SHARING INFORMATION ON SOCIAL MEDIA CAN BE DANGEROUS…



COMPANIES ARE EXPOSED TO SOCIAL-DRIVEN RISKS AND OFTEN THERE IS NO PERCEPTION OF HOW EXTENDED THE RISK IS

A SOCIAL ENGINEERING ATTACK WITH A CONTEXTUALIZED HOOK CAN BE EFFECTIVE

LOTS OF EMPLOYEES COULD BECOME A **RISK** FOR THE ENTERPRISE JUST FOR A **DISCOUNT ON A SANDWICH .. OR A SLICE OF CAKE**

***PS**: no chick was harmed during the preparation of these slides.*

PERFORMING APT ATTACKS IS BECOMING EXTREMELY SIMPLE, IT MAINLY MEANS HAVING A BUSINESS (DEVILISH) PLAN..

THAT’S ALL FOLKS …