# The Intention-behaviour gap in cybersecurity

What we say we'll do is not what we do

July 14th, 2022

apalala

# Attitude - Intention - Behaviour

- Survey focusing on attitudes and intentions are often use to "measure" the human aspects of cybersecurity

- Attitudes and intentions are poor predictors of behaviours (it's called the intention-behaviour gap), hence, they shouldn't be used as a key performance indicator

- Even self-reported behaviours and actual behaviours are often poorly correlated (Dang, 2021)

apalala

## ATTITUDE

- What we think about something

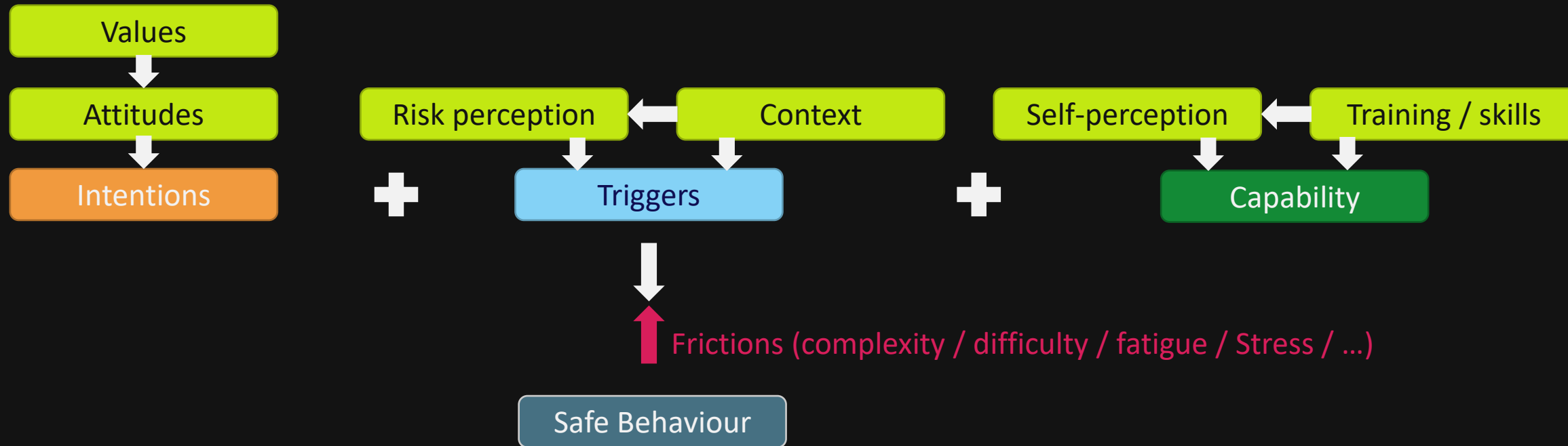- Ex.: *"I think it is important to use complex password"*

## INTENTION

- What we plan to do or how we plan to behave

- Ex.: *"I will use a 14 characters password"*
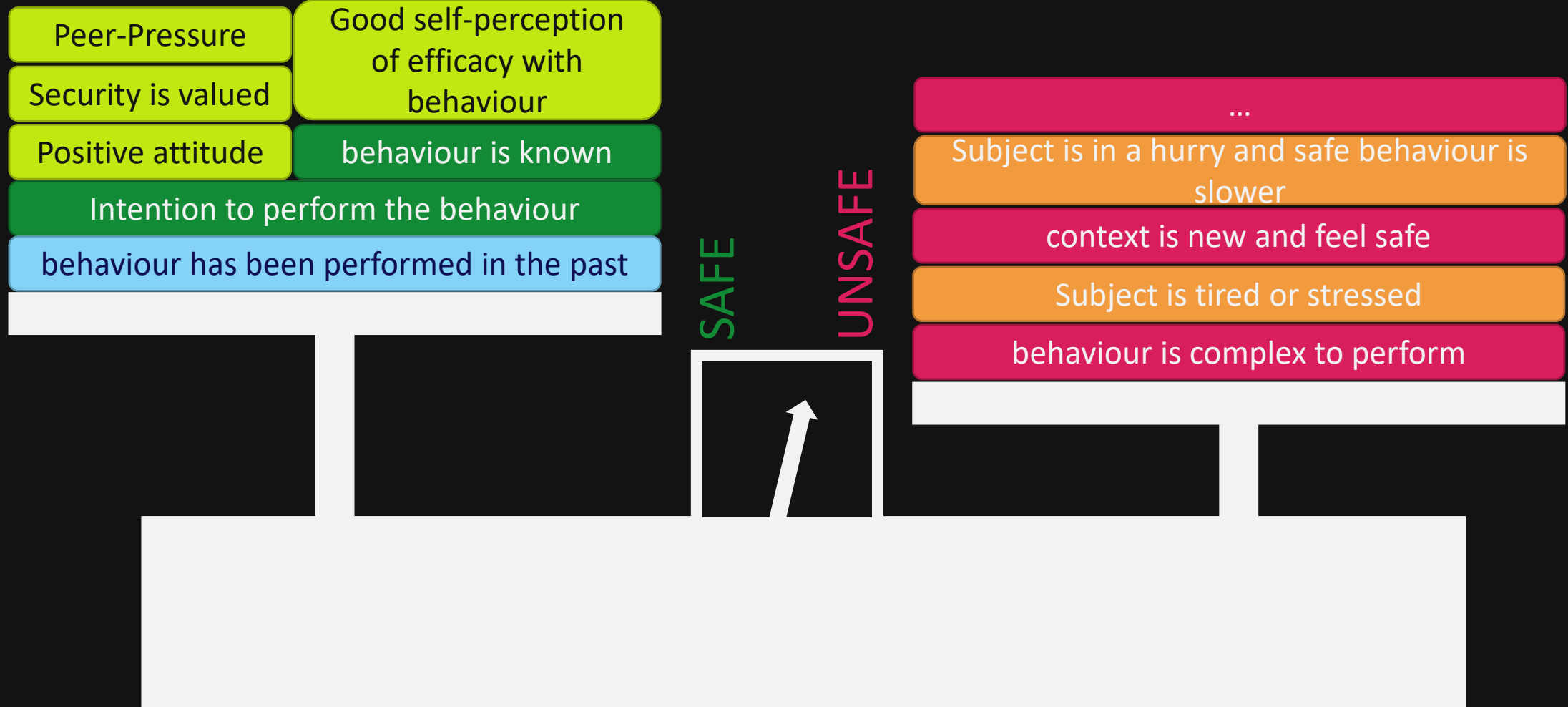
## BEHAVIOUR

- What we actually do

- Ex.: Passwords used are complex

- Ex. of self-reported behaviour: *"I always use complex passwords"*

# Factors influencing safe behaviours

apalala

Values
↓
Attitudes
↓
Intentions

➕

Risk perception ← Context
↓ ↓
Triggers

↓

↑ Frictions (complexity / difficulty / fatigue / Stress / …)

Safe Behaviour

➕

Self-perception ← Training / skills
↓ ↓
Capability

For a safe behaviour to happen, factors like positive attitudes and an intent to perform the behaviour, a perception of the risk, a perception of the cues to trigger the behaviour, a practical knowledge of the behaviour (practical skill more than theoretical) as well a positive self-perception of our capability to perform the behaviour are necessary. Frictions like task complexity, fatigue or time pressure will reduce the likelihood of the safe behaviour occurrence.

# Factors influencing safe behaviours

Peer-Pressure

Good self-perception of efficacy with behaviour

Security is valued

Positive attitude

behaviour is known

Intention to perform the behaviour

behaviour has been performed in the past

**SAFE**

**UNSAFE**

...

Subject is in a hurry and safe behaviour is slower

context is new and feel safe

Subject is tired or stressed

behaviour is complex to perform

# Reduce frictions, reduce the gap

- Values, Attitudes and Intentions can be used to assess the culture, not risks

- If safe behaviour doesn't occurs, look for frictions or mixed / opposite messages

- Ensure people know when to perform the behaviour, keep it simple, fast, easy to remember, effortless. Reduce the burden on humans as much as possible.

# Measure & report Safe Behaviours

- Values, Attitudes, Intentions and Self-Reported behaviours are "technical" indicators for Security Awareness Specialists, not for CxOs

- Actual safe Behaviours should be reported to senior management

- Following a training is NOT a safe behaviour, it's just a step towards it.

# Questions?

? [info@apalala.be](mailto:info@apalala.be)

Emmanuel Nicaise