Stupid Human Tricks

InfoSec-Human Interaction

Problem

- Humans
- Automatons

My Background

- Regulatory examination, audit, social engineering, pentest, training, consulting
- Regulated industries
- Failure!
- Humanity

Scenarios

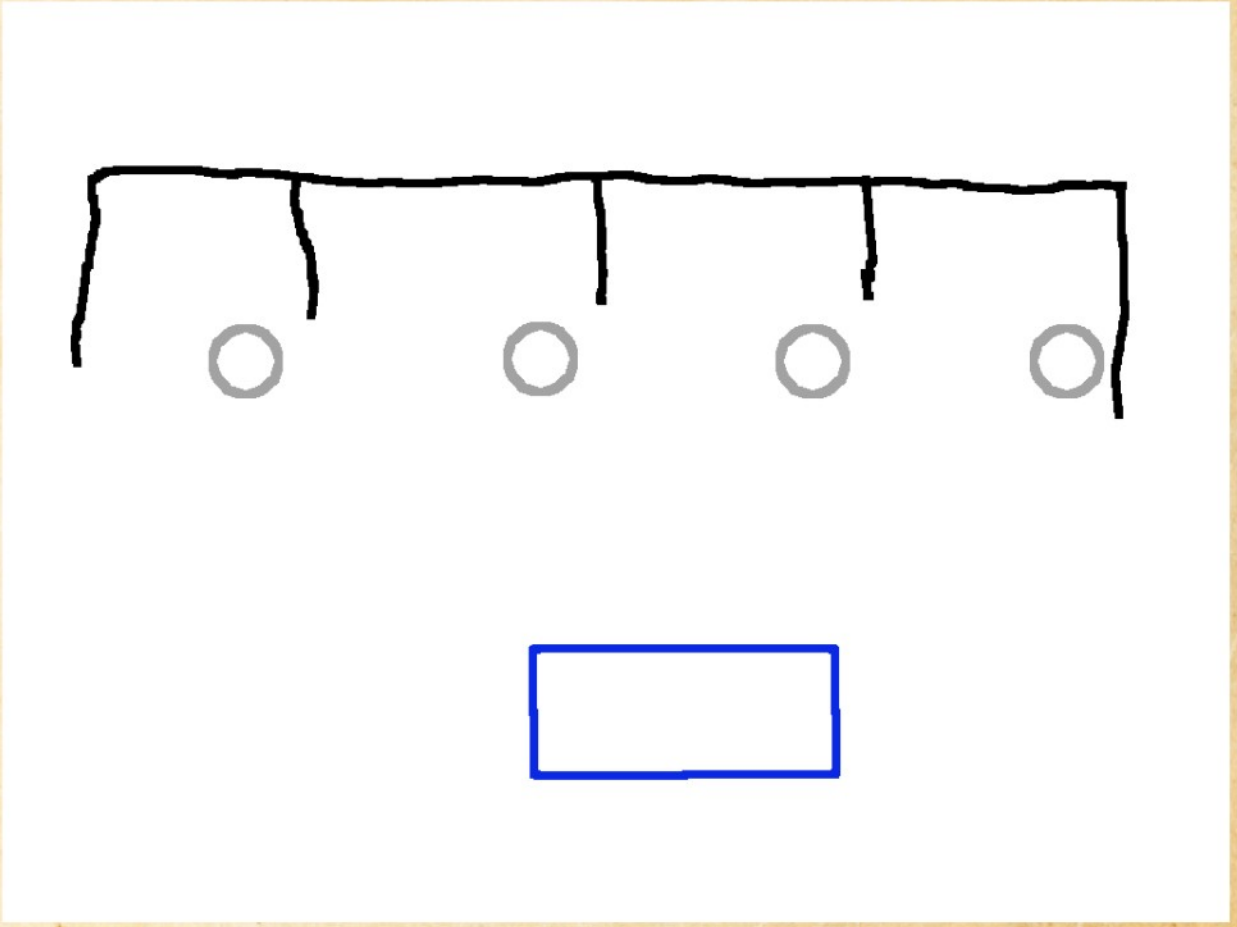
- Description
- Ideal World
- Reality
- Problem Areas
- Solution

Three Weird Tricks!

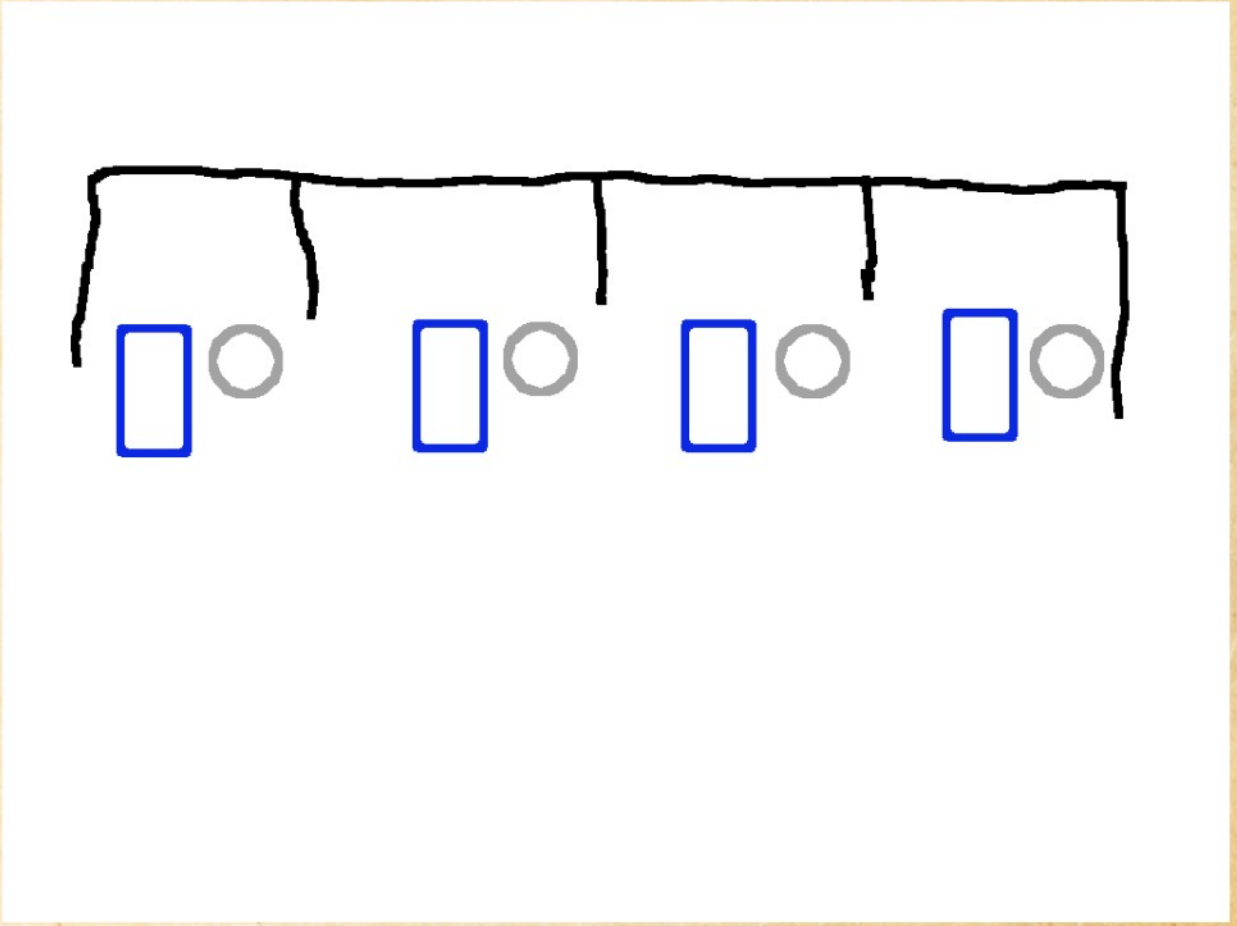
- Psychology
- UX design
- Automation

Scenario 1
Trash vs. Shred

1 – Description



1 – Description

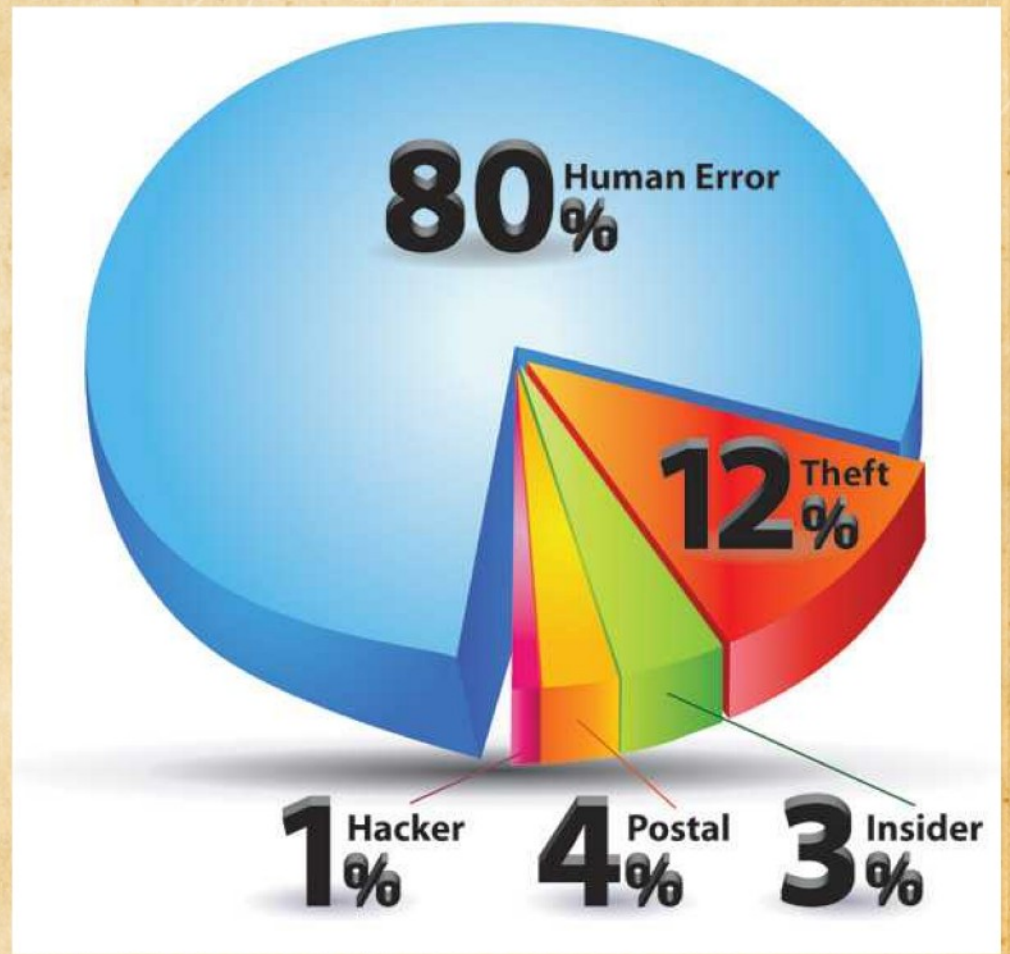


1 – Ideal World

- Teller leaves station to place PII in central shred bin
- Teller PII identification rate 100%

1 – Reality

- Stacking until worth the trip
- Wrong bin!
- Busy



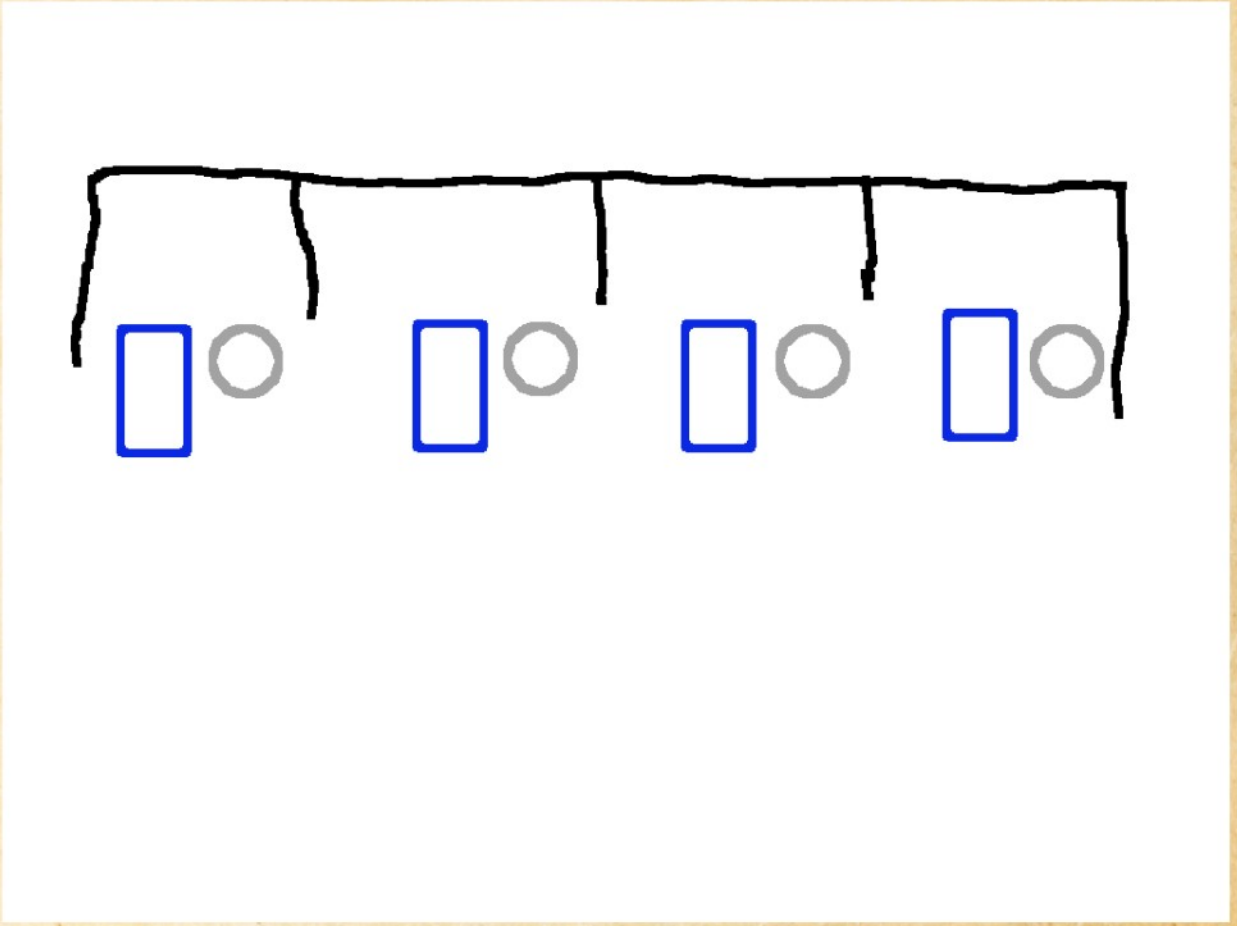
1 – Problem Areas

- What to shred?
- Stacks fall
- Too busy to notice (or care)

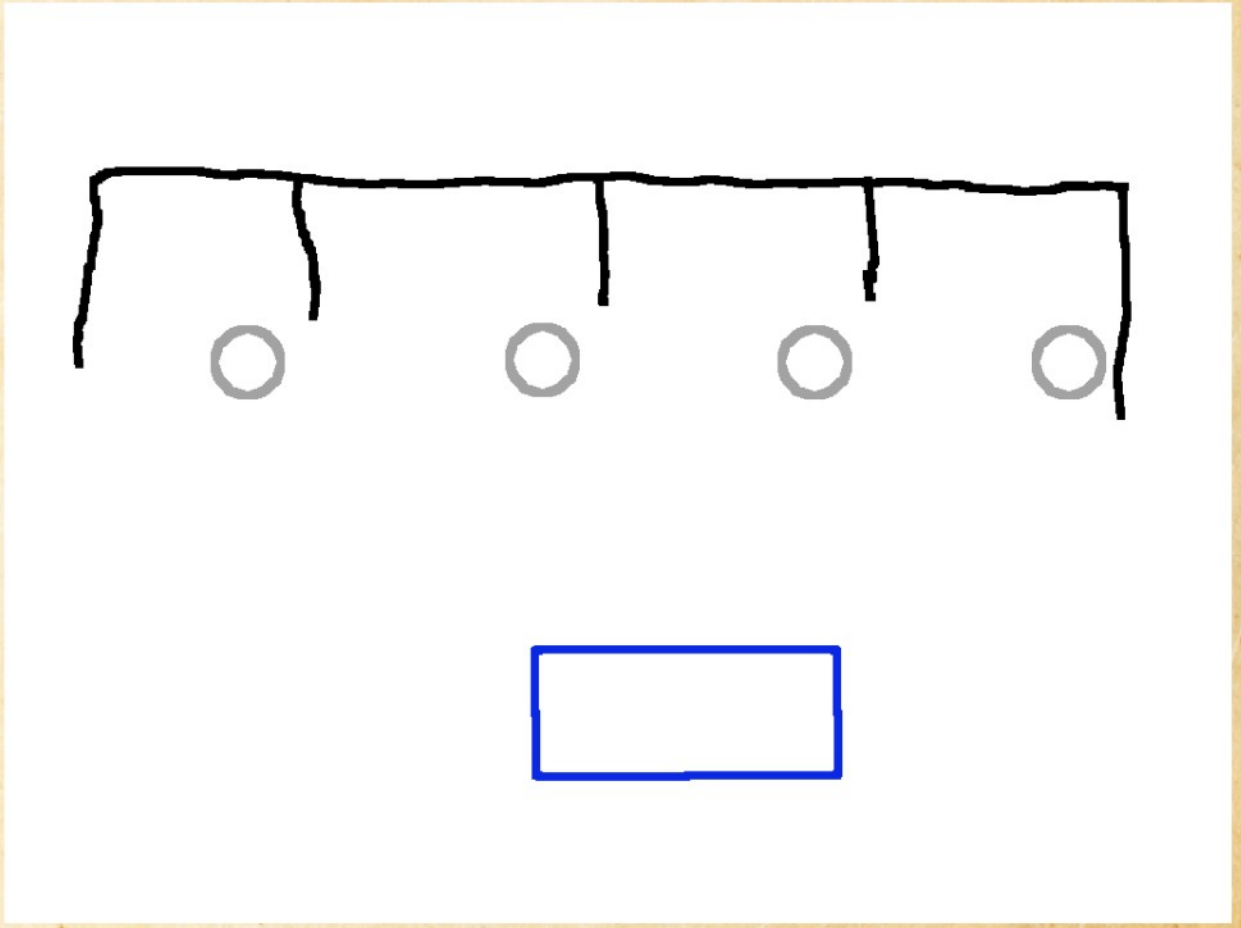
1 – Solution

- Flip the script

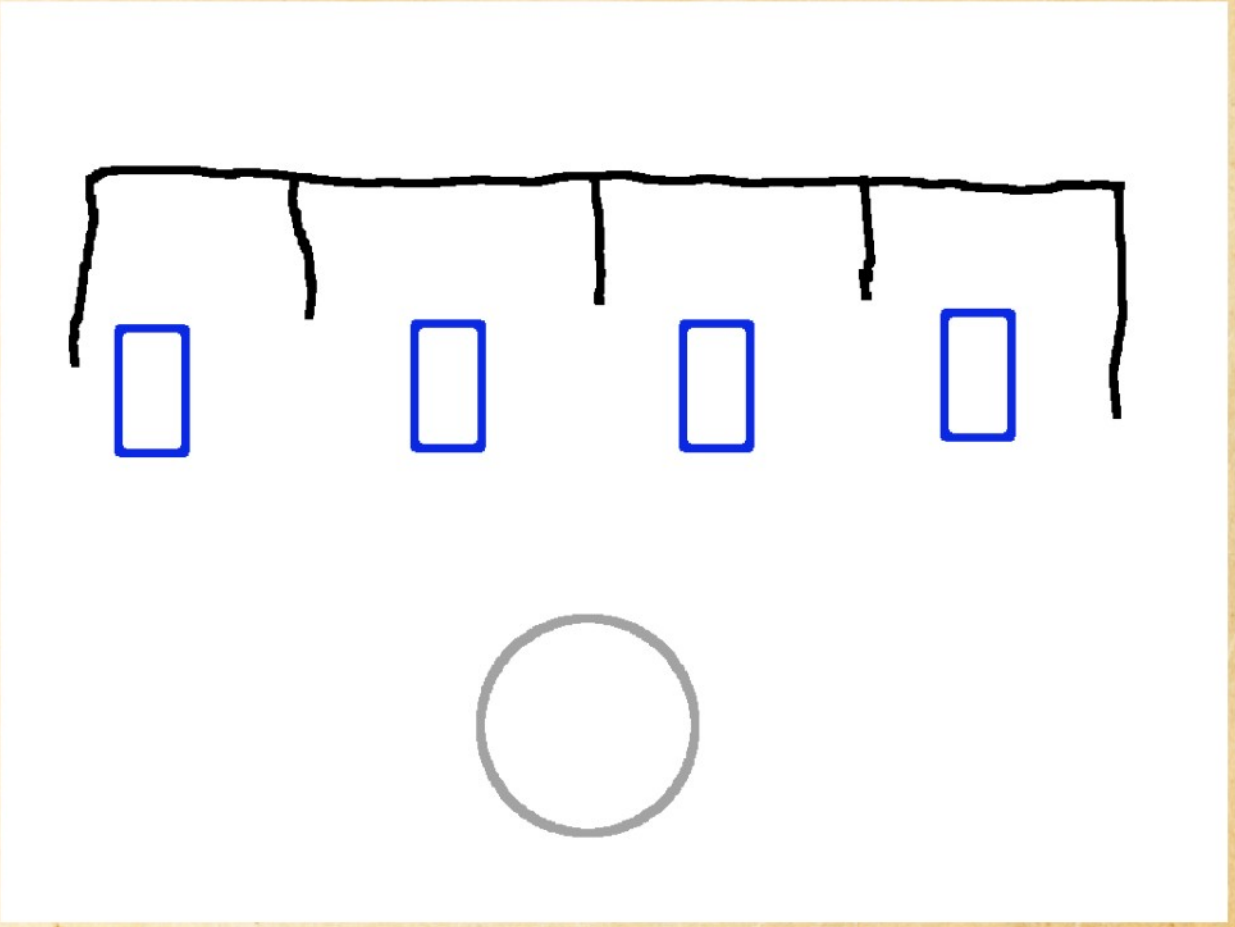
1 – Bad :-(



1 – Bad :-(



1 – Good! :-)



1 – Solution

- Flip the script
- Shredders

Scenario 2
Call Center

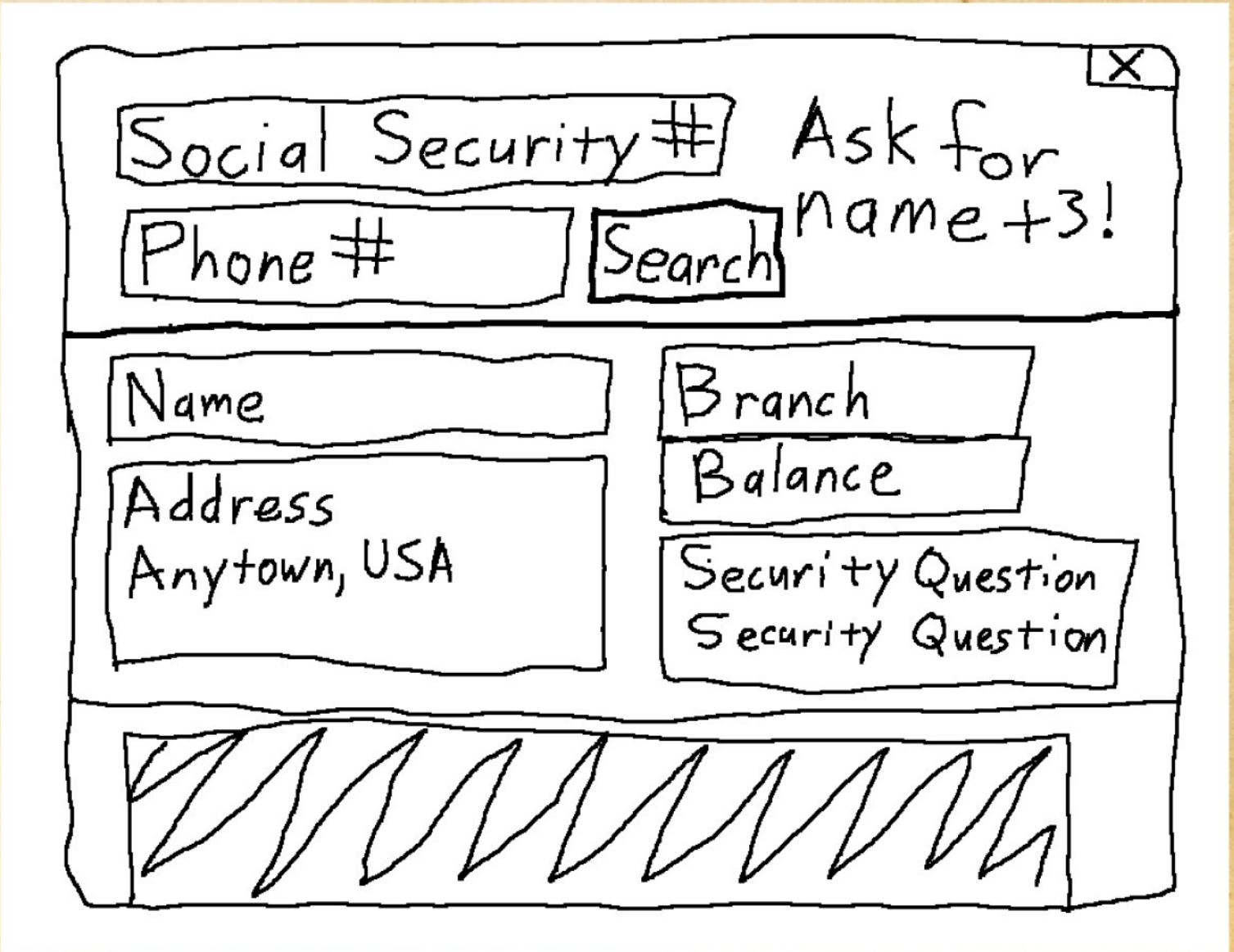
2 – Description

- Verify customers
  - Address *
  - Phone number *
  - Social security number *
  - Branch
  - Balance
  - Security questions (2)

2 – Description

- Verify customers
- 3 correct (+ name)

2 – Description



2 – Ideal World

- Robo-CSR!
- Full and correct answers required

2 – Reality

- Keep asking questions until 3 right
- Give hints!
- L2 CSR can override with < 3

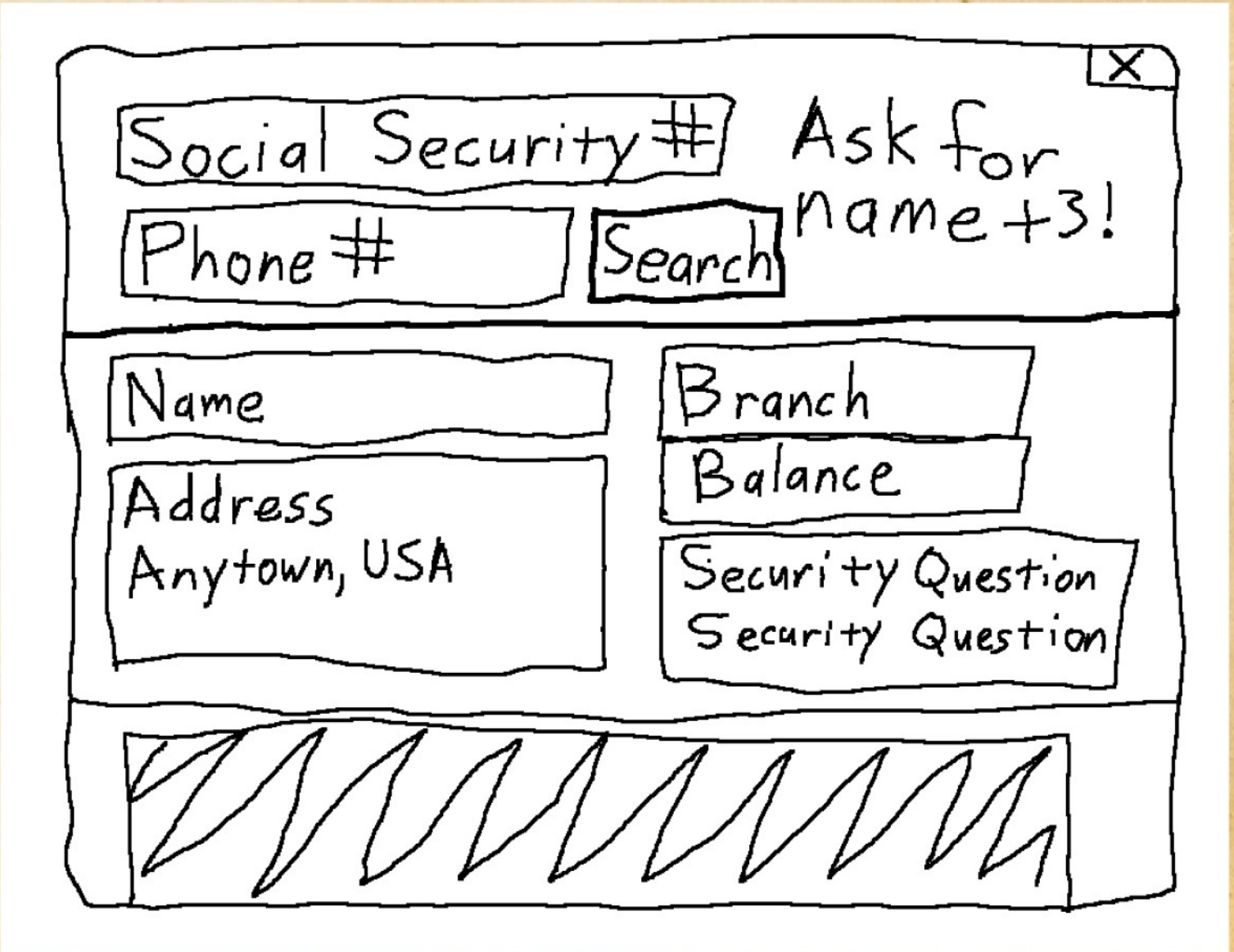
2 – Problem Areas

- L1 CSR vulnerabilities
  - Slow social engineering
  - Hints
  - Training doesn't stick
- Policy hole
- L2 override!

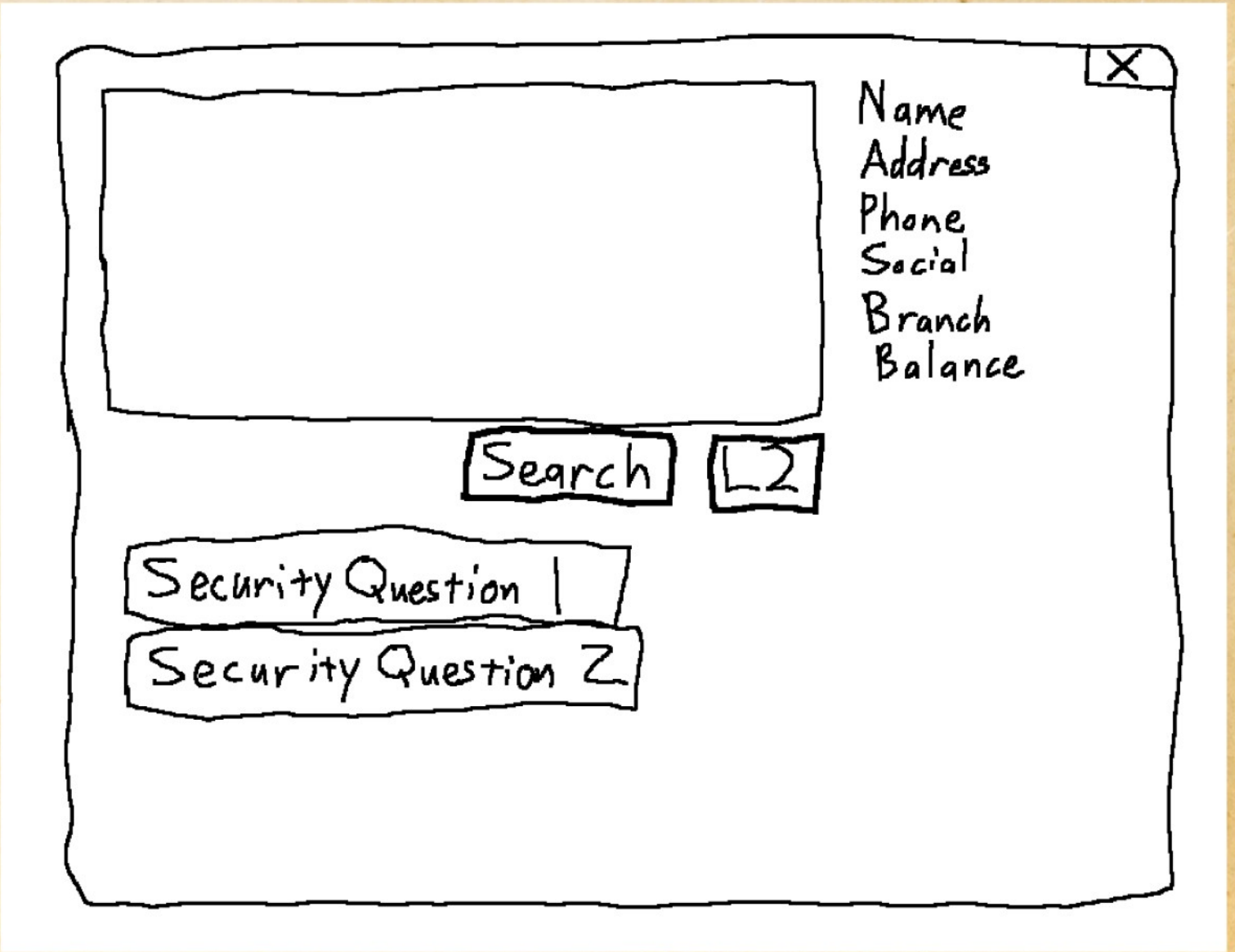
2 – Solutions

- Change the L1 CSR's UX entirely!

2 – Bad :-(


Social Security #
Ask for name+3!
Phone #
Search
Name
Branch
Balance
Address
Anytown, USA
Security Question
Security Question

2 – Good! :-)


X
Name
Address
Phone
Social
Branch
Balance
Search
L2
Security Question 1
Security Question 2

2 – Solutions

- Change the L1 CSR's UX entirely!
  - White box
  - No info until validation
  - No more hints!

2 – Solutions

- Change the L1 CSR's UX entirely!
- Behind the scenes
  - Look up hard numbers (phone, social)
  - Fuzzy logic on names and words
  - Log unsuccessful attempts (catch social engineering)
  - Guaranteed failure

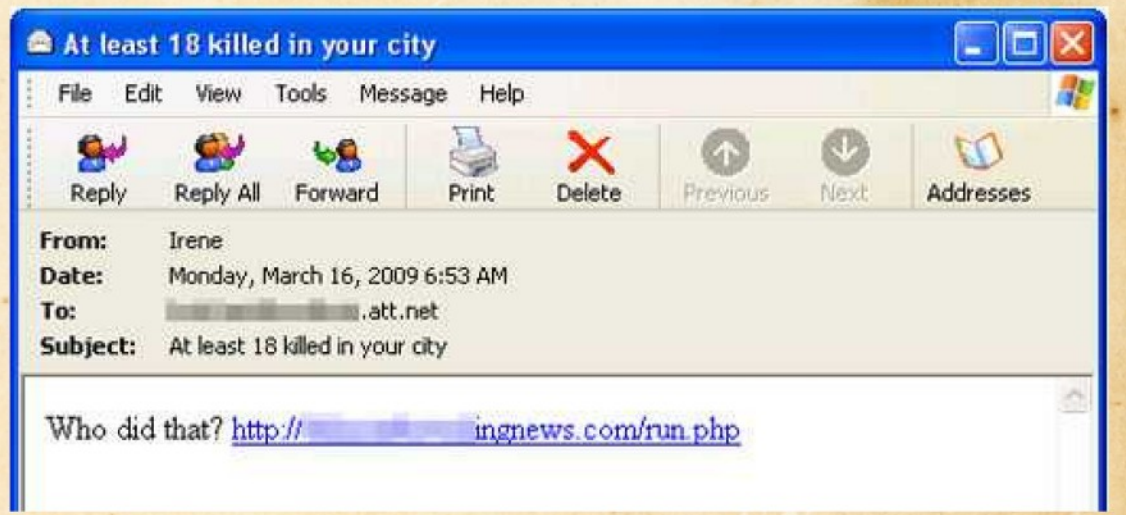
2 – Solutions

- Change the L1 CSR's UX entirely!
- Behind the scenes
- L2 CSR
  - Normal search screen
  - Can see why validation failed at L1
  - Trained more intensively

Scenario 3
Social Engineering

3 – Description

- Outside company
- Bogus link or file



- Aggregate report

3 – Ideal World

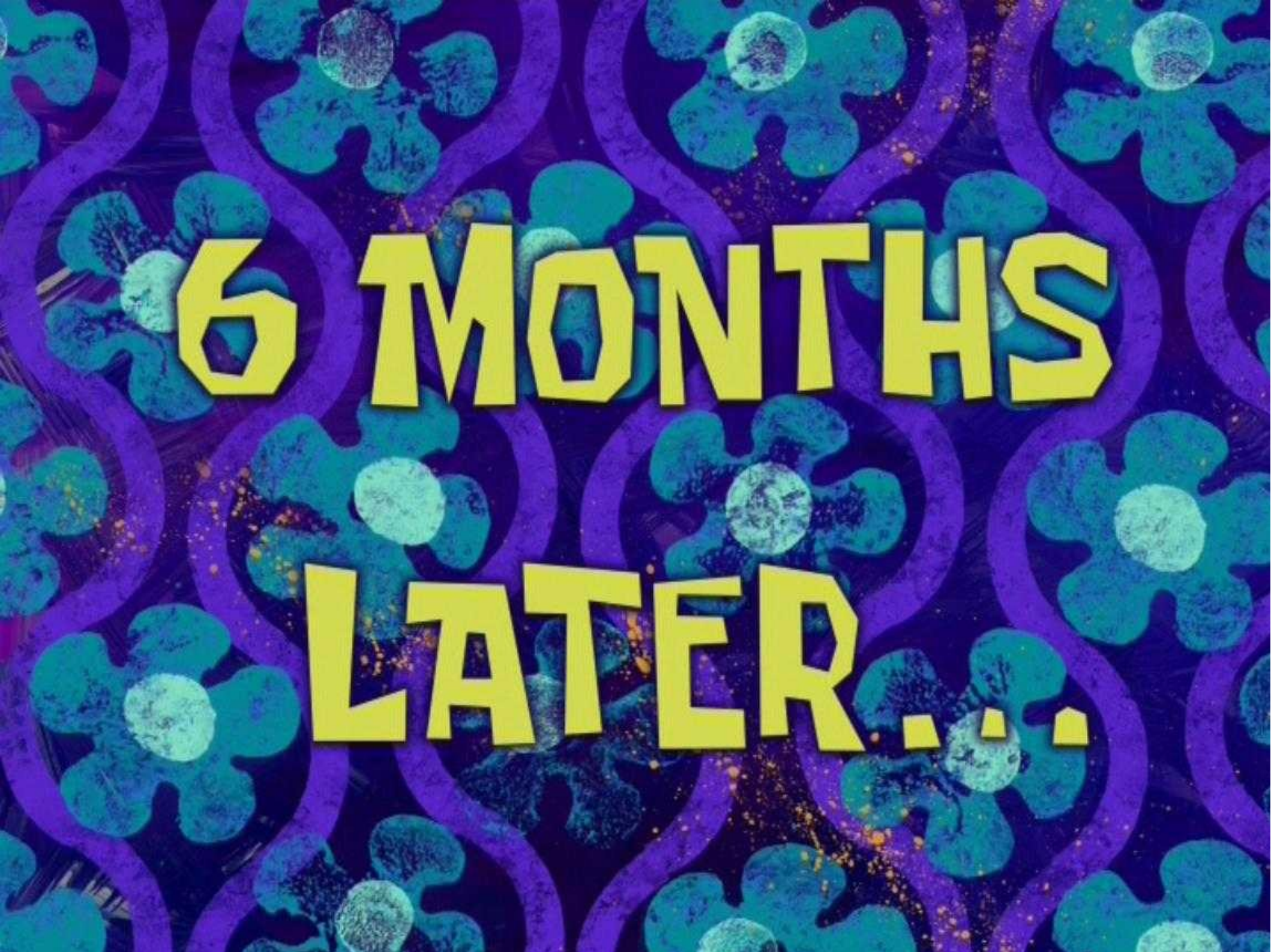
- Report delivery swift!
- Management action!
- Training!
- Learning!
- No more bad clicky!

3 – Reality


SEVERAL
MONTHS
LATER...

3 – Reality

- Report in 1-3 months


6 MONTHS
LATER...

3 – Reality

- Report in 1-3 months
- Meeting in 1-3 months


MANY
MONTHS LATER

3 – Reality

- Report in 1-3 months
- Meeting in 1-3 months
- Management acts!

3 – Reality

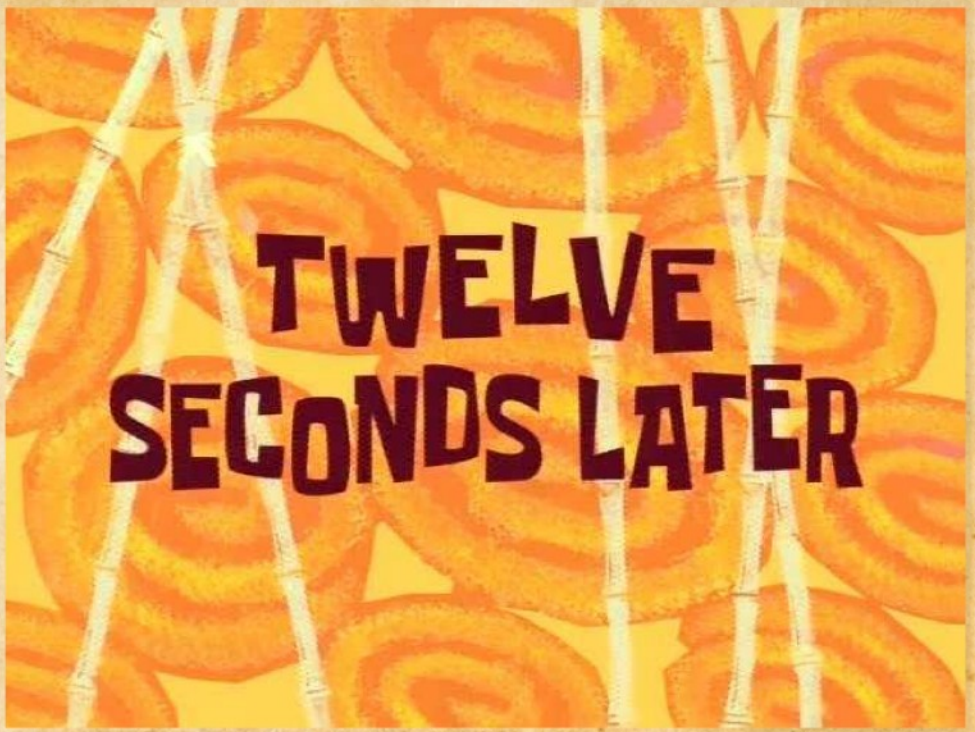
- Training
  - Déja vu
  - Generic
  - Test it, maybe?
- Incapable of getting it

3 – Problem Areas

- Multi-modal training will fail
- Time lag
- Inhuman training quality expectations

3 – Solution

- Internal social engineering emails
  - Link to corporate IAMS
  - Notify & lock account
- Psych 101



3 – Solution

- Inherent shame
- Trackable = accountable
- HR involvement
- Backed by policy and tech ability

Wrap-Up

Wrap

- Humans mess up perfectly designed information security
- Work with human psychology


All those times I said 'Kill all humans,' I'd always whisper, 'Except one.'
Fry was that 'one,' and I never told him so...