TOLLETATEN
NORWEGIAN CUSTOMS

Phishing-simuleringer

- Den gode, den onde og den grusomme

25. September 2024

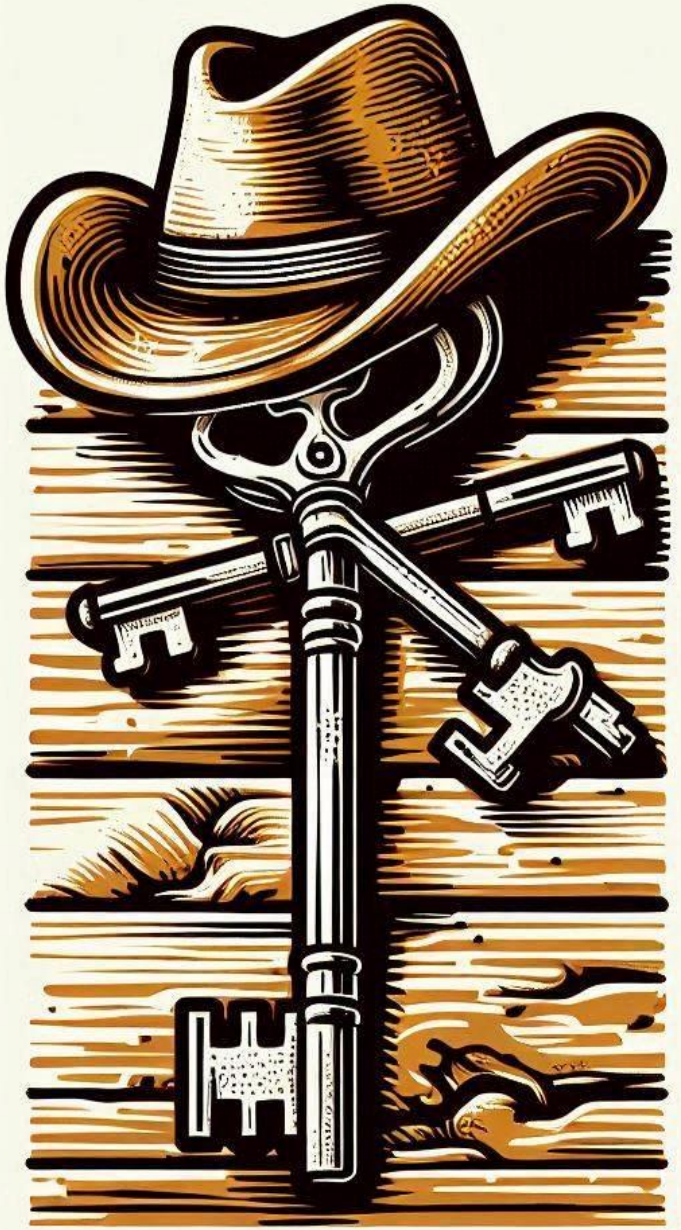
Ragnhild “Bridget” Sageng
Senior rådgiver

Hvem er jeg?

- Ragnhild / Bridget
- Jobbet tidligere som en etisk hacker
- Jobber i Tolletaten
- Elsker å snakke om mennesker relatert til cybersikkerhet

Dagens nøkkelpunkter

- **#1. Finn ut hvordan en phish, selv en simulert en, kan påvirke mennesker.**
- **#2. Kunne skille mellom en god og en dårlig phishing-simulering.**
- **#3. Hvordan planlegge en phishing-simulering og involvere de rette personene i prosessen.**



Agenda

- **Phishing-simuleringer som et verktøy for å trene**
- **Reaksjoner: Vi er bare mennesker**
- **Se på eksempler på phishing-simulering**
- **Hvordan gjør vi en phishing-simulering god**

Phishing og phishing simuleringer

- Hva er det?
- Hvorfor fungerer det?
- TIBER-EU og Red team tester

Testing + Mennesker = Problemer?

- Mennesker, ikke maskiner
- Ikke noe klart rammeverk
- En dårlig gjennomført test kan gi negative konsekvenser

Den menneskelige psyken

- Føle seg lurt
- Selvklandring og klandre andre
- Noen er mer hardføre

- Vi er alle forskjellige og vi alle reagerer forskjellig

«Gone Phishing”.
- men bruker feil agn

Gamer Trash D.Va
@GamerTrashDva

My work just did this, said there was malware in the company and you need to click here to update to be safe. It was internal, authentic, etc

I knew it was fake because our IT department is next to useless and wouldn't want to actively do work. They told me to shh it was a test

Oversett innlegg

7:17 p.m. · 12. nov. 2018

1 · 8

Publiser svaret ditt

Svar

Gamer Trash D.Va @GamerTrashDva · 12. nov. 2018

I dunno if this is the best way to go when half of my coworkers don't know the difference between IE and Chrome

1 · 2

Froyton
@Froyton

I received a test phishing email from my company and I passed the test by reporting it as phishing, but why did they have to say "this is HR, you got a bonus"? Like... Give me a bonus still. 😔

Oversett tweeten

3:09 p.m. · 2. aug. 2023 · **23** visninger

R.H
@rhassan___

just failed a Phishing test at work cuz the email was offering a promotion 😭

Oversett innlegg

11:18 a.m. · 9. aug. 2024 · **553** visninger

4 · 1 · 18 · 1

Nina Luong
@nina_luong

my university sent an email about providing $7,500 in assistance to those experiencing financial hardship due to the pandemic....turns out it was a PHISHING exercise...

is this a joke???

Oversett tweeten

InfoSecSherpa ⛰️
@InfoSecSherpa

I just heard about a diabolical phishing simulation. Company faked an email from their own HR department, asking users if they were tired of phishing simulations and provided an unsubscribe link. Those who unsubscribed failed the simulation. I'm not sure how I feel about this.

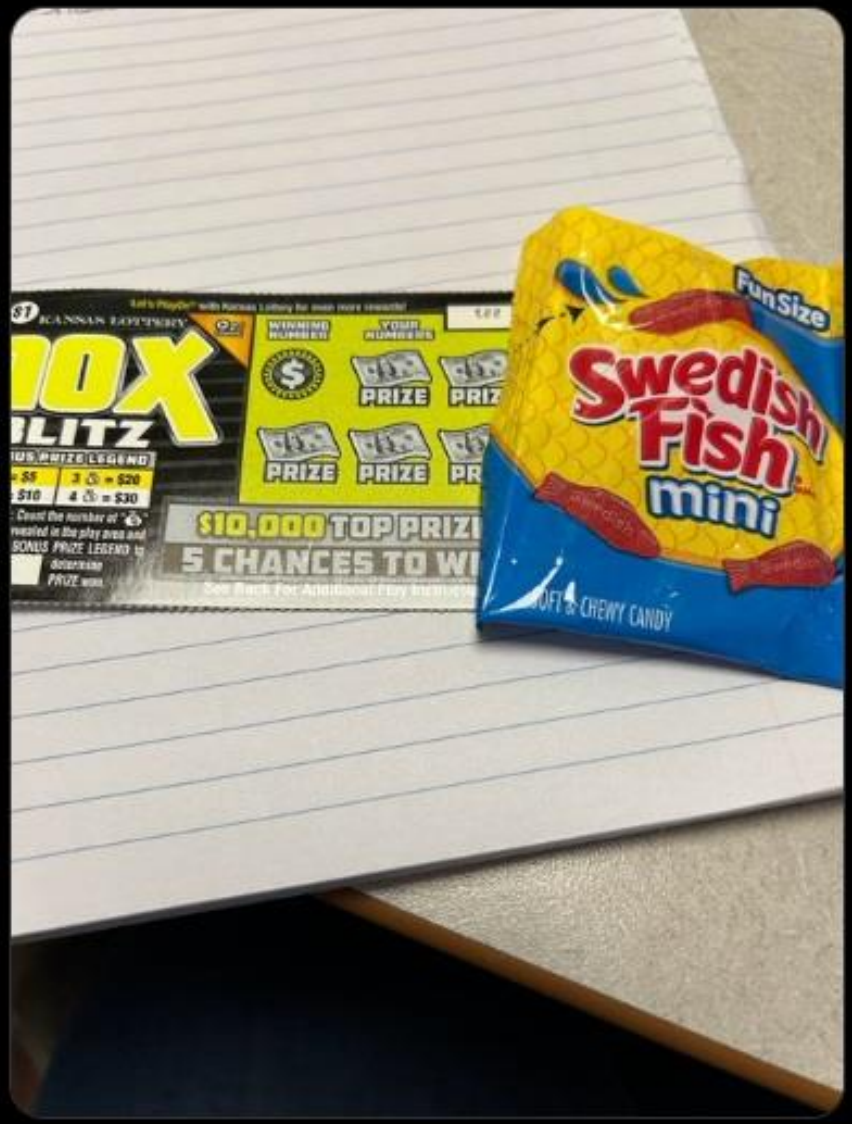
Oversett innlegg

6:36 p.m. · 12. nov. 2018

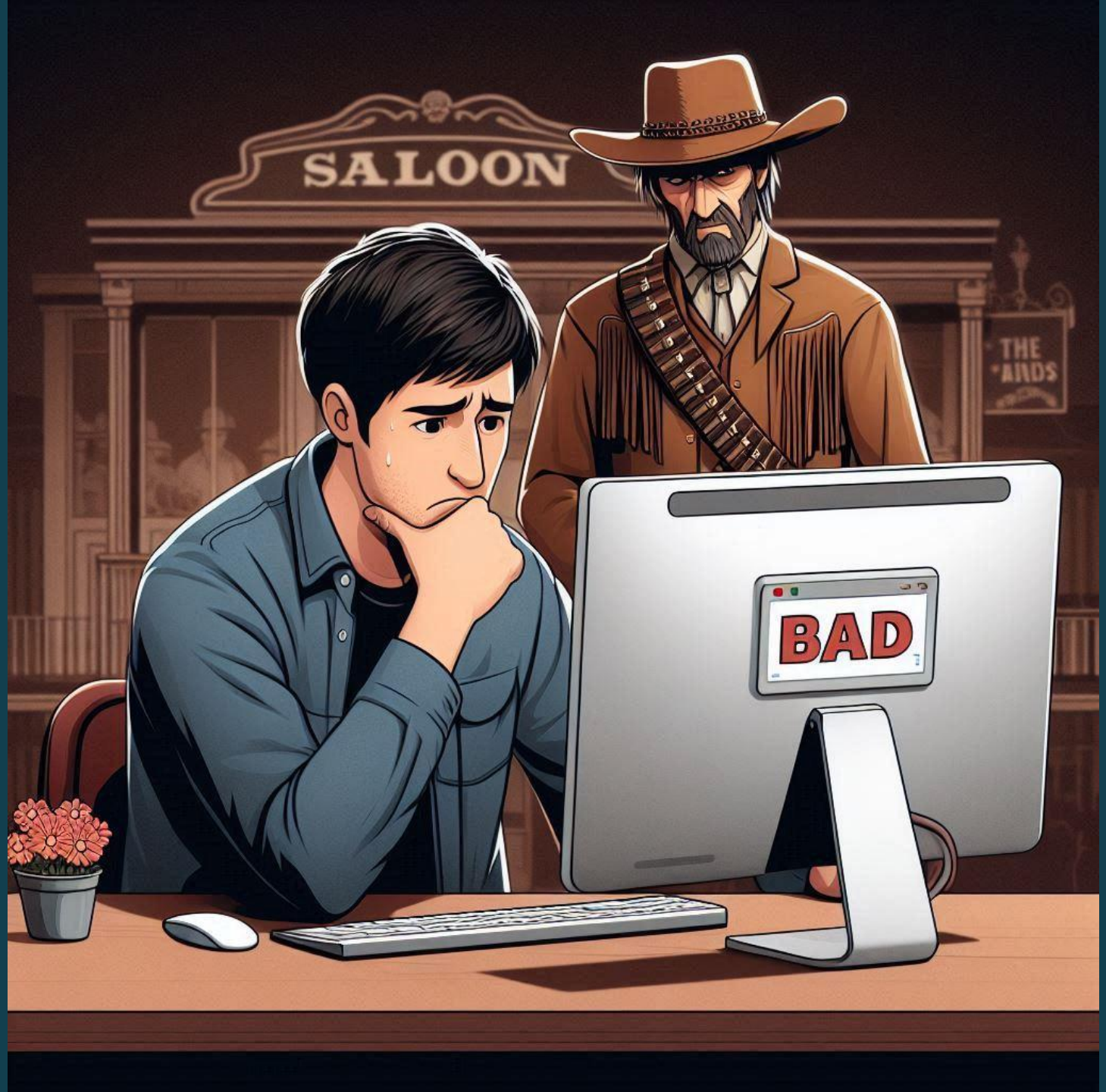

SALOON
HANOVER
PEONECTION
THE GOOD
SALIING
SMINING

Lindsay Shelton 🏳️‍🌈 **MVP** 🖤🤍💜 @LShelton_Tech · 5. des. 2023

I may not have won the lotto today, but I did successfully report the three **phishing simulation** emails I received, and I got a sweet reward for it (thanks Jessica)! Guess I'll keep working since I didn't hit it big.



1 7 363


SALOON
BAD

Important notice: Salary increase

HR Human Resources <admin@hr-benefits.site>
To [redacted]

Reply | Reply All | Forward | ... [redacted]

You forwarded this message on [redacted]

HR-salary-increase-information.docx
16 KB

Message originated from outside Knights

Hi [redacted]

After assessing the current salary structure as provided under the terms of your employment, it was discovered that you are due for a [redacted] annual salary increase beginning in the upcoming fiscal quarter.

The details of your salary increase are enclosed in the attached document.

Please ensure all details are correct to avoid any problem with this adjustment

Cordially,
HR Team

Knights

www.knightsplc.com

Knights

"You've got a pay rise...Not really! Joke's on you!"

Train firm's 'worker bonus' email is actually cybersecurity test

West Midlands Trains workers discover email promising one-off payment is 'phishing simulation test'

A West Midlands Railways train. The firm emailed about 2,500 employers to tell they would getting a get a bonus. Photograph: Aaron Chown/PA

Du vet aldri hvordan mennesker reagerer


THE
RECIGIN
Phinch phig simulation..

[External] Reserve Your Vaccine!

Martha Stoffel via Vaccine Reservations <mstoffel@reserve-vaccines.com>
[redacted]

Reply | Reply All | Forward | ...

Tue 2/16/2021 4:11 AM

Retention Policy HC Inbox 180 (6 months) Expires 8/15/2021

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Reserve Your COVID-19 Vaccine Today!

Hello [redacted]

This is a reminder that you are able to reserve your dose of the COVID-19 vaccine through your healthcare portal. Everyone is eligible to receive the vaccine.

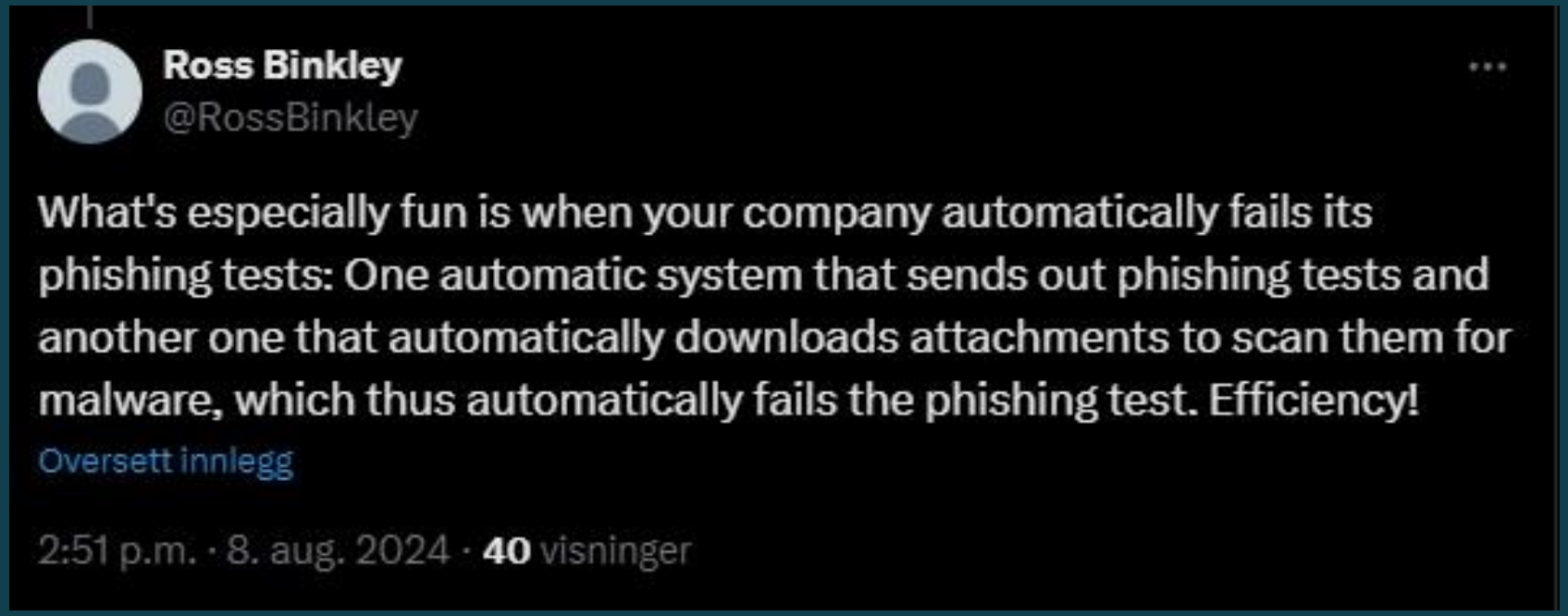
If you are interested, please take the time to fill out the proper information by using the button below:

Reserve Vaccine Here

If you have trouble filling out the required information, please let our patient services team know and someone will be able to assist you.

Thank you,
Martha Stoffel
Customer Outreach Representative

Det går ikke alltid som planlagt…



Ross Binkley
@RossBinkley

What's especially fun is when your company automatically fails its phishing tests: One automatic system that sends out phishing tests and another one that automatically downloads attachments to scan them for malware, which thus automatically fails the phishing test. Efficiency!

Oversett innlegg

2:51 p.m. · 8. aug. 2024 · **40** visninger

"

Et individ som feiler på en social engineering test er ikke en indikasjon på at individet har feilet, det er en indikasjon på en systemisk svikt. Hvis en person mislykkes, kan alle andre også mislykkes.

Tinker Secor, Hacker

Phishing simuleringer: Fordeler og ulemper

- Øke bevisstheten og få folk til å snakke om cybersikkerhet
- Finne røde flagg
- Statistikk (ikke klikk-rate!)

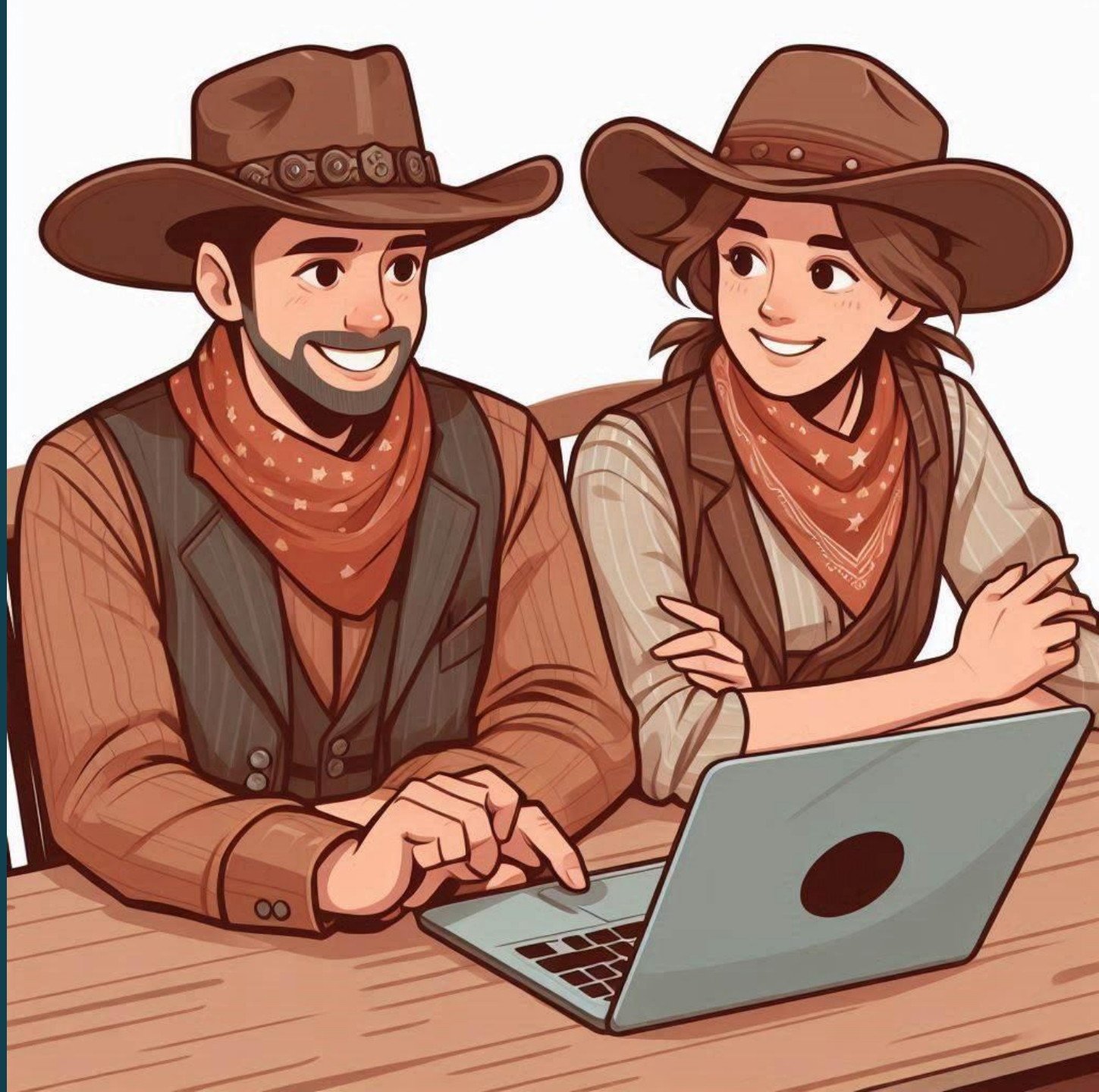
- Brudd på tilliten og den psykologiske sikkerheten til de ansatte
- Mange dårlige scenarioer blir brukt
- Langsiktig tillit mellom arbeidsgivere og arbeidstakere må bygges

Debriefing

- Debriefing av selskapet og de ansatte er viktig
- Folk kan ha forskjellige behov
- Noen ganger kan en debrief av enkeltindivider være nødvendig

HR og andre avdelinger

- Samarbeid mellom avdelingene
- Tiltaksplan for å håndtere emosjonelle reaksjoner
- Klare retningslinjer for oppfølging



Hvordan gjøre simuleringen «god»

- Det handler ikke om «å ta» folk, men å hjelpe dem. Ikke alt handler om klikk-rate!
- Fokuser på adferden du ønsker
- Husk at phishing-simuleringer bare er et verktøy og ikke svaret

Nøkkelpunkter

1. Social engineering pentest-planlegging burde bli utført av flere avdelinger som samarbeider om dette

2. Avstraffelse gir ikke grunnlag for læring

3. Folk kan føle seg elendig i etterkant, behandle dem pent

Er phishing-simuleringer den riktige tilnærmingen for din bedrift?

Referanser og annet

Noen bokanbefalinger:

- Practical Social Engineering by Joe Gray
- The Art of Attack by Maxie Reynolds
- Social Engineering Penetration Testing by Watson, Mason, and Ackroyd
- Transformational Security Awareness by Perry Carpenter
- Cybersecurity ABCs by Barker, Davis, Hallas and McMahon

Noen folk å følge på sosiale medier:

(For å nevne noen)

- Joe Gray
- Lance Spitzner
- Perry Carpenter
- Jessica Barker
- Kai Roer
- Thea Mannix
- Scott Wright

Lenker

https://x.com/FriendLIbrarian/status/1361768076937752587

https://www.youtube.com/shorts/Iz9Z8B09bjM

https://www.youtube.com/watch?v=cauLKI9Qywg

https://www.theguardian.com/uk-news/2021/may/10/train-firms-worker-bonus-email-is-actually-cyber-security-test

https://www.rollonfriday.com/news-content/exclusive-incredulity-firm-sends-lawyers-fake-pay-rise-emails

https://x.com/RossBinkley/status/1821529756988248214

@ragnhild_bss

https://www.linkedin.com/in/ragnhildsageng

ragnhild.sageng@toll.no

Takk for meg!