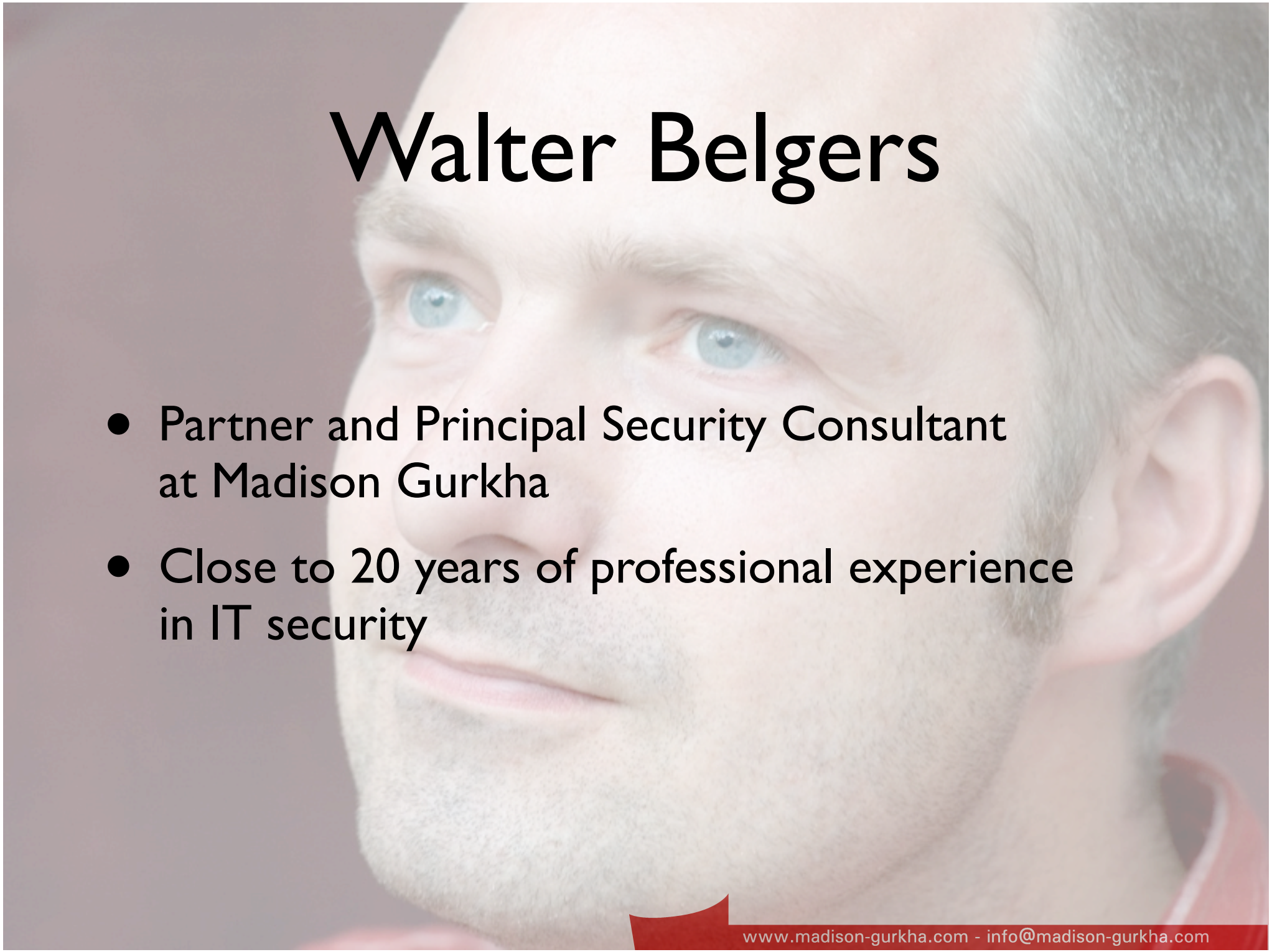
Madison Gurkha
Your Security is Our Business

Social Engineering

Walter Belgers M.Sc. CISSP CISA
walter@madison-gurkha.com

www.dilbert.com



Walter Belgers

- Partner and Principal Security Consultant at Madison Gurkha
- Close to 20 years of professional experience in IT security

Madison Gurkha

Your Security is Our Business

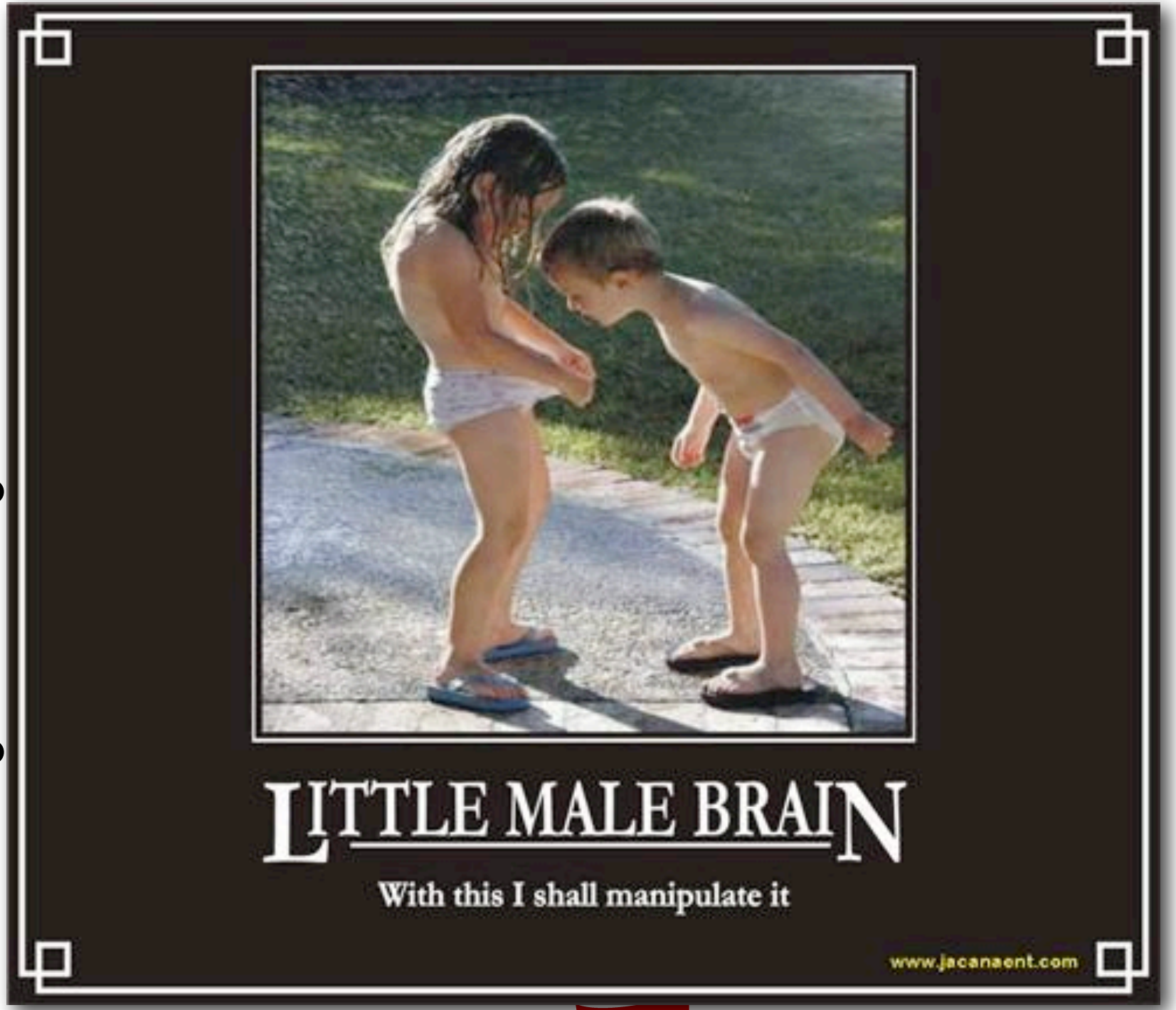
- Madison Gurkha supports organisations with high quality services to efficiently identify, decrease and prevent IT security risks

  - With a focus on *technical* security aspects

Social Engineering

- Persuading people into giving you (access to) confidential information

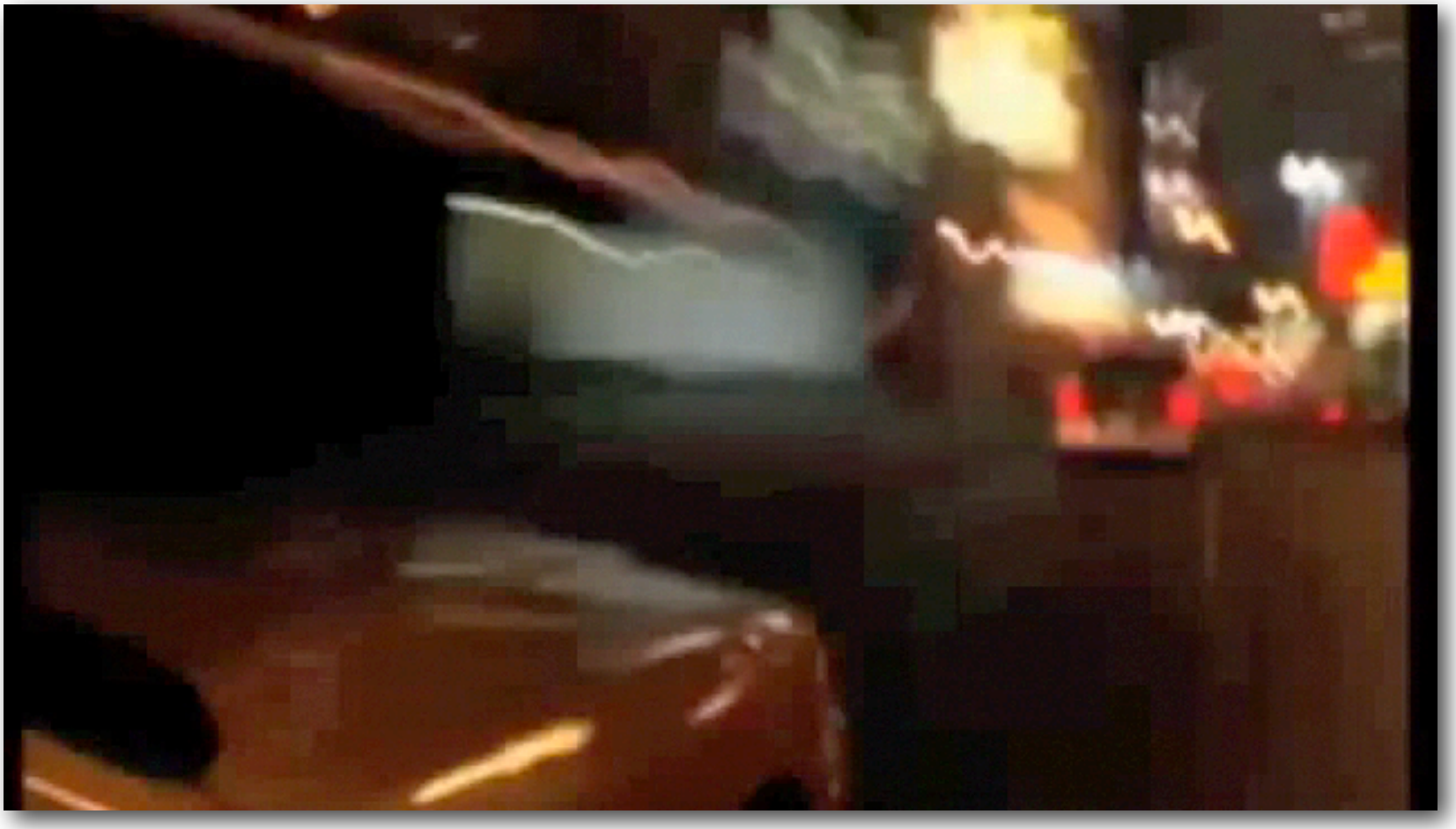
- From the social sciences, manipulation


LITTLE MALE BRAIN
With this I shall manipulate it
www.jacanaent.com


Credit Card Protection
Card
Check
Has your credit card number been STOLEN on the Internet?
card number
/
expires
Check It


EXIT 107
25
Rd
WARNING
Narcotics Check Point Ahead
1/2 MILE BE PREPARED TO STOP
DRUG DOG IN USE
1/2 MILLA HAY CHEQEO DE DROGAS

http://www.youtube.com/watch?v=0UIdI8khMkw



http://derrenbrown.co.uk/

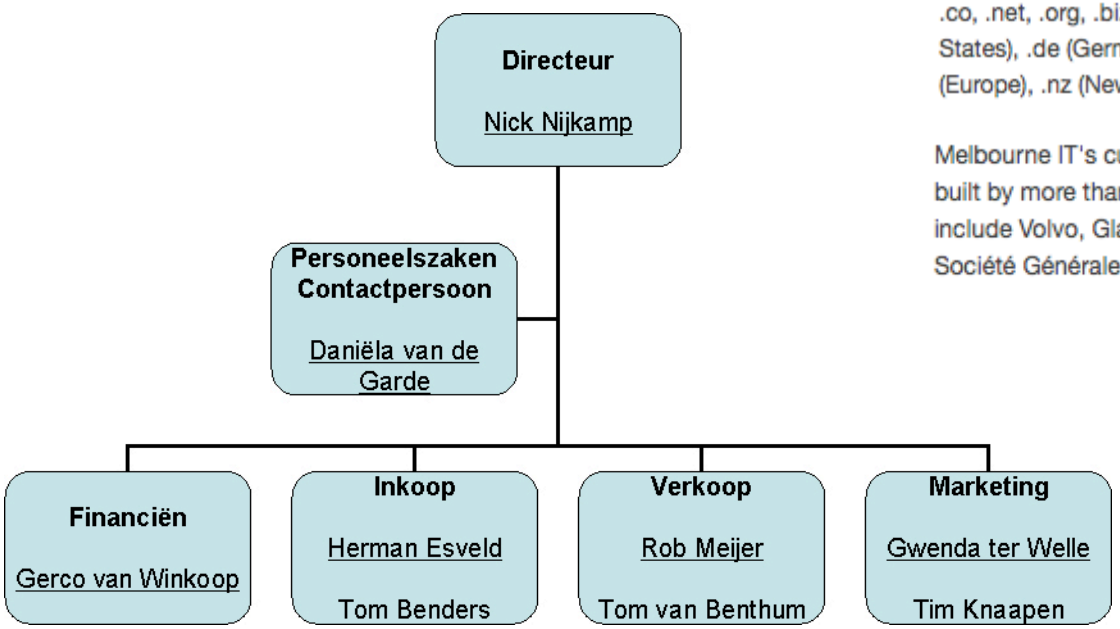
http://video.google.com/videoplay?docid=5464925144369700635

Social Engineering

- Become an *insider*!

- Preparation, collecting information
- Talking the talk (learn the jargon)


Madison Gurkha – Welcome
www.madison-gurkha.com/en/index.php
Madison Gurkha
Your Security is Our Business
Company
Welcome to Madison Gurkha
Latest news
madison gurkha – Google Search
www.google.com/search?hl=en&source=hp&q=madison+gurkha&oq=madison+gurkha&aq=f&aqi=g3&bav=on.2,or.r_gc.r_p...
Web Images Videos Maps News Shopping Gmail more
Google
madison gurkha
About 110,000 results (0.20 seconds)
Sign in
Everything
Images
Videos
News
Shopping
More
All results
Timeline
More search tools
Madison Gurkha - Welkom
www.madison-gurkha.com/ - Cached
Ondersteuning bij het efficiënt identificeren, verminderen en voorkomen van (technische) ICT beveiligingsrisico's.
Vacatures
Contactgegevens
Management team
Technologie
Overige
More results from madison-gurkha.com »
Welcome to Madison Gurkha - Madison Gurkha - Welcome
www.madison-gurkha.com/en/index.php - Cached
Madison Gurkha has chosen to specialize in technical IT security ...
Madison Gurkha - "Gurkhast" podcast
www.madison-gurkha.com/en/gurkhast.php
The interviews, news and agenda can
People Search Results | LinkedIn
www.linkedin.com/search/fpsearch?type=people&keywords=madison+gurkha&pplSearchOrigin=GLHD&...
LinkedIn
Account Type: Basic
Home Profile Contacts Groups Jobs Inbox 32 Companies News More
Find People
Advanced People Search
Reference Search
Saved Searches
Search
madison gurkha
Keep filter selections
Search
Refine By
Current Company
All Companies
Madison Gurkha (19)
Verizon Business (1)
Airadius (1)
FreeBSD (1)
Achmea (1)
Show more...
Relationship
All LinkedIn Members
1st Connections (24)
2nd Connections (1)
Company results for madison gurkha
Madison Gurkha
Computer & Network Security
Eindhoven Area, Netherlands | 11-50 employees
27 results
Save
People results for madison gurkha
Laurens Houben 1st
Medior Security Consultant at Madison Gurkha
Nijmegen Area, Netherlands | Computer & Network Security
In Common: 22 shared connections
Serge van den Boom 1st
Security Consultant at Madison Gurkha
Eindhoven Area, Netherlands | Information Technology and Services
In Common: 22 shared connections 2 shared groups
Ward Wouts 1st
Account Manager at Madison Gurkha
Upgrade
or Learn more
Master Degree Year
Online Master in Leading
Amazon.com: Walter Belgers
http://www.amazon.com/gp/registry/search.html?index=us-xml-wishlist&field-name=Walter+Belgers
amazon.com
Hello. Sign in to get personalized recommendations. New customer? Start here.
Your Amazon.com
Today's Deals
Gifts & Wish Lists
Gift Cards
Your Digital Items
Your Account
Help
Cart
Wish List
Baby Registry
Gift Wrap
Gift FAQ
Shop All Departments
Search
All Departments
Amazon Gift Cards
More Gift Cards
Gift Guides
Gift Organizer
Wish List
Wedding Registry
Gifts
Hello. If this is your Wish List, please sign in.
Find someone's Wish List
Enter name or e-mail
Wishlist
Print This List
Walter Belgers
Remember
This list is for: Walter Belgers
Ship-to: No address entered
Birthday: None entered
About me: Nothing entered
See Walter's Profile page
Page 1 of 1 (2 items)
Show Unpurchased
Category All Products
Sort by Date Added
View Normal
Added September 20, 2006
Hackers - Wizards of the Electronic Age
Steve Wozniak (DVD)
(9)
$14.95
In Stock. Offered by Amazon.com
2 Used & New from $14.95
Add to Cart
Buying this gift elsewhere?
Added May 19, 2006
Computing in the Middle Ages: A View From the Trenches 1955-1983
by Severo Ornstein (Paperback)
(9)
$14.95 $13.45
In Stock. Offered by Amazon.com



Melbourne IT's domain name registration services provide a full range of ICANN names (.com, .co, .net, .org, .biz, .info, .name, .eu) and ccTLDs (for over 100 countries), including .us (United States), .de (Germany), .au (Australia), .fr (France), .jp (Japan), .es (Spain), .ca (Canada), .eu (Europe), .nz (New Zealand), .in (India), .uk (United Kingdom).

Melbourne IT's culture of integrity, innovation, collaboration and customer centricity has been built by more than 690 employees spread across 18 offices in 10 countries. Our customers include Volvo, GlaxoSmithKline, LEGO, Queensland Department of Education and Training, Société Générale, Aurecon Asia-Pacific, Coca-Cola Amatil and Twitter. For more information,

Onze vestigingen

Kies een van de vestigingen op onderstaande kaart:

Of kies uit onderstaande lijst met adresgegevens:

Credion Agrarisch Team (Oost)
Slangenburg 11
7608 RS Almelo
T: (0546) 49 19 26
E: **salland@credion.nl**

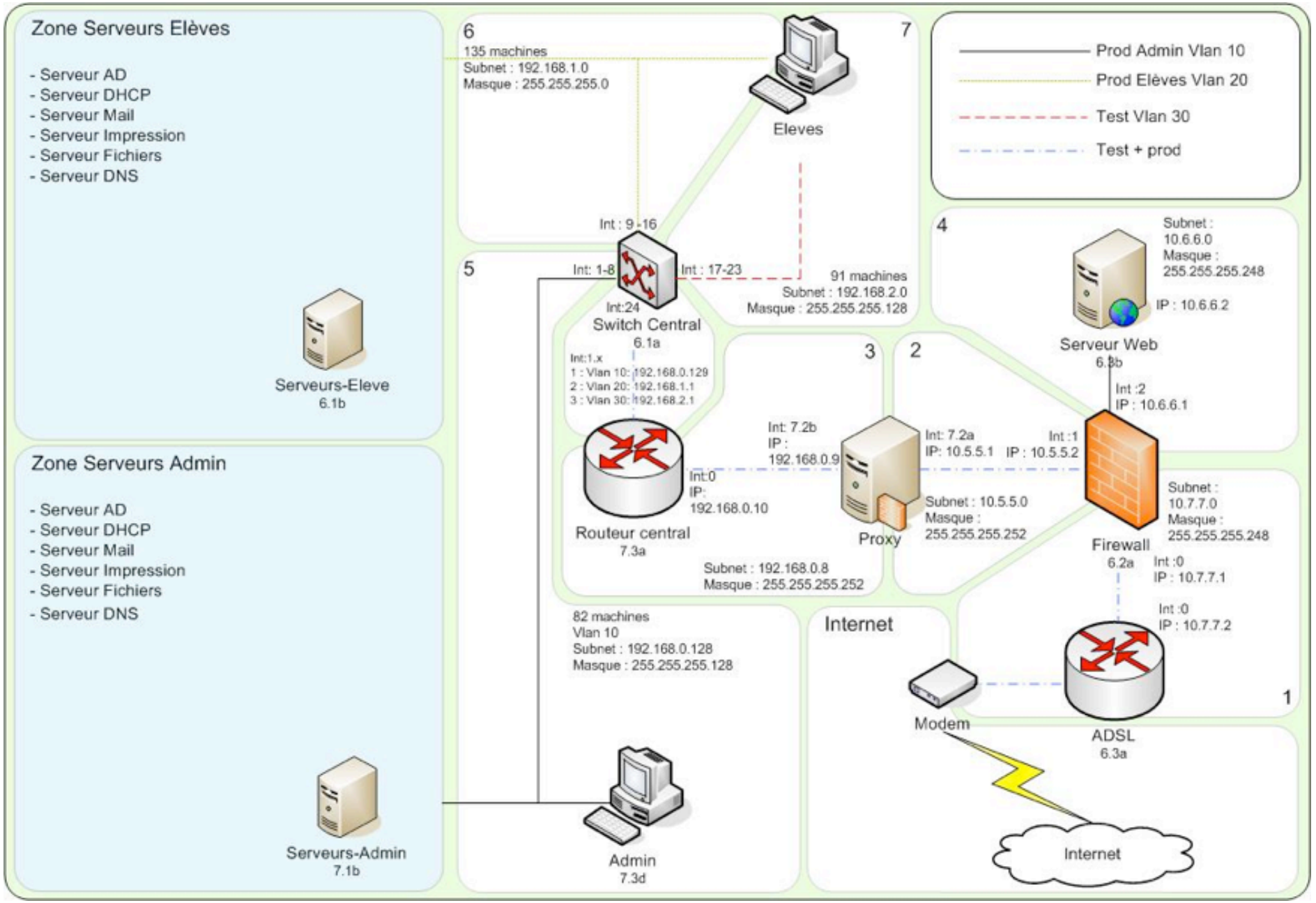
Credion Alkmaar
Robijnstraat 10A
1812 RB Alkmaar
T: (072) 820 02 04
E: **alkmaar@credion.nl**

Credion Amsterdam Oost Noord
Zuideinde 30
1121 CL Landsmeer
T: (020) 482 03 08
E: **mfvanuden@credion.nl**

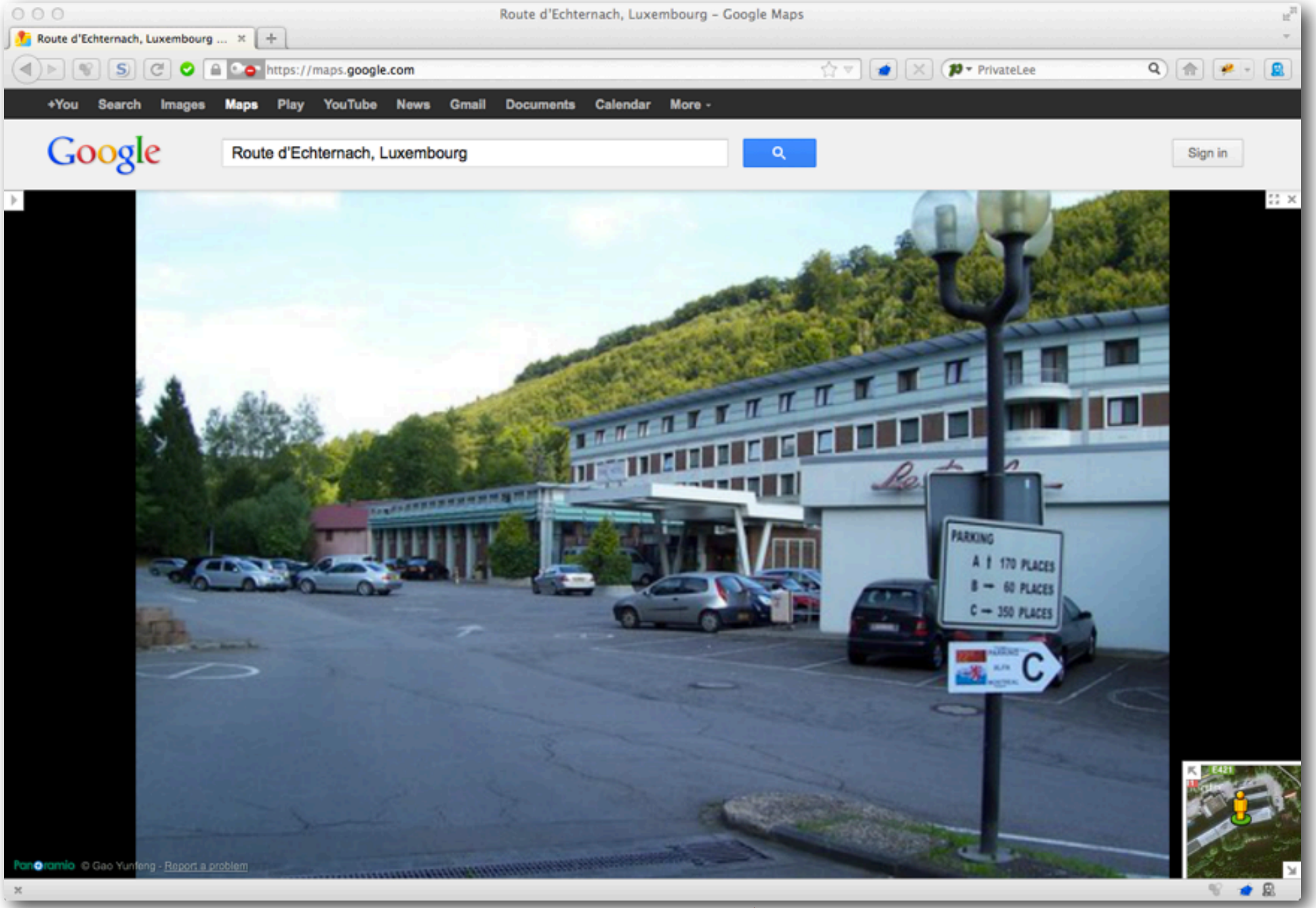
Credion Amsterdam-Amstelland
Amsteldijk Noord 40
1184 TD Amstelveen
T: 020-472 04 69
E: **amstel@credion.nl**

Credion Arnhem
Stationsweg 46
6861 EJ Oosterbeek
T: (0513) 65 68 77
E: **arnhem@credion.nl**

Credion Assen
Hoofdvaartsweg 109
9405 VC Assen
T: 0592 - 820 002
E: **assen@credion.nl**

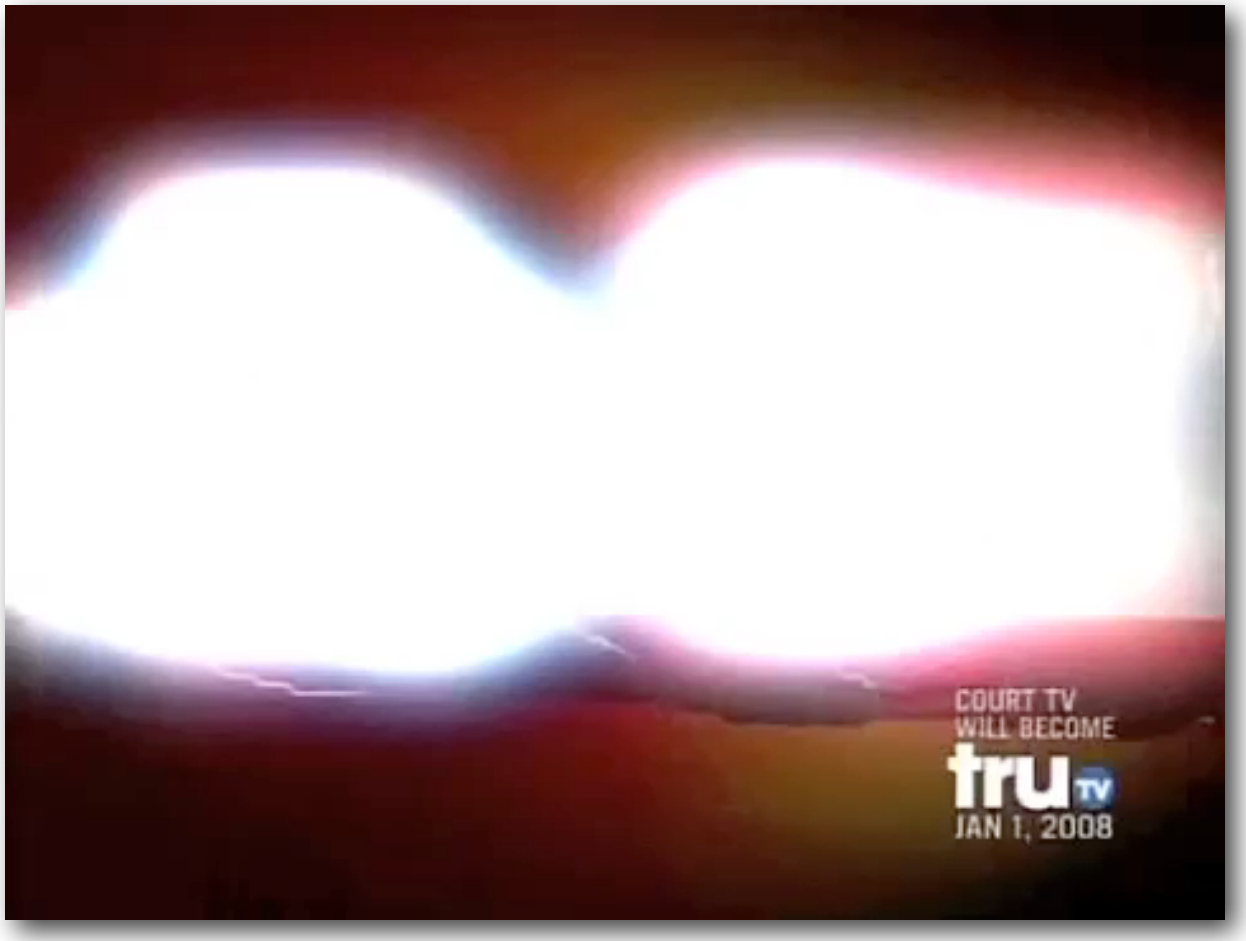


www.ratemynetworkdiagram.com


Route d'Echternach, Luxembourg – Google Maps
Route d'Echternach, Luxembourg ...
https://maps.google.com
PrivateLee
+You Search Images Maps Play YouTube News Gmail Documents Calendar More
Google
Route d'Echternach, Luxembourg
Sign in
PARKING
A 170 PLACES
B 60 PLACES
C 350 PLACES
C
Panoramio © Gao Yunfeng - Report a problem

DISCOVERY

Sometimes, the greatest treasures are found beneath piles of trash.

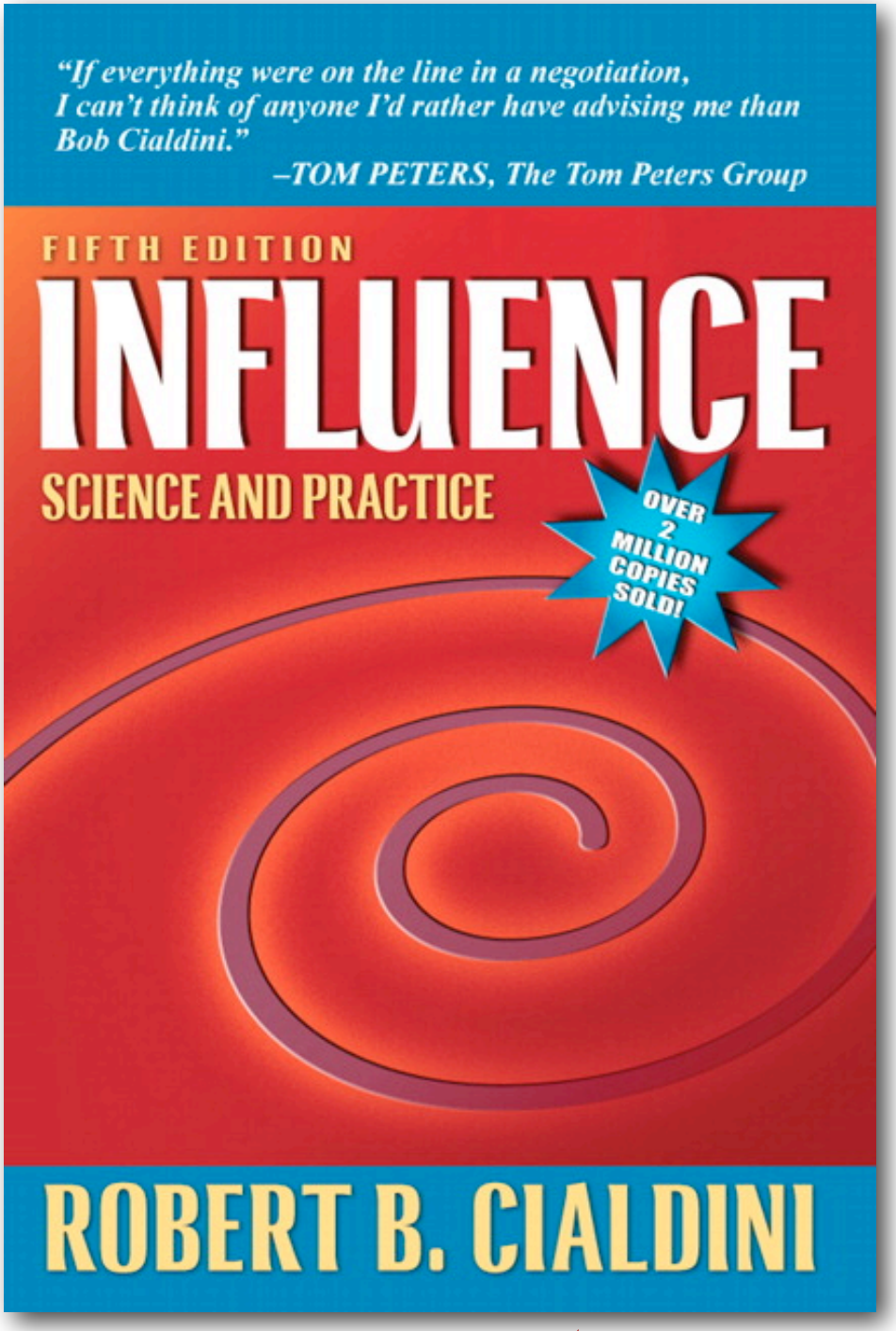


http://www.trutv.com/

Classic examples

- I lost my password and my boss wants me to finish this today, could you please help me?

- Hi, this is the system administrator, we have a technical problem and need you to change your password into “monday”



Social proof

Scarcity

ULTRA RARE VOX BULLDOG MADE FOR ONLY ONE YEAR !!!!!!

Item condition: --

Time left: 24d 06h (Aug 19, 2011 13:23:58 PDT)

Price: **US $1,500.00** Buy It Now

or

Best Offer: Make Offer

Add to Watch list

Shipping: **$49.00** Standard Shipping | See all details

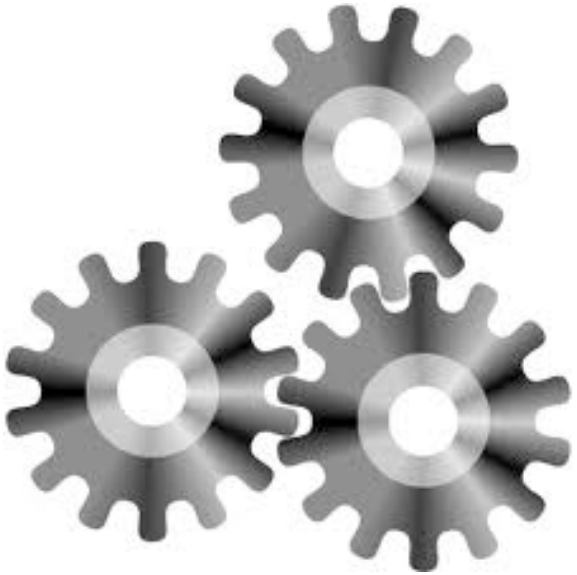
Delivery: Estimated between **Fri. Jul. 29 and Thu. Aug. 4**

Returns: No Returns Accepted

eBay Buyer Protection
Covers your purchase price plus original shipping.
Learn more

Shortcuts

- "Judgmental Heuristics"
- Automated responses



- It is expensive, therefore, it's good
- He is an expert, therefore, he is right


WALTER BELGERS
ICT-beveiliger Madison Gurkha


Undergraduate
Admissions 2/2007


ต้องใช้บัตร

www.netwerk.tv

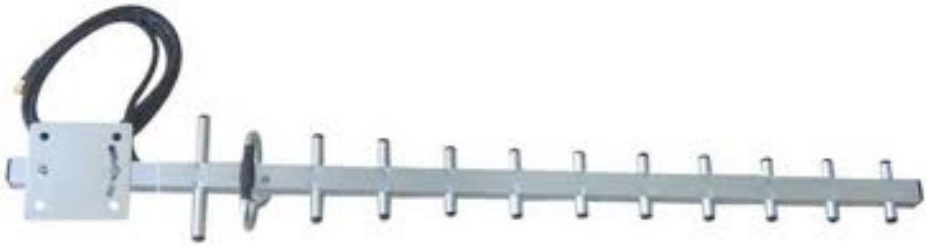

Inleggen
Inschuiven
PIN privé!
030 283 65 55

http://www.massimodecarlo.it/

Authority

- Clothing and/or accessories

- Sly sincerity



Liking

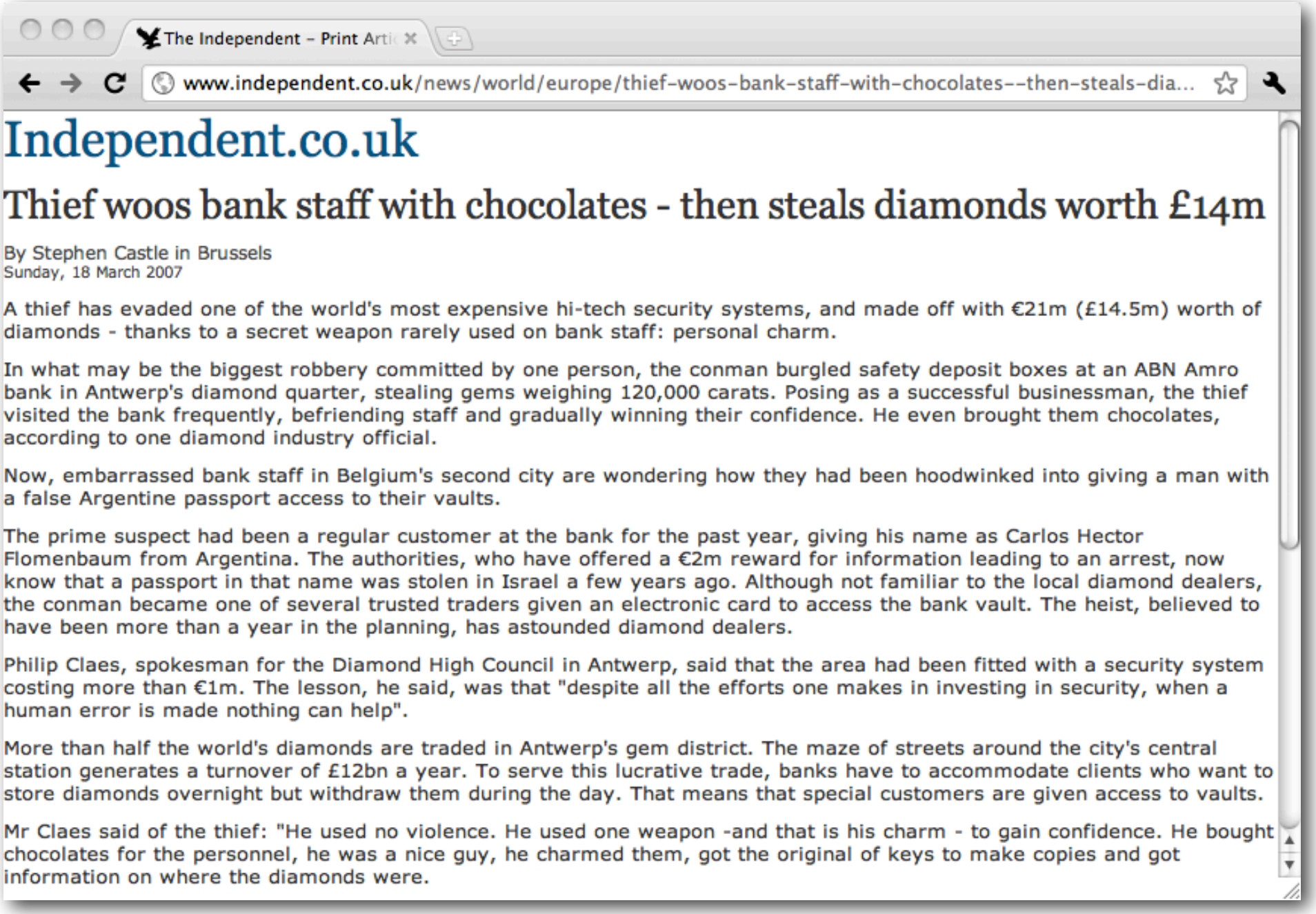
- People tend to help people they like better
- You like people that:
  - Are physically attractive
  - Make (fake) compliments
  - Are similar to them

"Have I ever told you what a great attitude you have about all the extra work I'm about to give you?"

Similarity

- Clothing
- (Body) language
- Interests
- Even name similarity

Picture: Hergé



Independent.co.uk

Thief woos bank staff with chocolates - then steals diamonds worth £14m

By Stephen Castle in Brussels
Sunday, 18 March 2007

A thief has evaded one of the world's most expensive hi-tech security systems, and made off with €21m (£14.5m) worth of diamonds - thanks to a secret weapon rarely used on bank staff: personal charm.

In what may be the biggest robbery committed by one person, the conman burgled safety deposit boxes at an ABN Amro bank in Antwerp's diamond quarter, stealing gems weighing 120,000 carats. Posing as a successful businessman, the thief visited the bank frequently, befriending staff and gradually winning their confidence. He even brought them chocolates, according to one diamond industry official.

Now, embarrassed bank staff in Belgium's second city are wondering how they had been hoodwinked into giving a man with a false Argentine passport access to their vaults.

The prime suspect had been a regular customer at the bank for the past year, giving his name as Carlos Hector Flomenbaum from Argentina. The authorities, who have offered a €2m reward for information leading to an arrest, now know that a passport in that name was stolen in Israel a few years ago. Although not familiar to the local diamond dealers, the conman became one of several trusted traders given an electronic card to access the bank vault. The heist, believed to have been more than a year in the planning, has astounded diamond dealers.

Philip Claes, spokesman for the Diamond High Council in Antwerp, said that the area had been fitted with a security system costing more than €1m. The lesson, he said, was that "despite all the efforts one makes in investing in security, when a human error is made nothing can help".

More than half the world's diamonds are traded in Antwerp's gem district. The maze of streets around the city's central station generates a turnover of £12bn a year. To serve this lucrative trade, banks have to accommodate clients who want to store diamonds overnight but withdraw them during the day. That means that special customers are given access to vaults.

Mr Claes said of the thief: "He used no violence. He used one weapon -and that is his charm - to gain confidence. He bought chocolates for the personnel, he was a nice guy, he charmed them, got the original of keys to make copies and got information on where the diamonds were.

Reciprocation

- I give you something
- You give me something

Picture: BBC

Perceptual contrast

- Ask for a lot..
  .. then for the little you actually wanted

www.calvinandhobbes.com

Commitment

- People strive to be *consistent*
- When we make a decision, we stick with it
  - Becoming more convinced it is the right one

Commitment

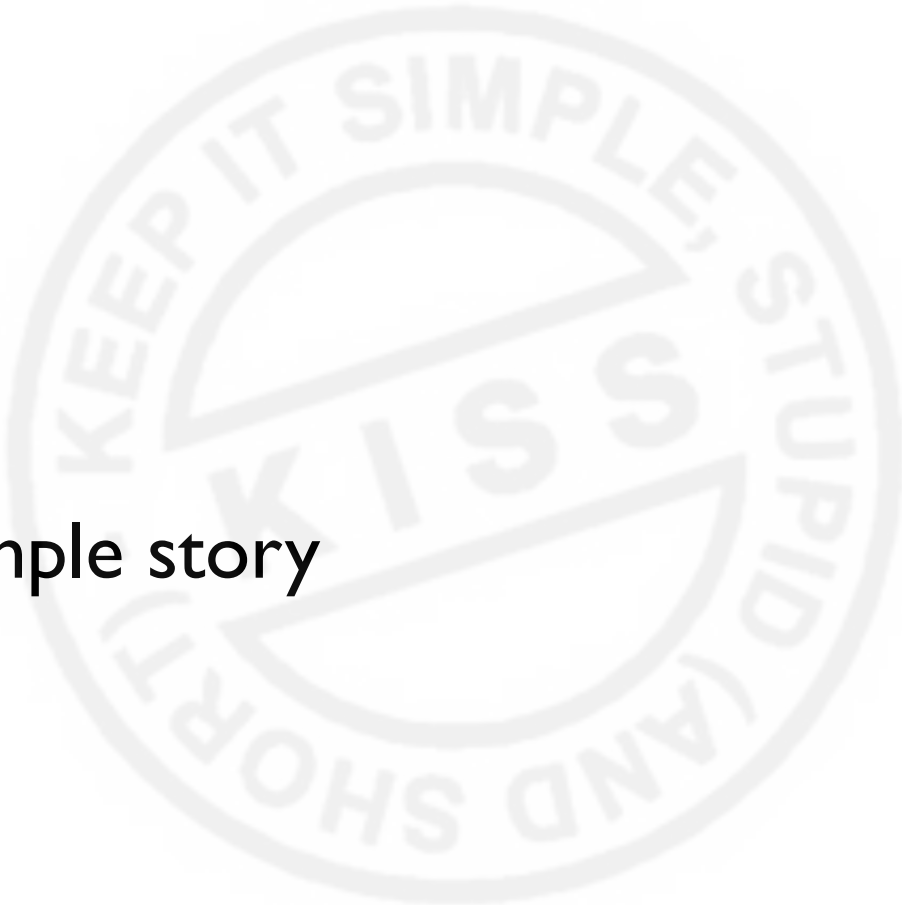
- Would you do me a favor because I need it?
- Yes.
- ...

Commitment

- Ask for a little...
- ...then for some more...
- ...and some more...

Tips

- Pretexting
  - "Making up a story"
  - Rule #1: make it a simple story



Soundclip: youtube, Phone Losers of America

Physical access

- Examine the neighborhood (entrances, exits)
  - Smoker's ~~exit~~ entrance (tailgating)
  - Parking garage
- When do people come in/have lunch?
- Do people wear id badges? Can you copy them?

Preparation

- Be sure to have a "Get Out Of Jail" card
  - Name of the customer
  - Your name
  - Period
  - What you are doing

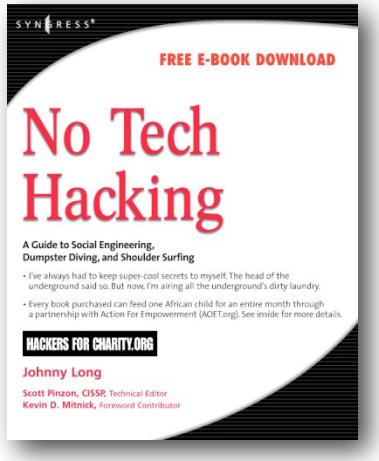

LEITZ
LIFT
LIFT
LIFT
KNOP INGEDRUKT HOUDEN
AFKEUR
Aantal :
Datum :
Naam :

Once inside..

- We have access to confidential information
- More worrisome: installing a base station

Once inside..

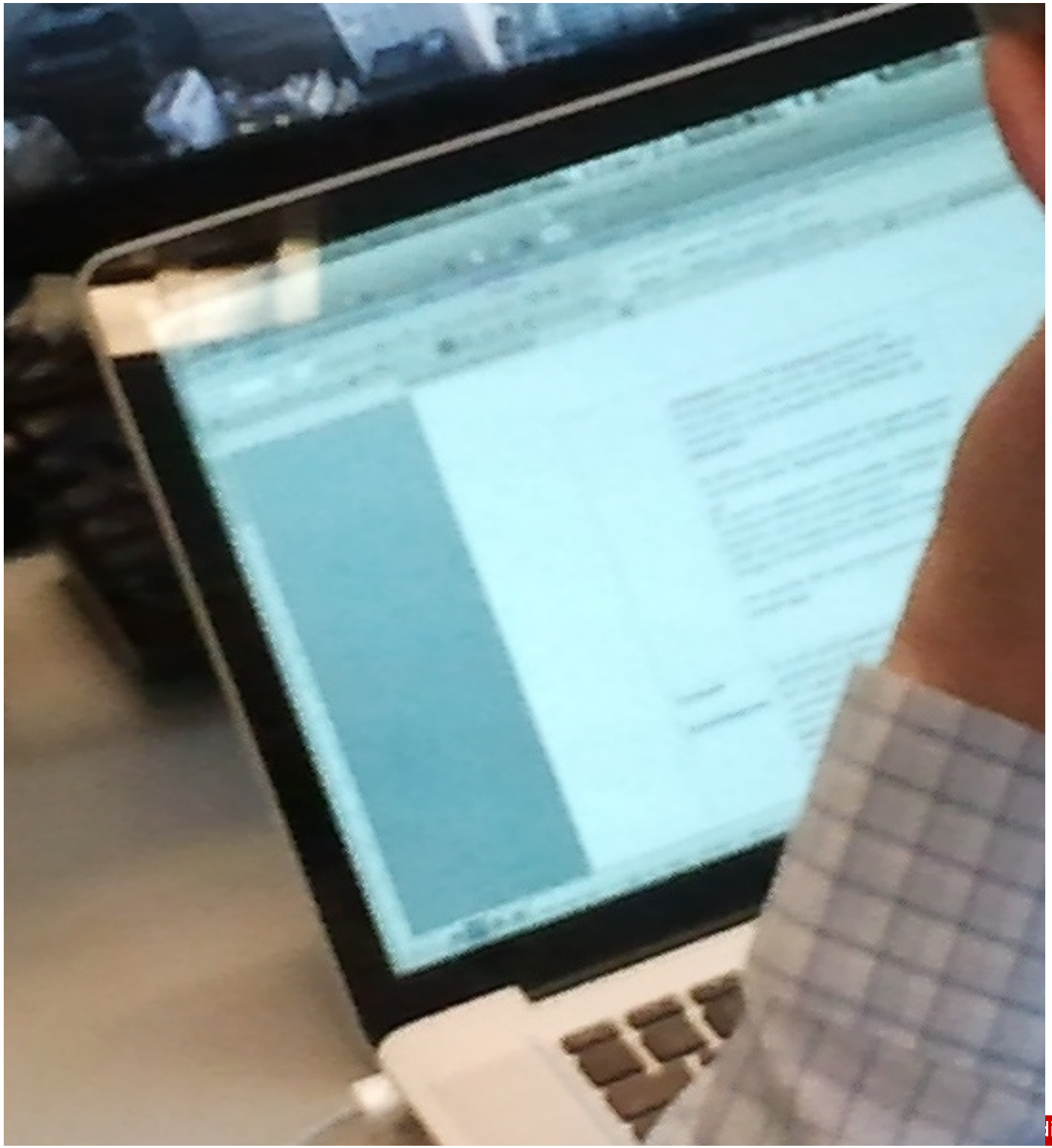
- Not many people dare talk to you directly
  - Fear of being considered impolite



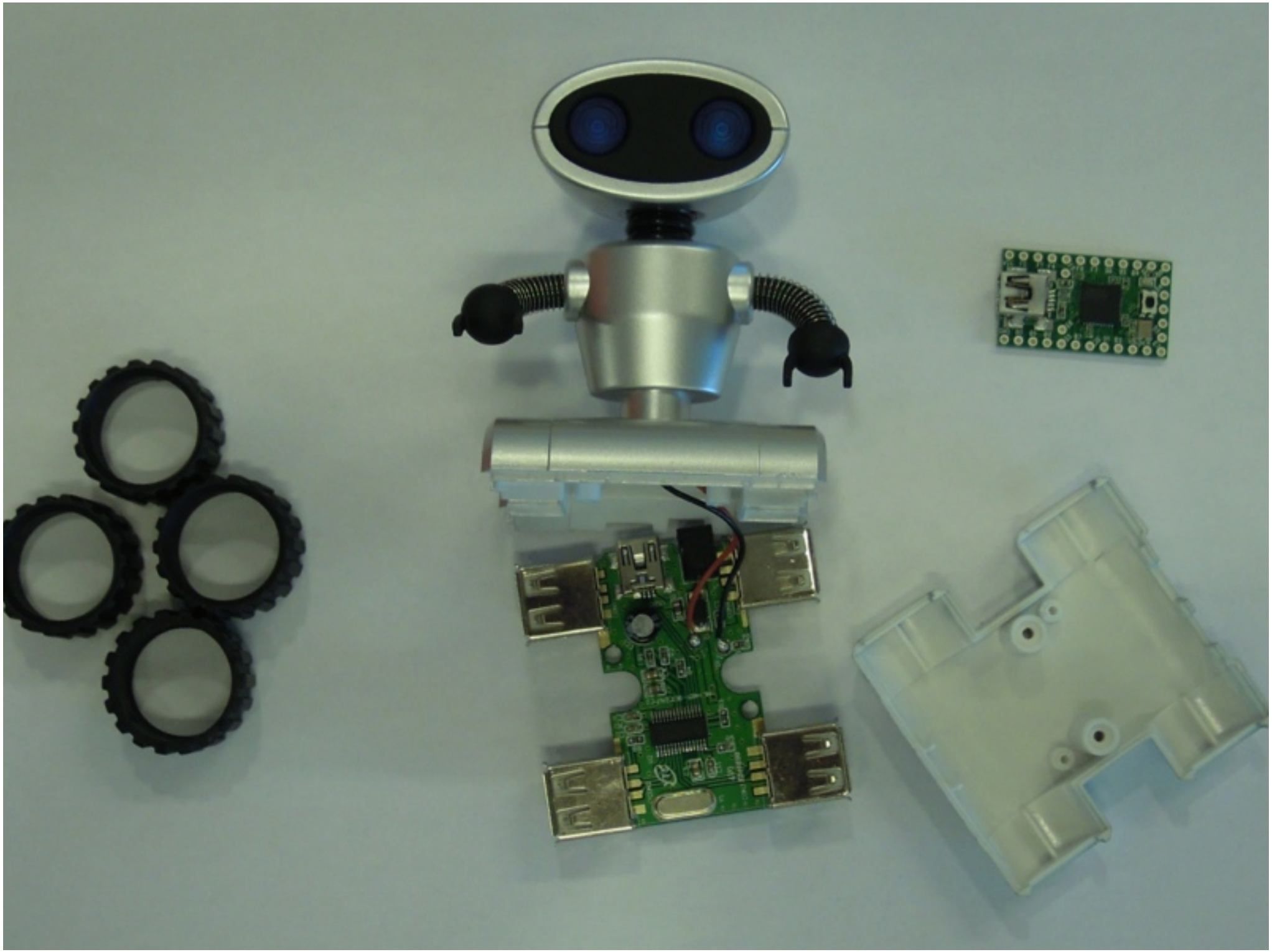
- Make pictures

- Get out (probably easy but might be hard)

More Examples




ROBOT
"4 PORT USB extension"
"INPUT! INPUT!"
POWERED BY USB
satzuma
LOVE IT WANT IT SATZUMA IT



SET

Computer Based Social Engineering Tools: Social Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the http://www.social-engineer.org launch and has quickly became a standard tool in a penetration testers arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Contents


A
Demo
N.R.
IN OUT
Normal Bias 120μs EQ

Follow Up

- Report with proof (pictures)
  - What has been tested
  - What has been found
  - What can be recommended
- Don’t naming individuals

Follow Up

- Results can be used for security awareness training
- Get people involved! They know vulnerabilities best!
- Keep on educating in different ways


CAUTION
PEDESTRIANS
ONLY CROSS
WHEN ROAD
IS CLEAR
COMPUTERS

Finding the right balance

- Be nice..
  but not too nice
- Be paranoid..
  but not too paranoid

walter@madison-gurkha.com