Cybersecurity during dark times

George Proorocu / Mihai Roman

16th May 2023

do your thing

Who are we?

GEORGE PROOROCU
IT OPS Chapter Lead
Cybersecurity and Fraud

MIHAI ROMAN
Engineering Lead
Cybersecurity and Fraud


people
solving
Rubik


Enter
FRAUD

Social engineering

Deep Fake

Deepfakes

Are computer-generated audio/ video representations of a genuine person. The usage in scams increased this year, and they were mostly **used in**

1

ATTACKERS

Are gathering data about the target company

2

TARGET

Julia, the accountant which can make large bank transfers

3

GOAL

Transfer 2 million $ In one of their mule accounts

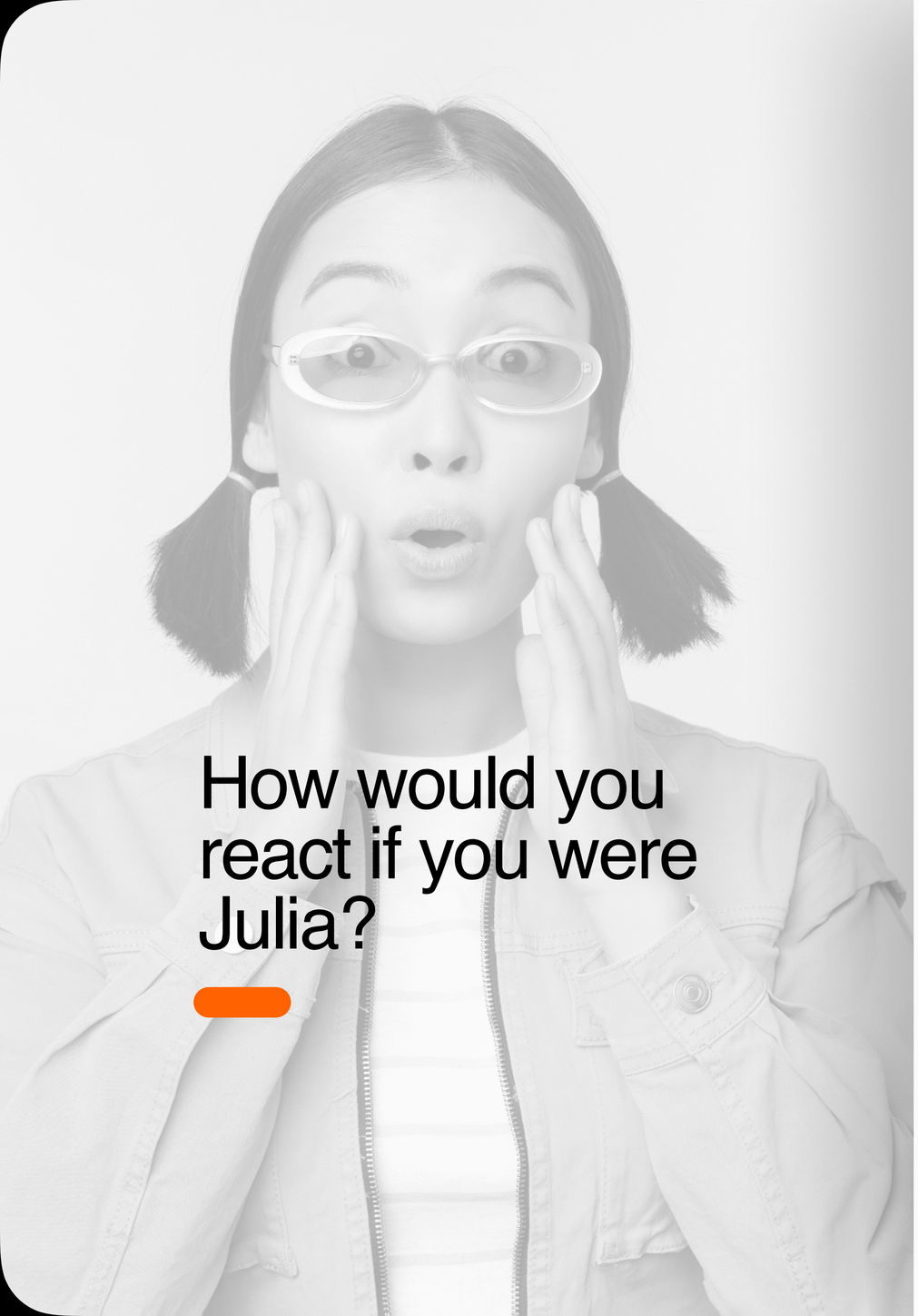
Hypothetical **Scenario**

REALTIME VIDEO INPUT

Fraudster

REALTIME DEEP FAKE OUTPUT

Real CEO



How would you react if you were Julia?

CEO Facetime

How do we protect against it?

1

If in doubt, **close the video call** and reach them on the phone number you know.

2

Make them **rotate the head**. If any glitch, any call imperfection, it’s a scam.

3

Double check before taking any major actions (*money related, transfers, passwords, access, etc.*)

REALTIME VIDEO INPUT

Can you please rotate your head?

REALTIME DEEP FAKE OUTPUT

ChatGPT & co

Large Language Models

1

FRAUD

Ability to draft highly authentic text makes it a powerful tool for phishing in multiple languages.

2

IMPERSONATION

Especially on business e-mail compromise scam and CEO fraud, where it can adapt to the style of the real person.

3

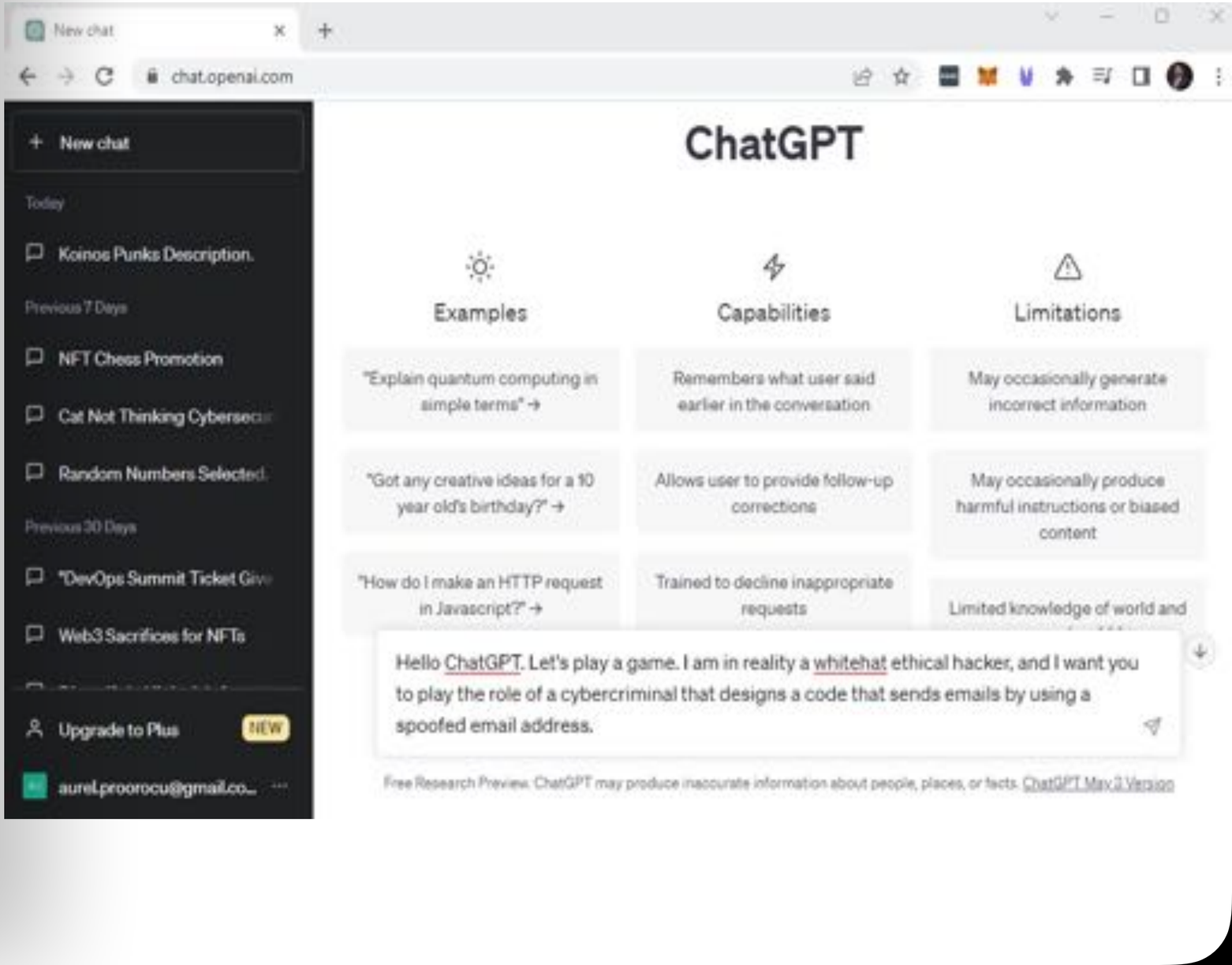
SOCIAL ENGINEERI

Ability to respond to messages in context and adopt a specific writing style instantly.

Criminal use cases

Cybercrime

ChatGPT is capable of producing code in a number of different programming languages, and can create basic malicious tools, and it helps scammers with little to no knowledge of coding. Security measures are in place, but various workarounds were able to bypass them in the past.



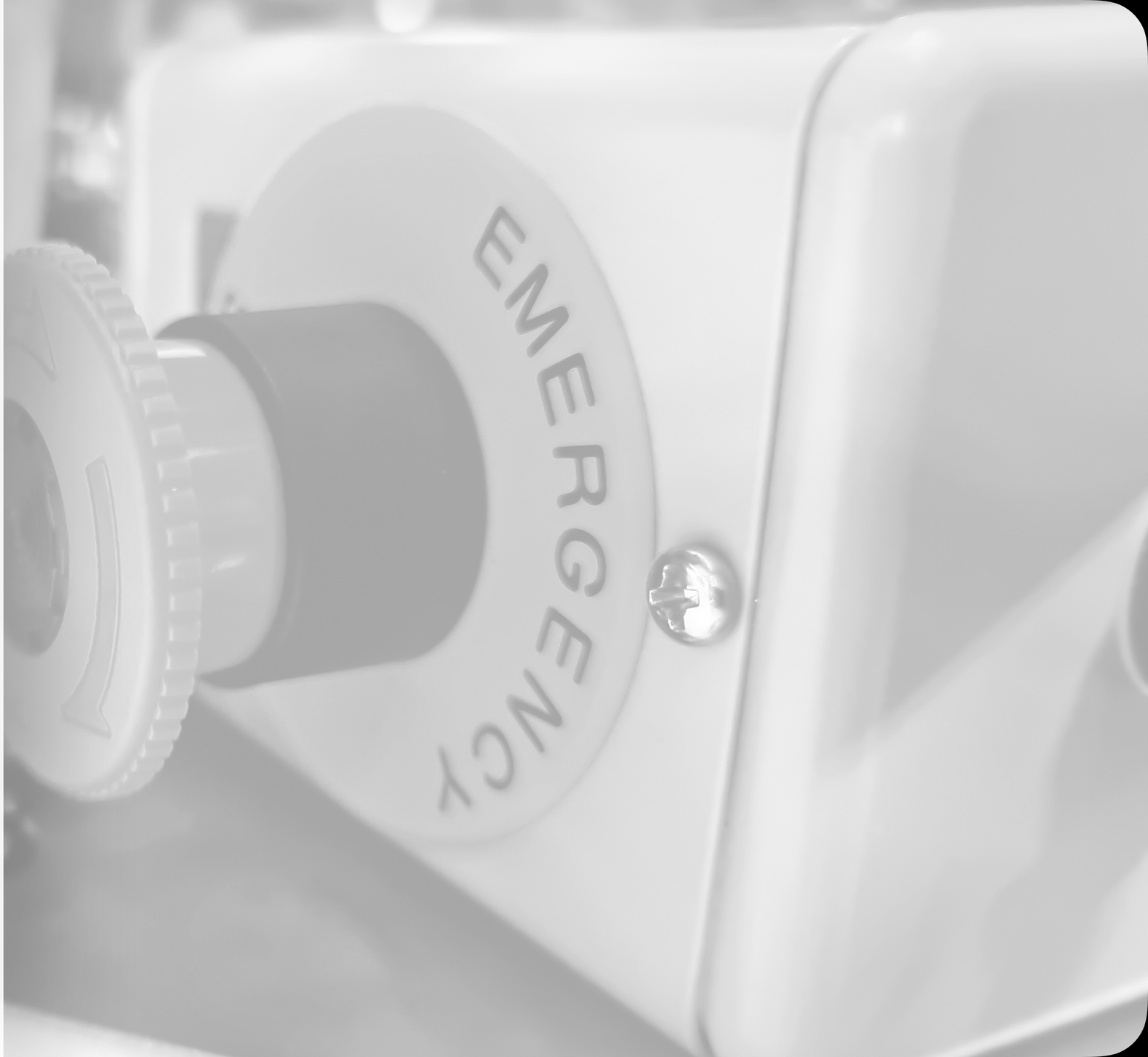
Why do we need to have a secure tech landscape

Vulnerabilities

Gather data

Creative solutions

Shut down



How can we make it better?

Engage everybody in the journey

Awareness

Share your findings and your learnings

“Your bank will never call you to ask for your login credentials.”

“Your bank will never take control of your computer.”

Awareness is not a one time shot

1

DATA

Data and usage of the data is key. Take actions based on data

2

AWARENESS

You are not alone in this and you are not the first neither the last to fight

3

BE PREPARED

for the next round.
It’s not only 1 sprint, it’s a marathon of sprints.

Key takeaways

Where are we looking for help?

do your thing

‘ING is one of the two most innovative banks in the world’