



Human Factors in Security

Research vs. Current Practices

Cornelia Puhze

GÉANT Security Days, 10 April 2024

Switch

NREN

-

National Research
and Education
Network

Registry

-

for .ch/.li ccTLDs

Switch

**Education,
Research &
Innovation
Community**

**Swiss universities on tertiary
level and their research
institutions**

**Internet
Community**

**Internet Service Providers,
Hosters, Domain Registrars**

Commercial

**Banking, Industry & Logistics,
Energy, Healthcare, Government**

Security Awareness

74%

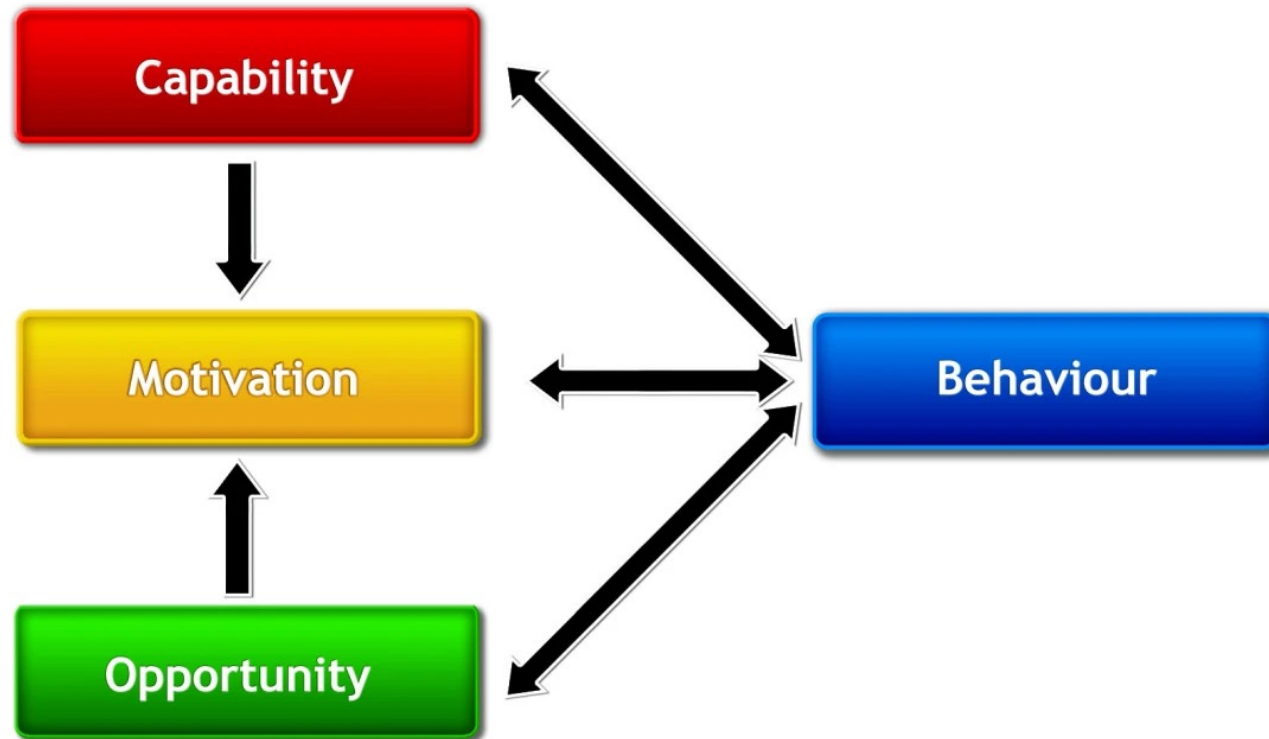
The path to behaviour change



Security managers typically only consider lack of knowledge ... Thus, their current efforts in „security education“ consist of repeating all policies and rules to everyone. This is the equivalent of shouting louder at someone who does not understand your language; we need a smarter, targeted approach if we want to meaningfully change behavior...

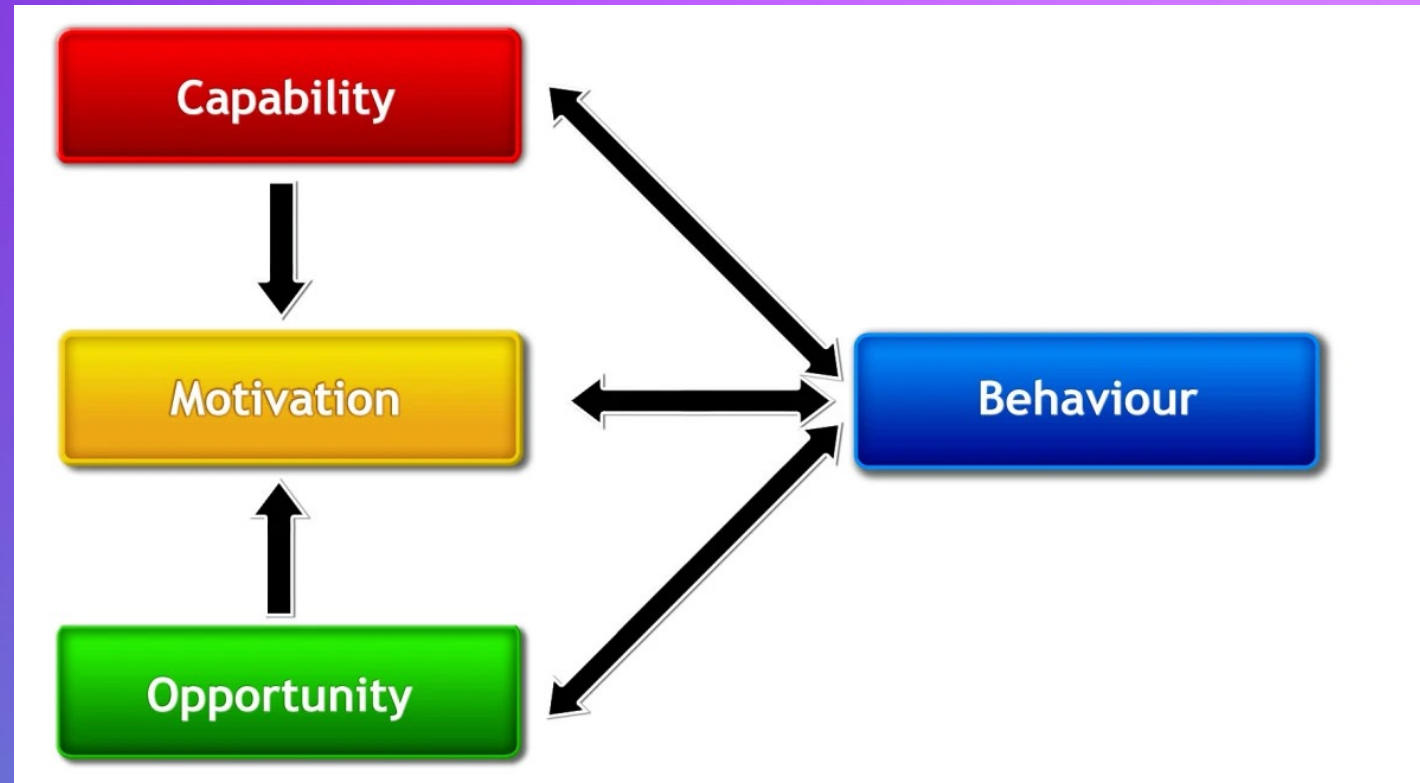
(Beris et al., 2015)

The behaviour change wheel: COM-B



Michie, S., van Stralen, M.M. & West, R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Sci* 6, 42 (2011). <https://doi.org/10.1186/1748-5908-6-42>

Communications



Hi all

Passwords are important. They protect your data.

Our policy says, your passwords

- must be 12 characters long.
- must contain numbers, special characters as well as lower and upper case letters.
- should be unique.

You must follow these rules!

Use a passwordmanager.

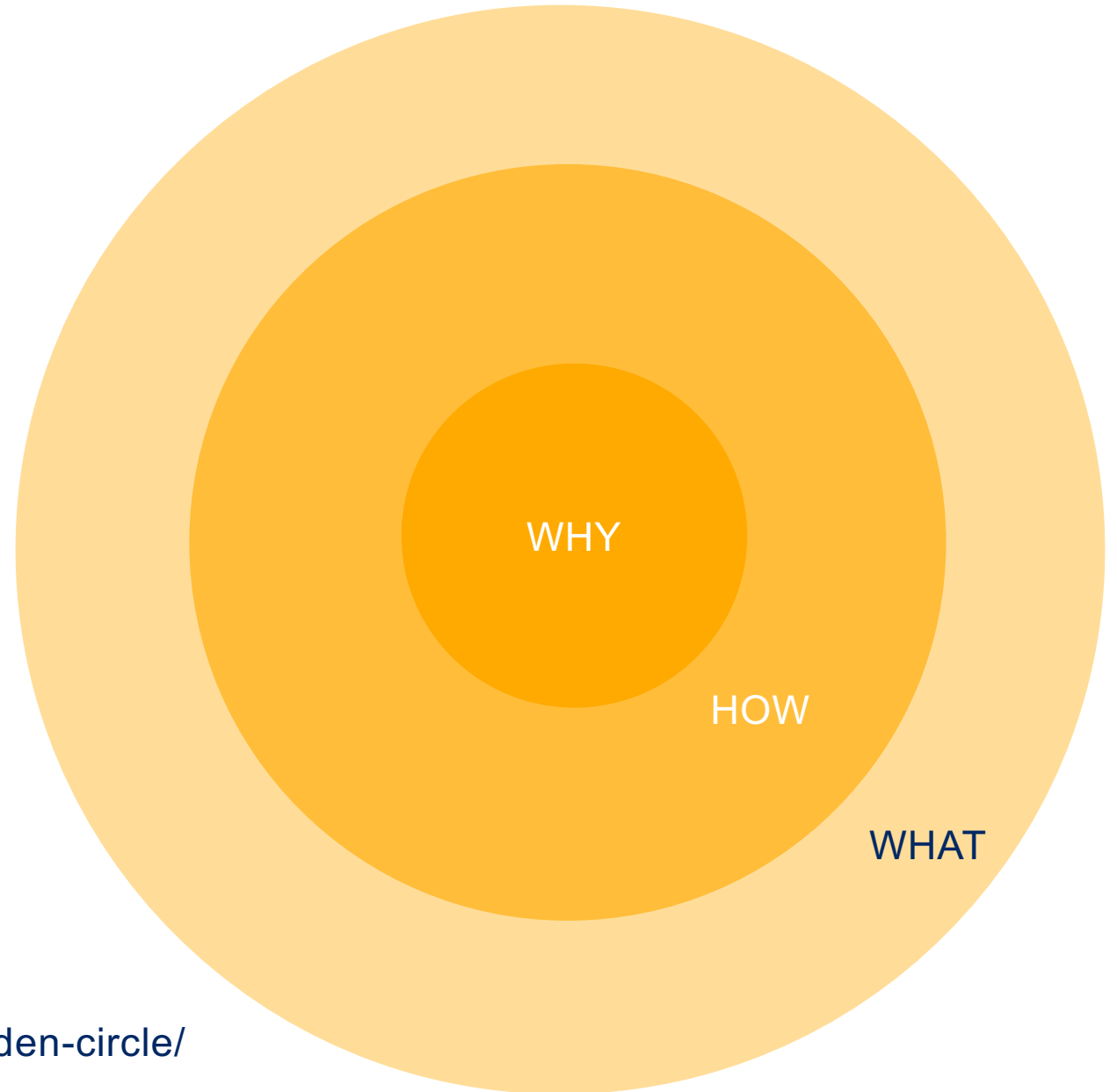
Cheers

Your security team

The Golden Circle

Always start with the WHY

Your WHY is your purpose, cause,
or belief



<https://simonsinek.com/golden-circle/>

The bait has to taste the fish,
not the fisher.



Messaging for change

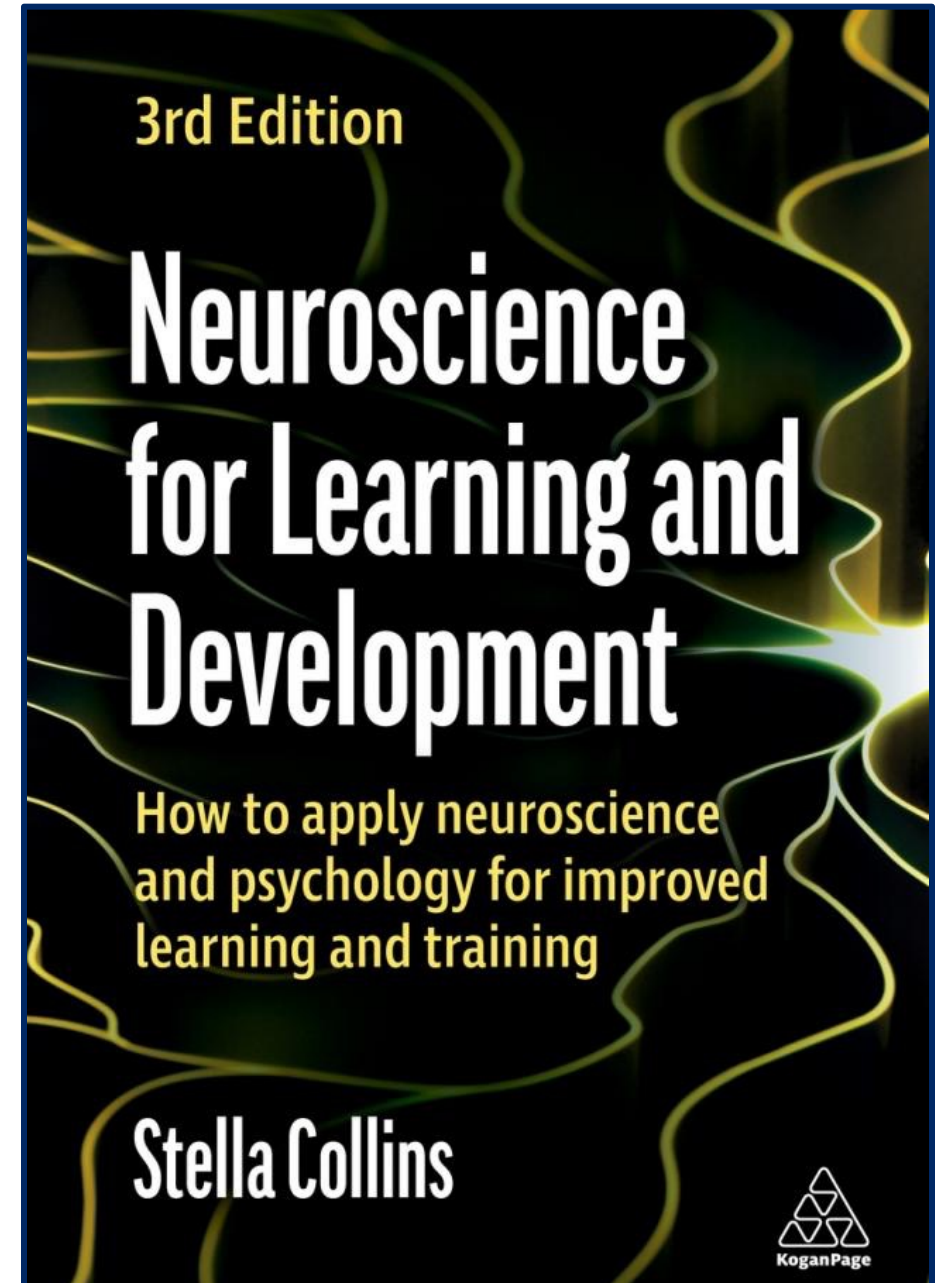
- Positive messages**
- Simple language**
- Clear instructions**

Adult Learning & Training

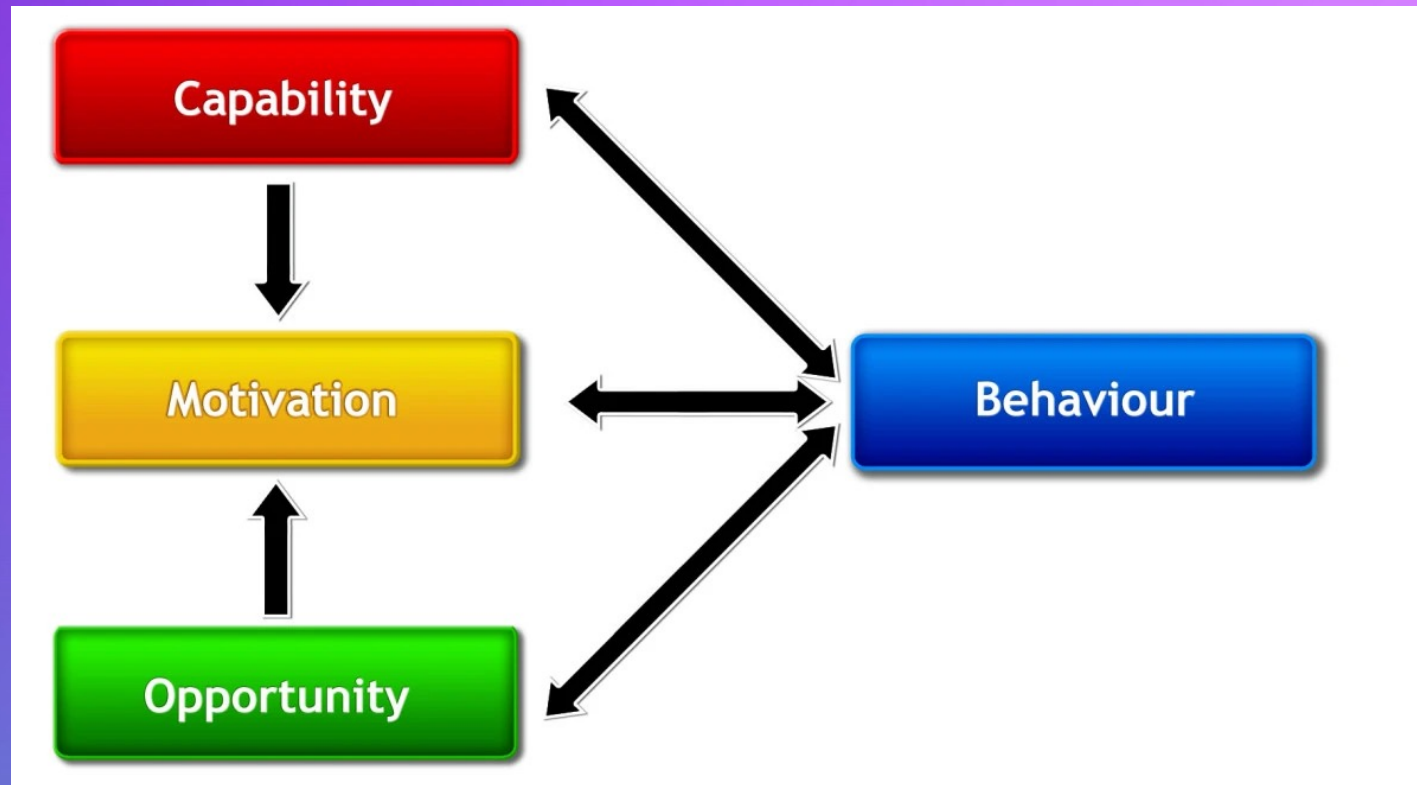
Chapter 5 – Motivation

How to motivate people to get their brains to learn:

- Curiosity
- Relaxation
- Persistence
- Goal orientation
- Creativity/playfulness



Learning




Google Security Awareness

All Images Videos Shopping News More Tools

About 1'230'000'000 results (0.36 seconds)


Sponsored

 KnowBe4 Germany
<https://www.knowbe4.de>

Security Awareness Training

KnowBe4® - Offizielle Seite — Wir zeigen Ihnen, wie Sie Ihr Training Programm in wenigen Minuten aufsetzen können.


Sponsored

 Proofpoint
<https://www.proofpoint.com>

Cybersecurity Awareness | Learn About Emerging Threats

Download the State of the Phish Report to Learn About Trends to Better Protect Yourself. IT Teams Continue to Face Cybersecurity Challenges. Learn More About Phishing Threats.


Sponsored

 SoSafe
<https://www.sosafe-awareness.com>

Security Awareness

SoSafe **Security Awareness** — Simuliertes Phishing-Training, das wirkt. Einprägsamer Content mit messbarem Lernerfolg.


Sponsored

 Hoxhunt
<https://www.hoxhunt.com>

Security Awareness - See How It Works

Turn real threats into instant learning. Drive engagement with positive strategies. Weave...

Sponsored

 Proofpoint
<https://www.proofpoint.com> secur... · [Translate this page](#)

Was ist Security Awareness Training? Definition

Was ist **Security Awareness** Training? **Security Awareness** Training ist eine

Training to Mitigate Phishing Attacks Using Mindfulness Techniques

Matthew L. Jensen, Michael Dinger, Ryan T. Wright & Jason Bennett Thatcher

To cite this article: Matthew L. Jensen, Michael Dinger, Ryan T. Wright & Jason Bennett Thatcher (2017) Training to Mitigate Phishing Attacks Using Mindfulness Techniques, Journal of Management Information Systems, 34:2, 597-626, DOI: [10.1080/07421222.2017.1334499](https://doi.org/10.1080/07421222.2017.1334499)

To link to this article: <https://doi.org/10.1080/07421222.2017.1334499>



Phishing-Kampagnen zur Mitarbeiter-Awareness

Analyse aus verschiedenen Blickwinkeln: Security, Recht
und Faktor Mensch

12.05.2020



An investigation of phishing awareness and education over time: When and how to best remind users

Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, and Reyhan Duezguen, *SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology*; Bettina Lofthouse, *Landesamt für Geoinformation und Landesvermessung Niedersachsen*; Tatiana von Landesberger, *Interactive Graphics Systems Group, Technische Universität Darmstadt*; Melanie Volkamer, *SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology*

<https://www.usenix.org/conference/soups2020/presentation/reinheimer>

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiainen, and Srdjan Čapkun
*Department of Computer Science
ETH Zurich, Switzerland*
{daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiainen, and Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland
{daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch

2021

15 months

14,000 study participants

- good effectiveness of warnings on emails
- Surprisingly, we find that **embedded training** during **simulated phishing exercises**, does make employees **NOT more resilient to phishing**, but instead it can have **unexpected side effects** that can make employees even **more susceptible to phishing**.
- using the employees as a collective phishing detection mechanism is practical in large organizations:
 - fast detection of new phishing campaigns
 - operational load for the organization is acceptable
 - employees remain active over long periods of time.

Mixing things up



- Passwords
- Clean Desk
- Wearing a Badge
- ...



- Phishing
- Social Engineering
- Tailgating
- ...

Security **measures** protect against **phenomena**.
Phenomena must be explained, security **measures** trained.



Teaching the adversarial mindset

Cybercrime for
Newbies with
#grannysmith85

Mini video series on
social engineering
attack cycle

Switch_



https://www.youtube.com/watch?v=riwPE_qU7f0

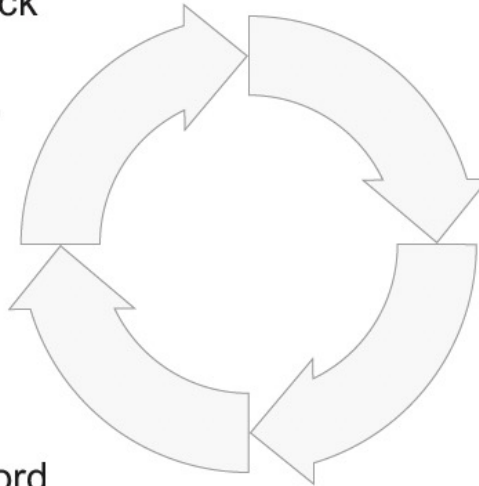
Social Engineering Attack Cycle

4. Execution

Accomplish ultimate goal of the attack (or end the attack without raising suspicion); address any loose ends, e.g., erase digital footprints

3. Exploitation

Using both information and relationships to actively infiltrate the target without raising suspicion, e.g., disclose username and password over the phone, hold the door open



1. Information Gathering

Systematically collecting information about the target; to become familiar with the target and/or to formulate strong pretext(s)

2. Establish Relationships and Rapport

Establishing a working relationship with the target, e.g., by smiling, sharing personal stories, using a fake profile on a dating site

Bild 3.1 Die vier Phasen des Social Engineering Attack Cycle (in Anlehnung an Nyriak, o. D.)

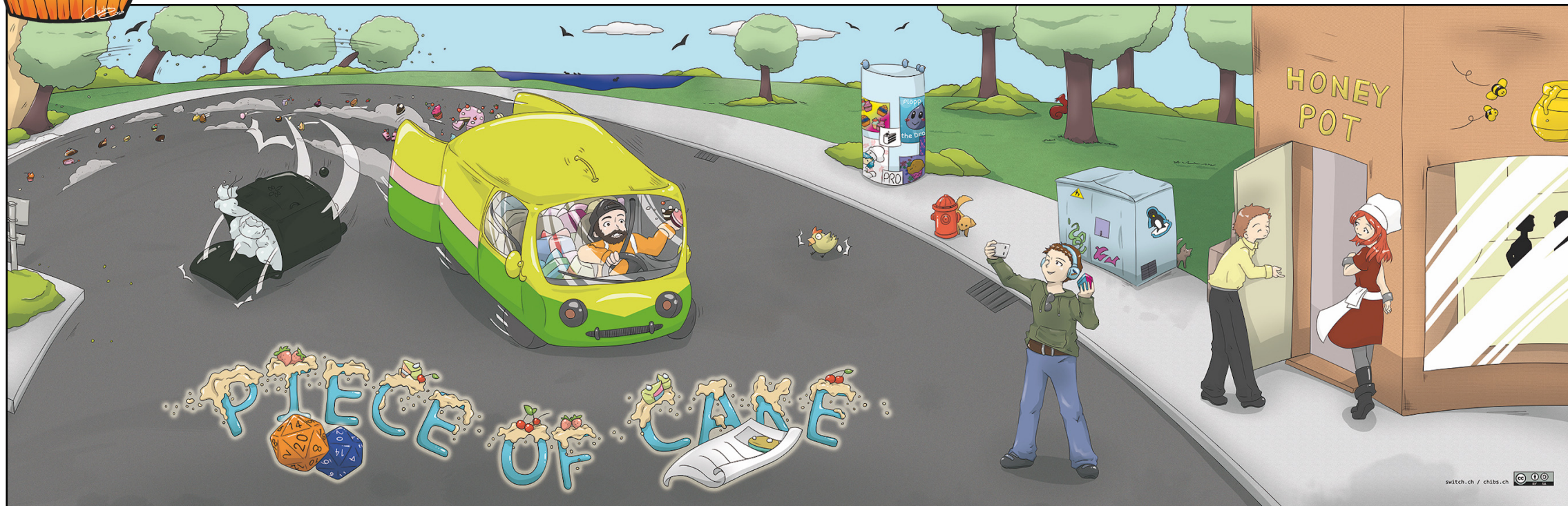
Weber, Kristin. (2024). Mensch und Informationssicherheit: Verhalten verstehen, Awareness fördern, Human Hacking erkennen. 10.3139/9783446480407.

Nyriak, A. (o. D.). The Attack Cycle. Social Engineer.
<https://www.social-engineer.org/framework/attack-vectors/attack-cycle/>

Training the adversarial mindset



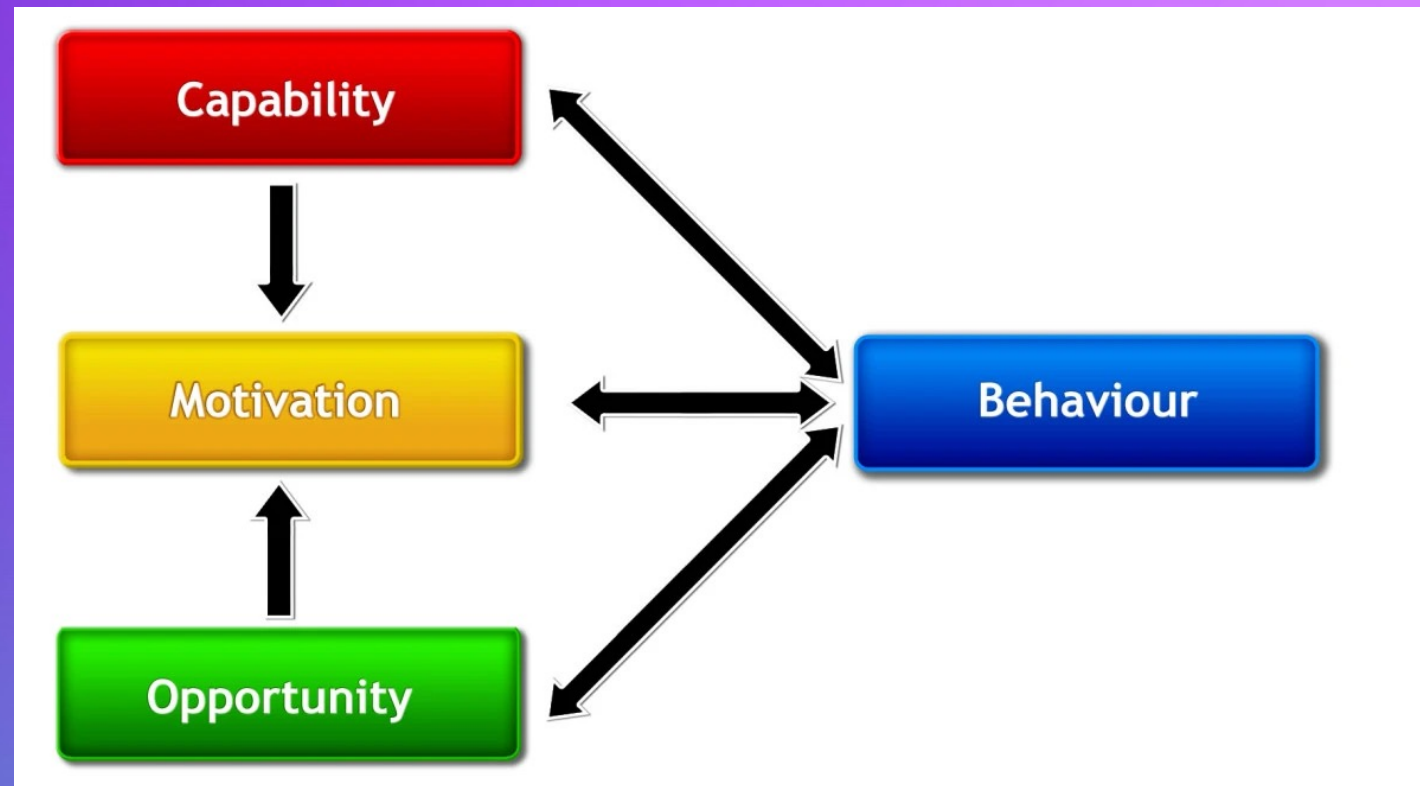
Piece of Cake – the role playing game



Psychology at use (Compliance Principles)

- Authority
- Social Proof
- Liking, Similarity & Deception
- Commitment, Reciprocation & Consistency
- Distraction

Usability



Security as an obstacle



Weber, Kristin. (2024). Mensch und Informationssicherheit: Verhalten verstehen, Awareness fördern, Human Hacking erkennen. 10.3139/9783446480407.

Adapting processes

Password change



Password-Change-Notification <service@[REDACTED]>

Dear employee

Your password expires in two days!

Last password change: 6th January 2019

Please click [here](#) to change your password. You could lose access to important systems if you do not change your password.

This is an automated email.

Best regards
User Help Desk
[REDACTED]

(a) Email prompting to change the organization's password.

Creating threats due to poor usability

TRAINED TO BE “YES-CLICKERS”

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

SECURITY WARNING Macros have been disabled.

- Warning messages appear directly after each other
- **A lot of false-positive warning messages**
- Similar appearance

→ **“Yes-Clicking Habit”**

12

Marco Gutfleisch: (Usable) Security Awareness in Software Development
SWITCH Security Awareness Day 2021

<https://tube.switch.ch/videos/UO15OG6CTz>

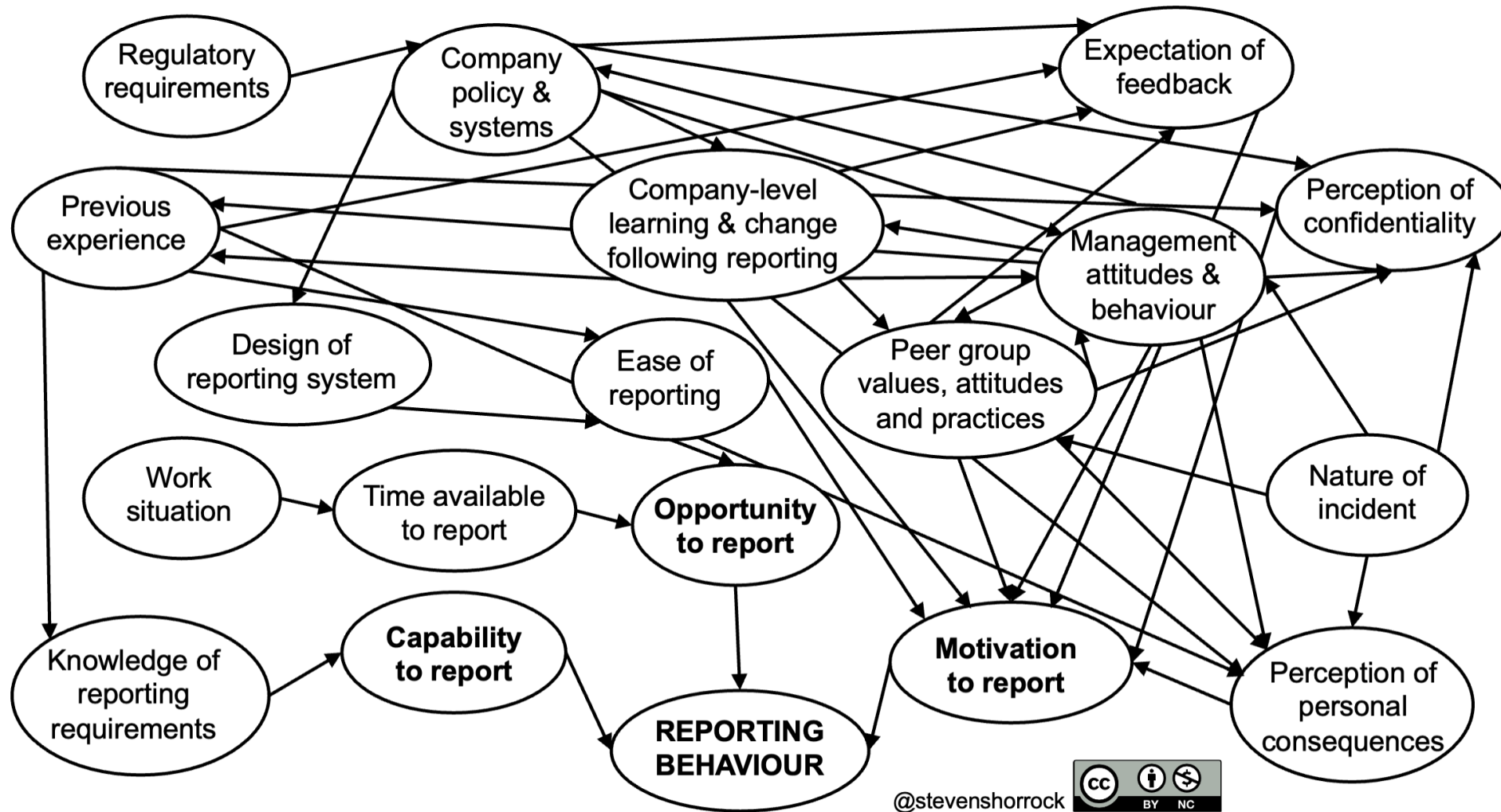
Some more research

Modeling influences on behaviour



Shorrock, S. (2023, November 17). "Why aren't they reporting incidents?" Influences on reporting behaviour. *Humanistic Systems*. humanisticsystems.com/2023/11/14/why-arent-they-reporting-incidents-influences-on-reporting-behaviour/

“Why aren’t they reporting incidents?”



@stevenshorrock

Learning from Safety Culture

Safety, leadership and learning is based on **Human Organisational Performance (HOP)** and is a further development of our existing approach to safety.



The HOP principles:

1. People make mistakes
2. Blame fixes nothing
3. Learning is the key to improvement
4. Context drives behaviour
5. How we respond matters



Learning from Safety Culture

Learning from safety science: A way forward for studying cybersecurity incidents in organizations

[Nico Ebert](#)^a  , [Thierry Schaltegger](#)^a, [Benjamin Ambuehl](#)^a, [Lorin Schöni](#)^b, [Verena Zimmermann](#)^b, [Melanie Knieps](#)^c

[Show more](#) 

 [Add to Mendeley](#)  [Share](#)  [Cite](#)

<https://doi.org/10.1016/j.cose.2023.103435> 

[Get rights and content](#) 

Under a Creative Commons [license](#) 

 [open access](#)

FIRST SIG Human Factors in Security

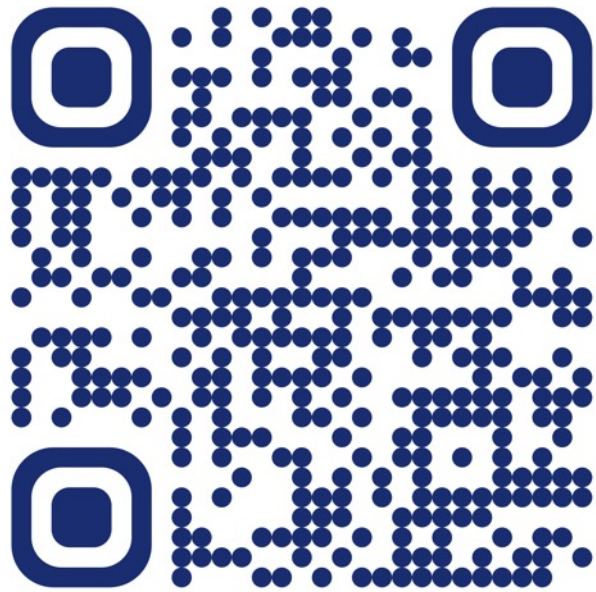
Topics Meetings 2024

- Learning from Safety Culture
- Social Engineering Framework
- Socio-technological Security
- Usable Security (HCI)
- Risk Communication
- Security Advocacy
- Games and TTXs



Security Awareness Adventures

In for some action?



Switch





Swiss Security Awareness Day

October 24th, 2024
Zentrum Paul Klee
Bern

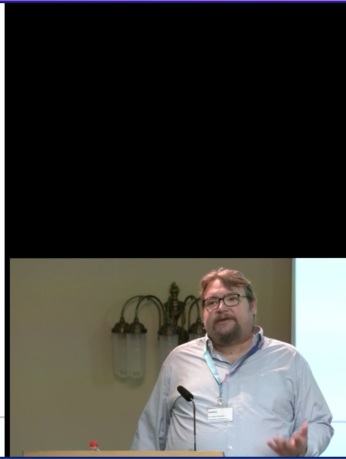
The social impact of IT security

Loss of trust, loss of employees

- Risk is not a viable foundation for any communication
 - Common risk perception cannot be assumed between individuals
 - Only interpersonal trust can provide a viable and sustainable foundation for communicating in IT security
- Frustrating employees through impediments will lead to ...
 - ...potential vulnerabilities in the best case
 - ...loss of employees in the worst case

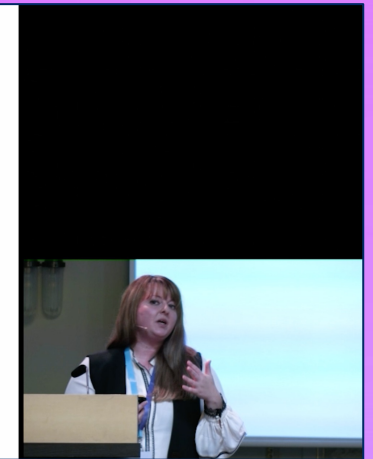
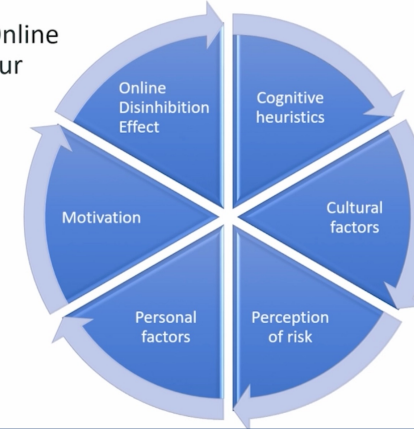


Fraunhofer IAO



The human factor in IT-security – How to improve acceptance of security measures
Dr. Heiko Roßnagel | Fraunhofer Institute for Industrial Engineering IAO

Changing Online Behaviour



Cybersecurity awareness: past practices and future needs
Maria Bada | Queen Mary University of London

Measure human risks

1. **Employees' knowledge** of essential cyber and security requirements.
2. **Employees' behaviour** in real-life situations.
3. **Root cause** of past incidents and breaches (or near-misses).
4. **Expert surveys with your SOC, IT security, risk management teams.**

Identify themes, patterns and near-misses



Understanding the human factor in cyber incidents
Leo Niedermann | Swiss Re

Knowing + ABC = Doing



Going beyond BS in CS: What is behavioural science and how we apply it to influence people's cyber security
Dr. Inka Kappinen | CybSafe

Improve your skills?

Security Awareness Training

21 - 22 November 2024 (d)

Switch, Werdstrasse 2, 8004 Zürich



Switch Security Awareness Competence Center

Fabio Greiner | Katja Dörlemann | Cornelia Puhze

awareness@switch.ch



„When it comes to security awareness, more is not better – less but relevant is.“

(Sasse et al., 2023)

Switch