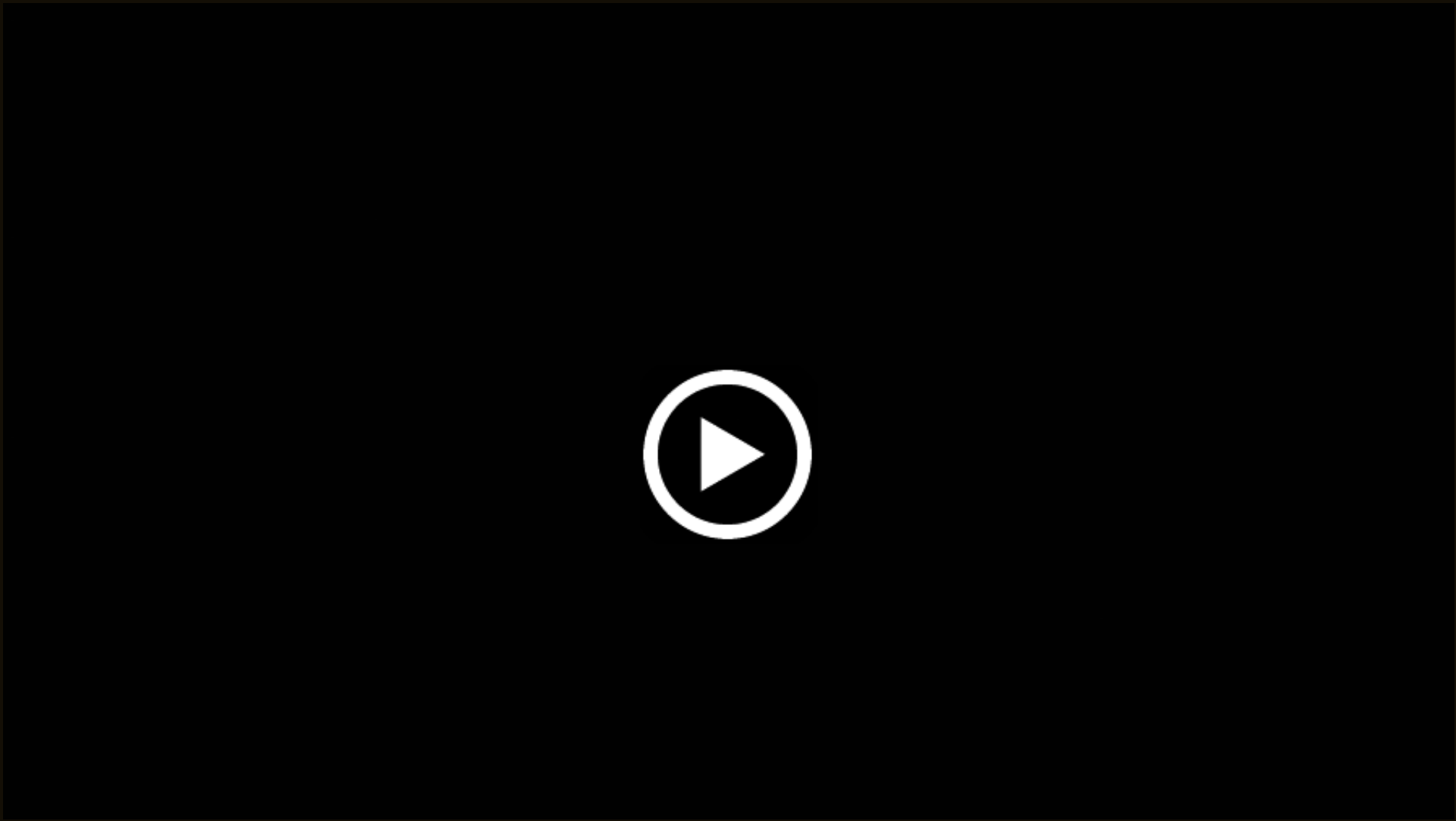
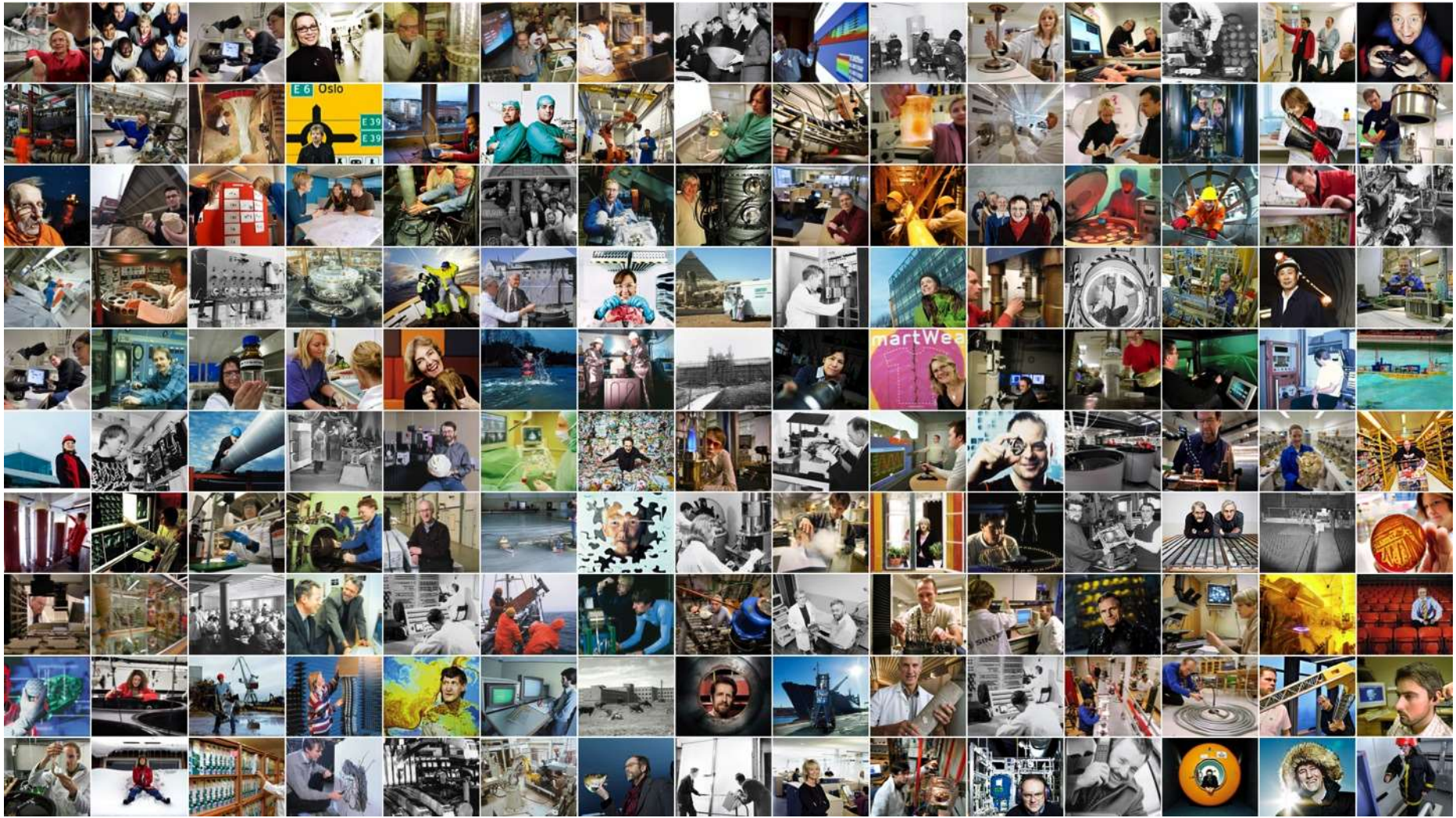
En smak av …

INFORMASJONSSIKKERHETSKULTUR

Erlend Andreas Gjære

@erlangsec




E 6 Oslo
E 39
E 39

Medarbeidere fra 73 nasjoner

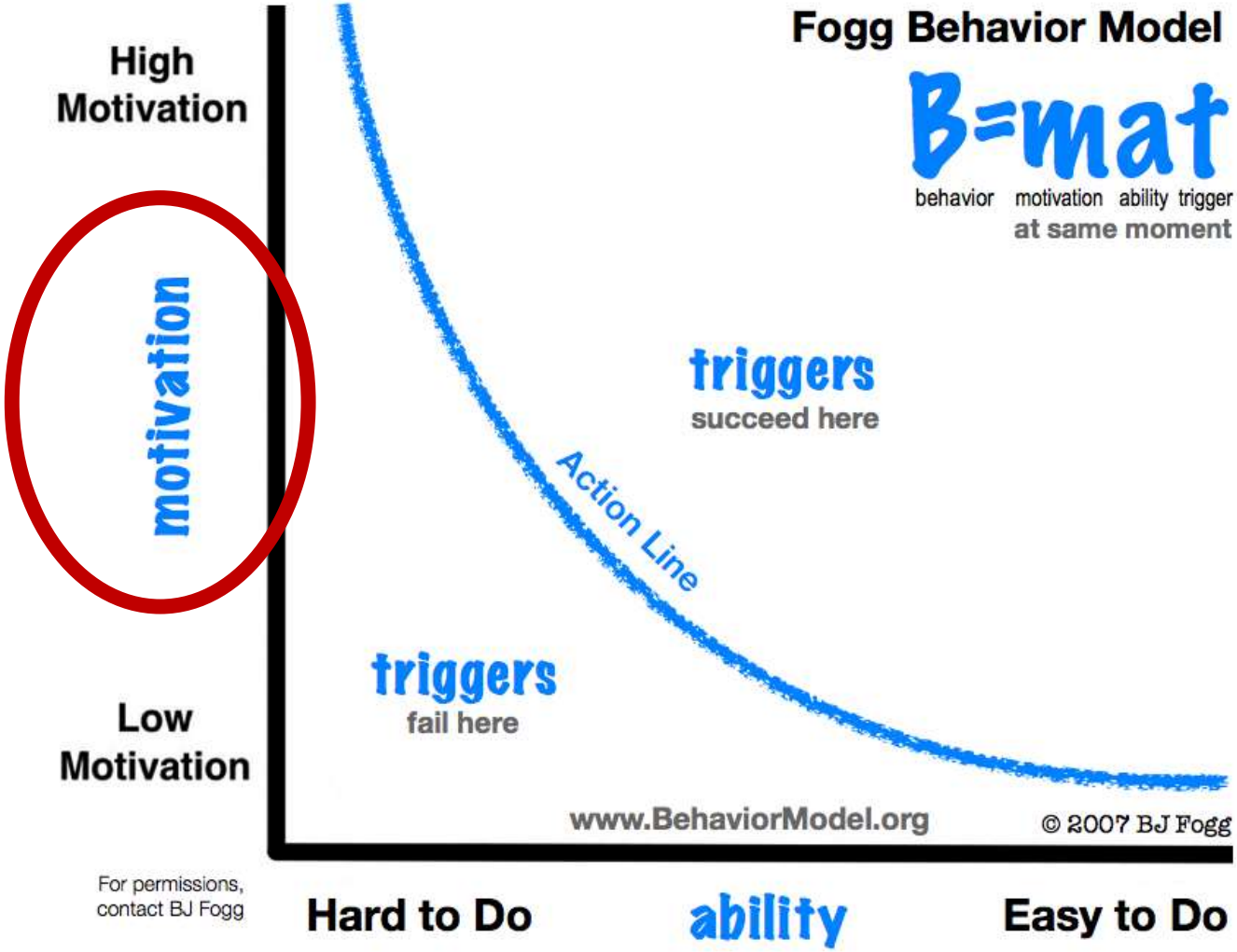

REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU?

En smak av sikkerhetskultur

- Organisasjonskultur
- Ønsket oppførsel/praksis
- Utvikling over tid
- Gjensidig påvirkning

- Hvor er vi og hvor vil vi?
- Kunnskap og motivasjon?
- Hvem må være med?
- Hvordan følger vi opp?


13 HEURES
DAVID DELOS
JOURNALISTE TV5 MONDE


Fogg Behavior Model
B=mat
behavior motivation ability trigger
at same moment
High Motivation
motivation
triggers
succeed here
Action Line
triggers
fail here
Low Motivation
www.BehaviorModel.org
© 2007 BJ Fogg
For permissions, contact BJ Fogg
Hard to Do
ability
Easy to Do

"Hand hygiene prevents **you**

from catching diseases."

vs.

"Hand hygiene prevents **patients**

from catching diseases."

Grant, A.M. & Hoffman, D.A.: *"It's Not All About Me. Motivating Hand Hygiene Among Health Care Professionals by Focusing on Patients"*, Psychological Science, December 2011, vol. 22 no. 12: http://pss.sagepub.com/content/22/12/1494

Med "OJ!" arbeider vi

blant våre medarbeidere for å sikre at

informasjon som tilhører **SINTEF,**

våre kunder og **samarbeidspartnere**

er i trygge hender.

«OJ!»?

Fra idé til konsept


SANS NorSIS

OUCH! | Juli 2013

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...
- Hva er spear phishing
- Effektiviteten til spear phishing
- Hvordan beskytte deg selv

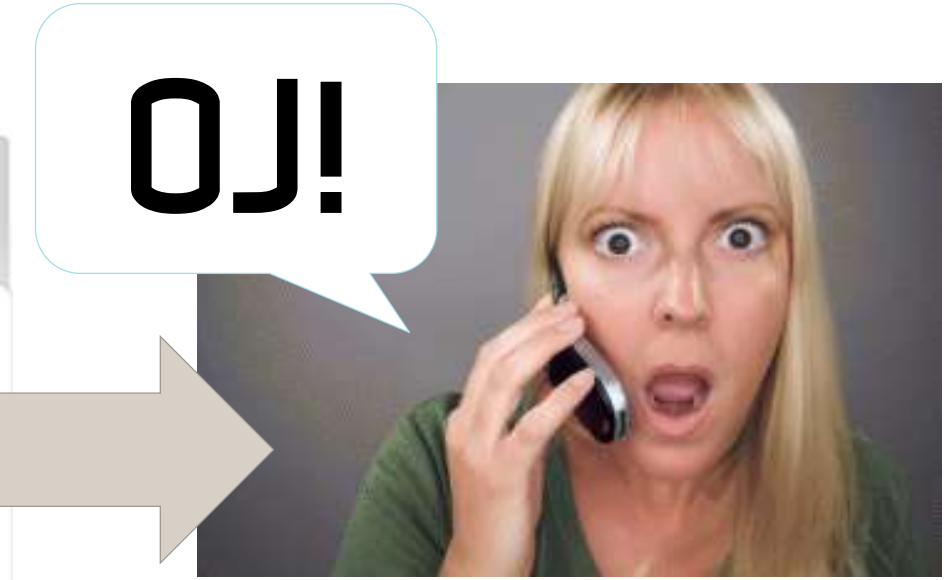
Spear Phishing

Hva er spear phishing

Du er kanskje kjent med phishing-angrep, dette er e-post sent av kriminelle til millioner av mulige ofre rundt hele verden. E-postene er lagd for å lure, villede eller angripe. Vanligvis ser disse beskjedene ut som de kommer fra en pålitelig kilde, som banken din, eller noen du kjenner. E-postene har ofte en beskjed som haster eller en avtale som er for god til å si nei til. Hvis du klikker på linken i en phishing

Gjesteredaktør

Lenny Zeltser er gjesteredaktør for denne utgaven av OUCH! Lenny fokuserer på å hjelpe kunders IT-operasjoner hos HGR Corp og underviser hvordan bekjempe malware på SANS institutt. Lenny er aktiv på Twitter som @lennyzeltser og skriver om sikkerhet på bloggen blog.zeltser.com.



Erlend Andreas Gjære

SINTEFskolen

Startside | Katalog | Min læring

OJ! Informasjonssikkerhet i SINTEF

Læringsløp

Fullført

0 20 40 60 80 100

Tue Mar 03 12:02:50 CET 2015

Vis og skriv ut fremdriften din

Leksjonene begynner med video/lyd – skru på volum/headset. Please notice that an English version is available for each lesson. The lessons start with a video/sound – please turn up the volume/headset

Ressurser

Etter dato | Etter navn

Ingen ressurser tilgjengelig for dette

Gå til element

OJ! 1. Informasjonssikkerhet i SINTEF - DU er viktig!

E-læring (30)

DU er viktig for informasjonssikkerhet i SINTEF! Bli kjent med læringsopplegget som følger OJ!-kampanjen. Forstå hvorfor dette angår også deg – uansett hvilken stilling du har. Det tar ca. 5 minutte...

Fullstendig beskrivelse

Gå til element

OJ! 2. Lås meg når du går / Lock me when you leave

E-læring (19)

Hvilke vaner tar du med deg på reise? Både gode og dårlige, men alle tar du med hjemmefra! Her er en god vane som holder deg unna OJ!-trøbbel. Det tar ca. 5 minutter å gjennomføre leksjonen. W...

Fullstendig beskrivelse

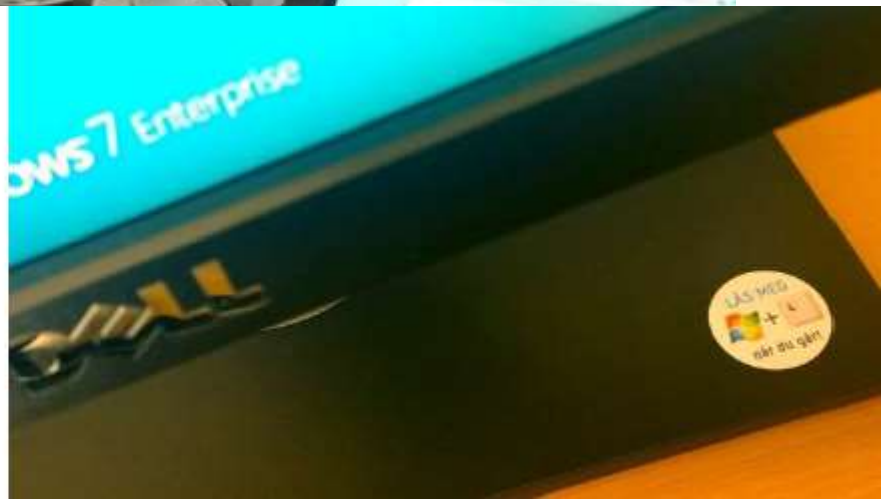
OJ! 3. Biter du på phishing? / Hooked by phishing?

E-læring (26)

OJ! Prøver en e-post å få deg på kroken ved å spille på følelser som nysgjerrighet, hastverk, frykt eller grådighet? Lær hvordan du holder hodet kaldt og tenker før du klikker! Det tar ca. 5 minutte...

Fullstendig beskrivelse

Forsterking av læringsinnholdet



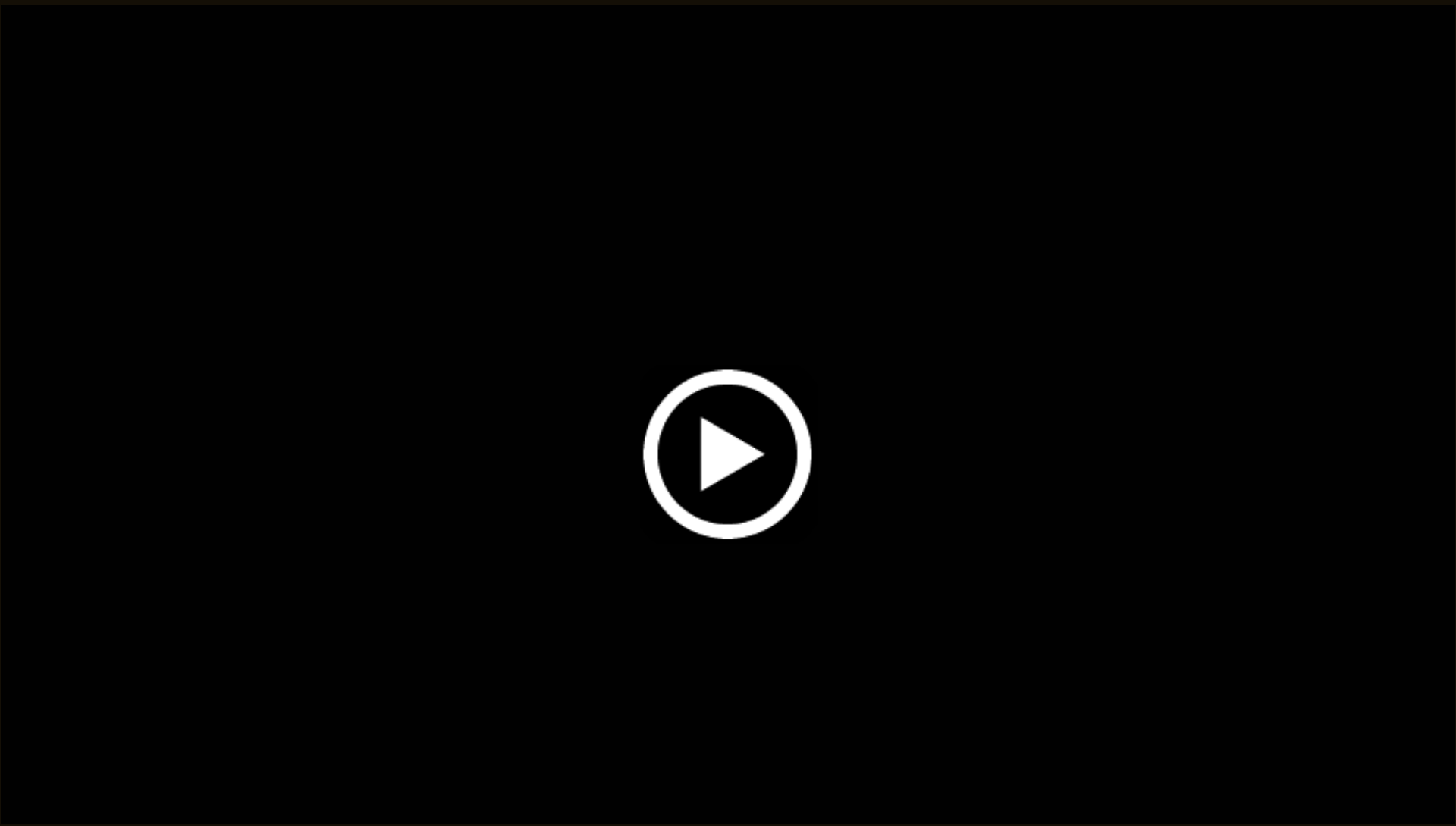

SINTEF
OJ!
INFORMASJONS SIKKERHETSKULTUR
TA ANSVAR FOR HVEM
DU SLIPPER INN

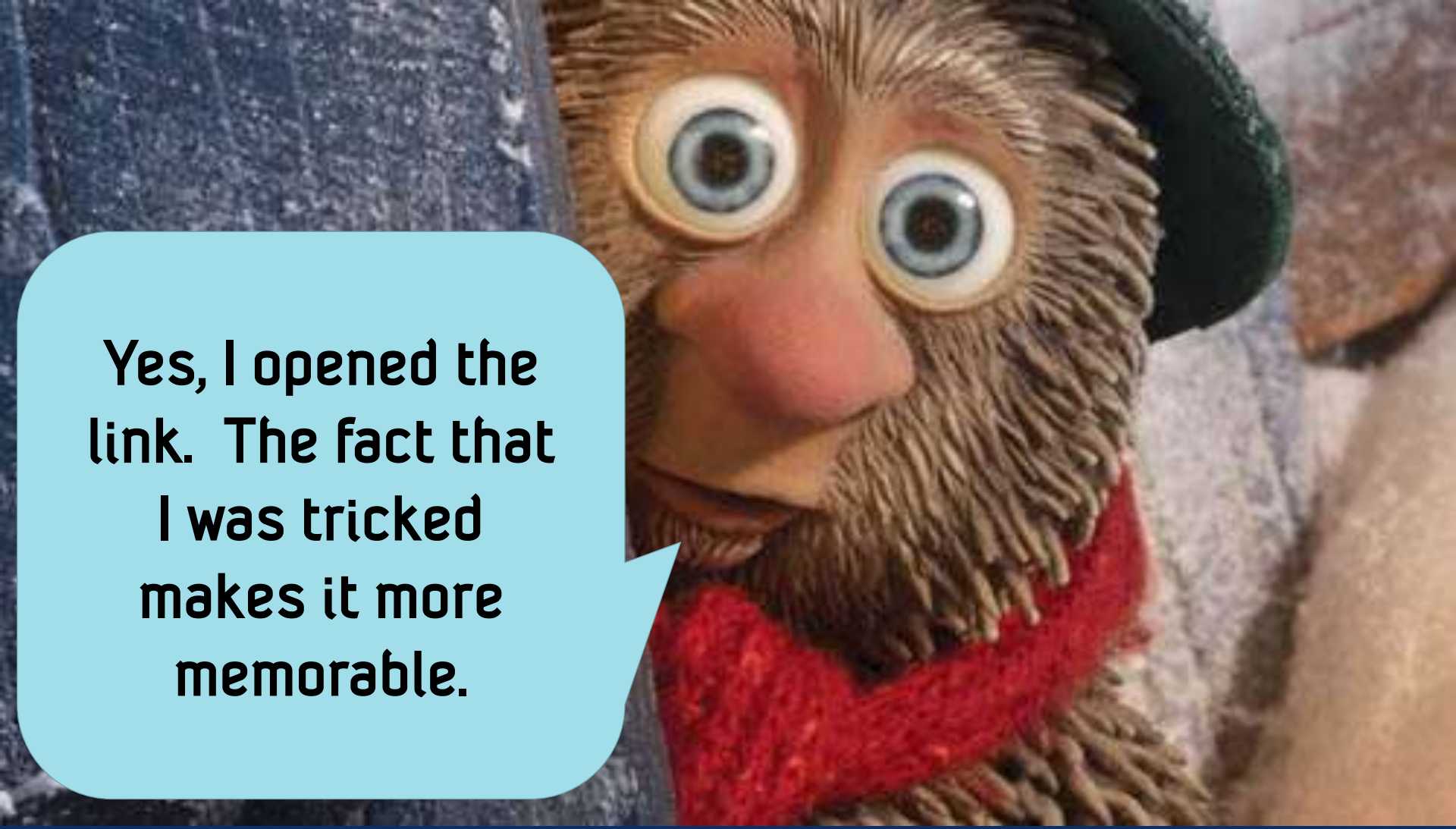

OJ!
IKKE LA DEG LURE


SINTEF
OJ!
SIKKERHETSKULTUR
Tenk før du klikker
Gi aldri fra deg passord til noen
Kan e-posten være lureri? Videresend til oj@sintef.no for å sjekke
Husk alltid å låse PCen når du forlater den
IKKE LA DEG LURE
VÆR DEN LURE
Lær flere triks på
oj.sintef.no
SINTEF
OJ!
SIKKERHETSKULTUR
LÆR ET TRIKS
TIL KAFFEN

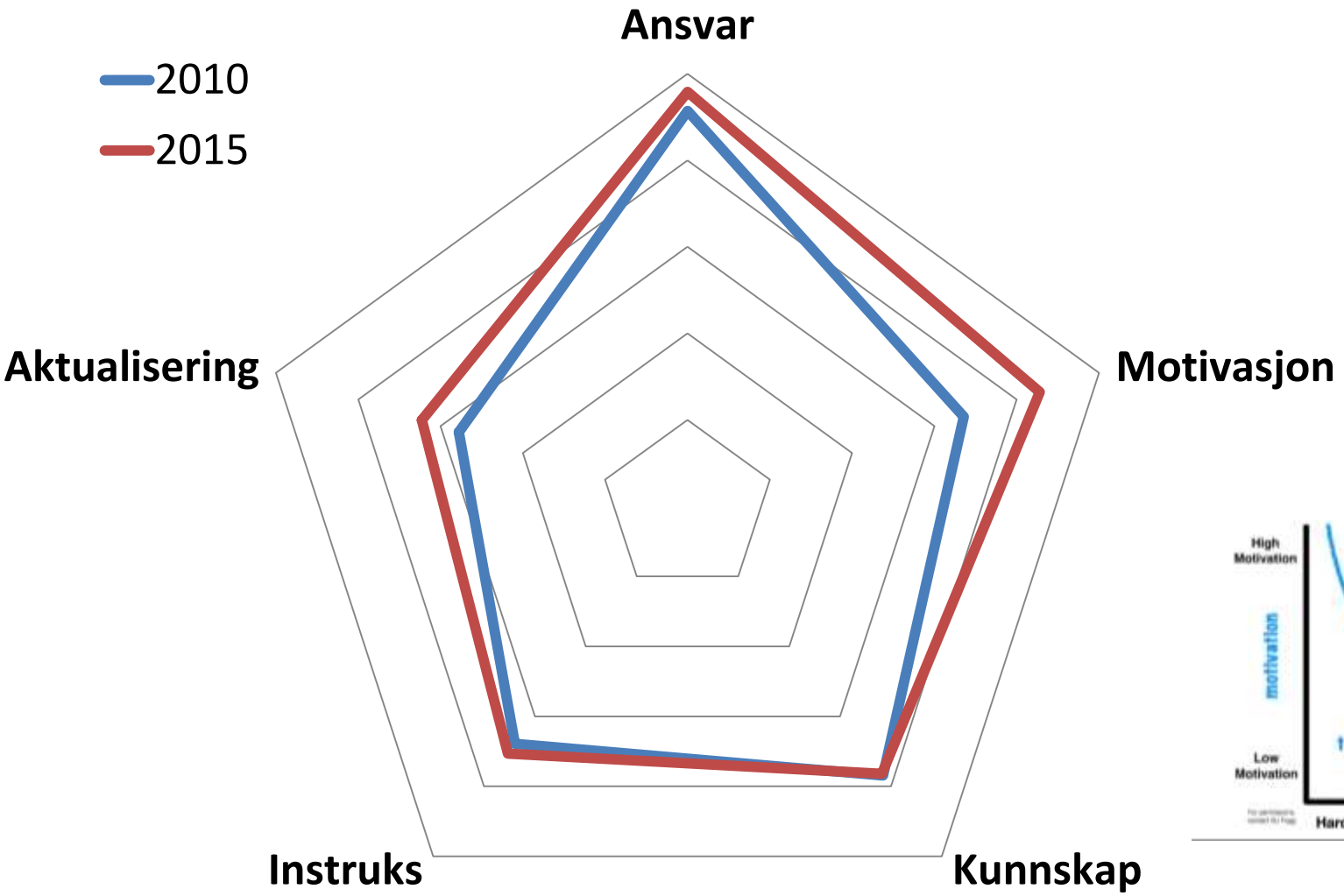

OJ!
OJ!

PHISHING FOR FUN AND PR




Yes, I opened the link. The fact that I was tricked makes it more memorable.


Videoer er ubrukelige som kommunikasjonsmåte.
Fint at det så mye film som vi kjenner oss igjen i.
Bedre med faktaliste/instruks enn en sånn litt barnslig kampanje.


Ansvar
2010
2015
Aktualisering
Motivasjon
Instruks
Kunnskap


Fogg Behavior Model
B=mat
High Motivation
motivation
Low Motivation
triggers
Action Line
triggers
Hard to Do
ability
Easy to Do

Metric Name	What Is Measured	How It is Measured	When Is It Measured	Who Measures?	Details
Phishing Awareness	Number of people who fall victim to a phishing attack	Phishing assessment	Monthly	Security team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviors change.
Phishing Detection	Number of people who detect and report a phishing attack	Phishing assessment	Monthly	Security team	Using the above methodology, but instead of tracking who falls victim it tracks who identifies the attacks and reports them. This number should increase over time.
Infected Computers	Number of infected computers.	Help desk or centralized AV management software.	Monthly	Help desk or security team.	Most infected computers are a result of human behavior (infected attachments, malicious links, etc.). As employees are trained this number should go down over time.
Awareness Survey	Number of employees understand and are following security policies, processes and standards	Online Survey	Bi-annually	Security team or HR	Employees take a survey on 25-50 questions that determine understanding and following of policy. Questions can include if people share passwords, know how to contact security, and if they have been hacked.
Behavior Survey	Top lessons employees have learned and top behaviors changed because of this.	Online survey	Bi-annually	Security team or human resources	This survey is not interested in peoples' understanding of policies. Instead we want to collect what are the key points people are taking away from the training, what are the most common behaviors we are changing.
Employee Feedback	Do employees like the training, are they engaged? If they do not like the training your program will not have an impact.	Online Feedback Forms	Bi-annually	Security team or human resources.	The ultimate goal is to create training that not only people want to take, but training they want to share with others. If you have employees asking if their family can take the training, you have created a truly engaging program.
Testing	Number of employees understand security expectations, specifically the behaviors they should change and how.	Online Testing	Bi-annually	Security team or HR	Questions that specifically test knowledge of security awareness training. Specifically if they know what behaviors they need to change and how.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walk through	Monthly or weekly	Information security or physical security team	Security team does walk through of organizational facilities checking each desktop or separate work environment. Looking to ensure that individuals are following organizational desktop policy.
Passwords	Number of employees using strong passwords.	Password brute forcing.	Monthly or quarterly	Security team	Security gains authorized access to system password database (such on AD or Unix server) and attempts to brute force or crack password hashes.
Social Engineering	Number of employees who can identify, stop and report a social engineering attack.	Phone call assessments	Monthly	Security team	Security team calls random employees attacking as an attacker would and attempting to social engineer the victim. Example could be pretending to be Microsoft support and having victim download infected anti-virus.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security team (or outsource)	Do extensive searches on sites such as Facebook or LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping.	Random	Information security or physical security	Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures.

http://www.securingthehuman.org/media/resources/presentations/STH-Presentation-SecuringTheHuman.pdf


temporary opportunity to do hard things
high
motivation
low
time
Kan f.eks. skyldes tidspress
natural periods when people cannot do hard things

TAKE AWAY

Mangfold i tilnærmingen

som reflekterer

mangfold blant medarbeidere

Kultur-arbeid tar tid

Motivasjon gir resultater

(og man kan slå seg litt løs!)

Blogg om informasjonssikkerhet

infosec.sintef.no

@SINTEF_Infosec

Spørsmål?

- Erlend Andreas Gjære

  erlendandreas.gjare@sintef.no

   **@erlangsec**

infosec.sintef.no