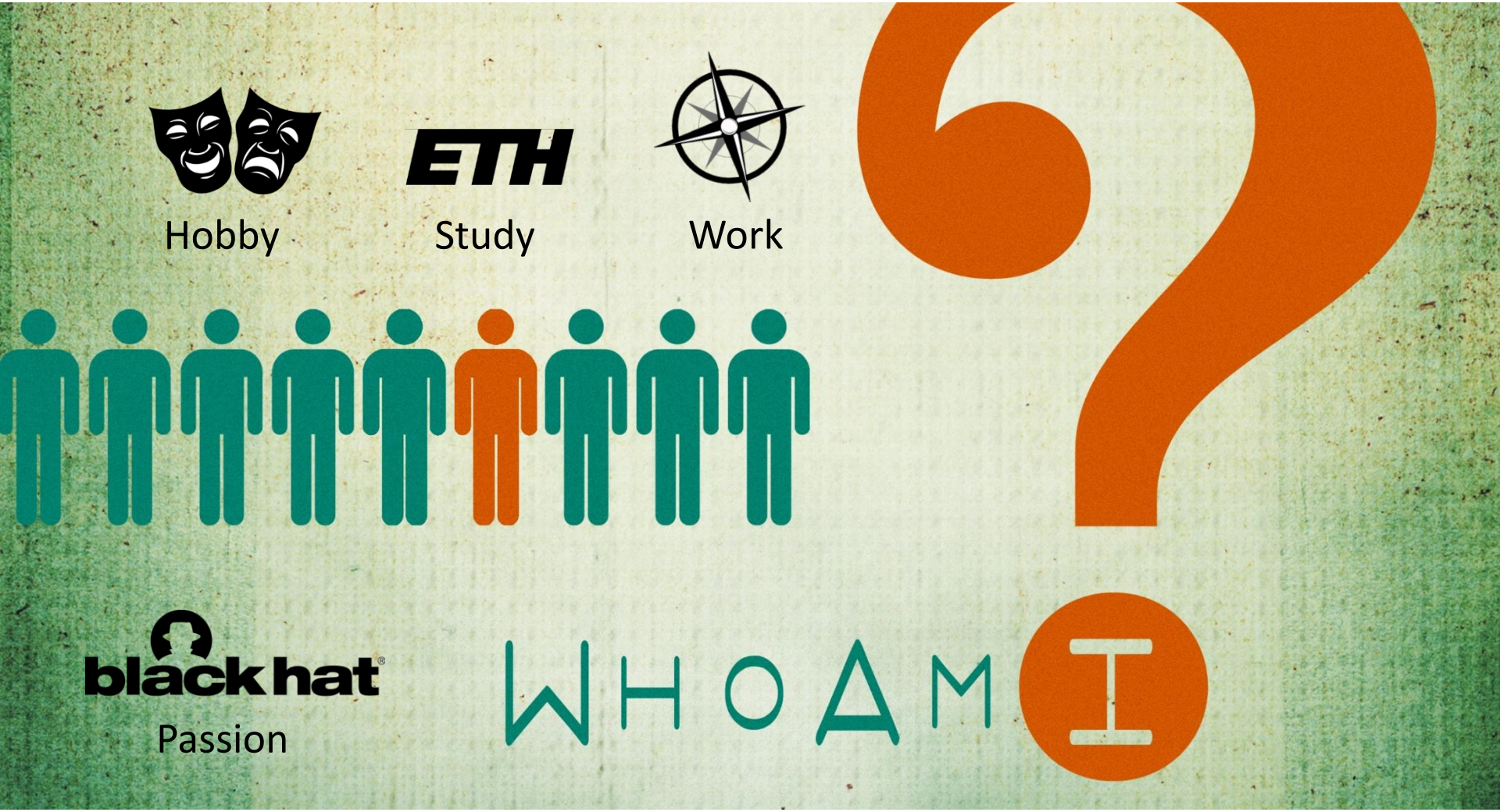
Social Engineering

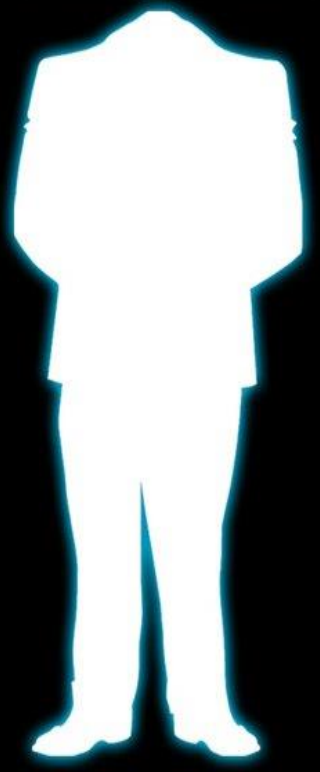
The devil is in the details

26th November 2019, Ivano Somaini @ CompassSecurity


Hobby
ETH
Study
Work
black hat
Passion
WHO AM I

My first experience…

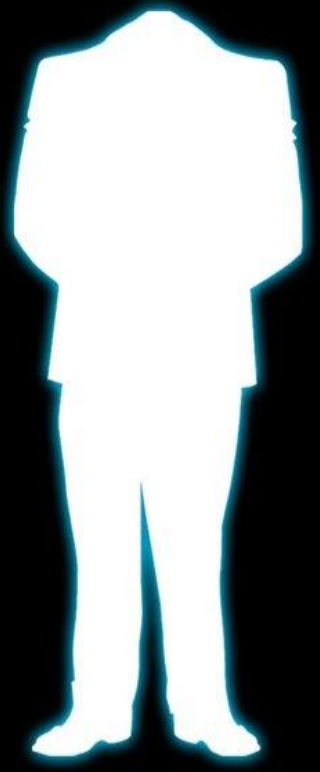
SOCIAL ? ENGINEERING



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

social-engineering.org

SOCIAL ? ENGINEERING

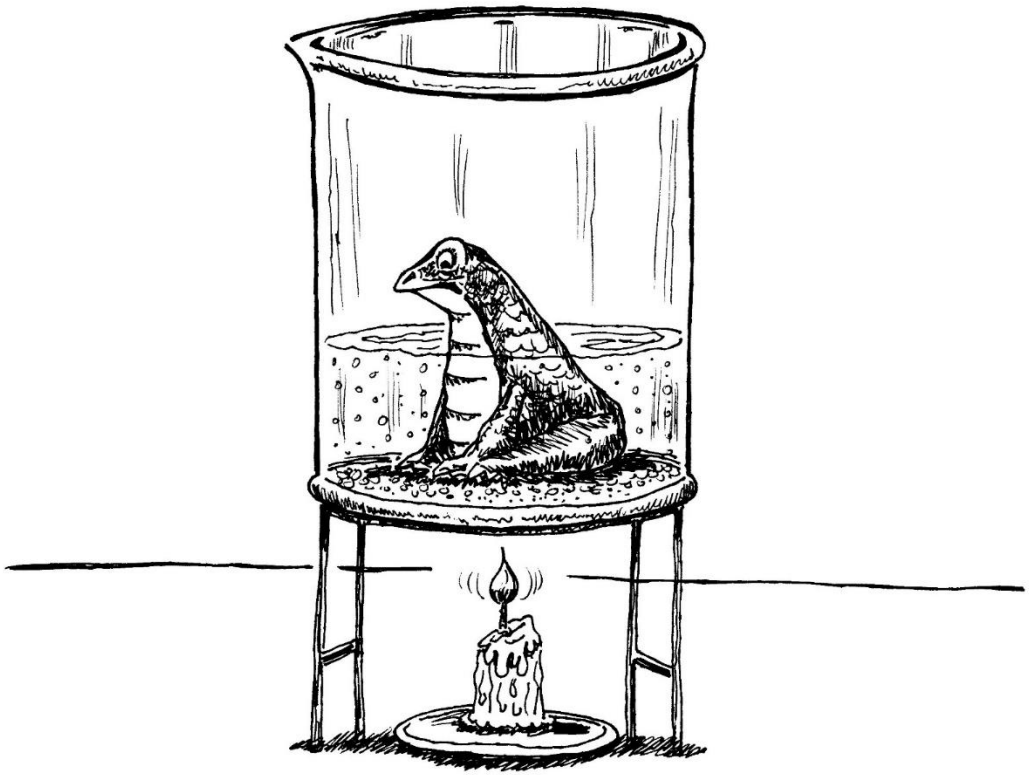


"*Any act that influences a person to take an action that is not in their best interest.*"

New attack vectors


Download
Upload

Today…boiled Frog




TRUST
Search contacts
Favourites
Recent calls
A-Z
Allan Hock
Bridgit Brucker
Joe Rogers
Annabella Wolske
Selena Pomerantz
Leo James
Jamie Adams
Amanda Jane Allens
Sian Anderson
Ali Arscroft
Kurt Avery
Jennifer Baxter
12:04
Share
It's open source.
Our global community is made up of thousands of people who want

Today I'll present you…

5 social engineering tests…

…which were successful!

Exploit 1 - Helpfulness/Authority

Mission

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 Gathering

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…

Attack Scenario

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

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

Exploit 2 - Curiousness

“Curiosity killed the cat” – Phishing/Baiting

“Lost” USB Stick

Mission

Goal

- Gain confidential information from employees through indirect attacks

Information from the customer

- Company name

Information Gathering

Information gathered

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

Attack Scenario

75th anniversary of the Bank

…time for a bonus?!?

«Wrong» delivery address

Exploit 3 - Holiday

Mission

Goal

- Get the IT support company to change a firewall rule

Information from the customer

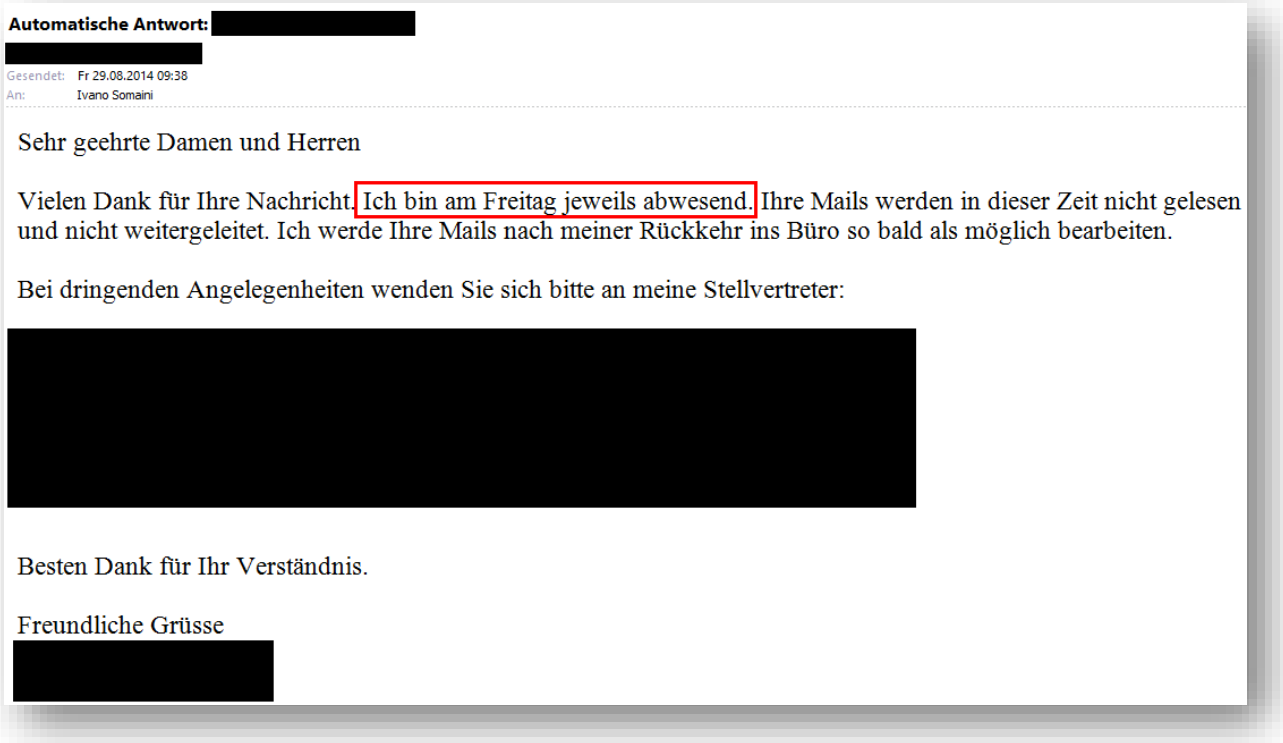
- Company name
- Support company name
- Contact data of the responsible technician

Information Gathering

Information gathered

- Name of the boss of the responsible technician
- And…

Attack Scenario



Automatische Antwort: [redacted]

[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:

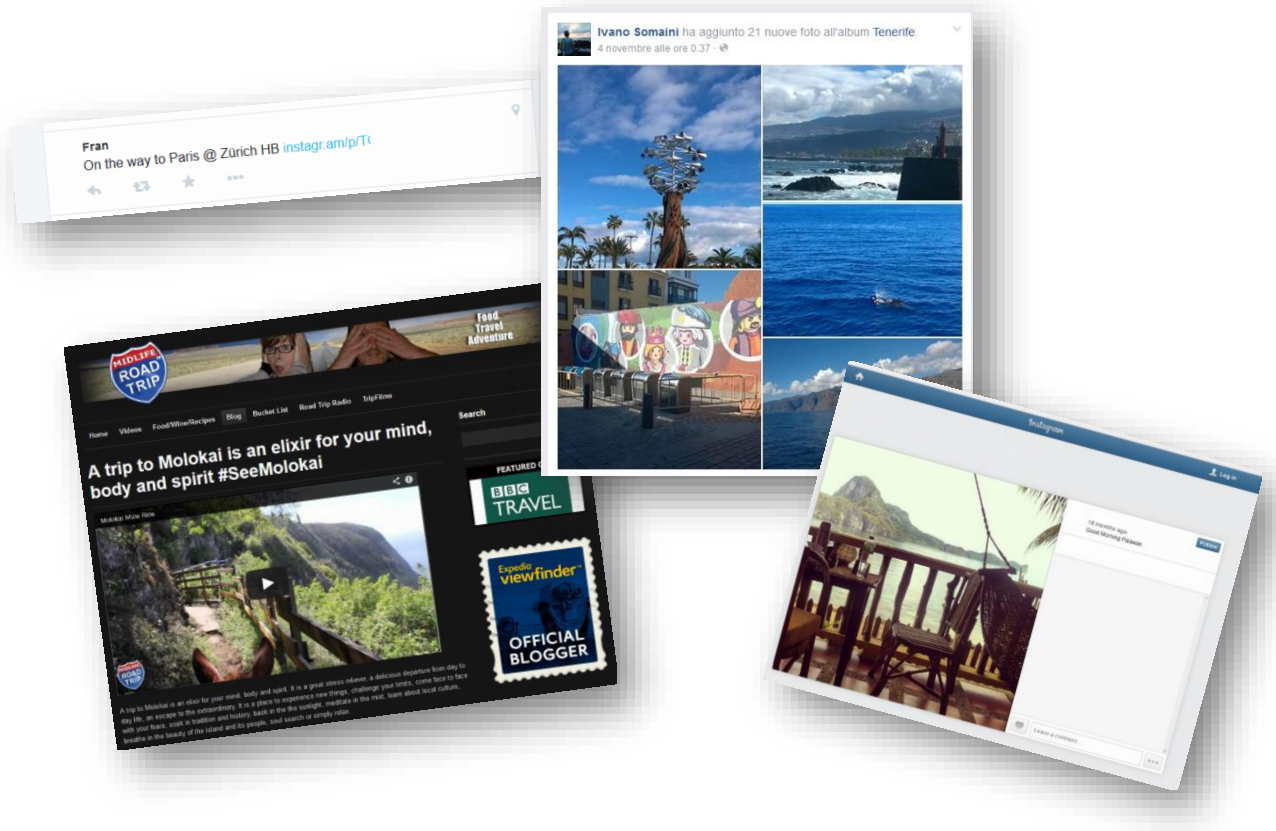
[redacted]

Besten Dank für Ihr Verständnis.

Freundliche Grüsse

[redacted]

Upload Generation



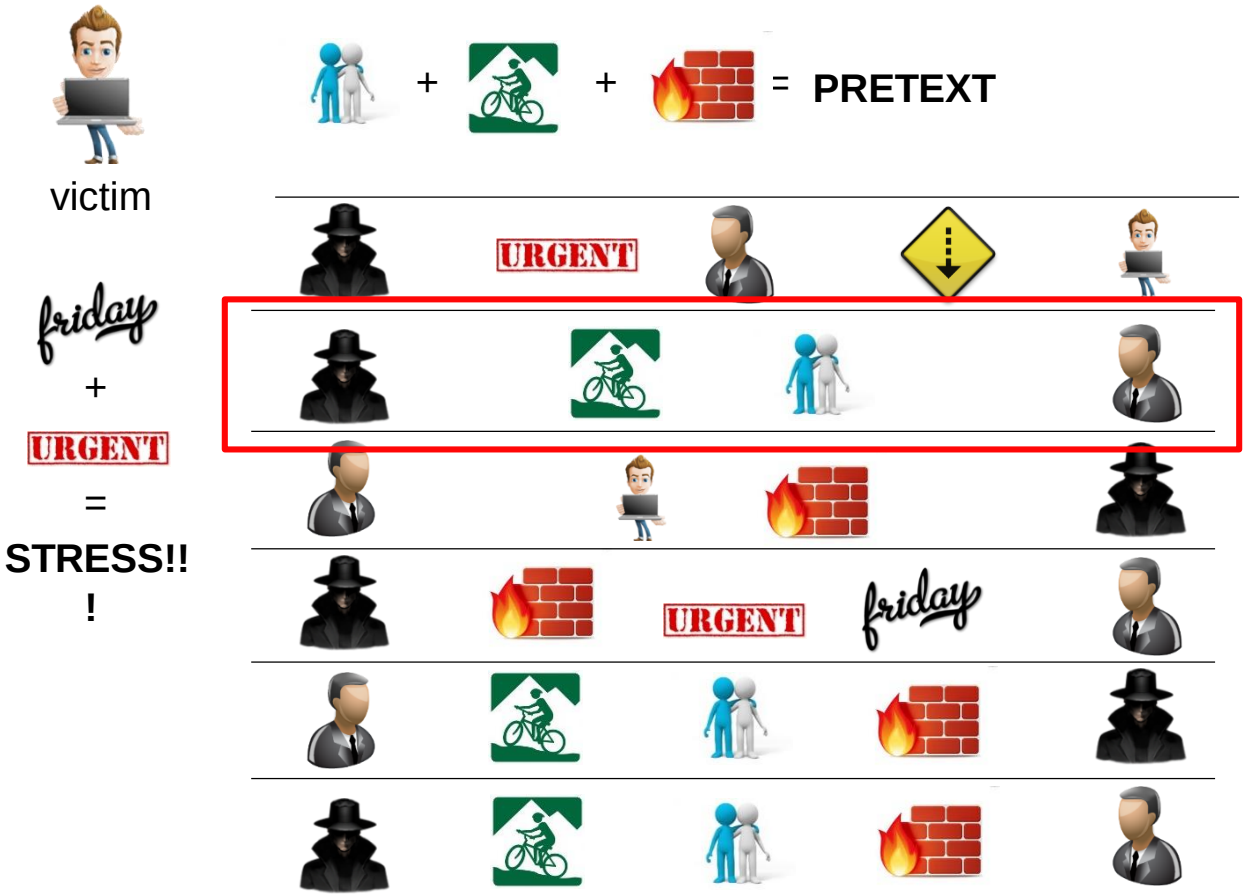
Pretexting

Weitere Informationen

Interessen

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

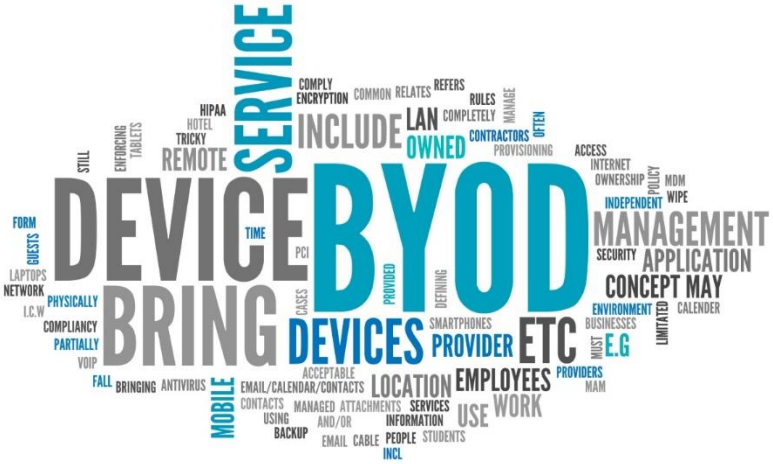
Fake e-Mail Conversation



Social Engineering Equation

PRETEXT + STRESS = 

Exploit 4 - BYOD



Mission

Goal

- Gain access to the confidential data of the CEO

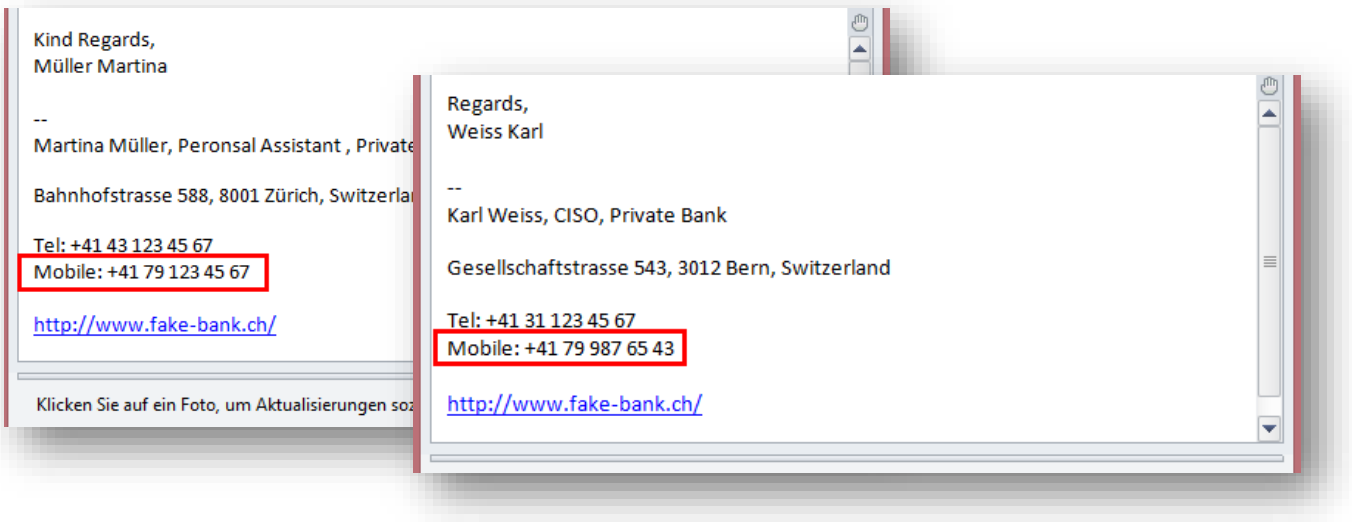
Information from the customer

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

Information Gathering

Information gathered

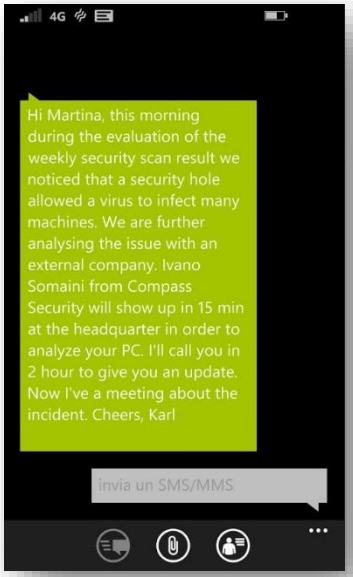
- Mobile phone number of CISO
- Mobile phone number of personal assistant of CEO



Attack Scenario

“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

Exploit 5 - Events/Festivity

Mission

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 Gathering

Information gathered

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

Attack Scenario

It was the 5th of December…

Would you ask Santa Claus for an identification card?

Unintended consequences

Conclusion

Question?