TOLLETATEN
NORWEGIAN CUSTOMS

Social Engineering Pentesting

- How it is done and what you should think about

August 29th, 2023

Ragnhild “Bridget” Sageng
Senior Security Advisor

TOLLETATEN
NORWEGIAN CUSTOMS

Who am I?

- Ragnhild/Bridget
- Worked with IT since 2007
- Previously worked as an ethical hacker
- Works at Norwegian Customs
- Loves to talk about the human element in Cyber Security

Today’s Talk...

- What is social engineering?
- How does a pentester work using social engineering?
- How to perform a social engineering pentest responsibly?
- A social engineering pentest story

What is Social Engineering?

Social engineering is defined as:

- Techniques used to get a person to perform an action or disclose information, regardless of it being for their benefit or not.

TOLLETATEN
NORWEGIAN CUSTOMS

How a Social Engineer Pentester Works

- Focus on the human
- Collect information
- Pretext
- Debrief
- Ethical responsibility
- Can be a part of a bigger red team operation

SO YOU'RE A COMPLETE STRANGER AND YOU WANT MY NAME, SOCIAL SECURITY NUMBER AND MOTHER'S MAIDEN NAME? SURE, WHY NOT?
SecurityElements.com

OSINT (Open-Source Intelligence)

- **All information you can find open on the web.**

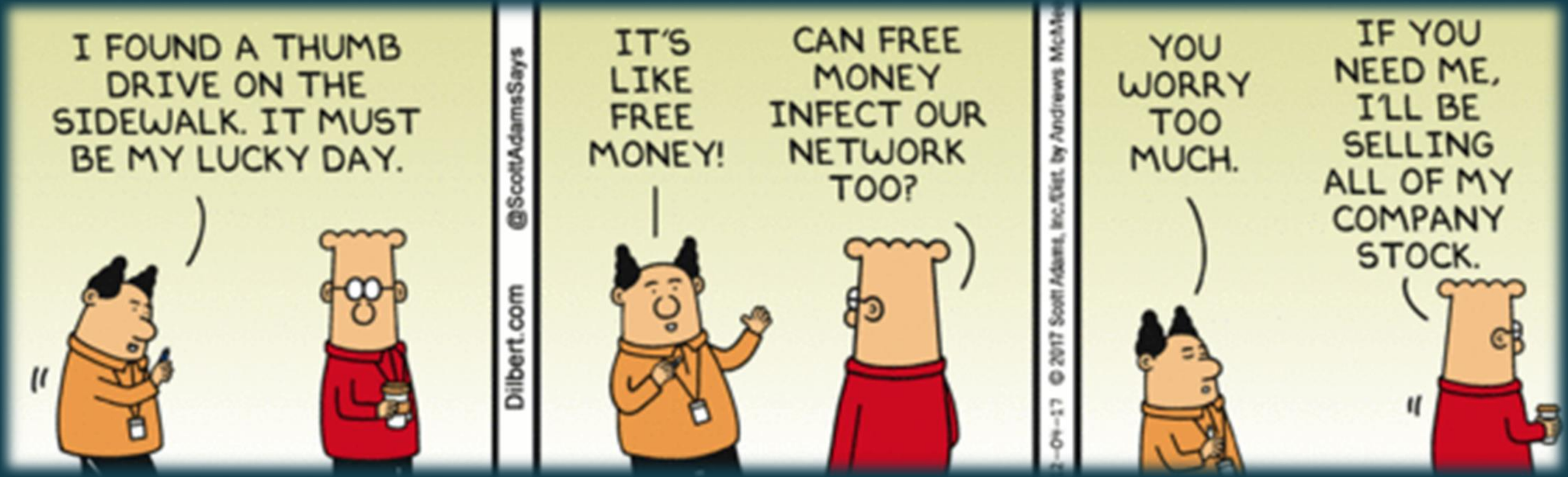
Examples:

  - Social media
  - Google searches
  - Other accounts
  - Google maps
  - Certificate information
  - DNS information

- **OSINT can be done on both individuals and companies**

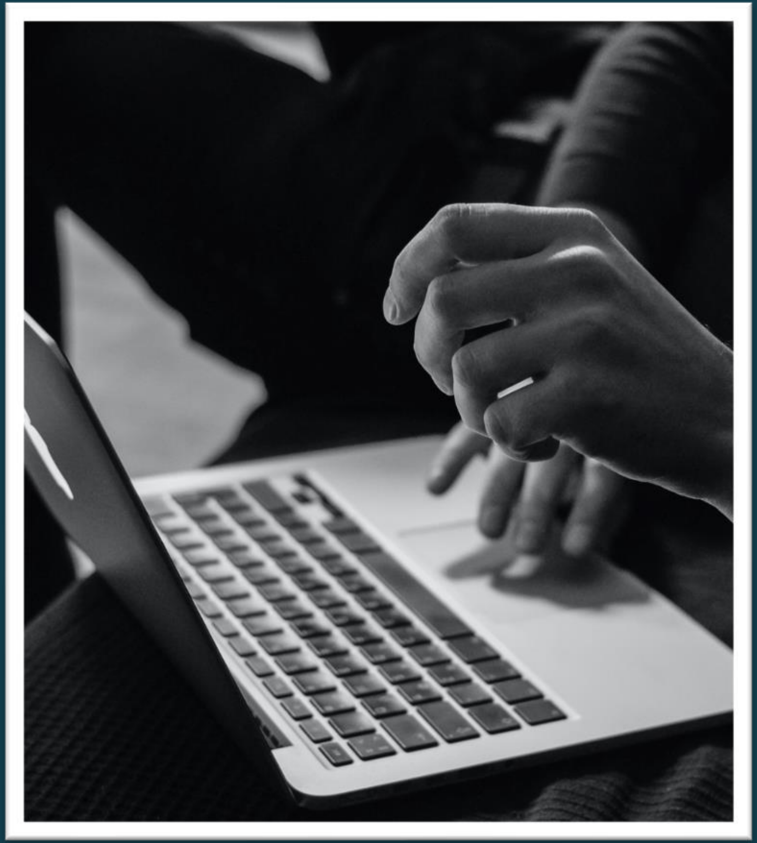
Vishing, Smishing and Phishing Tests

- Tests performed using email, Social media, SMS or phone
- Often done towards a large group or more targeted
- OSINT is often used to make a pretext
- Some preforms tests regularly to measure awareness


I FOUND A THUMB DRIVE ON THE SIDEWALK. IT MUST BE MY LUCKY DAY.
Dilbert.com @ScottAdamsSays
IT'S LIKE FREE MONEY!
CAN FREE MONEY INFECT OUR NETWORK TOO?
2-04-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMe
YOU WORRY TOO MUCH.
IF YOU NEED ME, I'LL BE SELLING ALL OF MY COMPANY STOCK.

TOLLETATEN
NORWEGIAN CUSTOMS

Pentest Reports

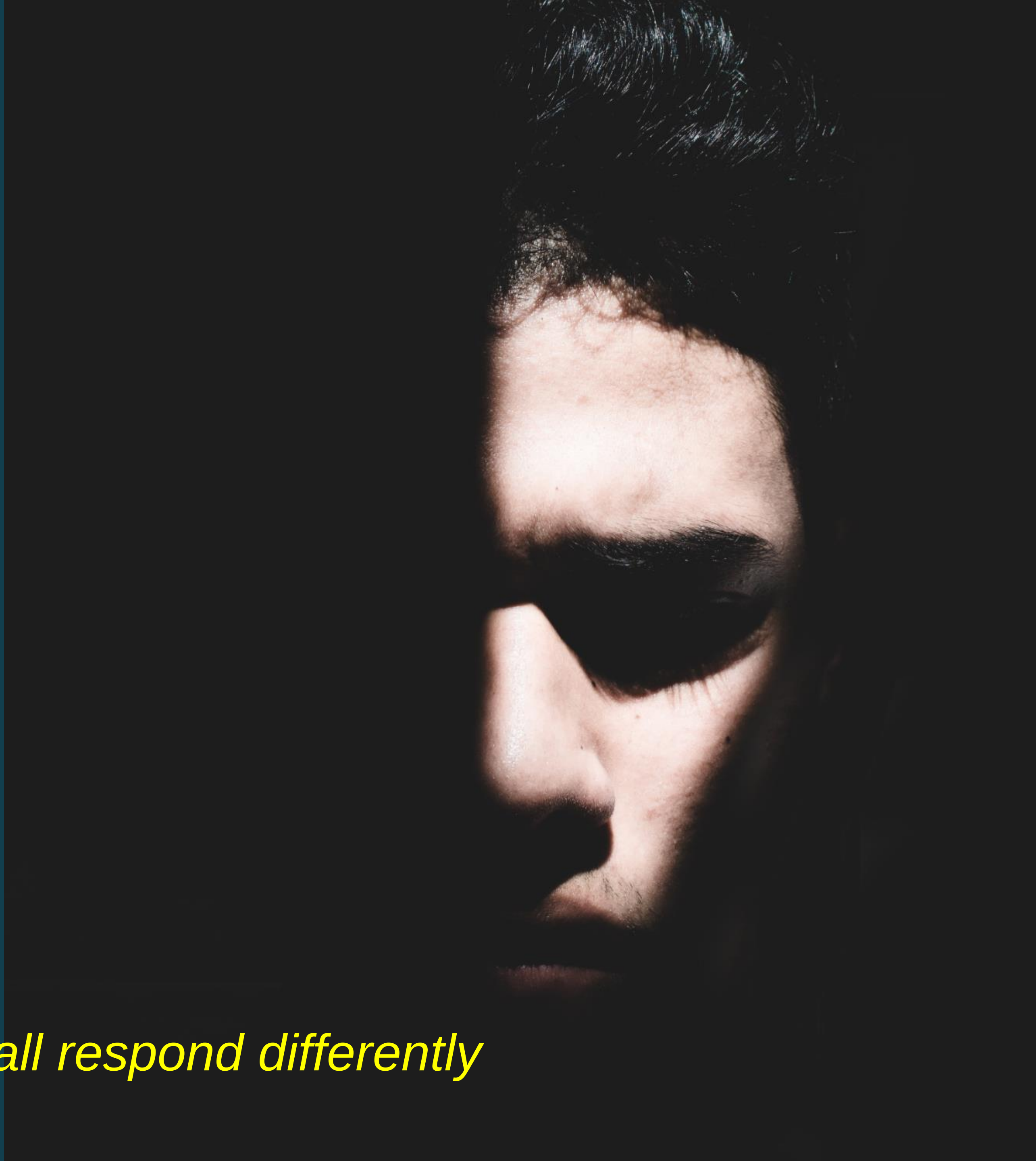


- **Pentest reports try to stay anonymous, but:**
  - Can reveal the victims unintentionally
  - The situation might call for them to be revealed
- **Consequences**
  - Third-party vendor losing their contract
  - Employees losing their jobs
  - Initiation of a blame-game

TOLLETATEN
NORWEGIAN CUSTOMS

The Human Psyche

- Same mental response as when being scammed
- Being duped
- The blame-game
- Some are more resilient



- We are all different and we all respond differently

"

> *One individual failing a social engineering test is not an indication of the individual's failure, it is the indication of a systemic failure. If one individual fails, everyone else can fail as well.*

Tinker Secor, Hacker

TOLLETATEN
NORWEGIAN CUSTOMS

Human Resources Perspective

- Cooperation between departments
- Measures in place to take care of emotional reactions
- Clear guidelines for follow-up

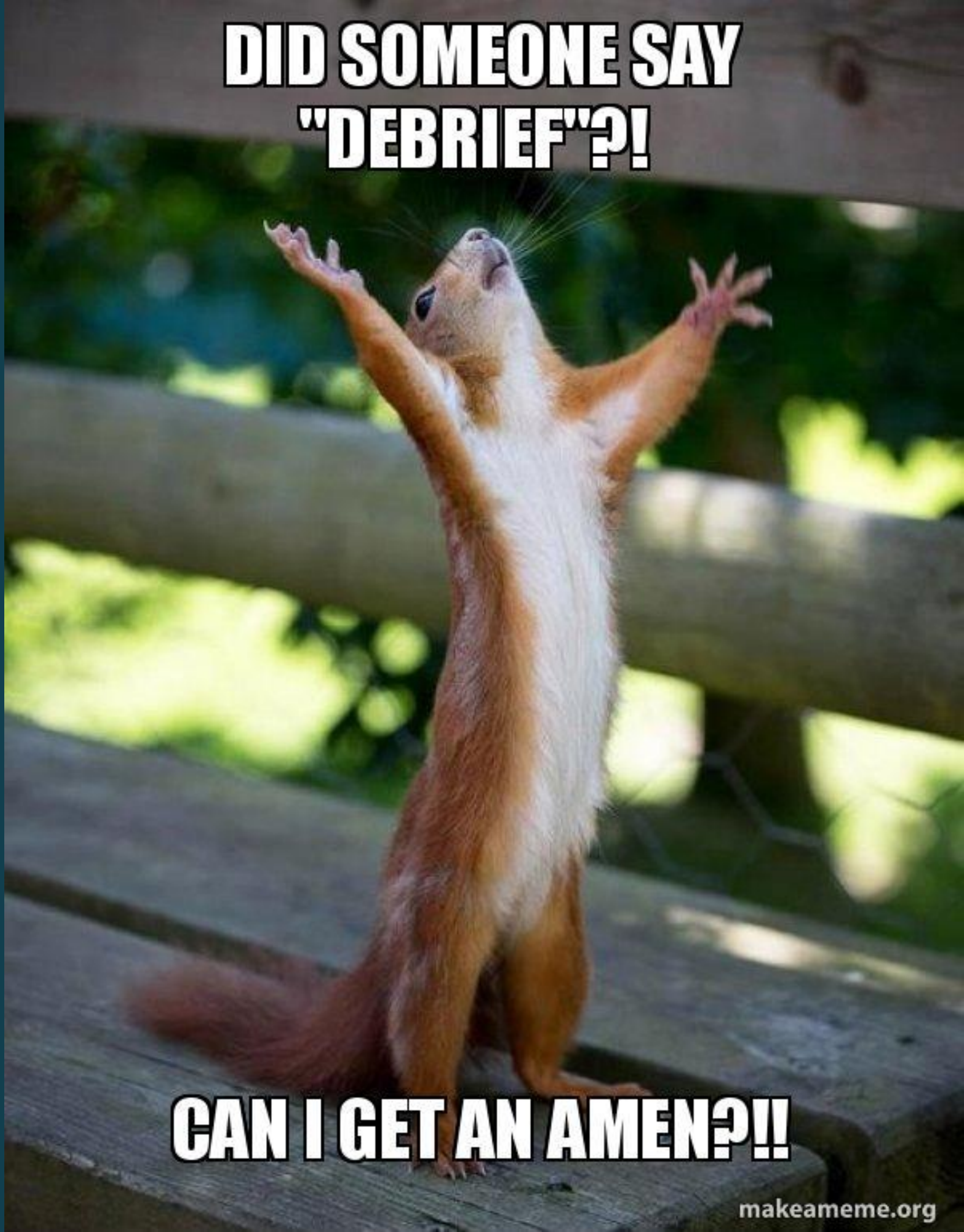
TOLLETATEN
NORWEGIAN CUSTOMS

Debriefing

- Debriefing the company is important

- People might have different needs for information in the aftermath

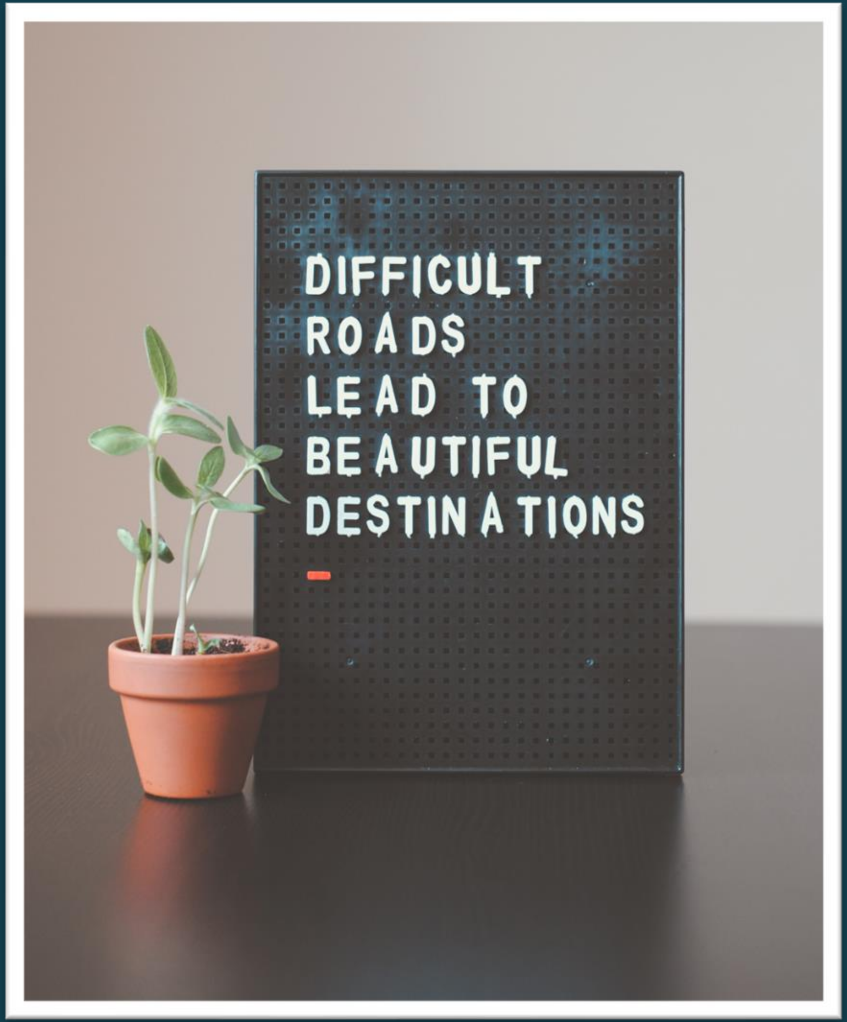
- Sometimes a direct debrief of victims can be beneficial for all parties involved



TOLLETATEN
NORWEGIAN CUSTOMS

So, Who is Responsible?

- Collaborative effort
- Processes are important
- Bad follow-up = Bad learning experience
- Everyone loses if the aftermath is handled badly



Real-life Story

- The story is anonymized and pre-approved for sharing
- Test at an IT department and their external location
- Names are fictious, and the presentation have no images from the locations themselves

What Were the Targets?

Server room at an upper elementary school

IT department’s main office

Goal: Get into the server rooms and look for attack vectors

TOLLETATEN
NORWEGIAN CUSTOMS

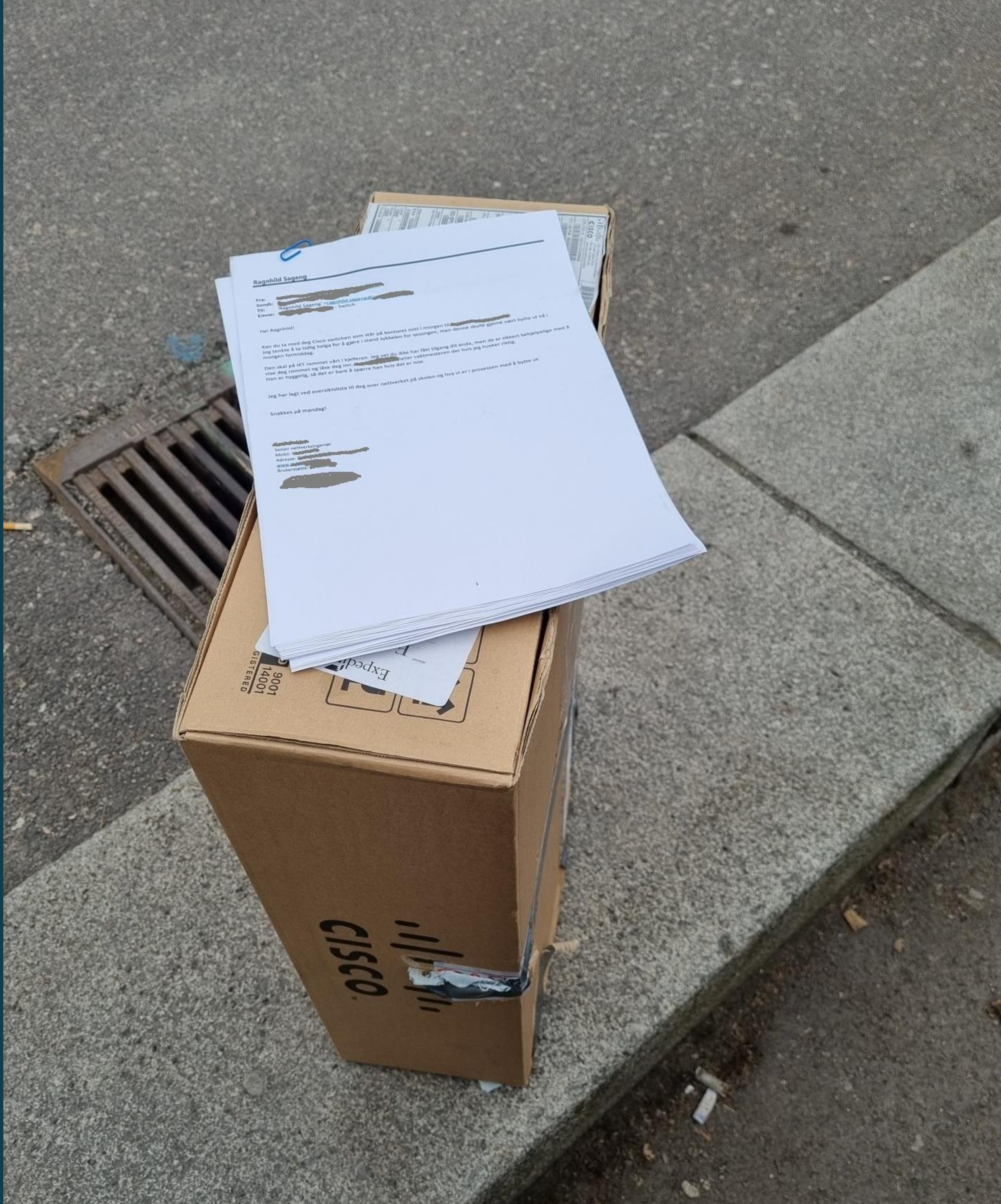
Prior to the Test

- Gathered information
- Agreed to a time for the test
- Made pretexts

TOLLETATEN
NORWEGIAN CUSTOMS

Target 1: The School Server Room

- **Read building articles and public documents**
- **Checked maps and social media for images of the location**
- **Searched for employees in key roles:**
  - Janitor, Headmaster, IT
- **Blueprints**
  - Contained infrastructure information



Ragnhild Sageng

Fra: [redacted]
Sendt: [redacted]
Til: 'Ragnhild Sageng' <ragnhild.sageng[redacted]
Emne: [redacted] - Switch

Hei Ragnhild!

Kan du ta med deg Cisco switchen som står på kontoret mitt i morgen til [redacted] Jeg tenkte å ta tidlig helga for å gjøre i stand sykkelen for sesongen, men denne skulle gjerne vært bytta ut nå i morgen formiddag.

Den skal på IKT rommet vårt i kjelleren. Jeg vet du ikke har fått tilgang dit enda, men de er sikkert behjelpelige med å vise deg rommet og låse deg inn. [redacted]heter vaktmesteren der hvis jeg husker riktig. Han er hyggelig, så det er bare å spørre han hvis det er noe.

Jeg har lagt ved oversiktslista til deg over nettverket på skolen og hva vi er i prosessen med å bytte ut.

Snakkes på mandag!

[redacted]
Senior nettverksingeniør
Mobil: [redacted]
Adresse: [redacted]
www.[redacted]
Brukerstøtte: [redacted]
[redacted]

Result

Parked the car

Saw the janitor

Called out

used pretext

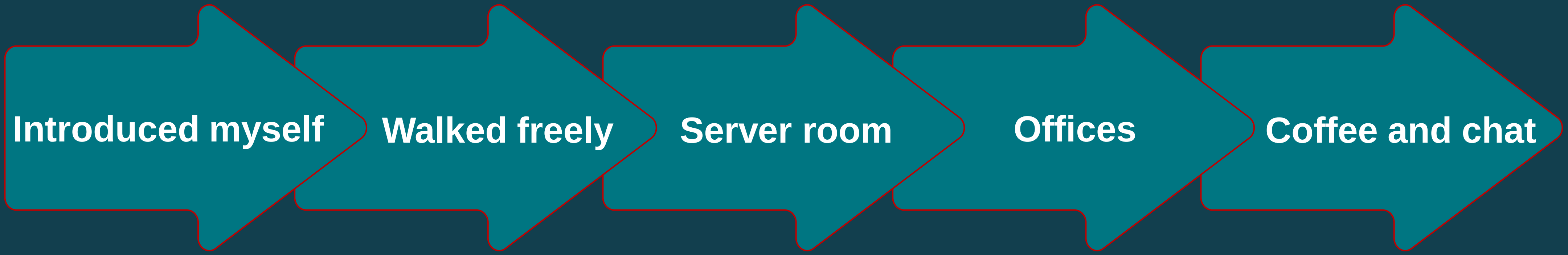
Inside after 2 min

TOLLETATEN
NORWEGIAN CUSTOMS

Target 2: IT Main Office

- Read building articles and public documents
- Checked maps and social media for images of the location
- Searched for employees
- Found a pretext

Result



Introduced myself

Walked freely

Server room

Offices

Coffee and chat

How to Avoid Social Manipulation?

- Awareness and courses
- Exercise
- Zero Trust vs Trust but Verify
- Security culture

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
Dilbert.com DilbertCartoonist@gmail.com
WAIT FOR IT
Enter your bank account number.
SCAM.
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

We can all be duped; the important thing is to not hide it when it happens

TOLLETATEN
NORWEGIAN CUSTOMS

Key Take-aways

1. Social engineering pentest-planning should be a collaborative effort in the company
2. Set demands
3. Punishment does not encourage learning

TOLLETATEN
NORWEGIAN CUSTOMS

Thank You!

@ragnhild_bss

linkedin.com/in/ragnhildsageng

ragnhild.sageng@toll.no