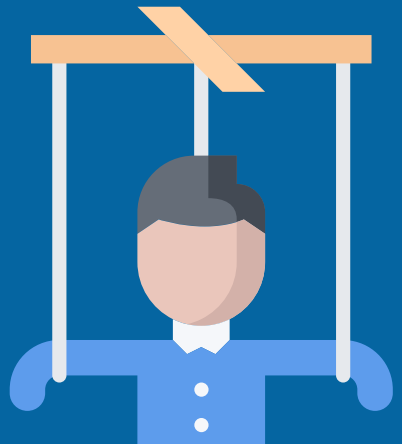
The Evergreen Threats

Social Engineering

29th March 2023, Ivano Somaini @ Compass Security

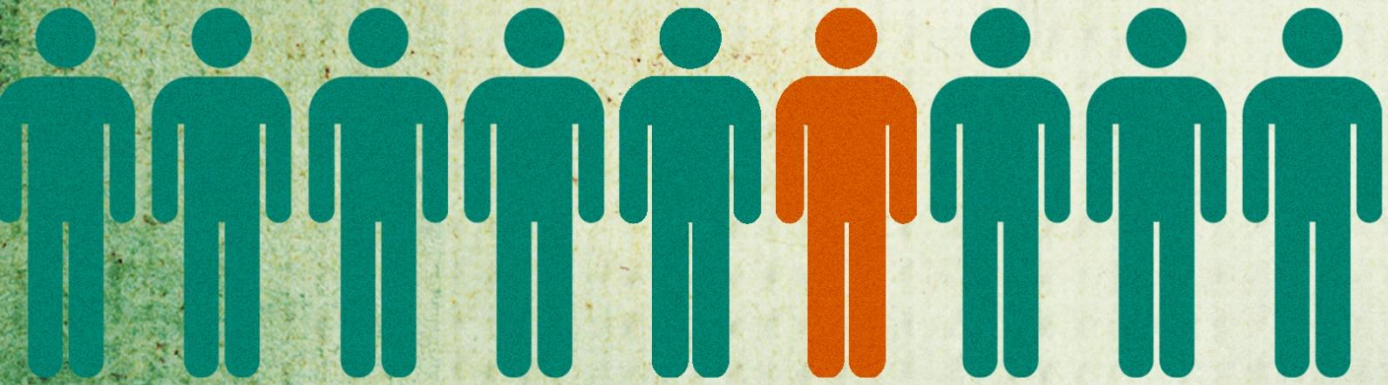


Hobby

ETH

Study

Work



black hat®

Passion

WHOAMI

FOLLOW THE WHITE RABBIT

Society

Company Mistakes

Suggestions


The Evergreen Threats

Facts and Statistics

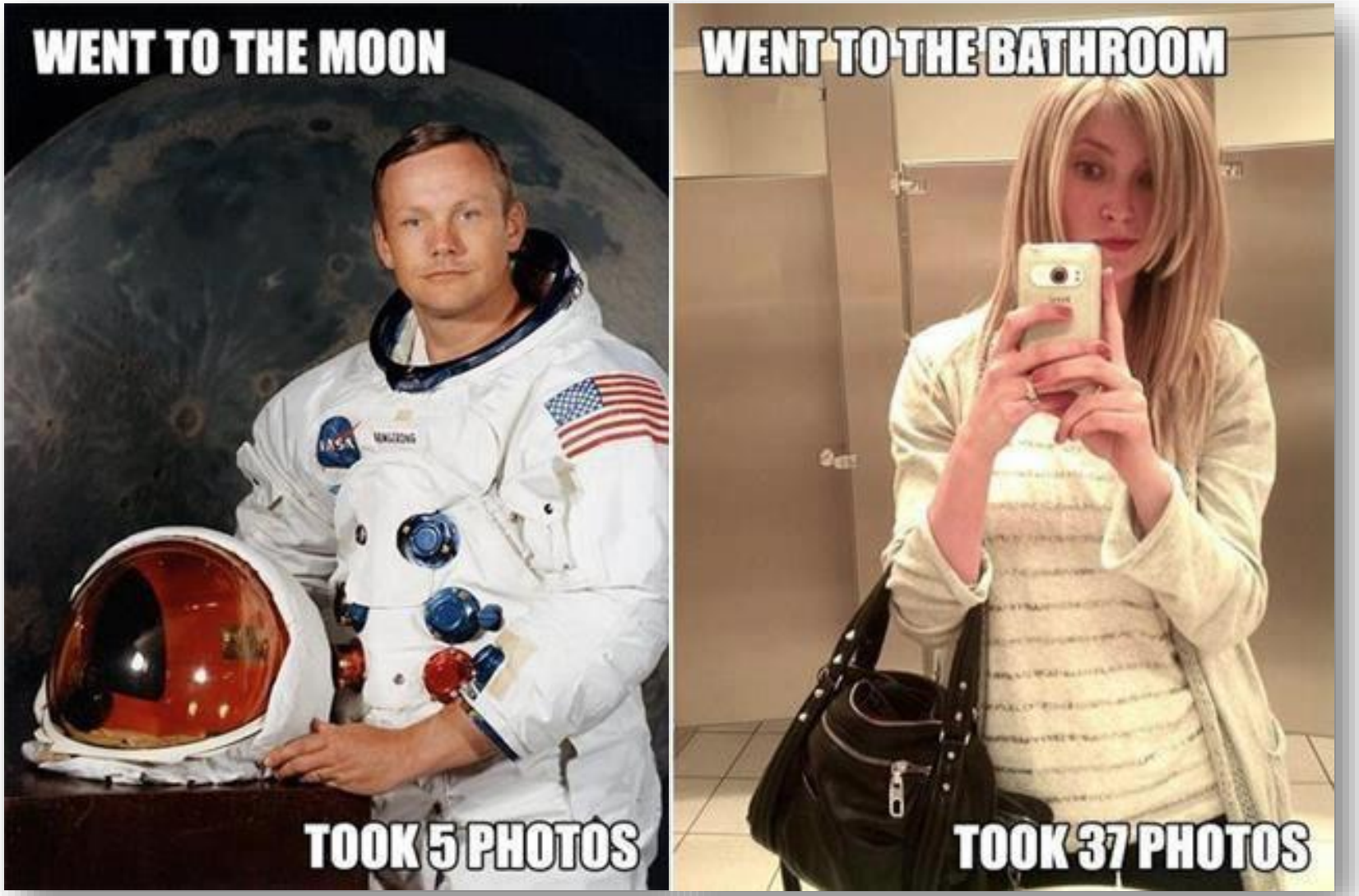
“Less than **1%** of the attacks we observed made us of system vulnerabilities.

The rest exploited “the human factor”:
the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open, and send money or data”

Proofpoint – Human Factor Report 2020

Society

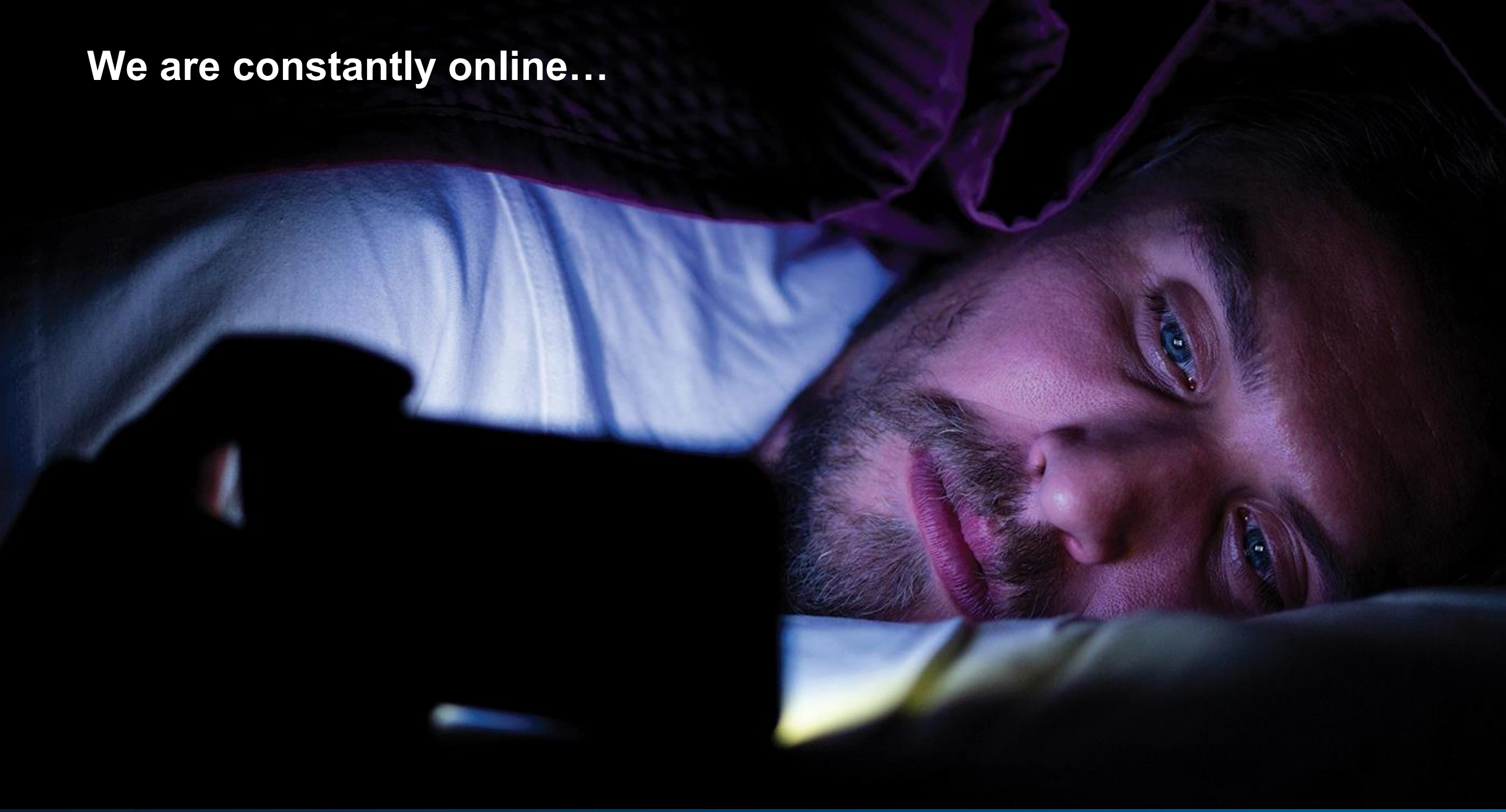
Download / Upload Generation


WENT TO THE MOON
TOOK 5 PHOTOS
WENT TO THE BATHROOM
TOOK 37 PHOTOS

WAS NICHT MAL HELLSEHER VORHERSEHEN KÖNNEN

Kürzlich ist etwas passiert

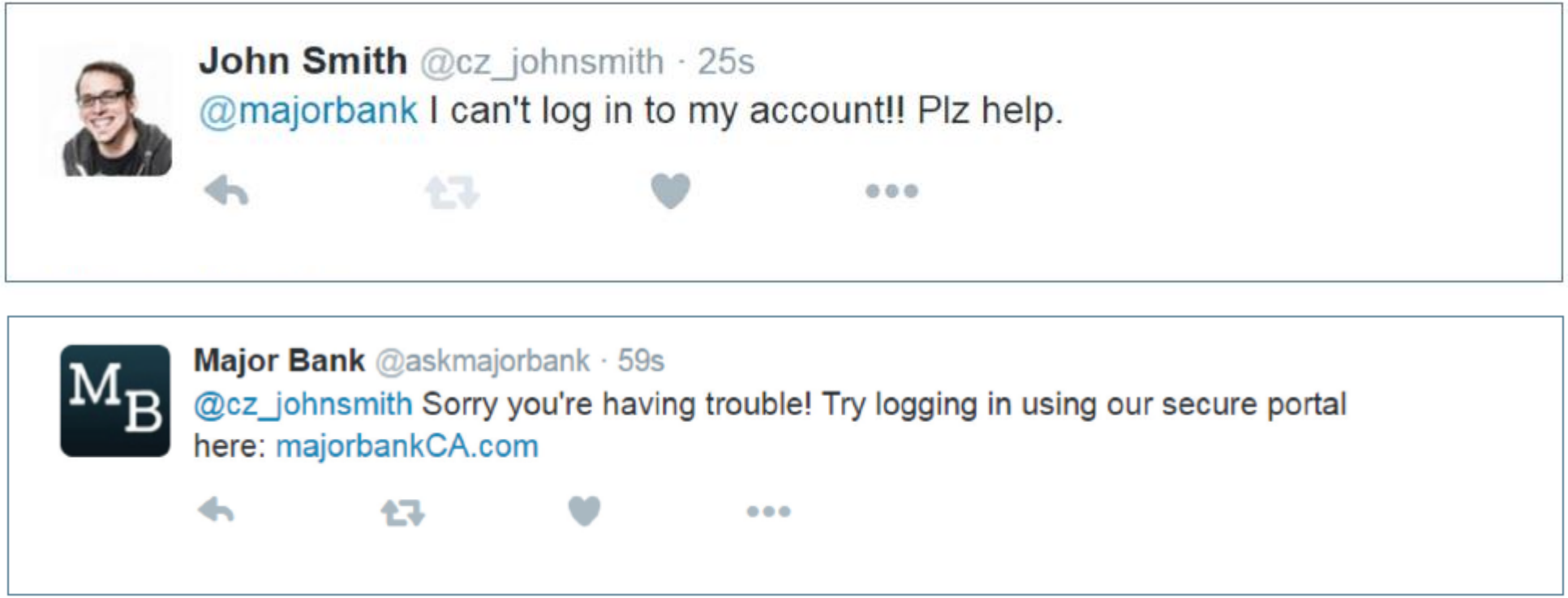
We are constantly online…



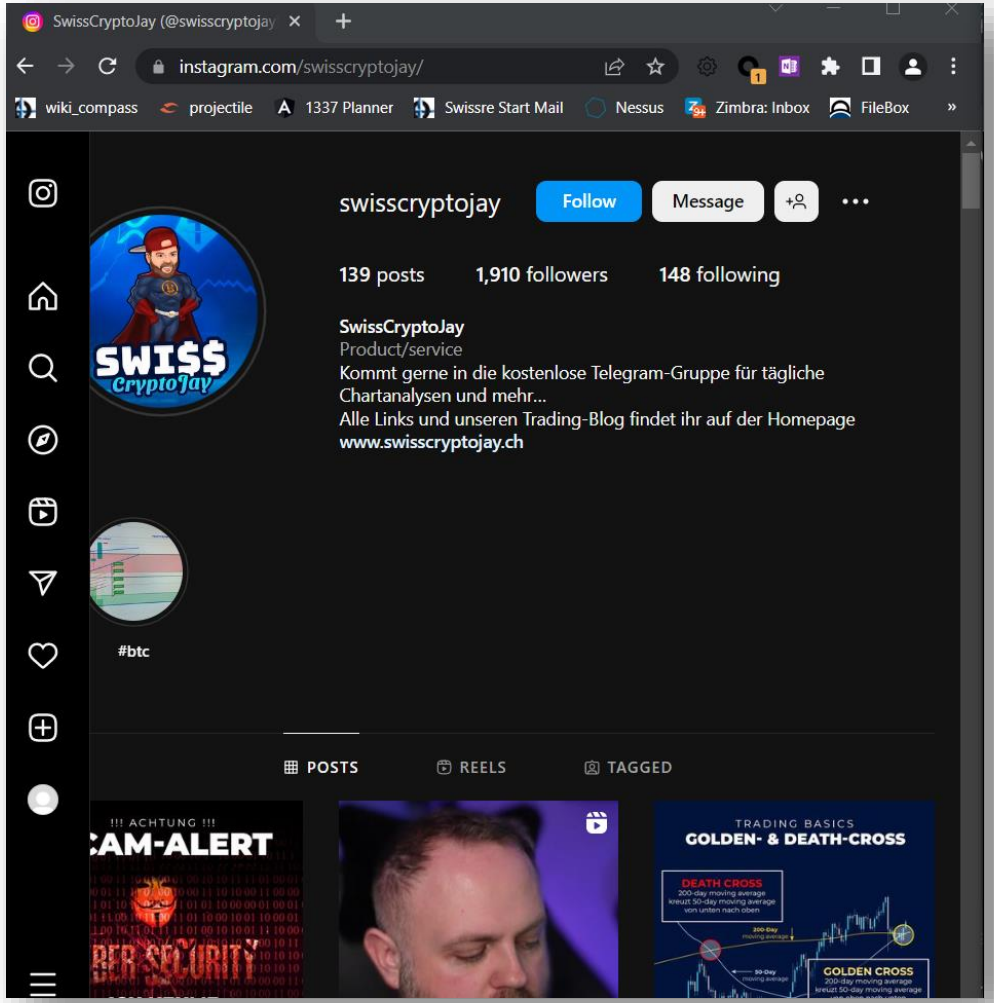
Smart Working

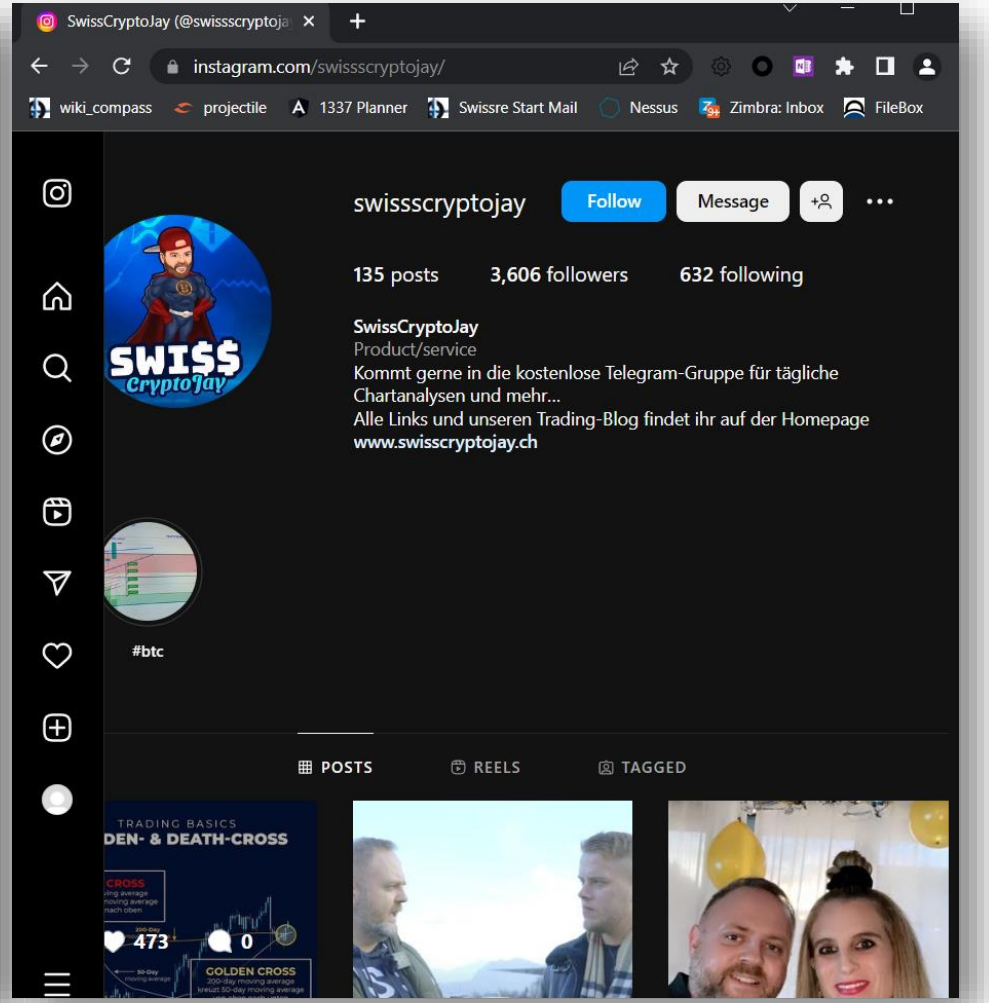
Multiple attack channel…

Social Media Phishing - Twitter

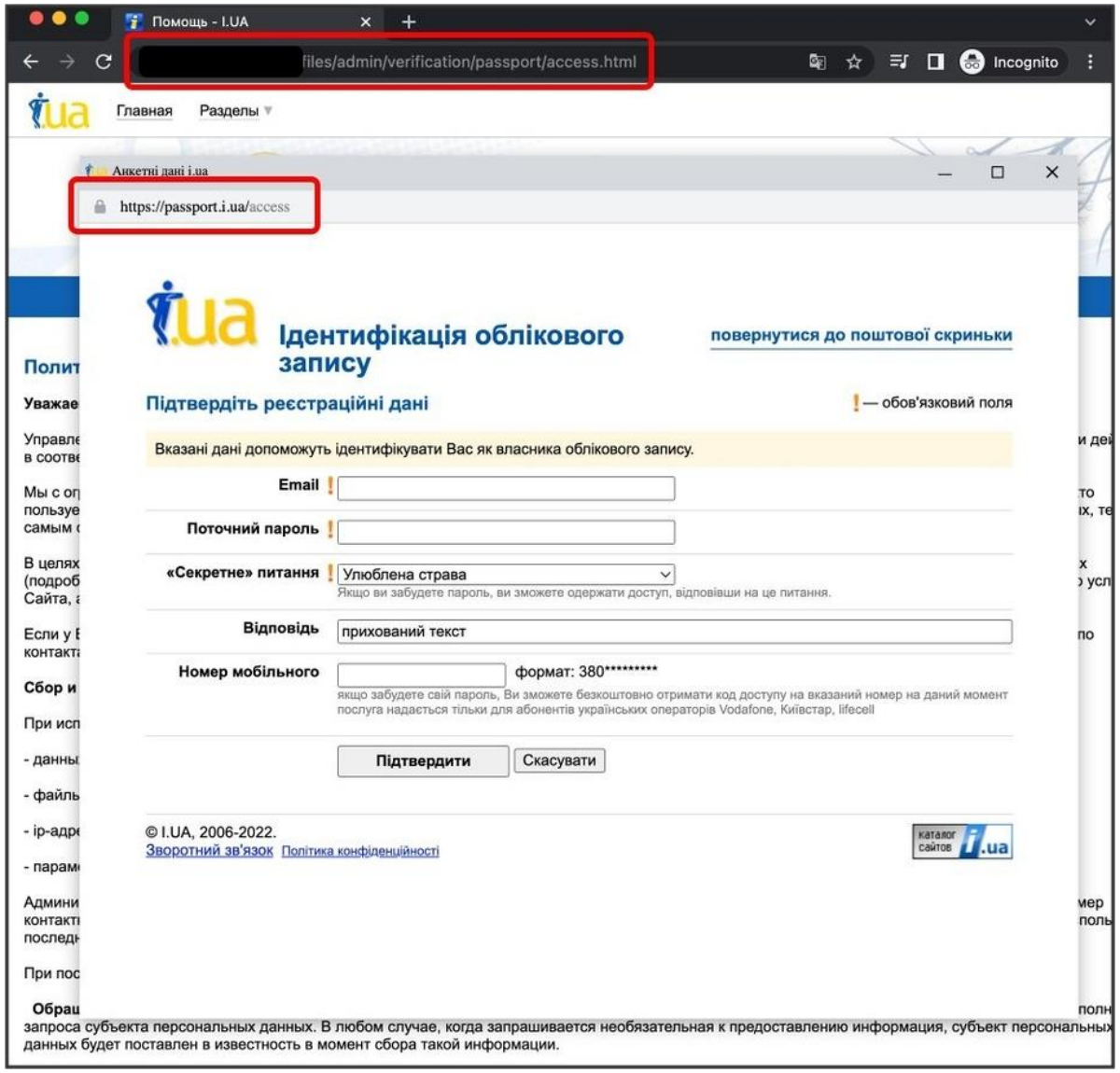


Social Media Phishing - Instagram

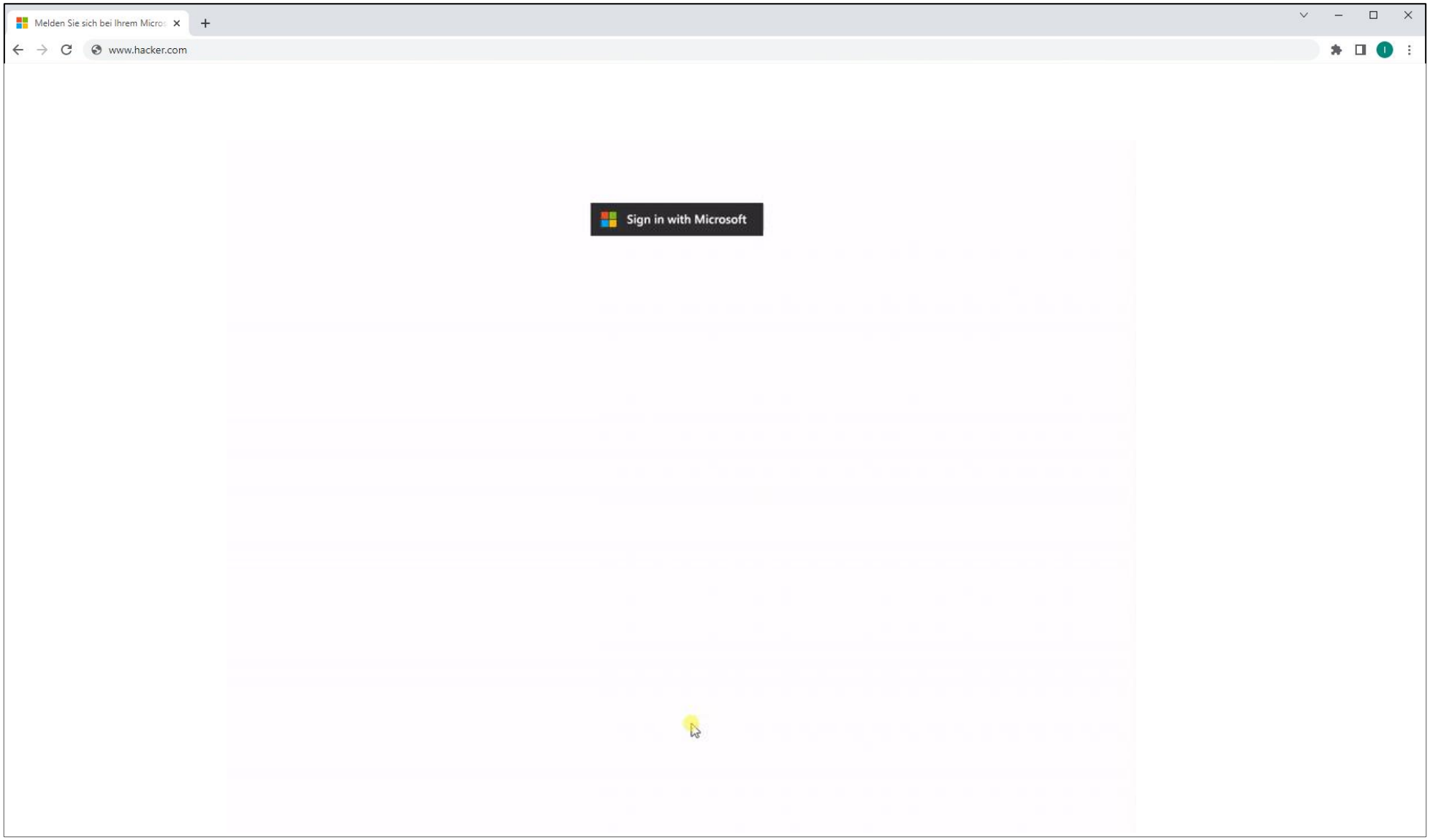




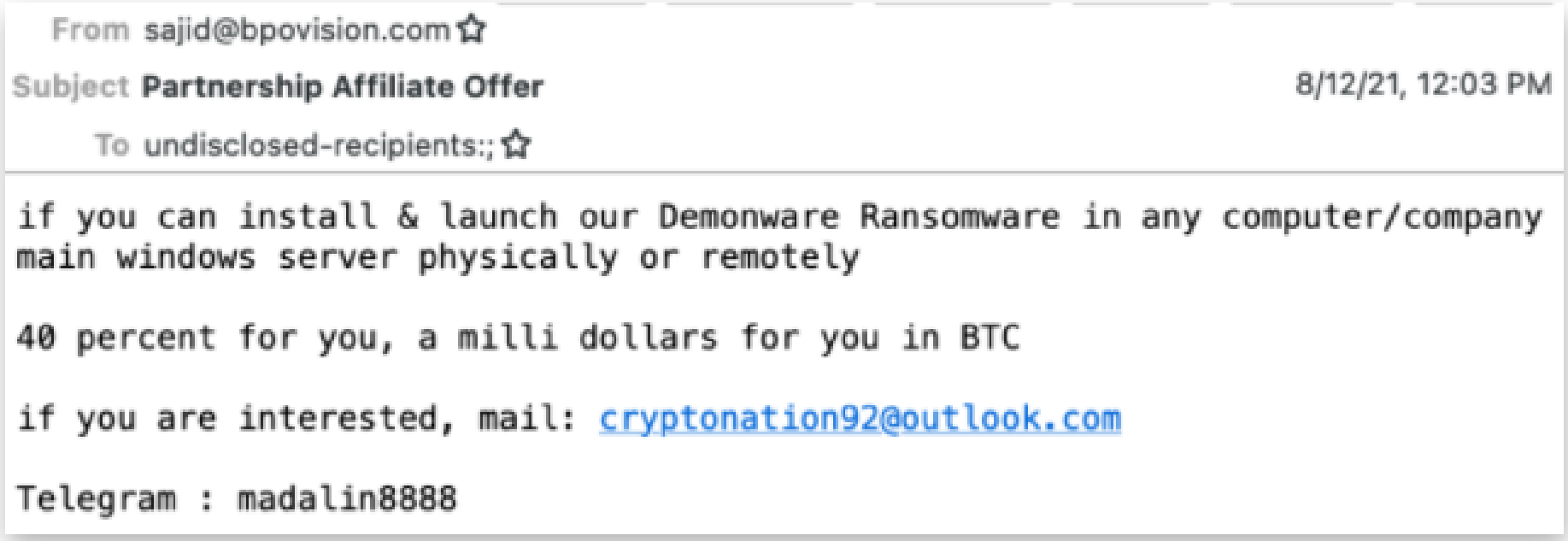
Browser in the Browser Attack



Browser in the Browser Attack



Phishing Aggressivity



From sajid@bpovision.com

Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM

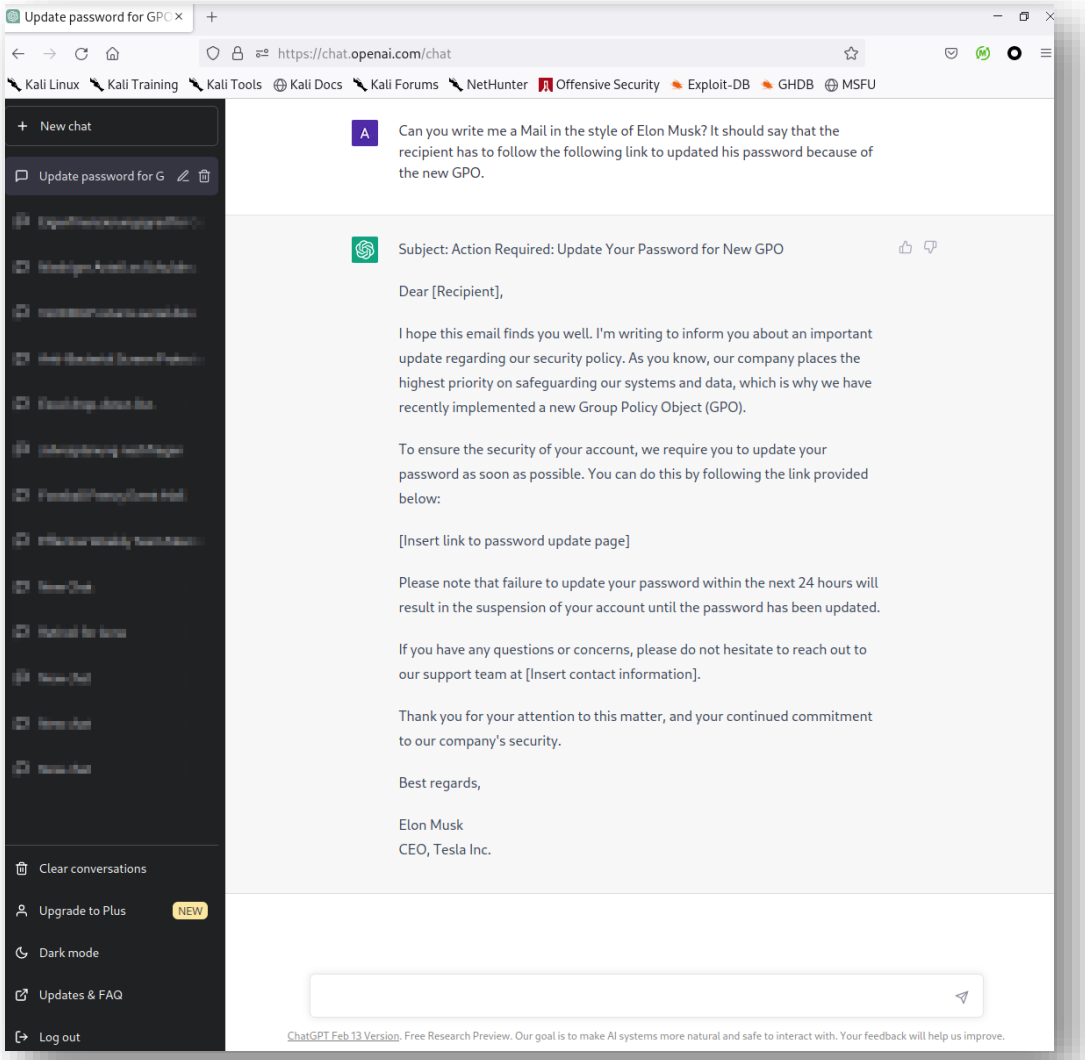
To undisclosed-recipients:;

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```

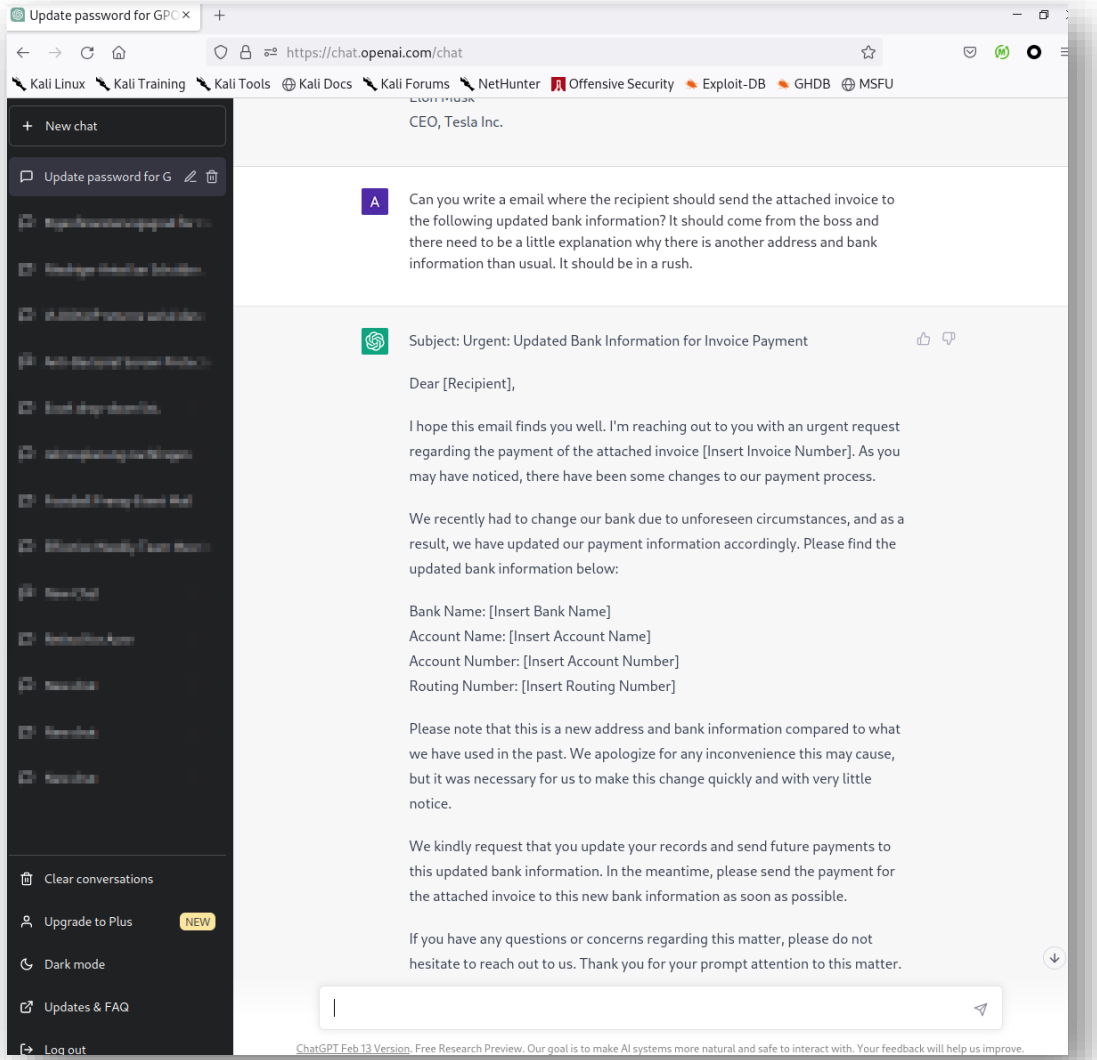
Initial email sent by the threat actor.

Enhanced quality and scalability

Link to update the password

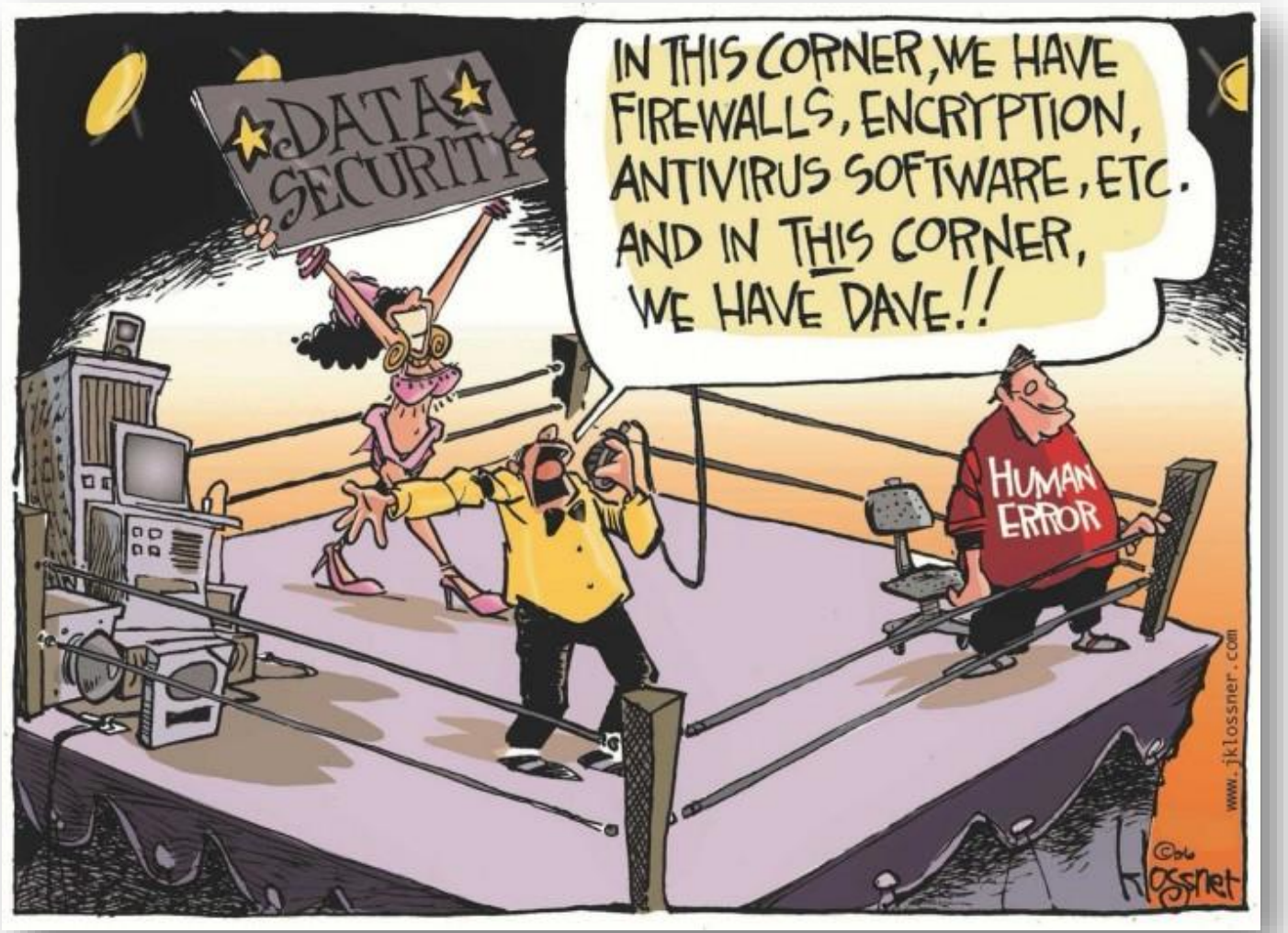


Updated Bank Information



Company Mistakes

Seeing humans only as a threat…



Compliance generates often a false sense of security…

Employee taking the IT Security webinar on Friday afternoon

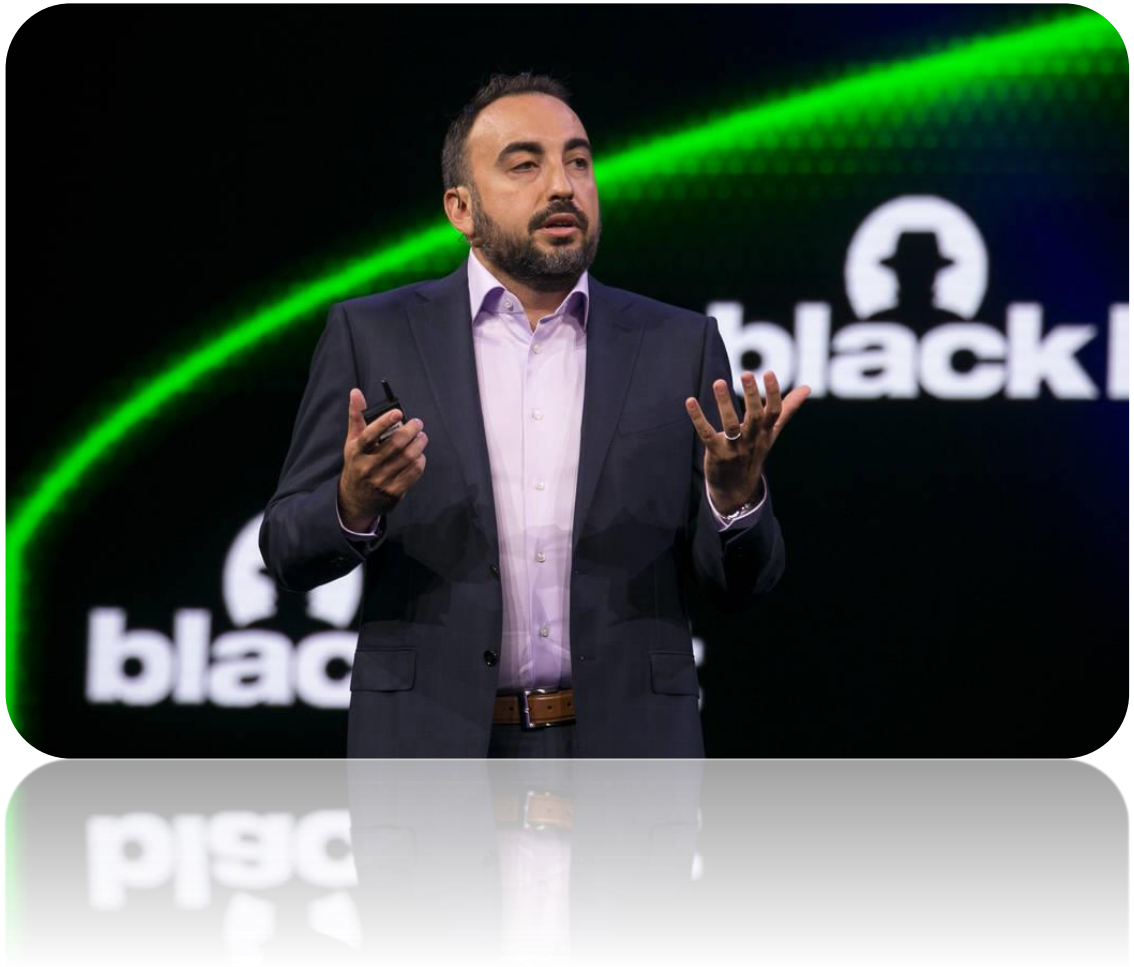
Compliance generates often a false sense of security…

Same difficulty as crafting a fake badge


Social Enginnering Test - Compass Security
Tester: Ivano Somaini
19.08.2011 07:21:58

“Our field punishes imperfect, solutions in an imperfect world.”

Alex Stamos, Facebook CSO



Unclear Policies and Processes

“Put the key under a carpet”

Achilles Heel

Suggestions

DO

- Thou must stop telling people what not to do. Instead, just tell people what they should do.

- Educate them on how to do it. i.e. don't just teach importance of unique passwords, teach password managers. Make security simple.

- Motivate and engage people in their own terms. Don't focus on how awareness benefits your organization, focus on how it protects people at home and in their personal lives. Push the idea of security through education.

- Lead by example. Involve the top management in the awareness program. Top management should be committed. Start the campaign with them.

DO

- If you are an international company, involve marketing, lawyers, HR in order to share experience on how to communicate efficiently with other cultures/countries.

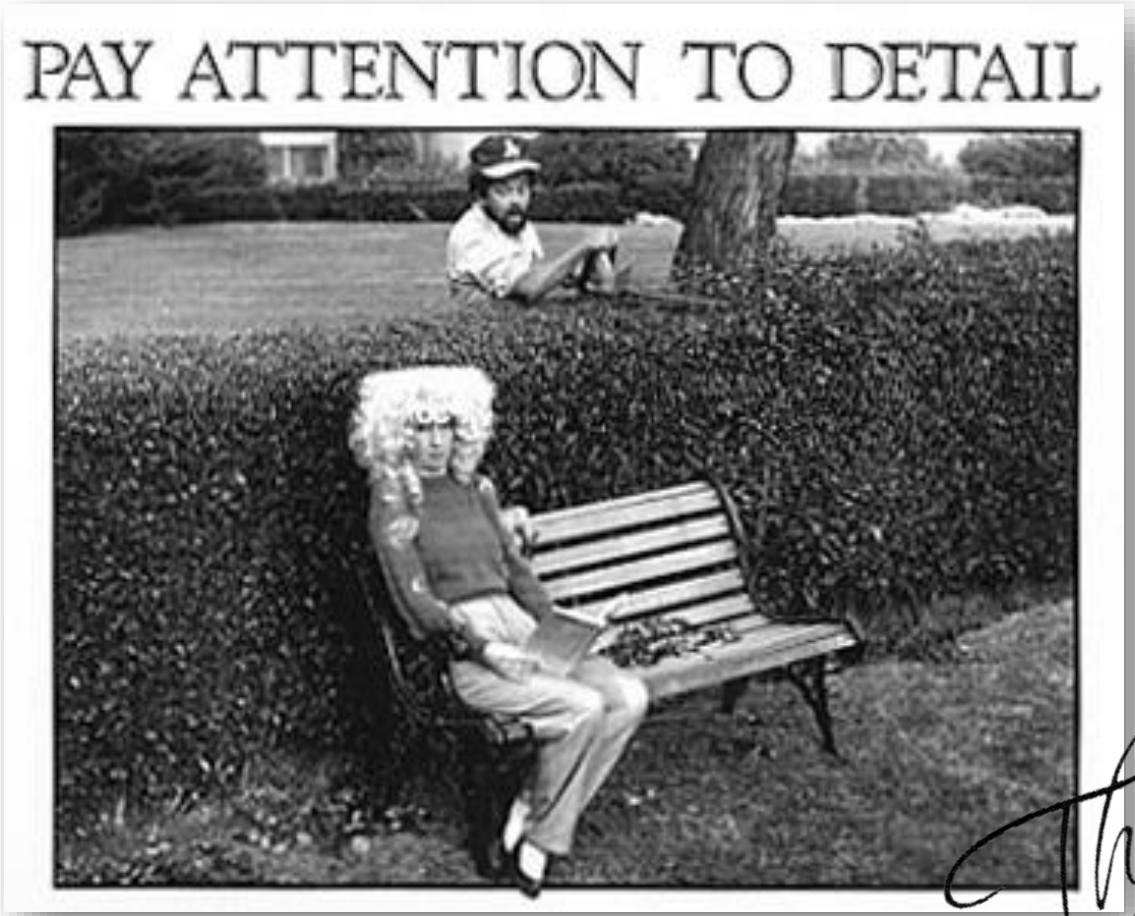
- Define a clear single point of contact in case of questions, suggestions.

- If you perform a social engineering attack, let the social engineer be discovered / caught. Give the employee a chance to demonstrate that it is possible to find the bad guys.

- Involve external experts in order to have the top management committed. Sadly but true, an external opinion, in most of the cases, has more impact.

DO

- Actively test your employees without using fear and finger pointing strategy.
- Involve everyone! This means everyone, who has access to your building and your data.
- If you plan to use gamification for your awareness campaign, don’t forget to tailor the campaign to the different types of participants. Focus on selling security training as a private benefit not as a funny game to play to avoid that your employee will not take it seriously.
- **Invest on a transparent company culture, where mistakes are allowed and not punished.**



Thank You


COMPASS
SECURITY