

# Defending Against Evolving Social Engineering Threats

Presenter: Stan Verwer, Founder of HackX & DDS

ISACA Webinar



## Short about me

Stan Verwer, Founder of DDS Cybersecurity & HackX

Ex-student



**HACKX**

'Only amateurs  
attack machines,  
professionals  
target people.'

The new way of cybersecurity



# Agenda

## Intro (5min)

## Part 1: Why the Latest Social Engineering Trends Demand Serious Attention (20min)

- Why the topic matters
- 5 upcoming social engineering trends and techniques

## Coffee break (5 min)

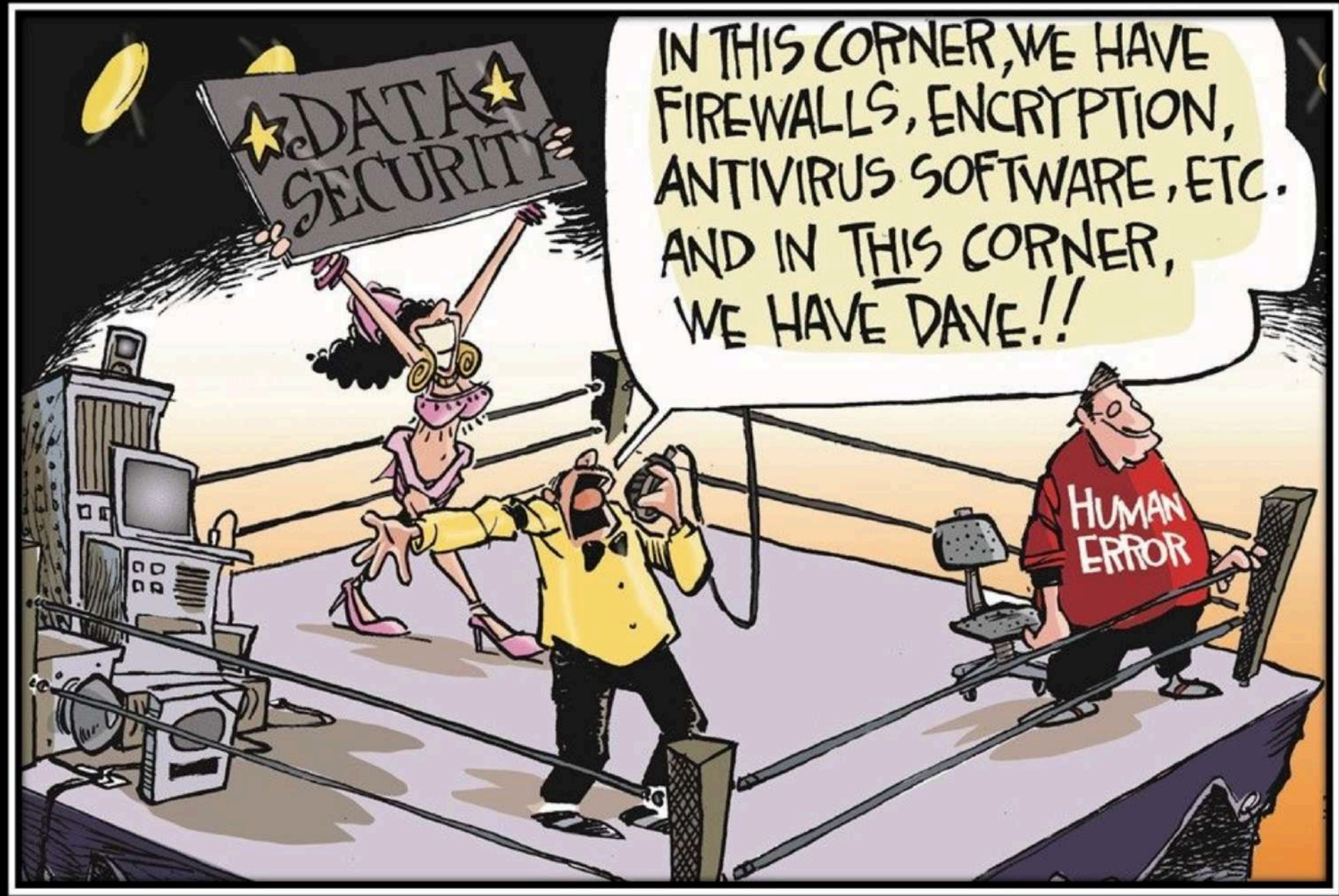
## Part 2: How to train people in 2025 and beyond (20min)

- 3 improved ways of tackling awareness problems
- Recent experiments & experiences

## Questions, discussion en wrap up (10min)



## Why the topic matters



## Why the topic matters

95% of all cyber attacks are dependent on social engineering as starting point

---

**95%**

56% of all IT-managers say that social engineering is the biggest risk factor

---

**56%**

66% of all malware infections is the result of a social engineering attack, without hacking

---

**66%**

WORLD  
ECONOMIC  
FORUM



## Why the topic matters

‘Where I live in London, bikes are regularly stolen by people wearing suits and ties, during the rush hour. Social engineering is definitely still the most effective attack tactic’

**Human psychology = crazy**



# Why the Latest Social Engineering Trends Demand Serious Attention



Cybercriminals are constantly refining their tactics, exploiting human psychology and leveraging emerging technologies to execute increasingly sophisticated attacks. **To stay ahead of the curve**, it is imperative to understand the latest trends and adopt proactive security measures.





## Trends social engineering

### Trend 1 - Voice Copying



Scam calls are rapidly evolving, increasingly mimicking the authenticity of a 'real' call through the use of cloned voices.

**Forbes**

FORBES > INNOVATION > CYBERSECURITY

PREMIUM • EDITORS' PICK

## Fraudsters Cloned Company Director's Voice In \$35 Million Heist, Police Find

**Thomas Brewster** Forbes Staff  
*Senior writer at Forbes covering cybercrime, privacy and surveillance.* [Follow](#)

Oct 14, 2021, 07:01am EDT  
Updated May 2, 2023, 08:37am EDT

The image shows a person wearing a white mask, likely representing a scammer or fraudster. The person is wearing a dark jacket and is looking down. The background is a plain, light-colored wall.



# Recent example | scenario 2025

Attacker

Attacker



Goal



## Real-world scenario



### Step 1: Gathering Intel:

Attacker researches on Facebook, LinkedIn, and Google.

Collects information about the organization, email structures, your assistant, hobbies, and even family details.



## Real-world scenario



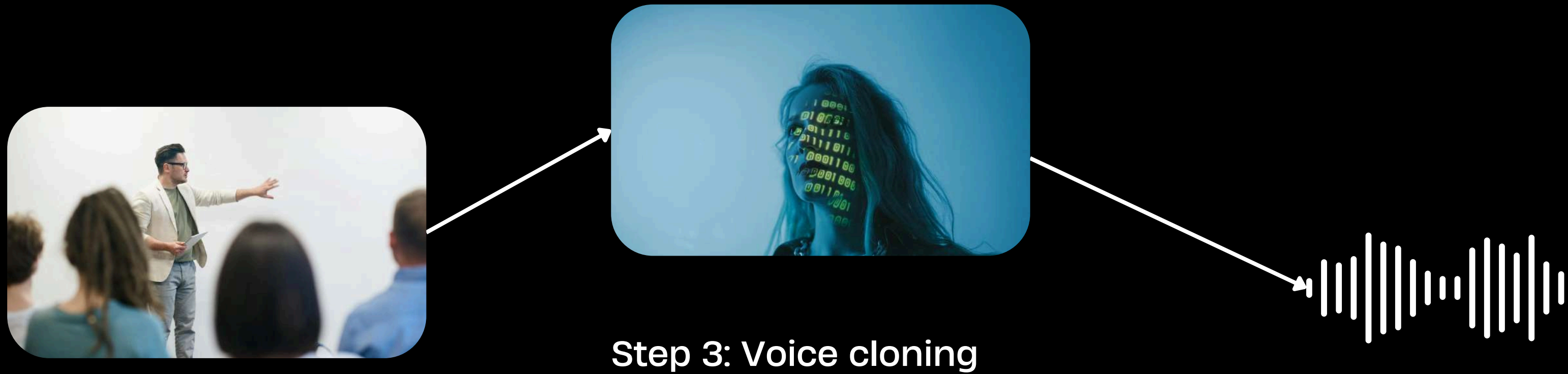
### Step 2: The Setup:

Hacker finds out you're attending a conference.

The attacker identifies your assistant as a key target.



## Real-world scenario



Step 3: Voice cloning

He finds a presentation video of you and clones your voice with AI



## Real-world scenario



### Step 4: The Attack:

Using a **random phone number**, the attacker calls your assistant's **voicemail**.

Attacker claims to be you and leaves a message:

“Something terrible happened and I need immediate access to critical IP documents.,,

“Send them to my **personal email** now, or I’ll lose my job—and so will you probably!.,



## Real-world scenario

### The Result:

- The assistant, under pressure, complies
- Sensitive intellectual property is stolen.



# Phishing yes or no?

Aan: PostNL <[info@klantenservice.nl](mailto:info@klantenservice.nl)>  
Datum: 09-1-2022  
Onderwerp: [SPAM] Uw pakket is aangekomen bij ons sorteercentrum!



Pakketnummer: 3SJ740B721

Geachte Meneer / Mevrouw,

Wegens grote drukte bij PostNL vragen wij uw om de verzendkosten van tevoren betalen.  
Wij hebben tot op heden geen betaling van u ontvangen.  
Zodra de verzendkosten voldaan zijn wordt uw pakket geleverd.  
Anders zijn wij genoodzaakt uw pakket terug naar het depot te sturen.

[Klik hier om te betalen](#)

Oorspronkelijke URL:  
<https://s.id/x7gzp>  
Klik om de koppeling te volgen.

Aan: ~~stanv...~~

## Ziggo - Ondersteunings team

**Uw McAfee Total Protection-abonnement vandaag verlopen [ Laatste waarschuwing ]**

Ref ID:	52551-716NL
Gebruiker:	<del>stanv...</del>
Vandaag korting:	90%
Beperkte tijd:	14-09-2024

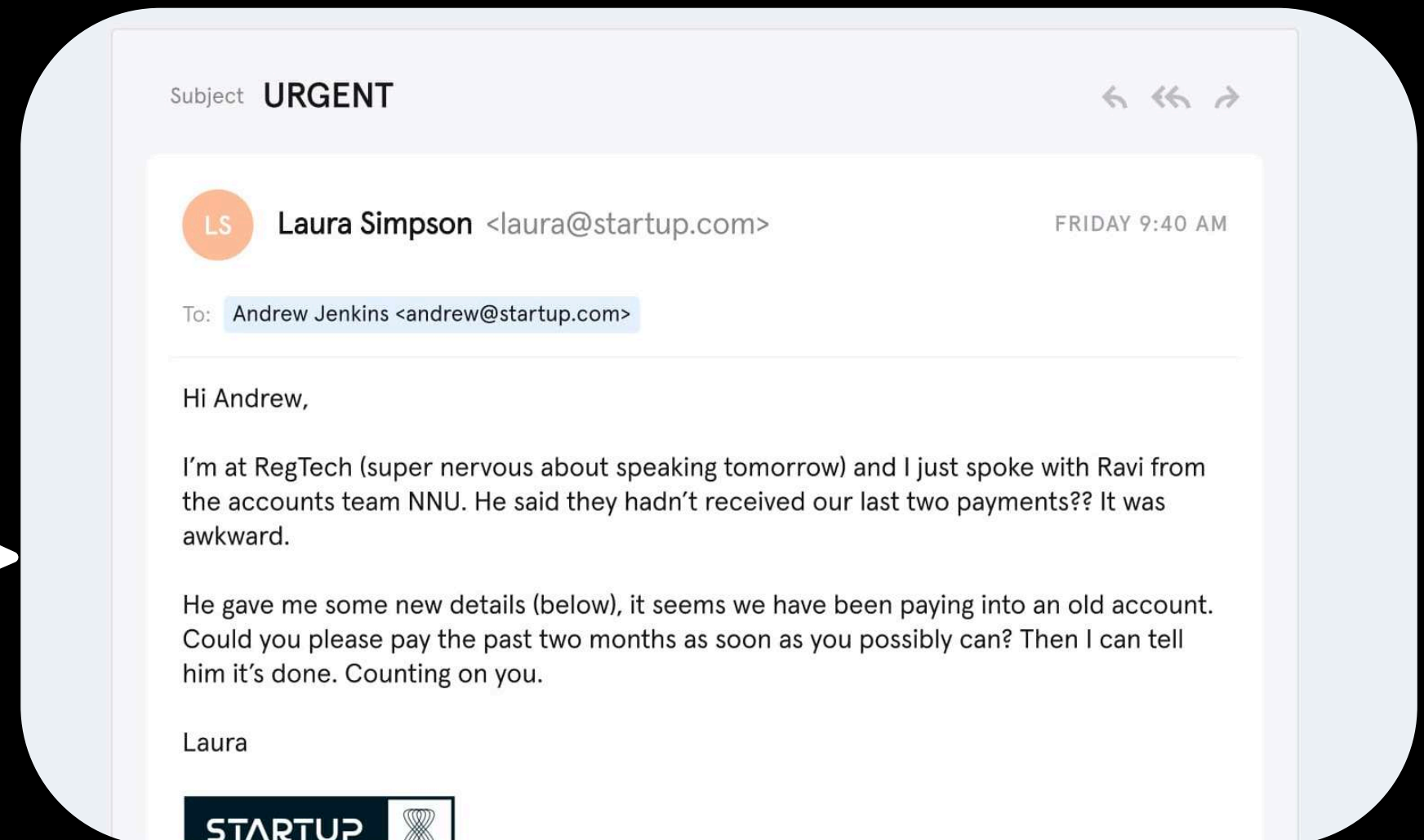
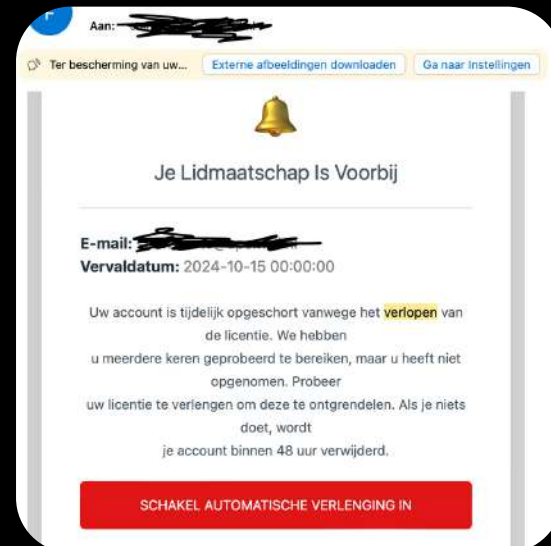
We hebben verschillende keren geprobeerd uw account te bereiken met meldingen en waarschuwingen, maar we





## Trends social engineering

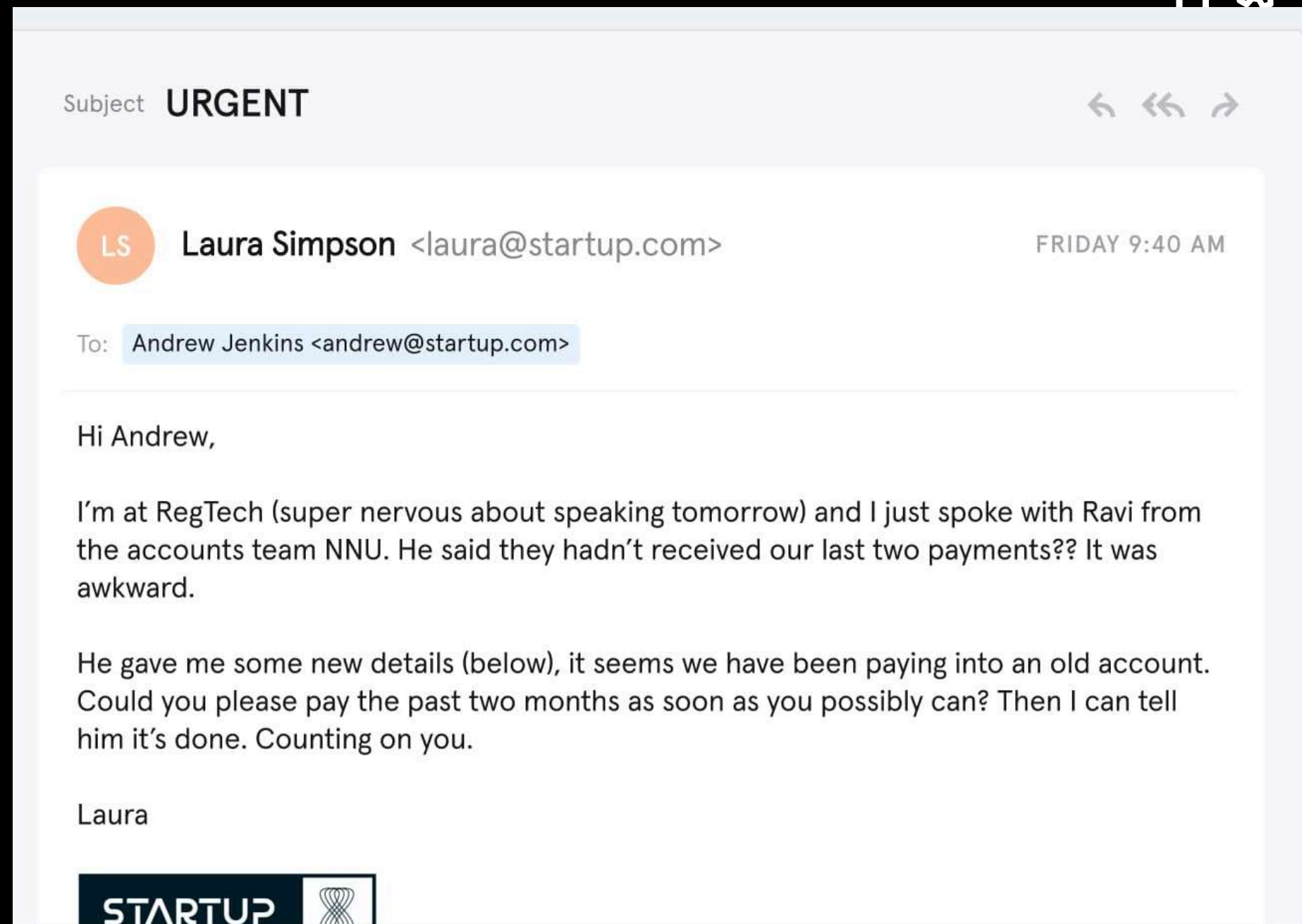
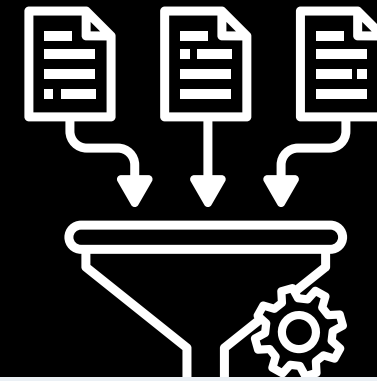
With **generative AI** → **phishing** will get **personalised** on scale (x1000) in seconds!





Trends social engineering

Trend 2 - Automated, large scale spearphishing



## Trends social engineering

Now tell me. Who is the deepfake? Type 1 or 2 in the comments.



Trends social engineering

Deepfake



## Trends social engineering

Which people are not real?

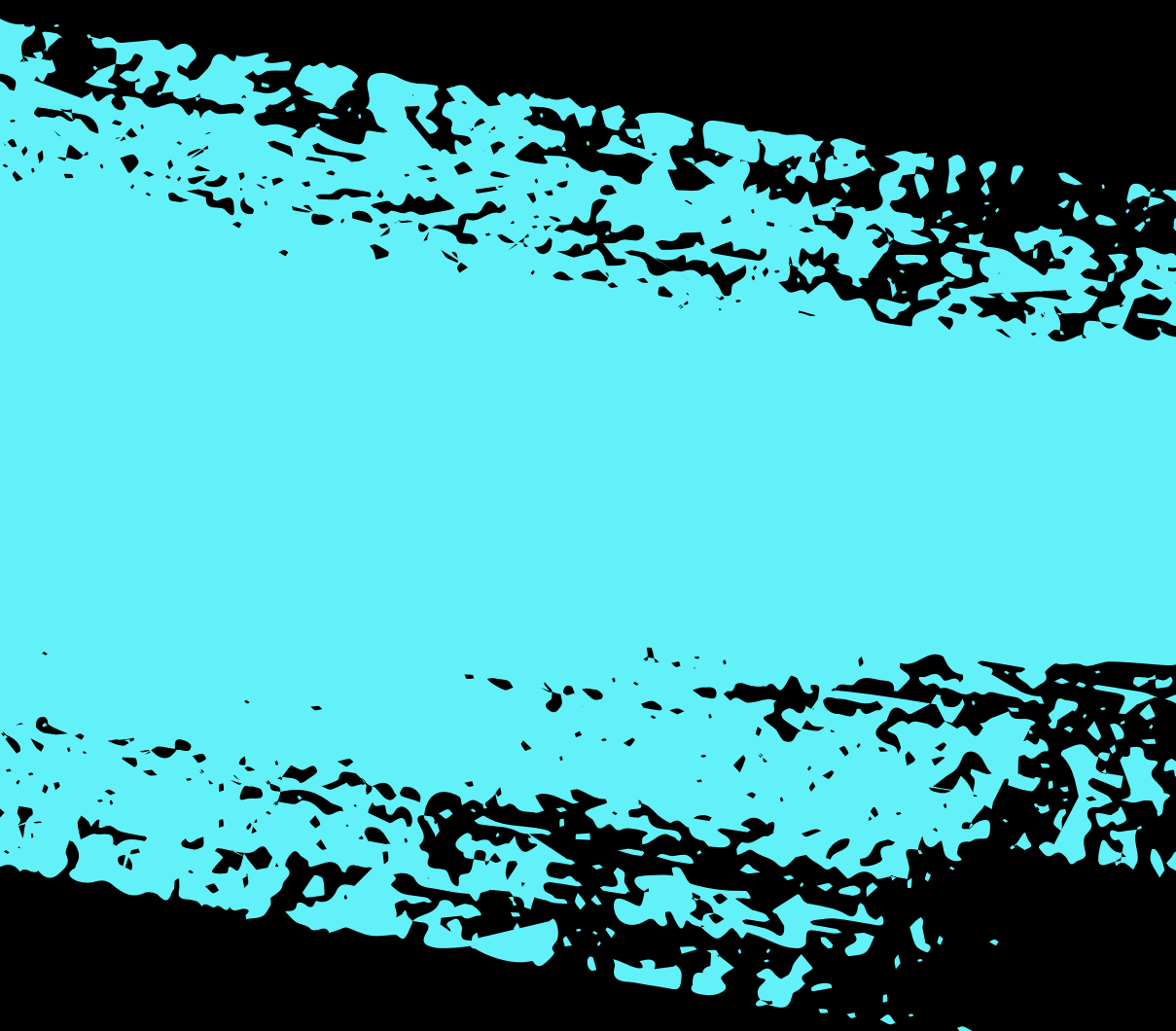


# Trends social engineering



Trends social engineering

Real or not?



Trends social engineering

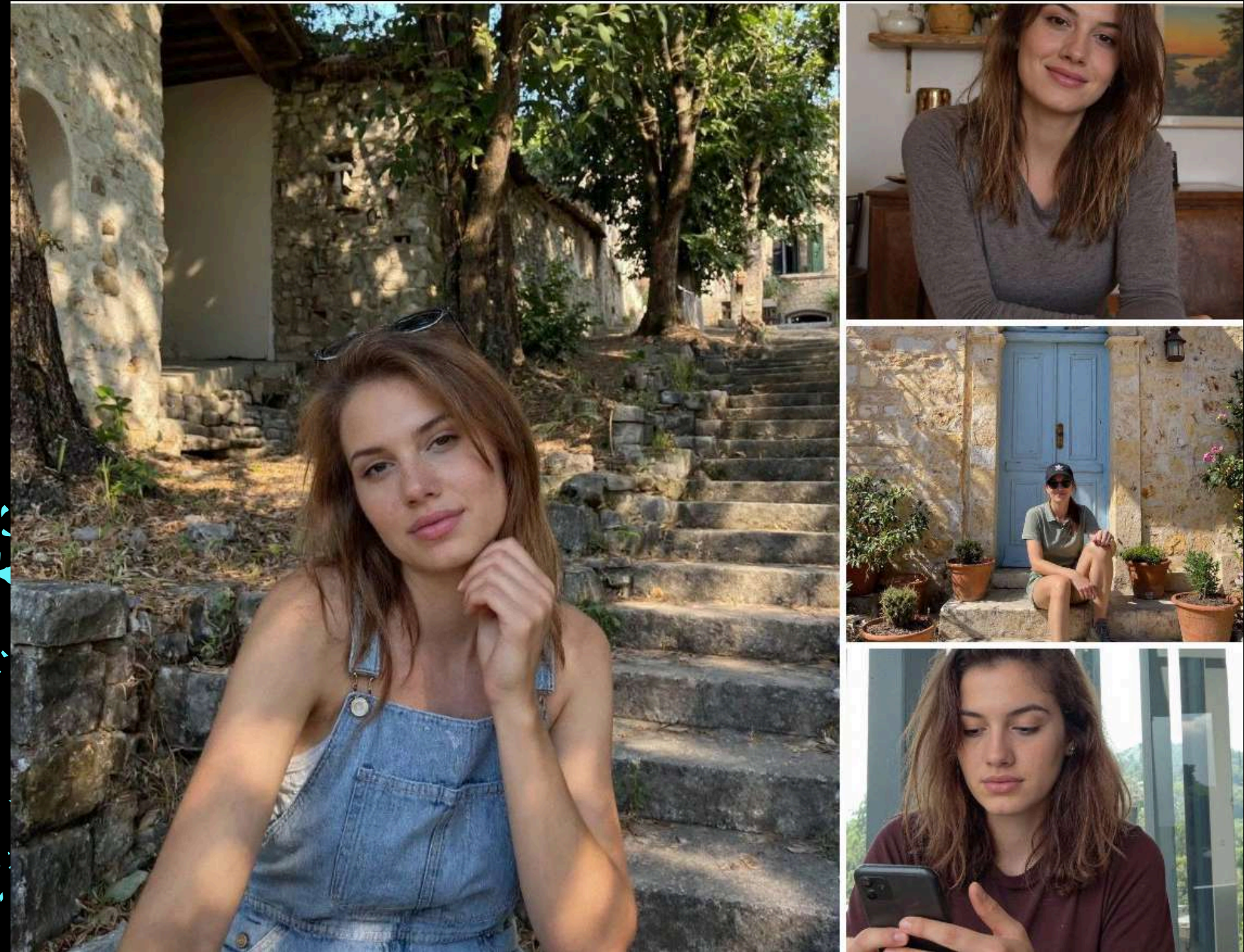
Real





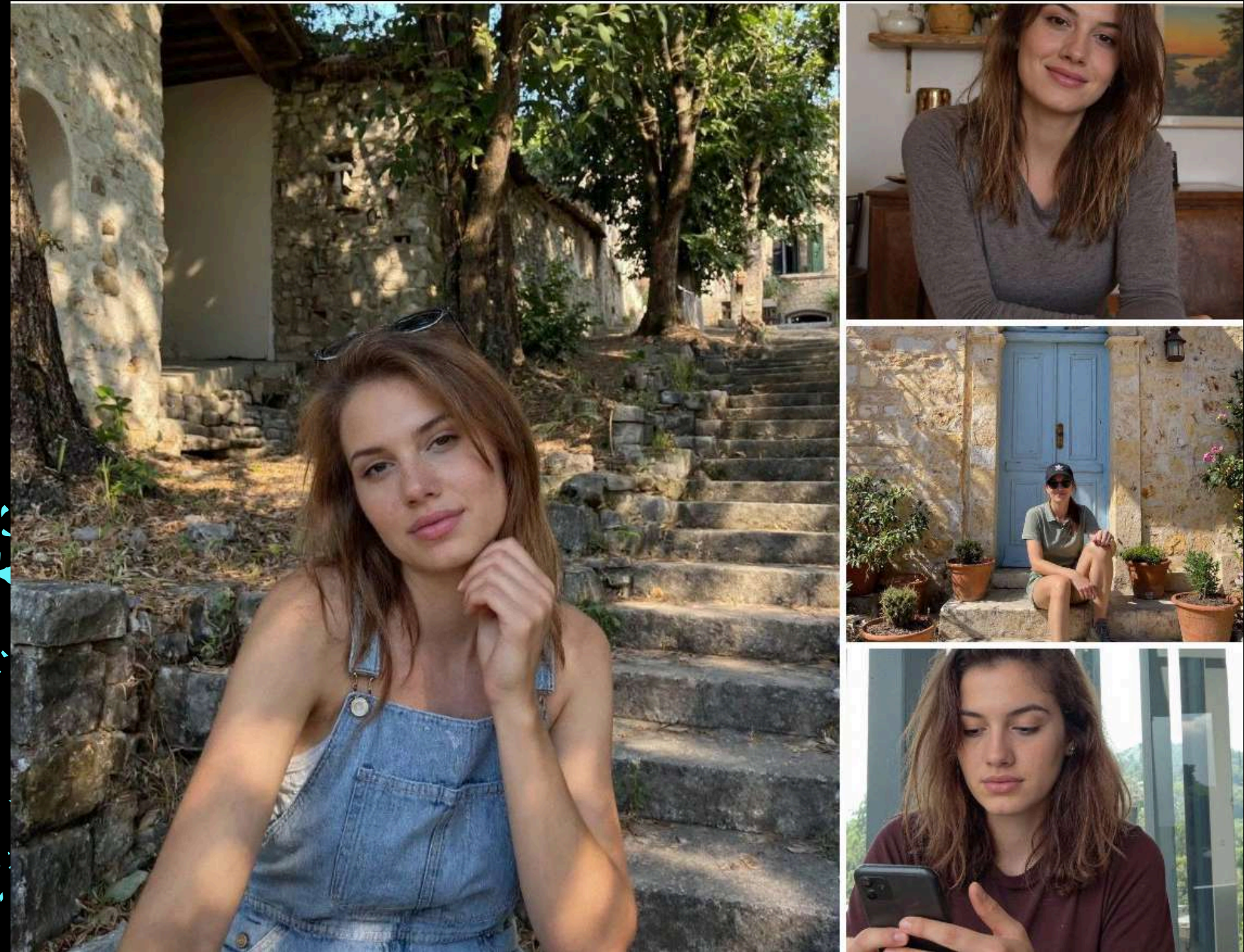
Trends social engineering

And this one?



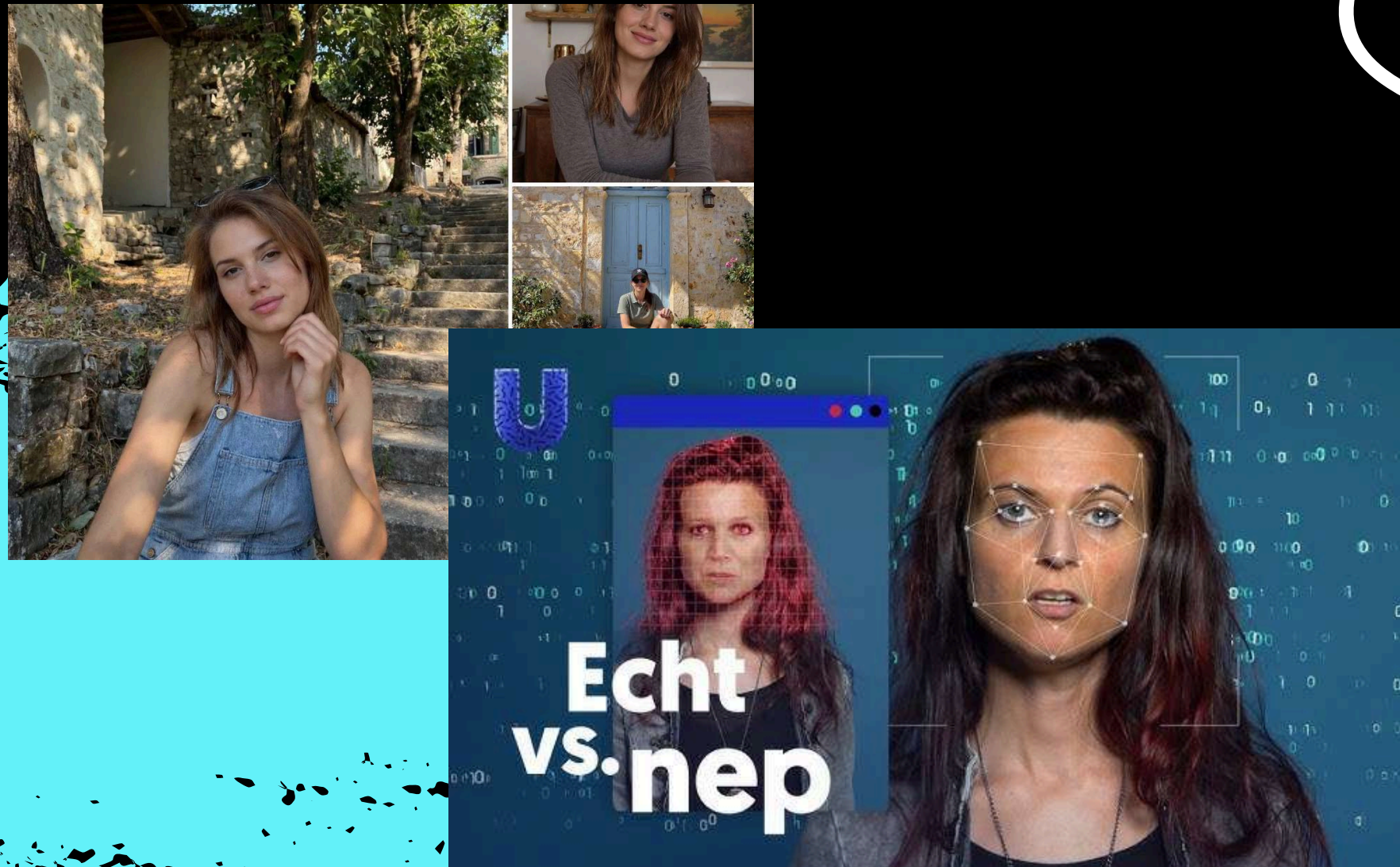
Trends social engineering

**Deepfake**  
Crazy is it not?



# Trends social engineering

## Trend 3 - Deepfake video's



Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

**(CNN)** — A finance worker at a multinational firm was tricked into paying out \$25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

"(In the) multi-person video conference, it turns out that everyone [he saw] was fake," senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.



## Trends social engineering

### Trend 4 - CaaS

Today everyone can buy ransomware, and **phishing services** on the dark web. Attacks will get more **intense!**

RDweb = Download ICON , Connect to Remote Desktop  
Zoom/Rev = 5kk  
Industry = Law Firm, ADVOCATEN  
Country = BE, Belgium  
Domain Computers = 36  
Domain Controlers = 2  
Level User Rights  
Network = Local Network  
Trust Domains = Only Primary  
Windows 2016  
AV = G Data Security + Windows Defender  
Extra Info : 500 GB + On C:/ Driver  
600 GB + Data on Local Share With Important data

Start 2000\$  
step 200\$  
Blitz 3000\$

**Sophos X-Ops**

Karmen

Dashboard

Dashboard Statistics Overview

1 Clients

0 Payments

0 Earned

1284\$ BtCoin Price

Updates

- New Design + Bug fix 22 Feb
- Critical bug fixed 20 Feb
- New program design 20 Feb
- Fix program bug 18 Feb
- Release new version 15 Feb
- Test new version 14 Feb

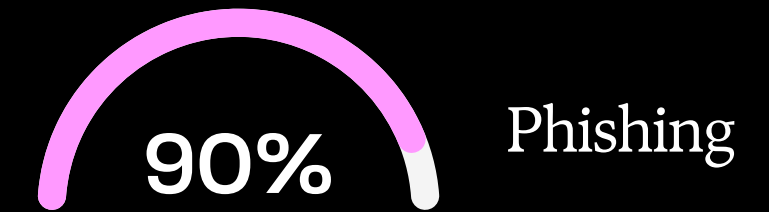
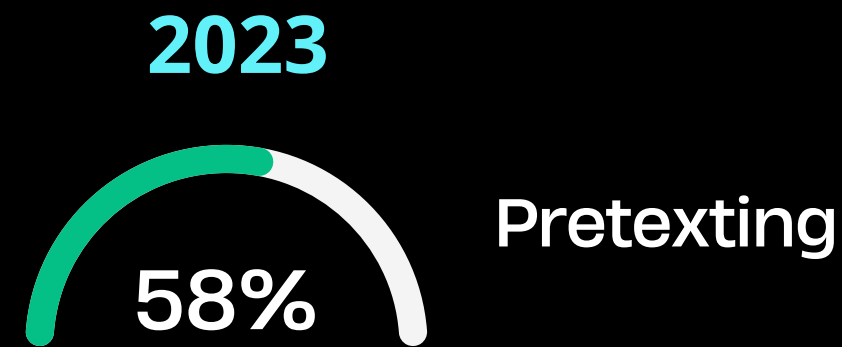
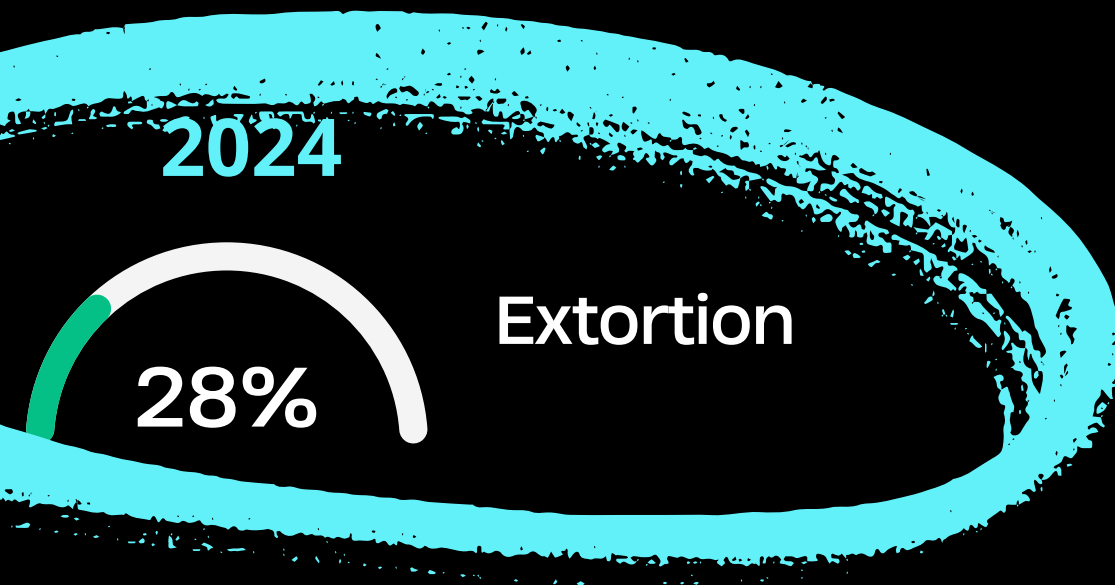
Infos

- Current version: 2.4
- Price to unlock: 1.2000 BtC
- Don't forget update you key!
- Contact jabber: @viblox@jms
- Contact Telegram: @DevBliss



# Trends social engineering

## Trend 5 - Extortion



Many organizations are **unprepared for unconventional or new tactics**, staying ahead requires continuous awareness and adaptation on changing or old tactics.



Many organizations are **unprepared for unconventional or new tactics**, staying ahead requires continuous awareness and adaptation on changing or old tactics.



**Break (5 min)**





# People will fall for it

I don't care who you are or how experienced you are, you're going to fall for a social engineering attack. It's just a matter of time and circumstance.



# How do you handle that?

Be careful with punishment:

Penalizing employees for mistakes (e.g., phishing clicks) **reduces job satisfaction** and **attachment** to the employer (Aurigemma & Mattson, 2017; Blythe et al., 2020).

Blaming employees **shifts focus** from the real perpetrator.



# What can you do?

Best example you can get

## Handling Mistakes Effectively:

Instead of shaming, sit down with employees to **understand what happened**.  
**Use these experiences** to train others and create **teachable moments**.

Repeating offenders → punishment in form of little fines, to make sure they also feel the financial damage they do to the company



What can we do to prevent though?

# How to train and handle people in 2025 | 3 improved ways



Pathé 2018



## How to train and handle people in 2025 | 3 improved ways

### 1. Start using local examples for maximum shock effect

Wij hebben wel een red-teamer laten komen. Die had hele mooie verhalen van wat ze in praktijk aantreffen. Deze presentatie heeft nog weken na gegonst bij koffie-machine.

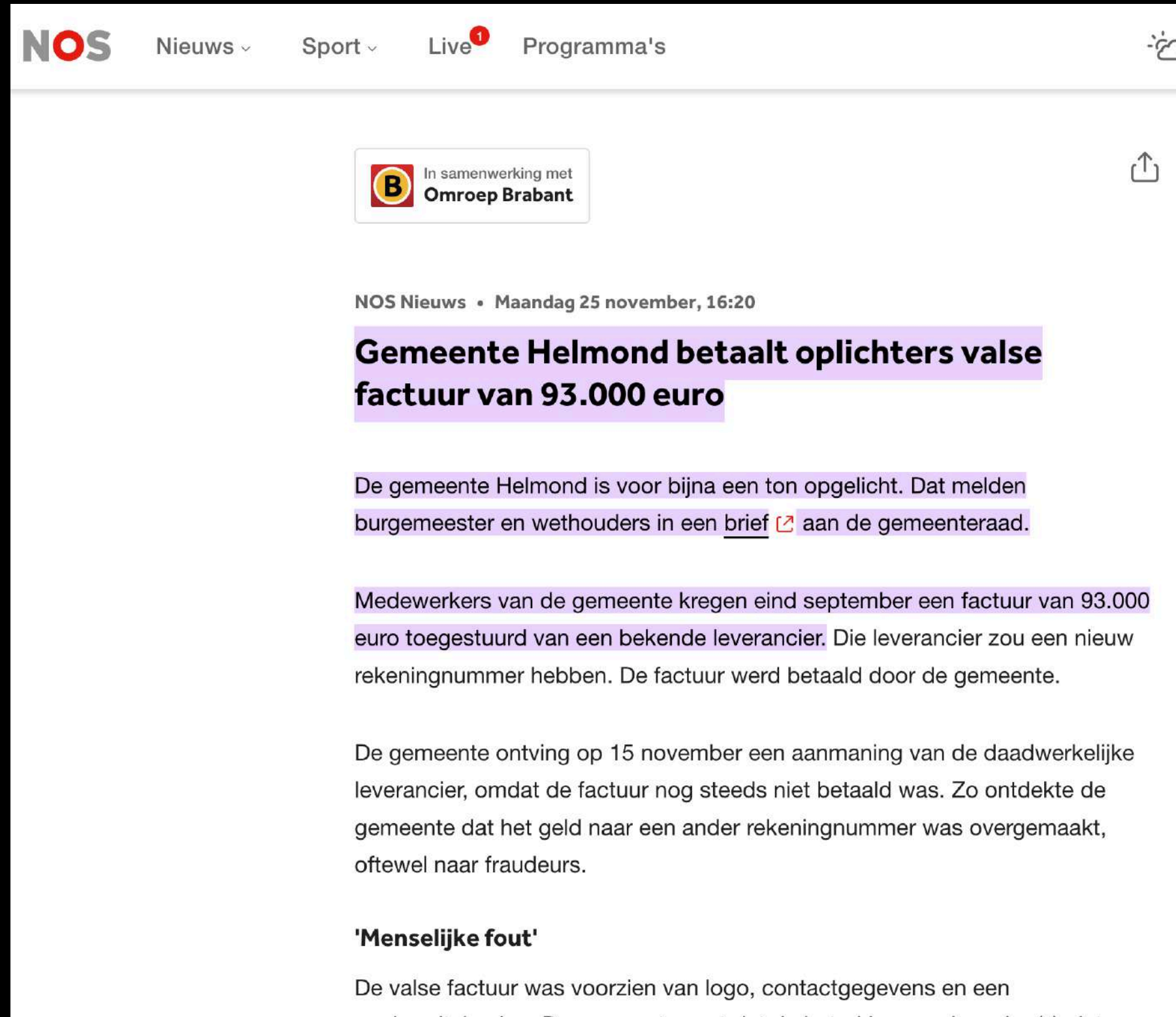
**Helemaal mee eens. Verhalen doen het beter dan generieke adviezen.**

Dat zou inderdaad erg helpen. We organiseren als [redacted] vaak awareness bijeenkomsten en dan is het vaak een klus om iemand te vinden die zijn of haar verhaal met andere ondernemers wil delen. We merken dat dat vaak veel eigen verhalen losmaakt en dan wordt het gesprek ook concreter en persoonlijker.

Ja, dit filmpje ken ik. Wat ik mis is zulke filmpjes met Nederlandse voorbeelden, dus waargebeurde voorbeelden naspelen.



# How to train and handle people in 2025 | 3 improved ways In my local municipality, too..?



The screenshot shows a news article from NOS Nieuws, dated Monday, November 25, 2024, at 16:20. The article is titled "Gemeente Helmond betaalt oplichters valse factuur van 93.000 euro" and is a collaboration with Omroep Brabant. The text describes how the municipality of Helmond was deceived by a false invoice for 93,000 euros. It mentions that employees received the invoice in late September and that the municipality was notified on November 15. The article concludes with the phrase "Menselijke fout" (Human error).

NOS Nieuws • Maandag 25 november, 16:20

## Gemeente Helmond betaalt oplichters valse factuur van 93.000 euro

In samenwerking met Omroep Brabant

De gemeente Helmond is voor bijna een ton opgelicht. Dat melden burgemeester en wethouders in een [brief](#) aan de gemeenteraad.

Medewerkers van de gemeente kregen eind september een factuur van 93.000 euro toegestuurd van een bekende leverancier. Die leverancier zou een nieuw rekeningnummer hebben. De factuur werd betaald door de gemeente.

De gemeente ontving op 15 november een aanmaning van de daadwerkelijke leverancier, omdat de factuur nog steeds niet betaald was. Zo ontdekte de gemeente dat het geld naar een ander rekeningnummer was overgemaakt, oftewel naar fraudeurs.

### 'Menselijke fout'

De valse factuur was voorzien van logo, contactgegevens en een non-handtekening. De gemeente zegt dat de betrokken medewerker(s) niet

9:03

Dank je wel Stan. Ik heb het gelezen en we komen er op terug. Het was een menselijke fout waar we natuurlijk ontzettend van balen, maar ook lessen uit trekken voor de toekomst. Groet, [redacted]



Gemeente Helmond



How to train and handle people in 2025 | 3 improved ways

## 2. Keep trainingscontent short and captivating

*What Makes TikTok so Addictive?: An Analysis of the Mechanisms Underlying the World's Latest Social Media Craze*



### Use the style

Who doesn't like short captivating content?  
I do. Give people that, it is just a matter of good  
production skills. We are lazy.

After learning, reward them with a juicy  
10 second shocking cyber video





## How to train and handle people in 2025 | 3 improved ways

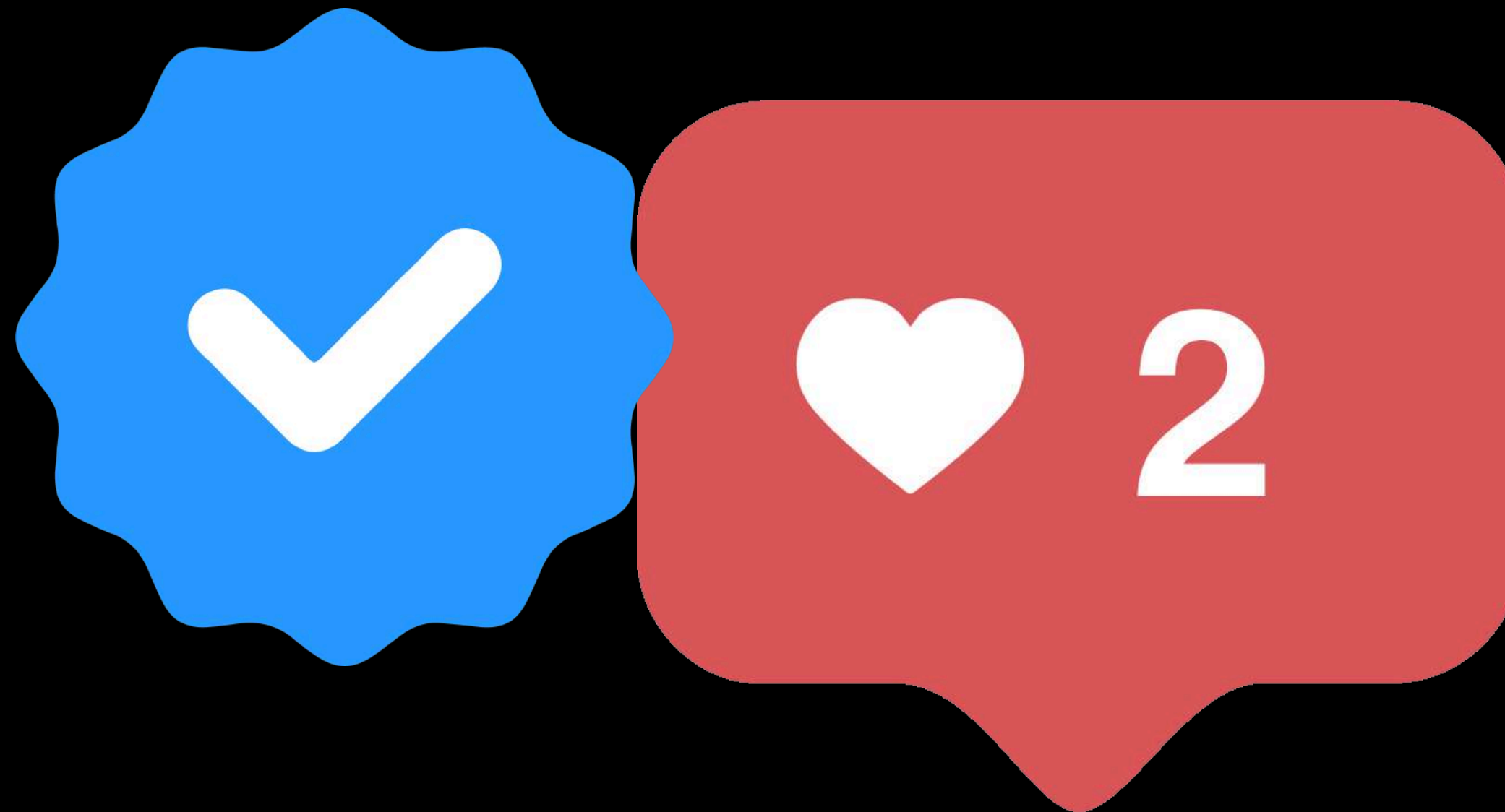
# Do it well or do not do it



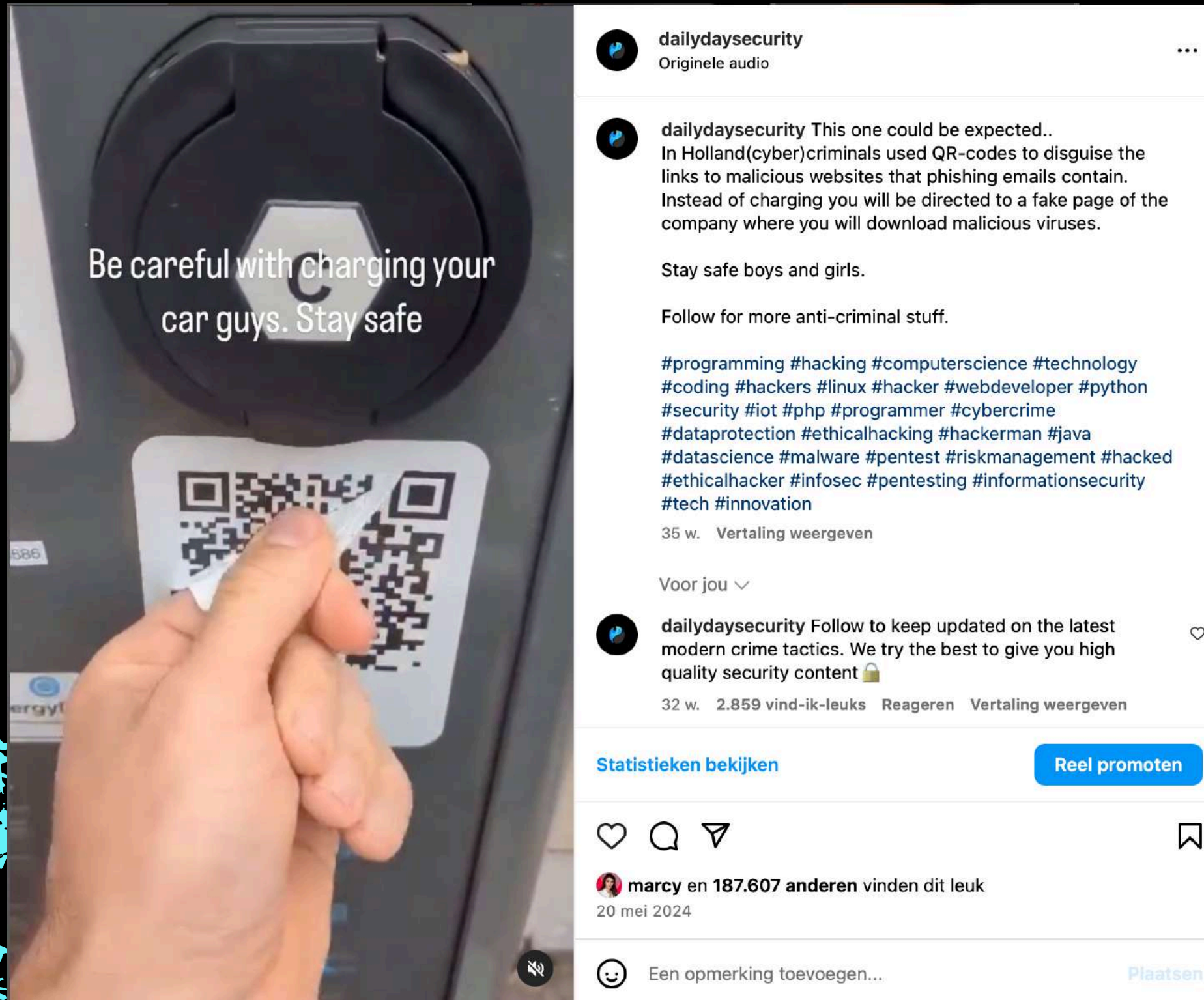
- Not engaging
- Not captivating
- Not fun
- Boring
- Ugly
- Stupid
- Not effective
- Shadow security



Short, captivating content -> where people can  
resonate with



# "We need fun & excitement" - Experiment



28,4 million views

187.607 likes

1.922 times shared

1.373 responses



# How to train and handle people in 2025 | 3 improved ways

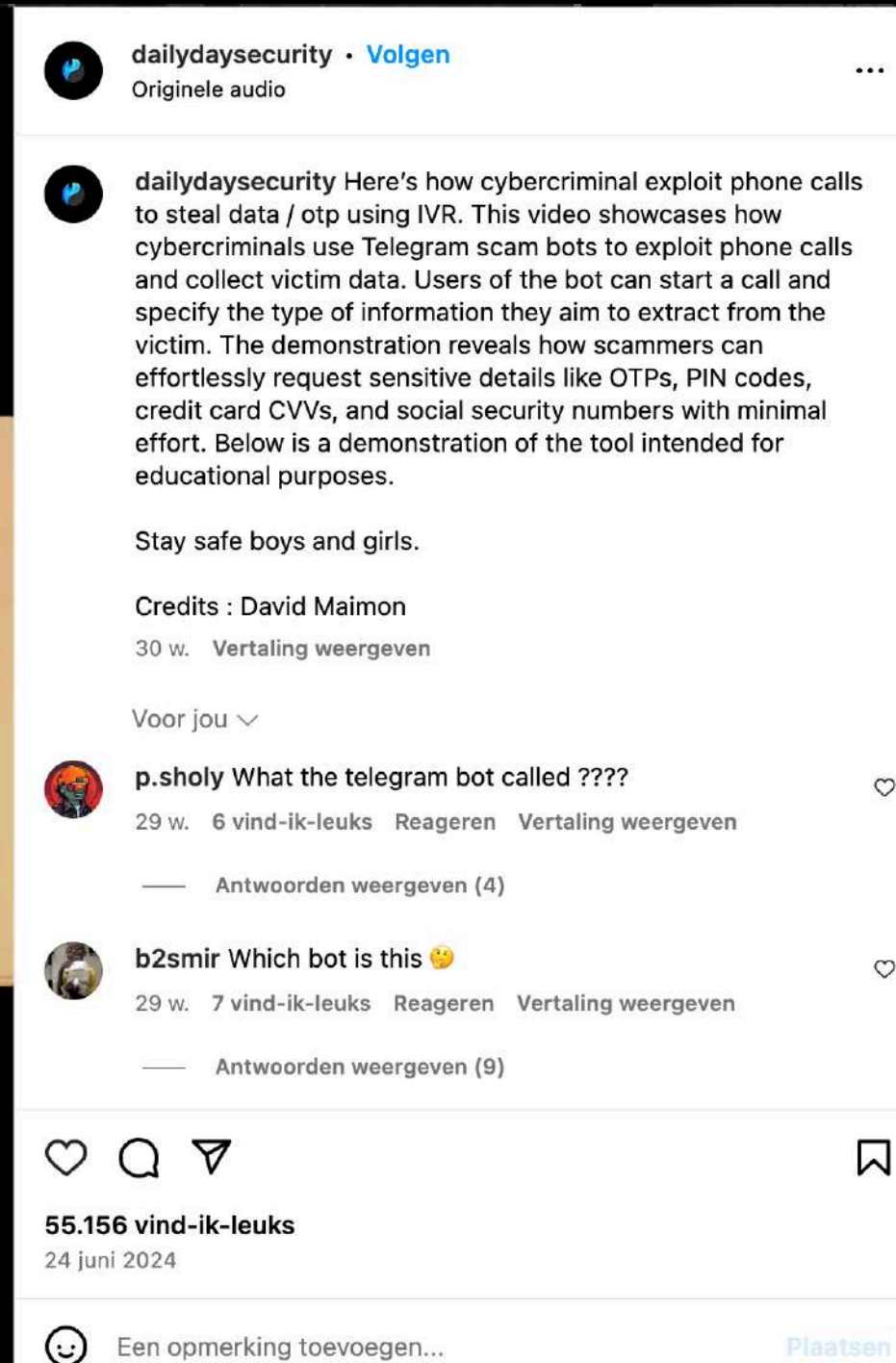
## “We need fun & excitement” - Experiment

How cybercriminals actually do phishing calls.. as simple as via Telegram. Stay safe guys



Criminal

Victim



2,4 million views

55.156 likes

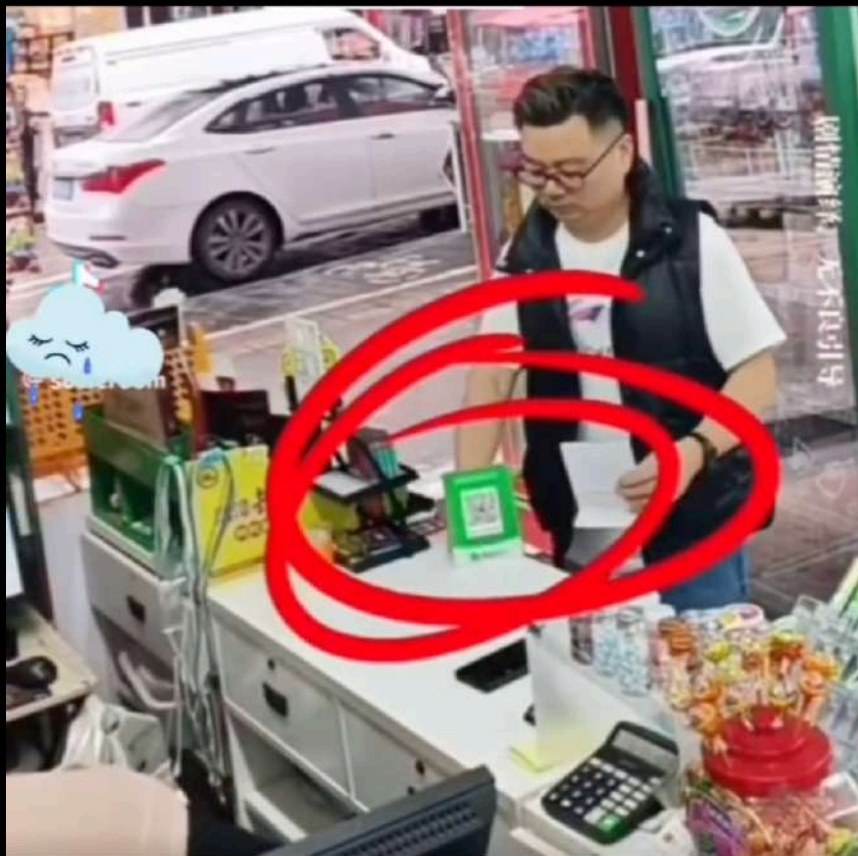
9.495 times shared

1.219 responses



# How to train and handle people in 2025 | 3 improved ways "We need fun & excitement" - Experiment

Be so careful with QR-codes. Stay safe guys.



The screenshot shows an Instagram post from the account 'dailydaysecurity'. The post features a video of a man at a counter with a QR code highlighted by a red circle. The post text reads: 'For cybercriminals it is far easier to get access to your data or assets via social engineering techniques like this, instead of brute force hacking techniques. Using QR-codes (qishing), is a common used technique that is getting more popular amongst criminals. Stay safe guys.' The post includes a list of hashtags such as #programming, #hacking, #computerscience, #technology, #coding, #hackers, #linux, #hacker, #webdeveloper, #python, #security, #iot, #php, #programmer, #cybercrime, #dataprotection, #ethicalhacking, #hackerman, #java, #datascience, #malware, #pentest, #riskmanagement, #hacked, #ethicalhacker, #infosec, #pentesting, #informationsecurity, #tech, and #innovation. The post has 48,450 likes and 2,371 responses. The date is 16 juli 2024.

10,8 million views

48.400 likes

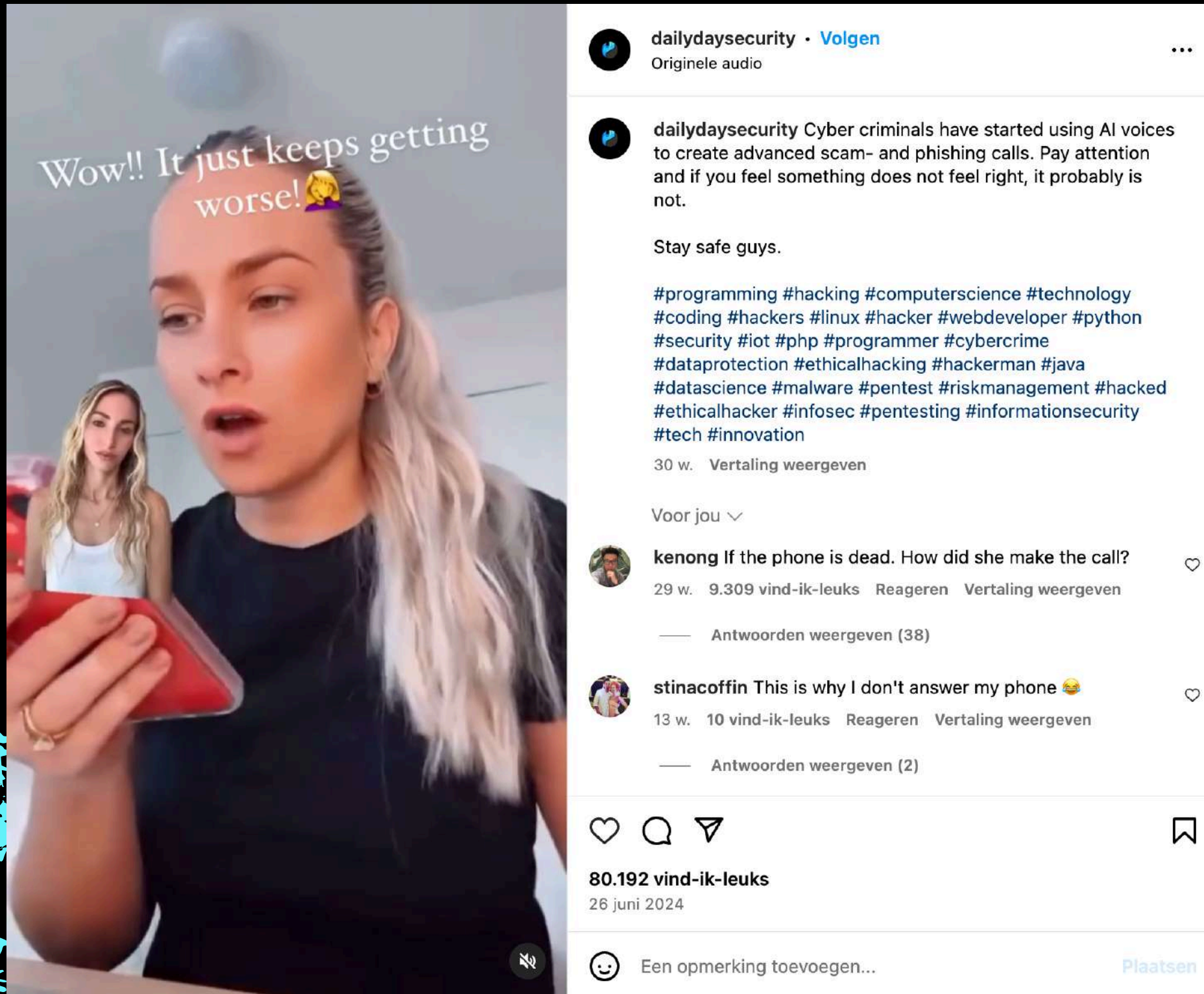
2.371 times shared

2.371 responses



# How to train and handle people in 2025 | 3 improved ways

## “We need fun & excitement” - Experiment



2,7 million views

80.100 likes

14.100 times shared

596 responses



How to train and handle people in 2025 | 3 improved ways

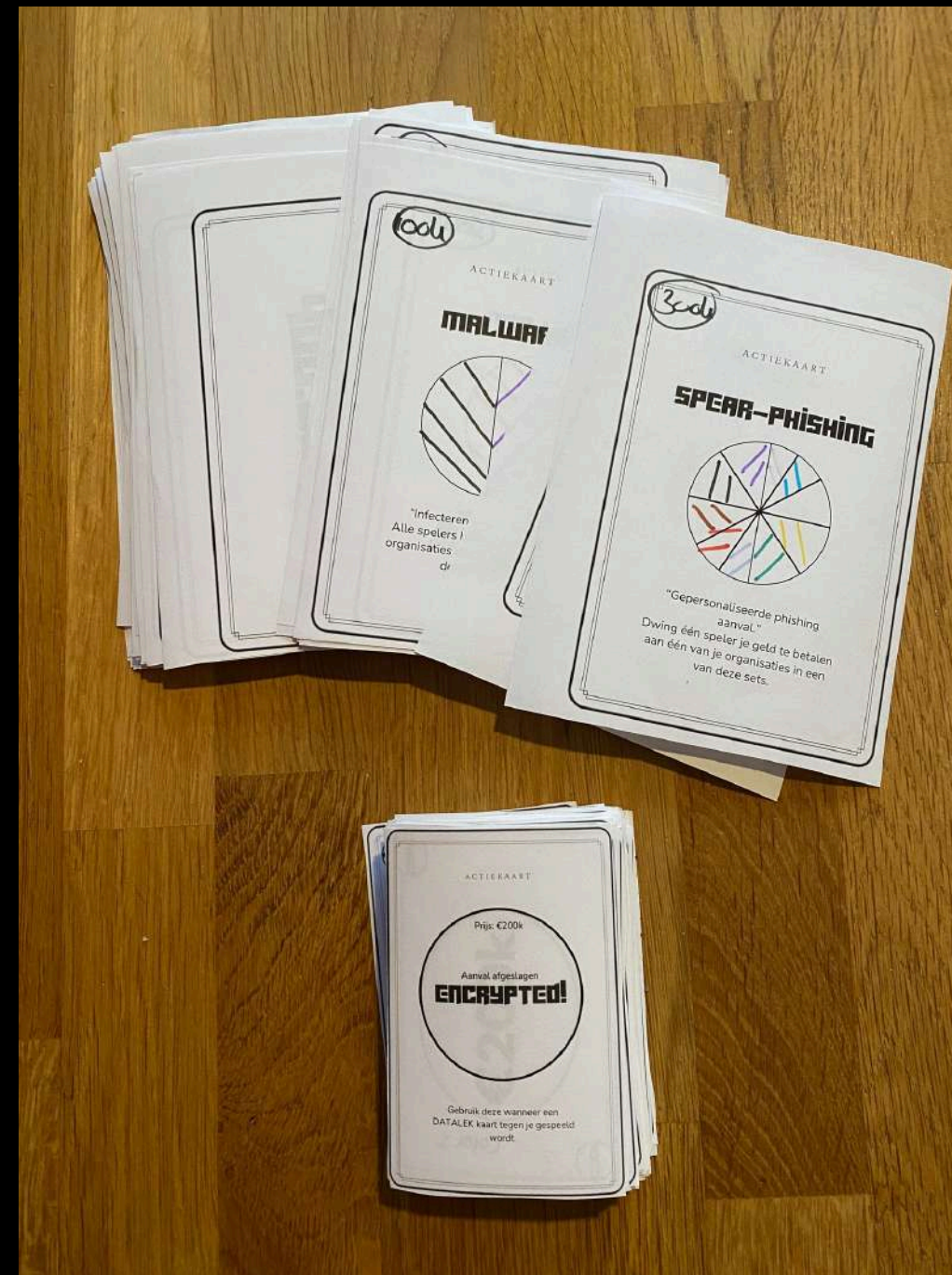
### 3. Keep it simple & make it fun

Keep it  
Simple.



### 3. Keep it simple & make it fun

From this



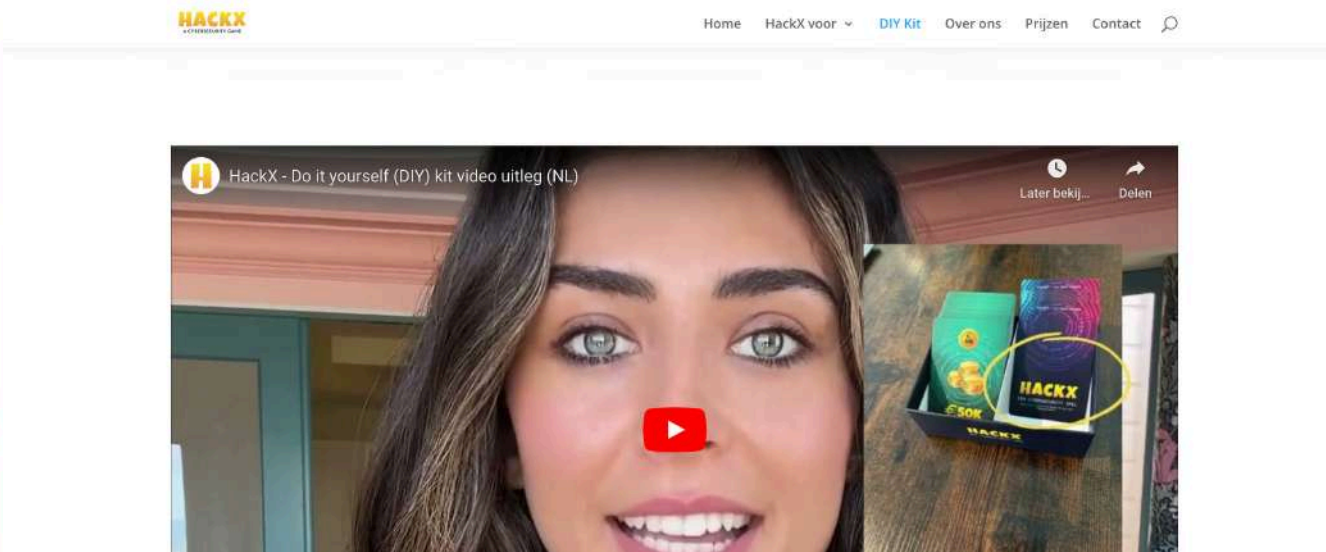
To this ->







# HACKX



## Key take-aways

- Trends: AI (spear)phishing, voice mimicking, deepfakes, extortion or a combination of those.
- Improve training methods with local stories, short captivating content or simple concepts
- People will fall for social engineering techniques, handle them well.



## Questions, discussion & wrap up

