

# Social Engineering

## The devil is in the details

05. March 2015, Ivano Somaini



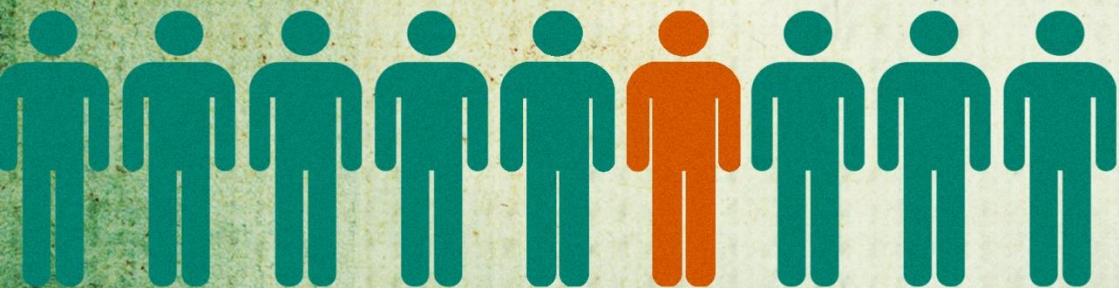




**Hobby**

**ETH**

**Study**



**Work**

W H O A M





**My first experience...**



# SOCIAL? ENGINEERING



*"Any act that influences a person to take an action that may or may not be in their best interest."*

[social-engineering.org](http://social-engineering.org)

# SOCIAL? ENGINEERING



*"Any act that influences a person to take an action **that is not in their best interest.**"*

# New attack vectors





A close-up photograph of a computer keyboard. The central focus is on two adjacent keys: a green key on the left and a red key on the right. Both keys have a textured, slightly raised surface. The green key is inscribed with the word "Download" in a white, sans-serif font, and the red key is inscribed with the word "Upload" in the same font. The surrounding keys are dark grey or black with a similar textured surface. The lighting is even, highlighting the colors and textures of the keys.

*Download*

*Upload*

<https://www.youtube.com/watch?v=F7pYHN9iC9I>



T  
R  
U  
S  
T



Today I'll present you



## **5 social engineering tests... ...which were successful!**



# Exploit 1 - Helpfulness/Authority



## Goal

- ✦ Gain access to the restricted employee area of the building
- ✦ Gain access to the internal protected area
- ✦ Steal confidential information (i.e. USB sticks, documents etc.)

## Information from the customer

- ✦ Company name
- ✦ Building address



## Information gathered

- ✦ Medium-sized private bank
- ✦ No public area
- ✦ Reception with security guard with full height turnstile with badge reader
- ✦ Garage entrance with badge reader
- ✦ And...

Coffee delivery service coming every  
day between 07:00 – 07:30



...has access to the garage and a  
badge for the secondary entrance







# Tailgating / Piggybacking





Very effective to indirectly communicate/suggest:

- ✦ Authority
- ✦ Need for help
- ✦ Internal Know-How – Pretexting
- ✦ Etc.



- ✦ Every entrance should have the same level of protection
- ✦ Teach staff that transitions into further internal protected zones are as critical as the checks performed on the first entrance
- ✦ Never let a visitor alone roam through your organization
- ✦ Employees and external suppliers should be trained to ask for visitor badges
- ✦ Accompany the visitor to the person he is intended to meet

### "Curiosity killed the cat" – Phishing/Baiting



## Goal

- ✦ Gain confidential information from employees through indirect attacks

## Information from the customer

- ✦ Company name

## Information gathered

- ✦ Swiss Bank
- ✦ 500 ~ 600 employee
- ✦ Mail address of 250 employee
- ✦ And...



75<sup>th</sup> anniversary of the Bank  
...time for a bonus?!?



# «Wrong» delivery address



- ✦ Deny delivering emails containing dangerous / unexpected file types (especially executables)
- ✦ Macro Settings should be controlled by a GPO. Either disallow the execution of macros completely, or selectively allow the execution of signed macros only.
- ✦ The authenticity and the origin of mails – or in general every form of requests and inquiries – should be checked before any other action takes place

# Exploit 3 - Holiday





## Goal

- ✦ Get the IT support company to change a firewall rule

## Information from the customer

- ✦ Company name
- ✦ Support company name
- ✦ Contact data of the responsible technician

## Information gathered

- ✦ Name of the boss of the responsible technician
- ✦ And...

**Automatische Antwort:** [REDACTED]

Gesendet: Fr 29.08.2014 09:38

An: Ivano Somaini

Sehr geehrte Damen und Herren

Vielen Dank für Ihre Nachricht. **Ich bin am Freitag jeweils abwesend.** Ihre Mails werden in dieser Zeit nicht gelesen und nicht weitergeleitet. Ich werde Ihre Mails nach meiner Rückkehr ins Büro so bald als möglich bearbeiten.

Bei dringenden Angelegenheiten wenden Sie sich bitte an meine Stellvertreter:

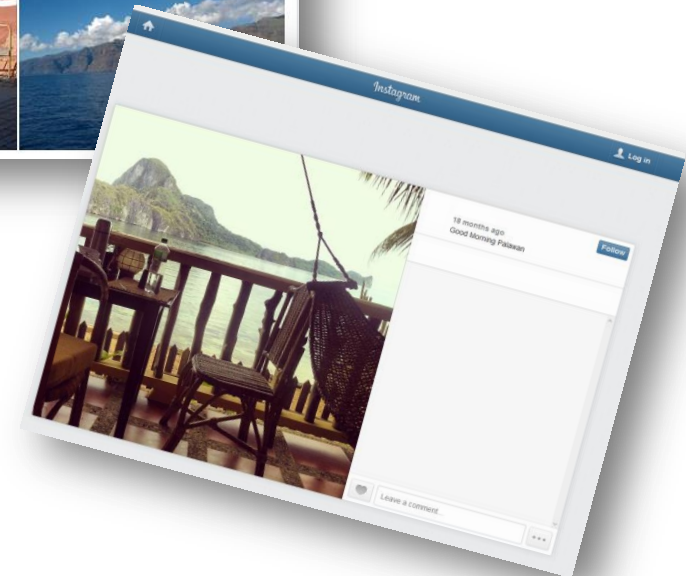
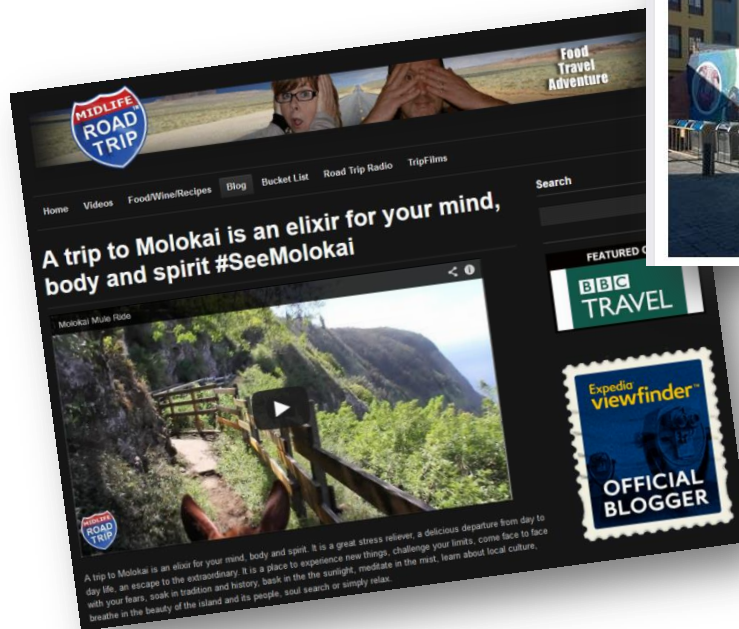
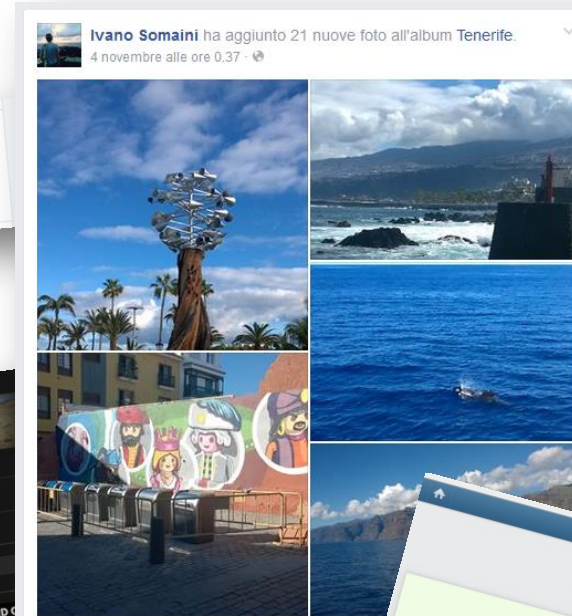
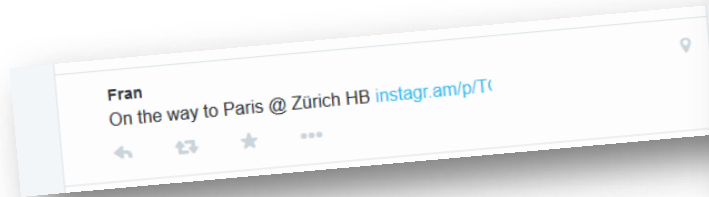
[REDACTED]

Besten Dank für Ihr Verständnis.

Freundliche Grüsse

[REDACTED]

# Upload Generation





## Other attack vector...



- ◆ Analyze social network activity
- ◆ Try to reach the target during school holidays



Weitere Informationen



## Interessen

Bicycles, design, table soccer, music, movies **mountain biking**

# Fake e-mail



victim



+



+



= PRETEXT

*friday*

+

**URGENT**

=

**STRESS!!!**



**URGENT**



**URGENT**

*friday*



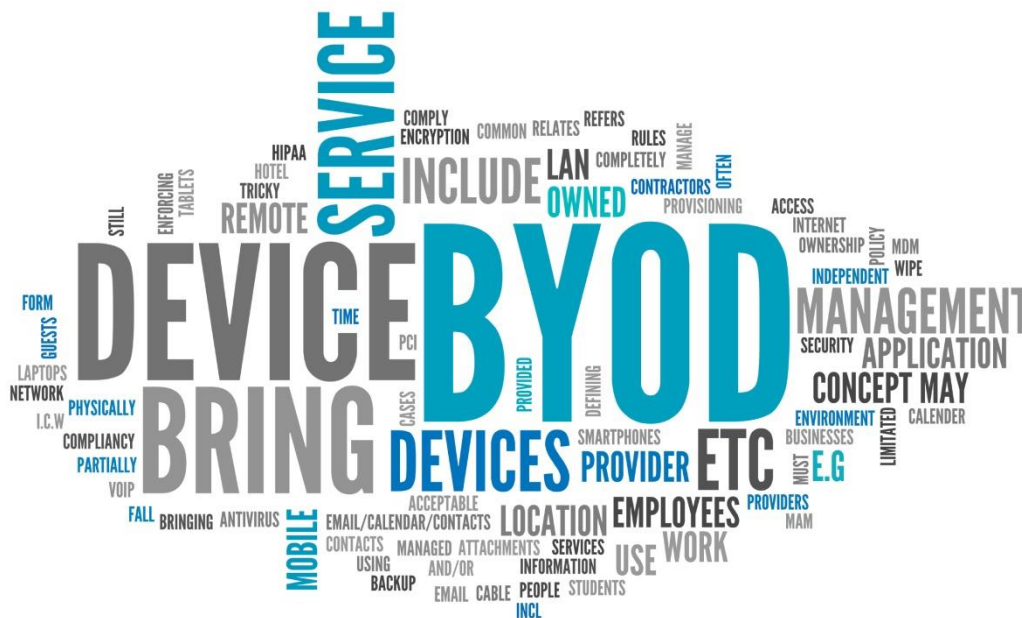
**PRETEXT + STRESS =**





- ✦ The authenticity and the origin of mails – or in general every form of requests and inquiries – should be checked before any other action takes place
- ✦ If possible, avoid automatic e-mail for 80% job
- ✦ Raise awareness about information disclosed on social network

# Exploit 4 - BYOD



## Goal

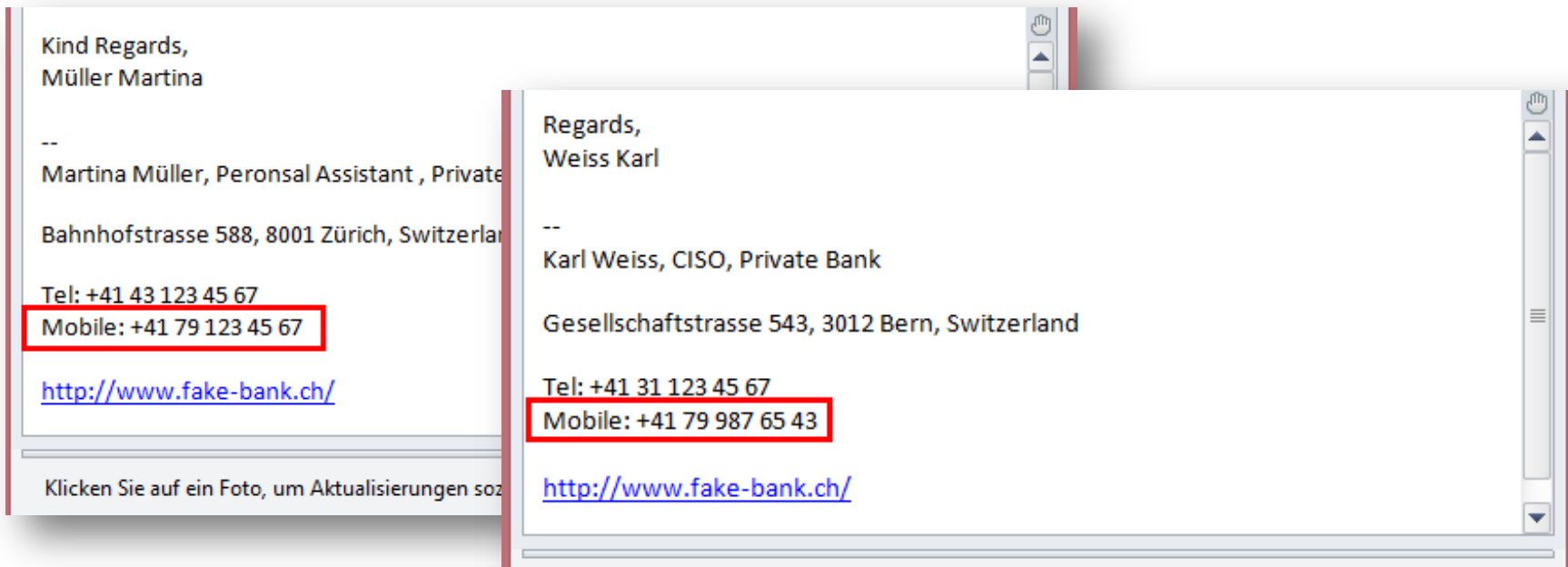
- ✦ Gain access to the confidential data of the CEO

## Information from the customer

- ✦ Company name
- ✦ Name of the personal assistant of the CEO

## Information gathered

- ✦ Mobile phone number of CISO
- ✦ Mobile phone number of personal assistant of CEO



Kind Regards,  
Müller Martina

--  
Martina Müller, Personal Assistant , Private Bank  
Bahnhofstrasse 588, 8001 Zürich, Switzerland  
Tel: +41 43 123 45 67  
**Mobile: +41 79 123 45 67**  
<http://www.fake-bank.ch/>

Klicken Sie auf ein Foto, um Aktualisierungen zu sehen

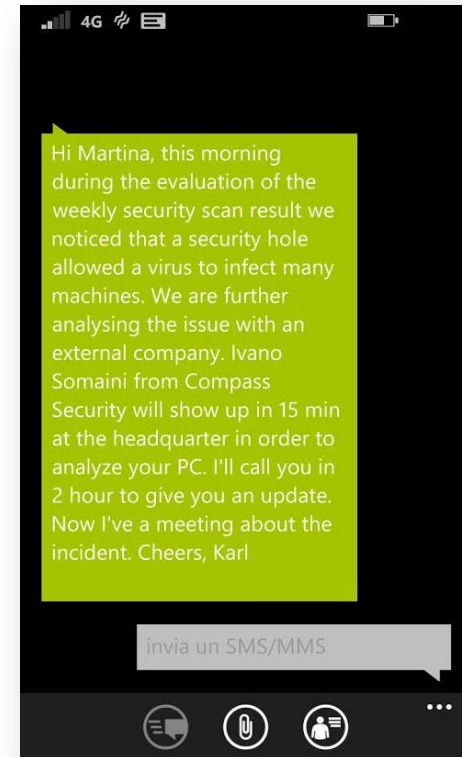
Regards,  
Weiss Karl

--  
Karl Weiss, CISO, Private Bank  
Gesellschaftstrasse 543, 3012 Bern, Switzerland  
Tel: +41 31 123 45 67  
**Mobile: +41 79 987 65 43**  
<http://www.fake-bank.ch/>



"Hi Martina, this morning during the evaluation of the weekly security scan result we noticed that a security hole allowed a virus to infect many machines. We are further analyzing the issue with an external company.

Ivano Somaini from Compass Security will show up in 15 min at the headquarter in order to analyze your PC. I'll call you in 2 hour to give you an update. Now I've a meeting about the incident. Cheers, Karl"



- ✦ SMS Spoofing
- ✦ Caller ID Spoofing

- ✦ Call the initiator back to confirm his identity and request
- ✦ Create awareness that phones are as vulnerable to spoofing attack as e.g. emails
- ✦ The authenticity and the origin of the SMS and phone calls – or in general every form of requests and inquiries – should be checked before any other action takes place
- ✦ Ideally disable signature in response mail
- ✦ Ideally don't insert mobile number in signature

# Exploit 5 - Events/Festivity



## Goal

- ✦ Gain access to the secured area of the building
- ✦ Steal confidential information (i.e. USB sticks, documents etc.)

## Information from the customer

- ✦ Company name
- ✦ Building address



## Information gathered

- ✦ Traditional Swiss company
- ✦ No public area
- ✦ Single Point-of-Entry
- ✦ Full height turnstile with badge reader

It was the 5<sup>th</sup> of December...



Would you ask Santa Claus for an identification card?

# Unintended consequences



- ✦ Never let a visitor alone roam through your organization
- ✦ The receptionist, and ideally, also the internal employee has to verify the identity of every person who get access to the secured area of the company
- ✦ Request a valid badge to exit the building

# Conclusions



PAY ATTENTION TO DETAIL



*Thank  
you*



Question?

