

AI & online fraud

- a double edged sword -

Luca Vlasceanu



Table of contents

- What is cybersecurity ?
- What is AI?
- AI in cybersecurity space
- Self protection in the digital space

What is Cybersecurity?

Cybersecurity = Security against electronic attacks
such cyberwarfare

Common threats

- Phishing attacks
- Malware and ransomware
- Deepfakes
- Data breaches
- Identity theft
- Fake news and disinformation

Importance of Cybersec.

A survey made by NordVPN on Dutch websites found that

5%

understand the risks
of AI in work contexts

23%

can understand how to
securely store passwords

35%

can spot phishing
websites

What is AI?

- AI is a mathematical model that can
 - predict values
 - create clusters
 - take decision based on gathered data
- There are different types of AI models:
 - supervised -> data is labelled and then a decision is made
 - unsupervised -> the model learns from computed clusters
 - large language model (LLM)

Simple linear regression

Primitive AI

K-means algorithm

Primitive AI

In a nutshell

What I have

- pictures
- videos
- data



What can I create

- deepfakes
- targeted phishing
- fake financial schemes

Targeted to seniors

- **Phishing** scams -> Fraudulent emails or messages made to reveal your identity
- **Deepfake** scams -> Fake voices or voices of loved ones to trick victims into urgent financial action
- **Retirement** scams -> Guaranteed returns are offered through fake investment or pension schemes

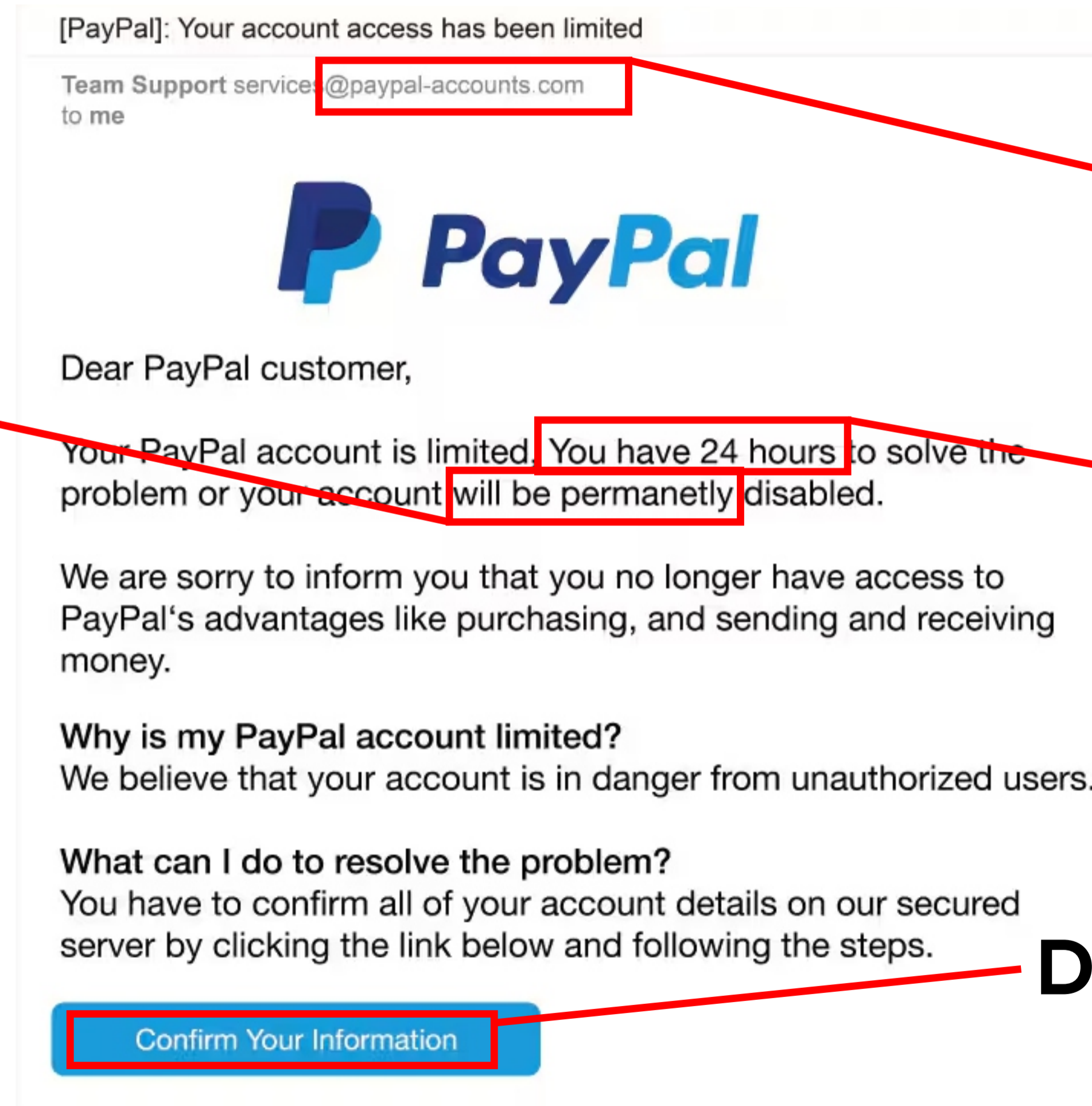
Phishing scam

Grammatical mistakes

Check the email address

Sense of urgency

Do not click !

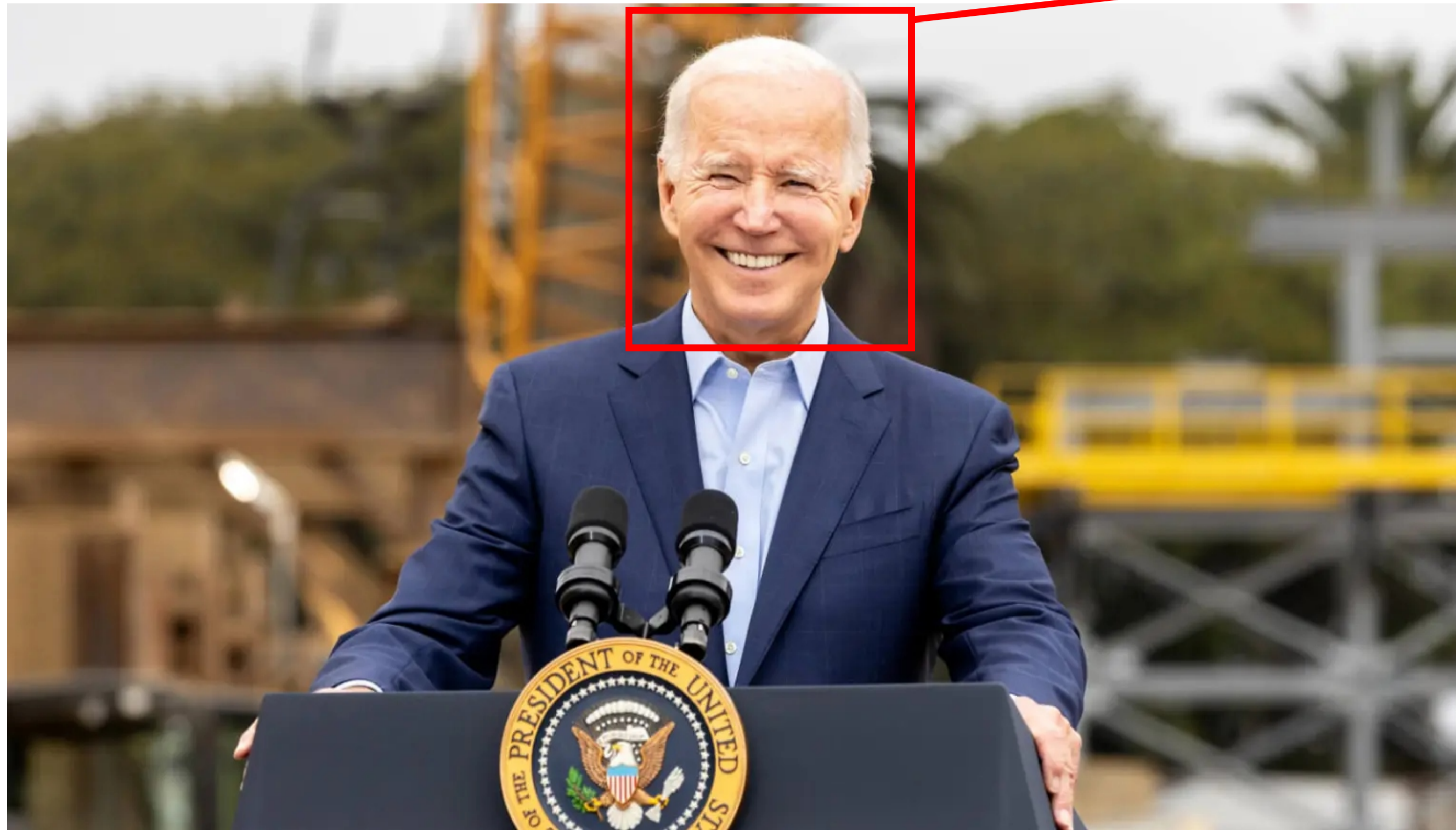


What to do

- Do not click the button !
- Do not download any content !
- Login from the official website !

Deepfake scams

This is not Biden



Do not give him your money !

What to do..seriously

- If someone dear to you is getting cloned, call them
- To not use the "path" attackers show you
- Always double check

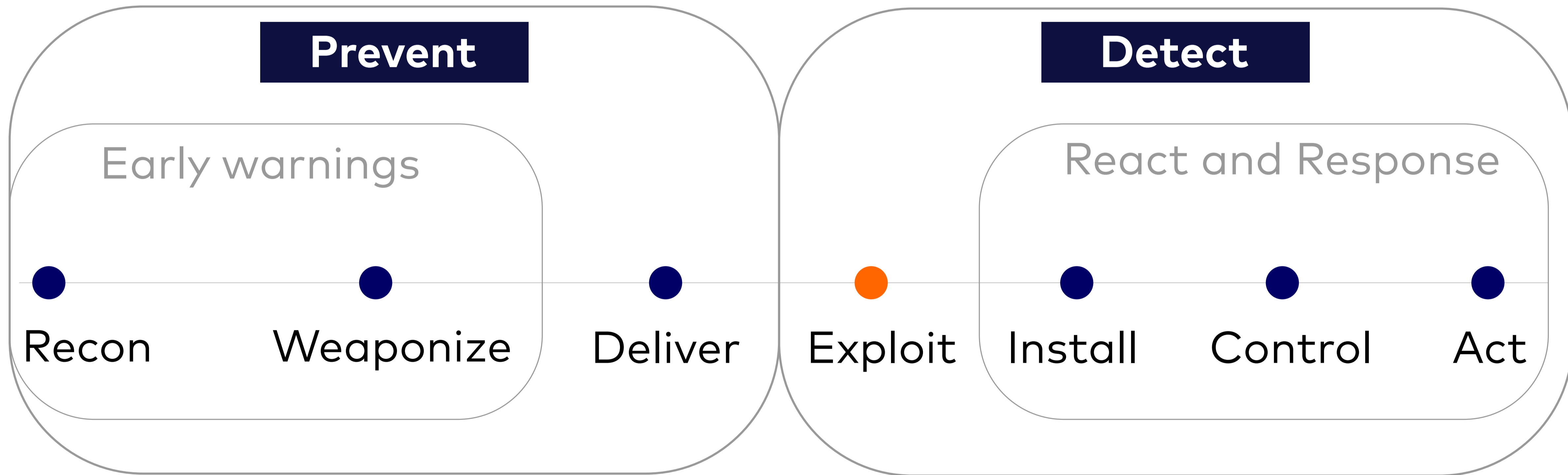
Retirement scams

How can I protect myself?

- Use temporary emails when you can
- Avoid sharing personal data
- Use strong passwords and regularly change them
- Use GDPR to your advantage
- Check for https when browsing

AI in cybersecurity

Cyber kill chain



AI in cybersecurity

Advantages

- Fast detection
- Expert usage alongside AI
- Better flexibility

Challenges

- Unable to maintain autonomy
- Data privacy concerns
- Lack of regulation
- Ethical concerns
- High volume data
- Uniform data encoding

How can we protect seniors?

My solution

1

Web platform

2

AI agent

Bibliography

I'm Luca

Thank you!

