Understanding attacker behaviors, motivations and common ways of operation

7ª edição Comunica+
24/10/2017

Pedro Queirós, Cybersecurity Engineer

multicert

Engineering for digital security

Summary

1. What is cyberspace?
2. What is cybercrime?
3. Who does it?
4. Why?
5. Hacker profiling
6. What about Portugal?
7. Social Engineering

What is cyberspace?

What is cyberspace?

"The notional environment in which communication over computer networks occurs."

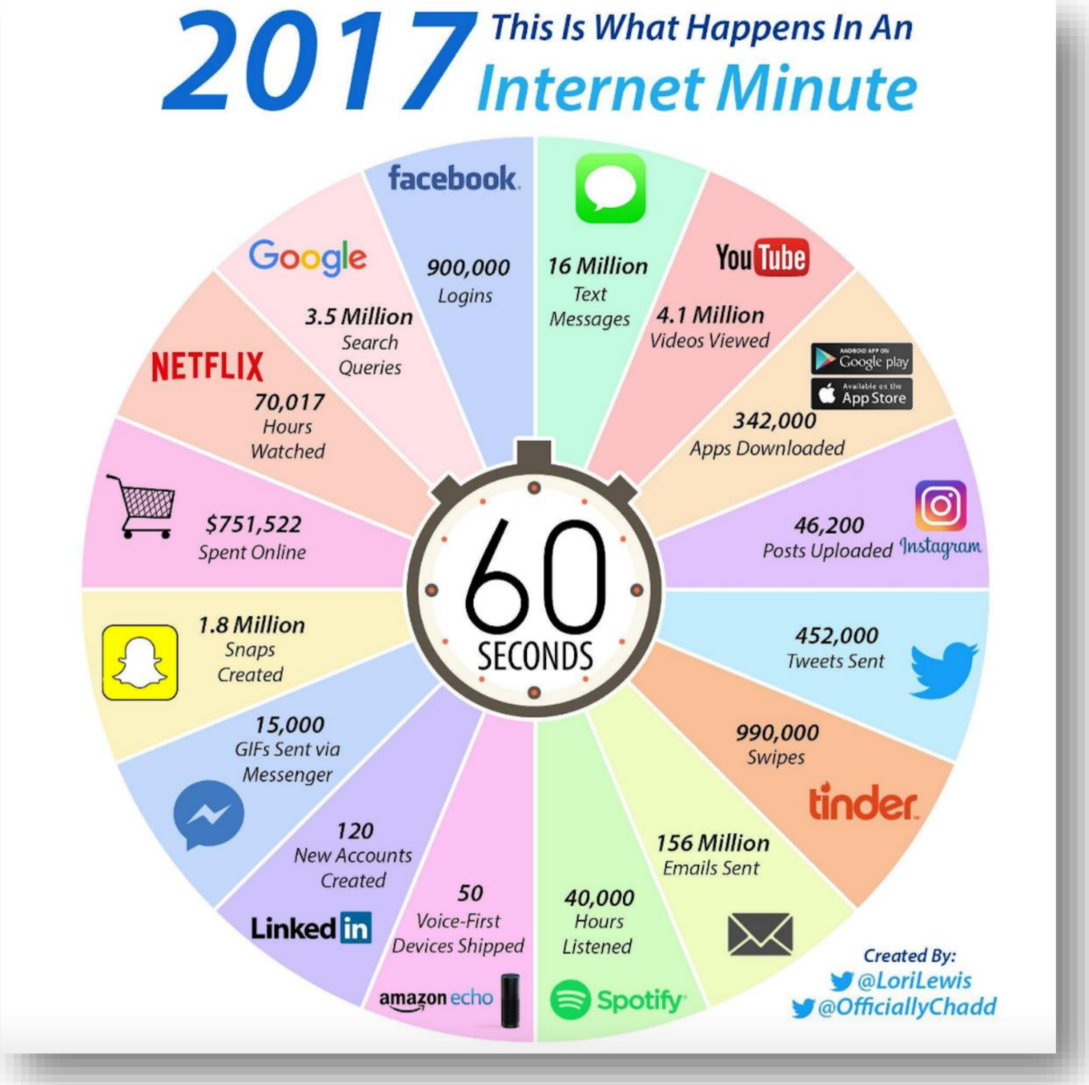
Source: https://en.oxforddictionaries.com/definition/us/cyberspace

What is cyberspace?

"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. ***Unthinkable complexity****."*

Source: William Gibson, Neuromancer (1984)

What is cyberspace?



What is cybercrime?

What is cybercrime?

“Criminal activities carried out by means of computers or the Internet.”

Source: https://en.oxforddictionaries.com/definition/cybercrime

What is cybercrime?

Traditional Crimes	Content-related crimes	Network-related crimes
Fraud	Child pornography	Cracking
Invasion of privacy	Piracy	Illegitimate access
Stalking	Copyright infringment	Illegitimate interception
Extorsion		
Bullying		
Sexual harrassment		
Identity theft		

What is cybercrime?

- No boundaries
- Practiced in a dynamic, high speed changing environment
- Easy and cheap
- Global reach
- Highly disproportional – one attacker can cause considerable damage in several people / organizations
- The strand of economic crime that has grown most in Portugal and internationally (http://apav.pt/cibercrime/)

Who does it?

Who does it?

- Script kiddies
- Malicious insiders
- Organized crime
- Activists
- Terrorists
- Nations

Why?

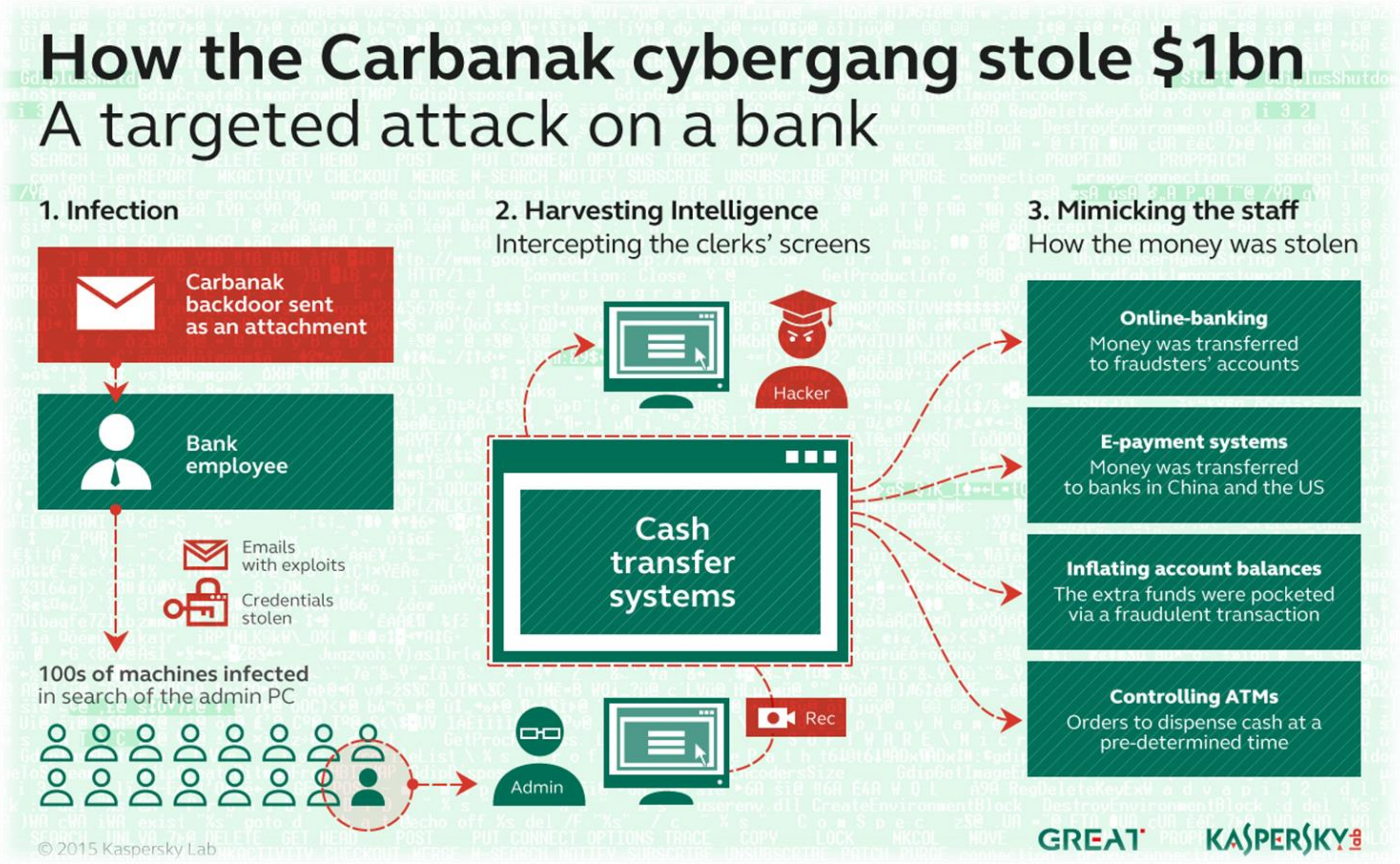
Why?

Political motivations

Source: http://osnetdaily.com/2016/10/october-surprise-dyn-cyber-attack-rehearsal-us-election/

Why?

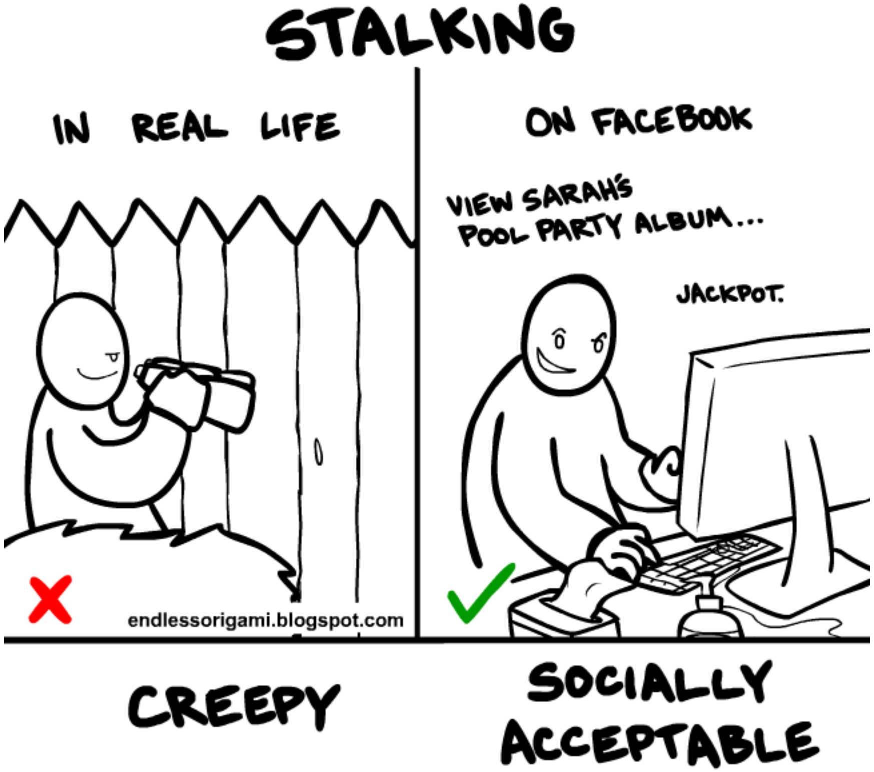
Economical motivations


How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Admin
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
© 2015 Kaspersky Lab
GREAT
KASPERSKY lab

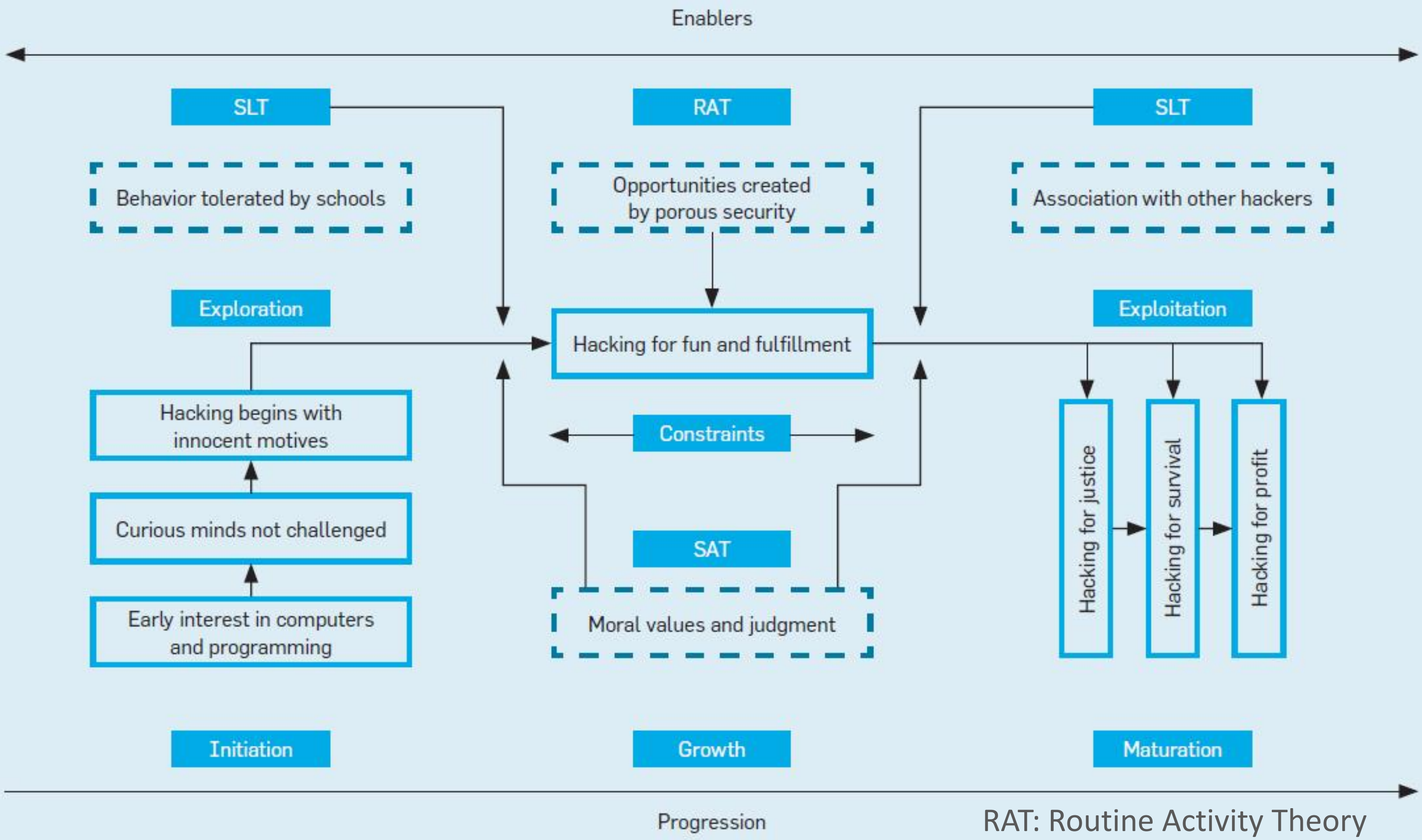
Source: https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

Why?

Socio-cultural motivations



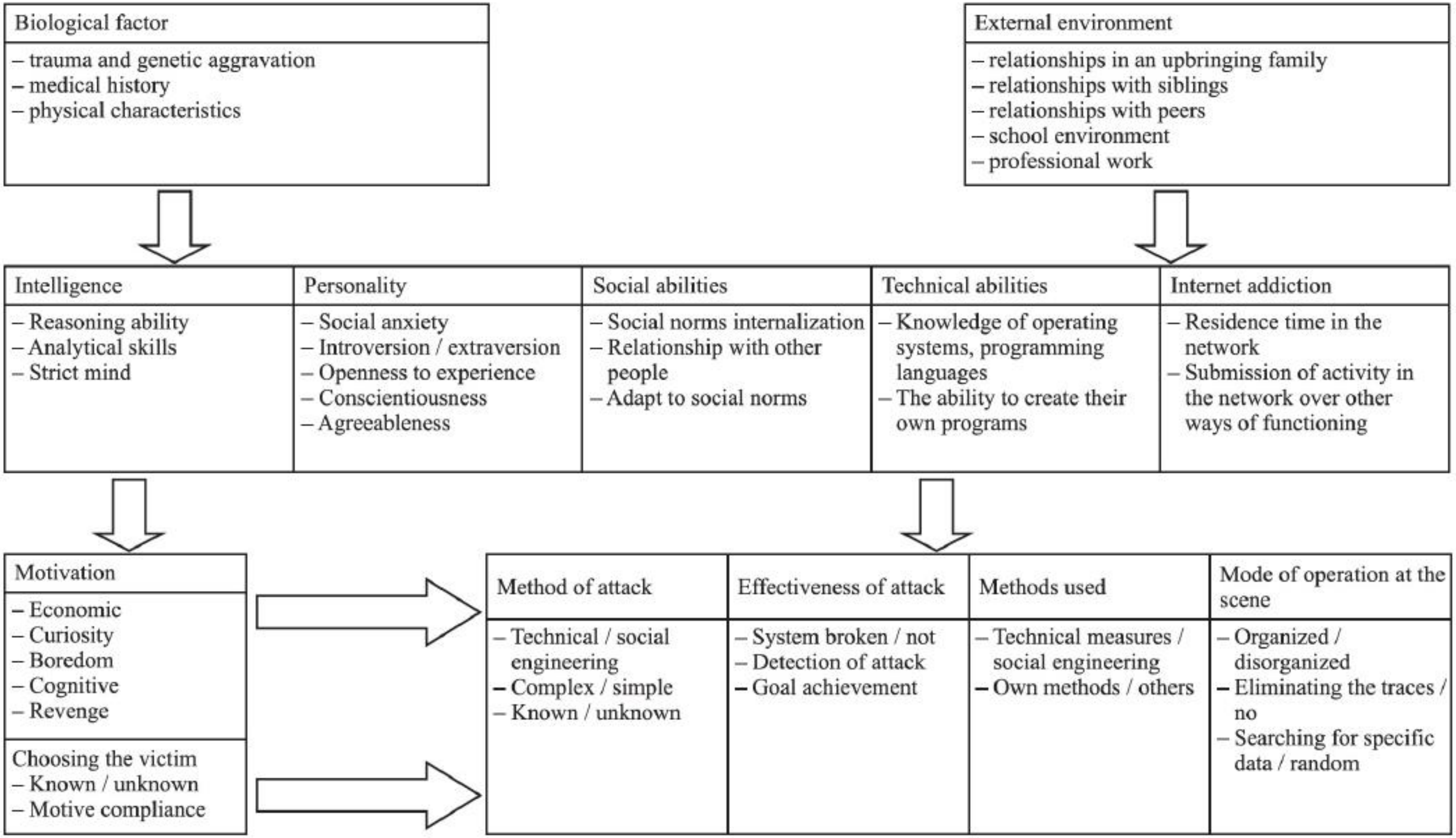
How does it start?


Enablers
SLT
RAT
SLT
Behavior tolerated by schools
Opportunities created by porous security
Association with other hackers
Exploration
Hacking for fun and fulfillment
Exploitation
Hacking begins with innocent motives
Curious minds not challenged
Early interest in computers and programming
Constraints
SAT
Moral values and judgment
Hacking for justice
Hacking for survival
Hacking for profit
Initiation
Growth
Maturation
Progression

Source: Why Computer Talents Become Computer Hackers
By Zhengchuan Xu, Qing Hu, Chenghong Zhang
Communications of the ACM, Vol. 56 No. 4, Pages 64-74

RAT: Routine Activity Theory
SAT: Situational Activity Theory
SLT: Social Learning Theory

Hacker profiling



Biological factor

– trauma and genetic aggravation
– medical history
– physical characteristics

External environment

– relationships in an upbringing family
– relationships with siblings
– relationships with peers
– school environment
– professional work

Intelligence

– Reasoning ability
– Analytical skills
– Strict mind

Personality

– Social anxiety
– Introversion / extraversion
– Openness to experience
– Conscientiousness
– Agreeableness

Social abilities

– Social norms internalization
– Relationship with other people
– Adapt to social norms

Technical abilities

– Knowledge of operating systems, programming languages
– The ability to create their own programs

Internet addiction

– Residence time in the network
– Submission of activity in the network over other ways of functioning

Motivation

– Economic
– Curiosity
– Boredom
– Cognitive
– Revenge

Choosing the victim
– Known / unknown
– Motive compliance

Method of attack

– Technical / social engineering
– Complex / simple
– Known / unknown

Effectiveness of attack

– System broken / not
– Detection of attack
– Goal achievement

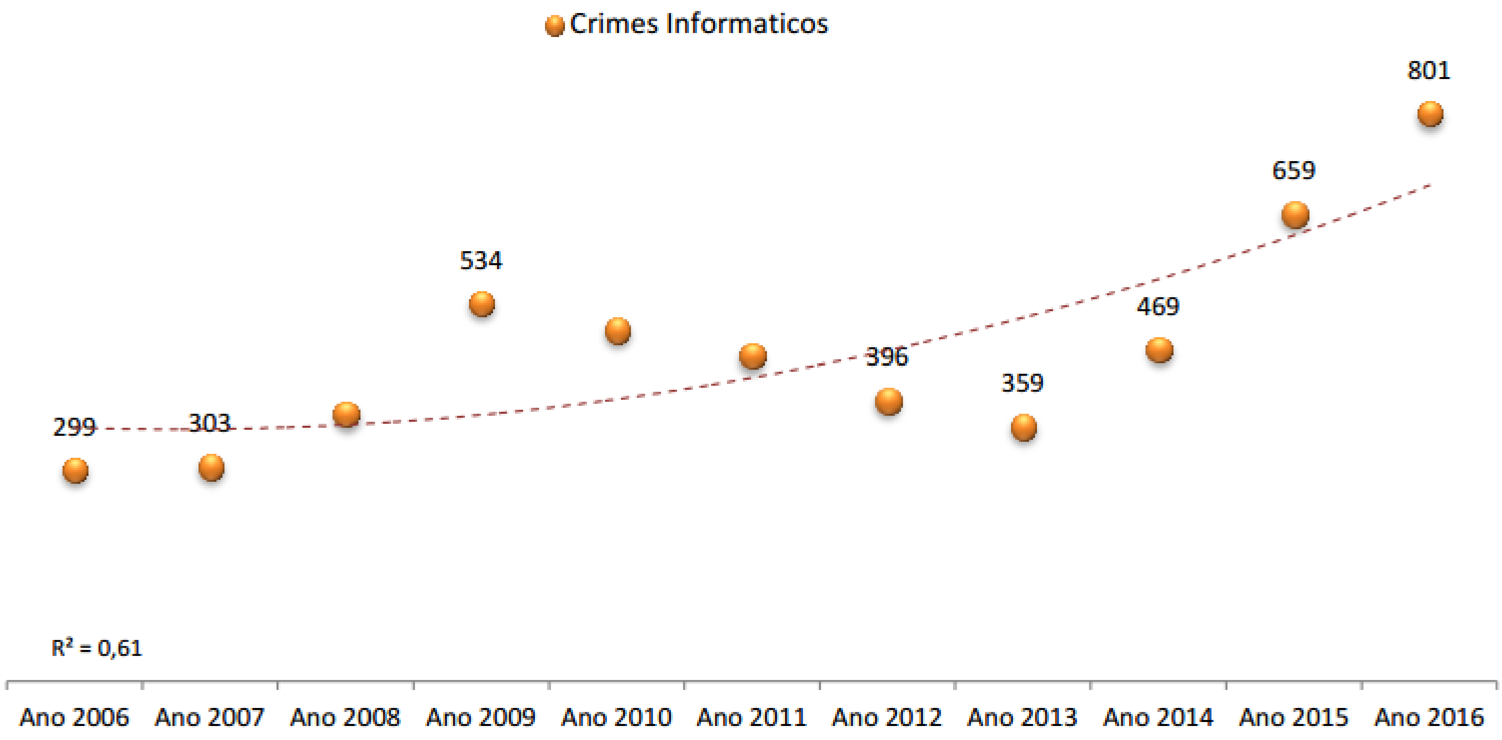
Methods used

– Technical measures / social engineering
– Own methods / others

Mode of operation at the scene

– Organized / disorganized
– Eliminating the traces / no
– Searching for specific data / random

What about Portugal?



Source: RASI 2016 - http://www.portugal.gov.pt/media/26816790/20170331-pm-rasi.pdf

Acesso indevido ou ilegítimo/interceção ilegítima, falsidade informática, outros crimes informáticos, reprodução ilegítima de programa protegido, sabotagem informática, viciação ou destruição de dados/dano relativo a dados/programas.

What about Portugal?

In 2016, we’ve seen a rise in all crime tipifications:

- Sabotagem informática - 140%
- Dano relativo a dados ou programas informáticos - 121%
- Falsidade informática - 58%
- Pornografia de menores - 36%
- Burla informática e nas comunicações - 19%
- Aumento generalizado de ataques de *ransomware*

Social Engineering

Social Engineering

“Getting people to do things they wouldn't ordinarily do for a stranger” – Kevin Mitnick

Social Engineering

- The oldest type of attack known
- Explores human vulnerabilities
- It might or might not use technology
- Most of the times, the victim doesn’t know it’s being manipulated
- It’s rarely detected, stopped or penalized
- Persuasion or manipulation?

Social Engineering

The 6 Principles of Persuasion:

1. Reciprocity
2. Scarcity
3. Authority
4. Consistency
5. Liking
6. Consensus

Source: https://www.influenceatwork.com/principles-of-persuasion/

Social Engineering

Reciprocity

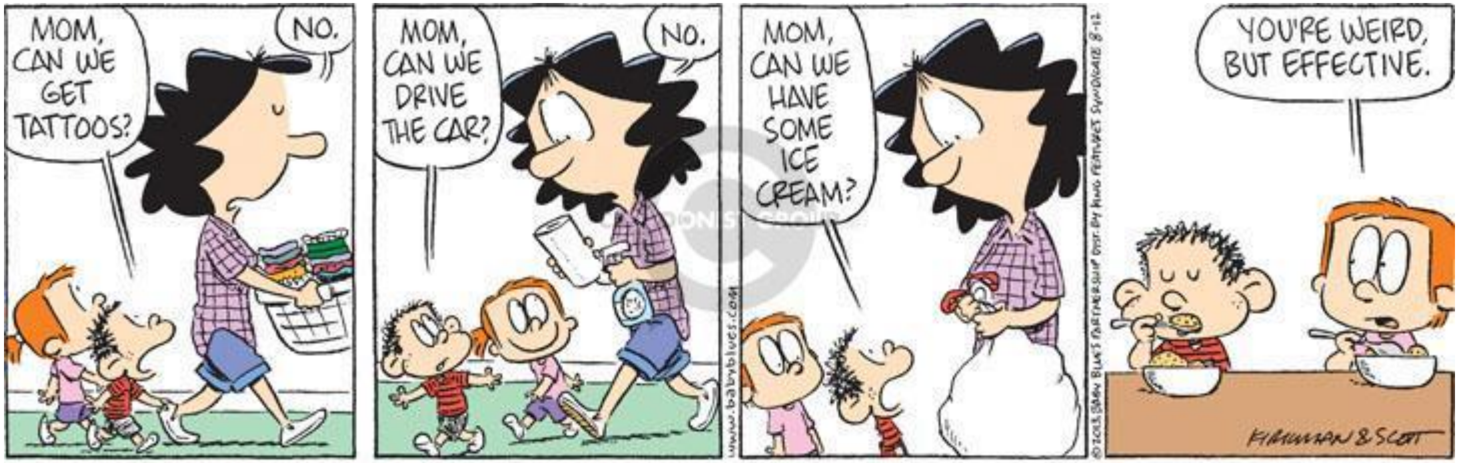
“(…) Social rule that says people ought to repay, in kind, what another person has provided for them.”

Social Engineering

Reciprocity

"(…) Social rule that says people ought to repay, in kind, what another person has provided for them."

It also works with concessions:


MOM, CAN WE GET TATTOOS?
NO.
MOM, CAN WE DRIVE THE CAR?
NO.
MOM, CAN WE HAVE SOME ICE CREAM?
YOU'RE WEIRD, BUT EFFECTIVE.
www.babyblues.com
KIRKMAN & SCOTT

©Baby Blues Partnership

Source: http://www.thecomicstrips.com/store/add.php?iid=100004

Social Engineering

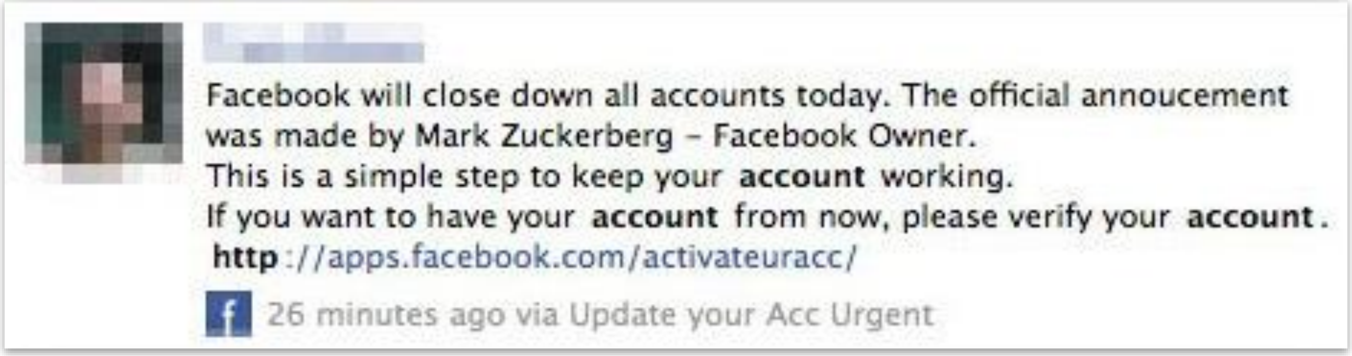
Scarcity

“People want more of the things there are less of.”

Social Engineering

Scarcity

“People want more of the things there are less of.”



Facebook will close down all accounts today. The official annoucement was made by Mark Zuckerberg – Facebook Owner.
This is a simple step to keep your **account** working.
If you want to have your **account** from now, please verify your **account**.
http://apps.facebook.com/activateuracc/

26 minutes ago via Update your Acc Urgent

Source: https://nakedsecurity.sophos.com/2011/02/01/facebook-will-close-all-accounts-today-rogue-app-spreads-virally/

Social Engineering

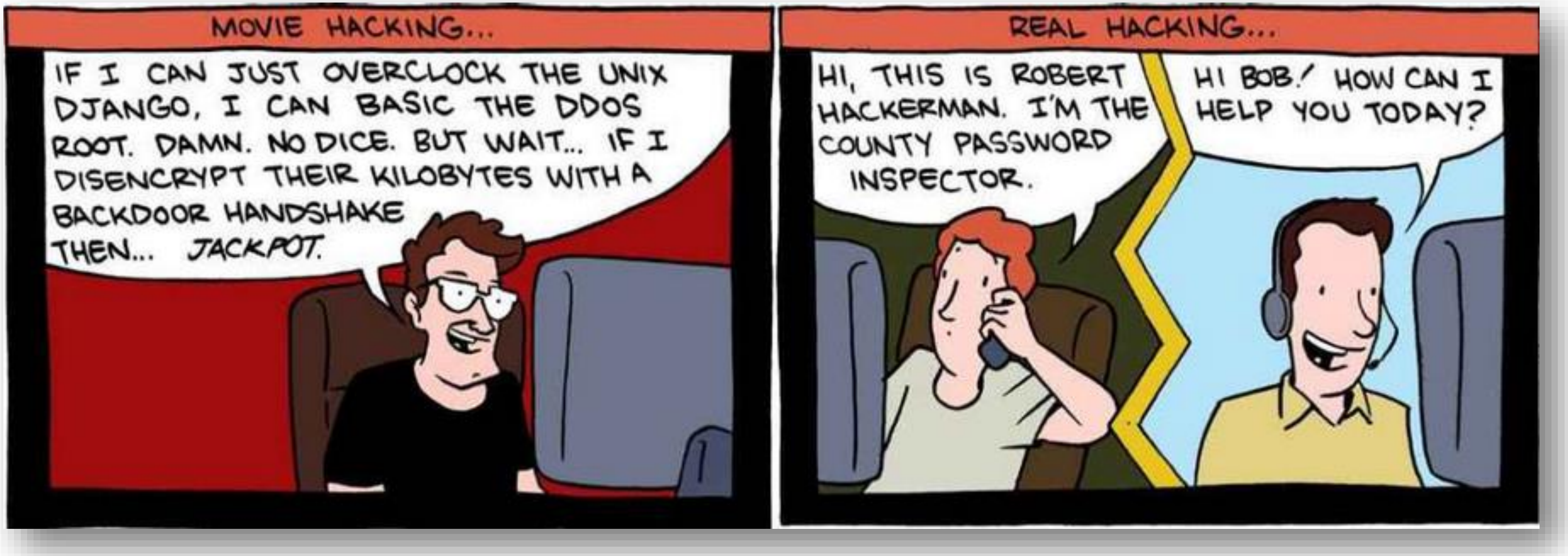
Authority

“People follow the lead of credible, knowledgeable experts.”

Social Engineering

Authority

"People follow the lead of credible, knowledgeable experts."


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Source: http://www.smbc-comics.com/?id=2526

Social Engineering

Consistency

“People like to be consistent with the things they have previously said or done.”

Social Engineering

Liking

“People prefer to say yes to those that they like.”

Social Engineering

Consensus

“People will look to the actions and behaviors of others to determine their own.”

Source: https://www.youtube.com/watch?v=BgRoiTWkBHU

Social Engineering

Where this is applied:

- Tailgating
- Impersonation
- Shoulder surfing
- Dumpster diving
- Phishing
- Vishing

Social Engineering

Adam and Eve case study

Company policies well defined: *"You can eat from all the trees in the Garden of Eden, except that one."*

Top management sponsorship: GOD!

User awareness in place: Adam and Eve knew the policies.

Hacker: Serpent

Source: Carlos Alexandre, Pós Graduação em Cibersegurança e Ciberdefesa - Engenharia Social

Social Engineering

Adam and Eve case study

Hacker uses social engineering on Eve: “If you eat the fruit from that tree, you will be like God.”

Eve accesses confidentional information: eating the fruit makes her know Good and Evil.

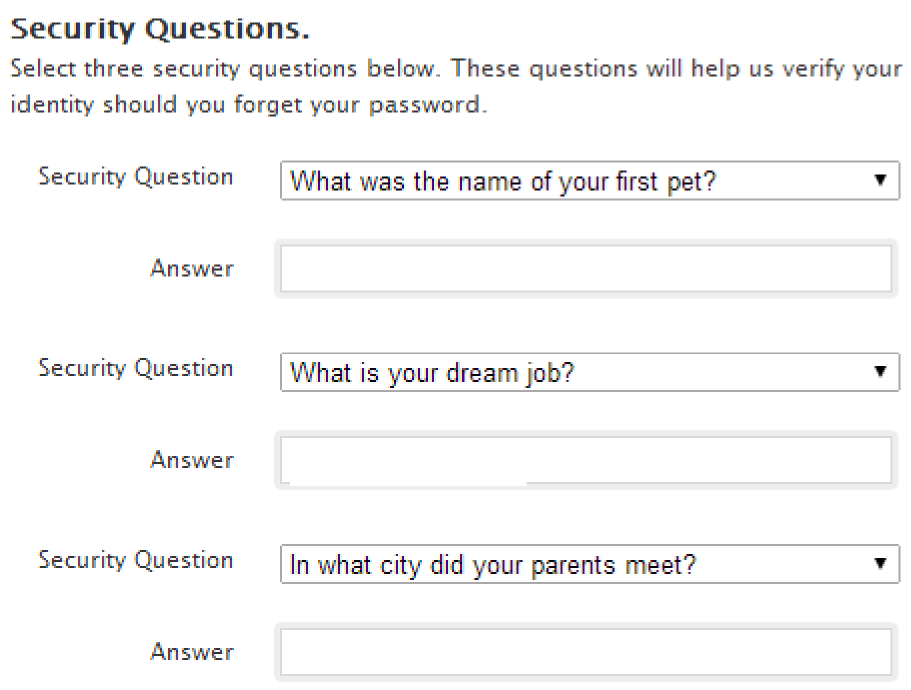
Eve shares confidentional information with Adam.

Internal auditing detects breach of policy.

Users are punished.

Source: Carlos Alexandre, Pós Graduação em Cibersegurança e Ciberdefesa - Engenharia Social

Real life example



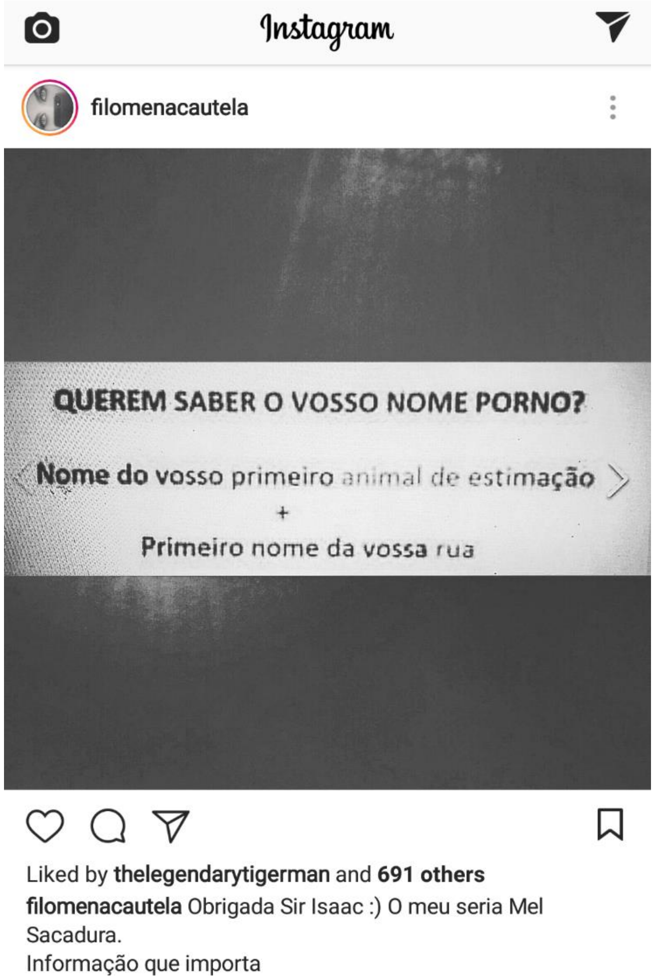
Security Questions.

Select three security questions below. These questions will help us verify your identity should you forget your password.

Security Question	What was the name of your first pet? ▾
Answer	
Security Question	What is your dream job? ▾
Answer	
Security Question	In what city did your parents meet? ▾
Answer	

Source: https://www.howtogeek.com/185354/security-questions-are-insecure-how-to-protect-your-accounts/

Real life example



filomenacautela

QUEREM SABER O VOSSO NOME PORNO?

Nome do vosso primeiro animal de estimação
+
Primeiro nome da vossa rua

Liked by **thelegendarytigerman** and **691 others**

filomenacautela Obrigada Sir Isaac :) O meu seria Mel Sacadura.
Informação que importa

Thank you!

Questions?

Pedro Queirós
pedro.queiros@multicert.com

multicert

Engineering for digital security

Lagoas Park, Edifício 3, Piso 3
2740-266 Porto Salvo
Oeiras – Portugal
Tel.: +351 217 123 010
Fax: +351 217 123 011

Avenida Sidónio Pais, 379
Edifício Hoechst A, Piso 3, Direito
4100-468 Porto – Portugal
Tel.: +351 223 391 810
Fax: +351 223 391 811

www.multicert.com