

# **Socijalni inženjering**

# Definicija

- Socijalni inženjering predstavlja tehniku manipulacije ljudima koja se zasniva na ljudskoj nepažnji ili neznanju.
- Cilj napadača uglavnom nije žrtva sama, već neki resursi koji su napadaču interesantni
- čovek najslabija karika u lancu bezbednosti informacionog sistema
- Radionica će obuhvatiti stvari koje ne uključuje definicija

A man with long brown hair, a full beard, and glasses is sitting on a brown couch. He is wearing a red and black plaid shirt over a grey button-down shirt. He is holding a small yellow card in his right hand. The background is dark and out of focus, with a lamp visible on the left.

**It's barely social engineering.**

**It's more like natural selection.**

# Kevin Mitnik

Knjige:

- Umetnost prevare
- Umeće provale
- Ghost in the wires



# Viktor Lustig



# Deca



# Neke tehnike socijalnih inzinjera

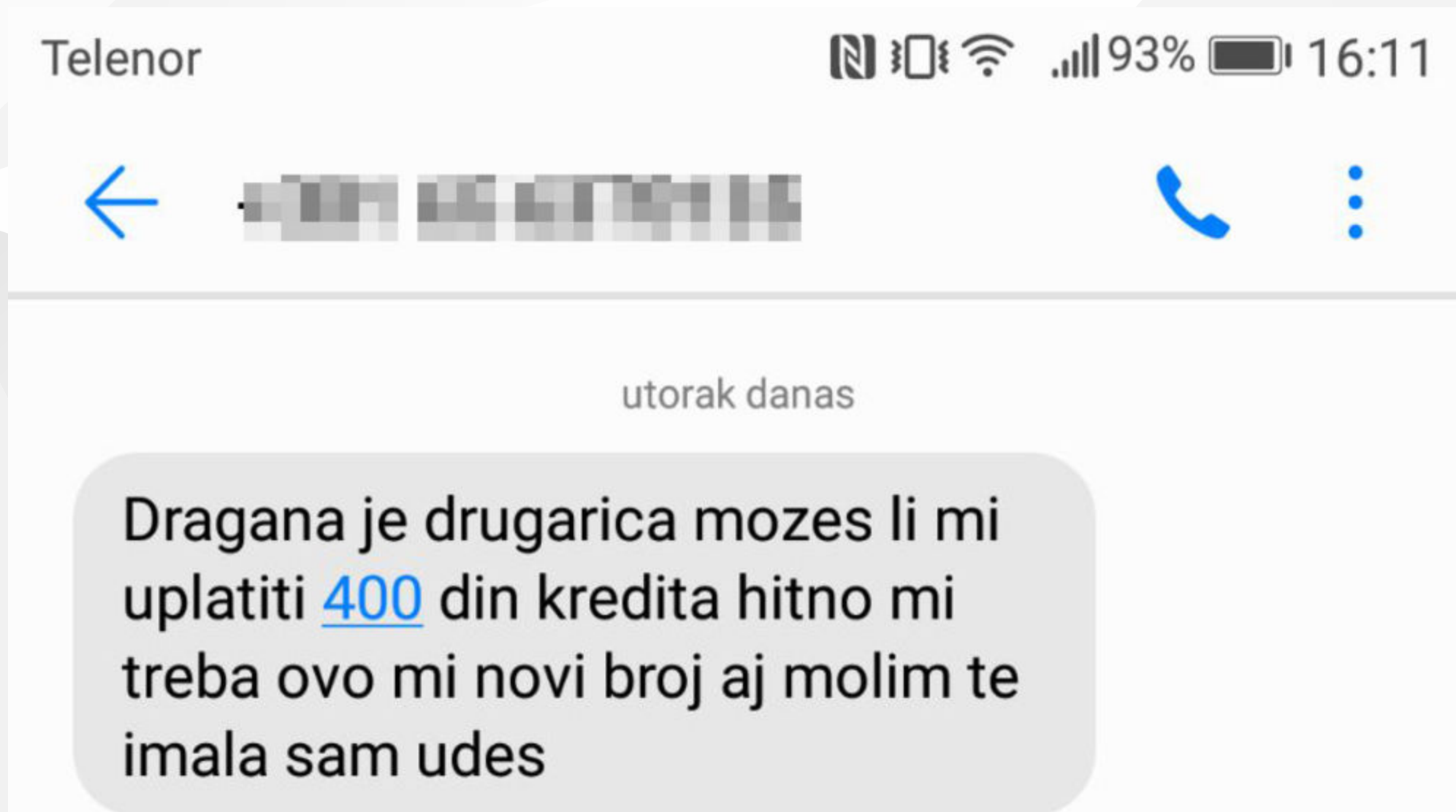
- Kopanje po kontejneru (Dumpster diving)
- Shoulder surfing
- Impersonation
- Maliciozne kopije sajtova





## Fišing (Spear-phishing and Whaling)

# Smishing



# Vishing



# Baiting

- Postavljanje klopke
- "Izgubljeni fleš", CD, DVD
- Preuzimanje zaraženih fajlova sa interneta
- Bluetooth

# Tailgating (Uhođenje)

- Pristup prostorijama za koje nema dozvolu
- Ući sa grupom, sa nekim ko ima dozvolu
- Duvan je štetan za bezbednost firme
- Drugacije oblačenje (glumiti zauzetost)
- Pozajmljivanje uređaja

# Psihologija

- Facijalna ekspresija
- Govor tela
  - [Bombards body language](#)
- Emotional hijacking
- Misdirection
- => Neurolingvističko hakovanje

# Psihologija

- Pretexting (izmišljanje scenarija)
- Quid pro quo (usluga za uslugu)
- Poverenje
- Želju osoba da nekom pomognu
- Želju za odredjenom materijalnom ili nematerijalnom koristi
- Znatiželju
- Strah od nepoznatog
- Strah od gubitka
- Nemarnost



*What's your Royal Guest name?*

TITLE.....Lord or Lady  
FIRST NAME.....Grandparent's name  
SURNAME.....Your first pet's name  
OF.....Street name



# Google-fu



# Napredne tehnike pretrage

- Najmoćniji alat
- [Napredni g<sup>u</sup>gl](#)
- site:
- type:
- -tekst , isključuje rezultate koji sadrže tekst nakon -
- allinurl: allintitle: allintext:

# Maltego

- Vizuelizacija povezanosti izmedju razlicitih informacija
- <https://www.maltego.com/> (Postoji vec u Kali Linuksu)
- Novi graf (ctrl+T)
- Domen -> DNS from Domain

# Recon-NG

- <https://github.com/lanmaster53/recon-ng>
- `./recon-ng --no-check`
- `workspaces add target.com`
- `show modules`
- `use netcraft`
- `run`

# MAN EDITS A WIKIPEDIA PAGE TO GET BACKSTAGE FOR A SHOW



**Peking Duk**

Musician/Band · 138,010 Likes · 21 hrs ·



Liked



last night someone edited our wikipedia page to say he was our family. showed security at our show, got into the green room and had a beer with the boys.. Spargo you legend

8,822 Likes · 918 Comments · 210 Shares



3,463 people like this.




80 shares



Write a comment...



**David Duey Spargo** Thanks for the evening lads.

Like · Reply ·  716 · about an hour ago



# Targeting

- Prikupljanje informacija je ključno
- Presonalizovanje napada
- Alati:
  - SET (Social Engineering Toolkit)
  - Cupp
  - Cewl
  - Shodan
  - Scythe
  - Creepy

# SET (Social Engineering Toolkit)

- <https://github.com/trustedsec/social-engineer-toolkit>
- tinyurl
- kopija gugla

# Cupp

- <https://github.com/Mebus/cupp>
- Common user passwords profiler
- Generate dictionary for dictionary attack
- Odgovaranjem na pitanja formira se personalizovan rečnik
- `./cupp.py -l`
- `./cupp.py -i`



# Cewl

- <https://github.com/digininja/CeWL>

```
./cewl.rb --write output.txt --email --email_file email.txt --  
verbose https://www.website.org/
```

# Shodan

- <https://www.shodan.io/>
- Libre tekstovi ([tekst 1](#), [tekst 2](#))
- Registracija
- explore
- webcamXP

# Scythe

- <https://github.com/ChrisJohnRiley/Scythe>
- accountfile.txt
- ```
./scythe.py --category social --summary --output output.txt
```

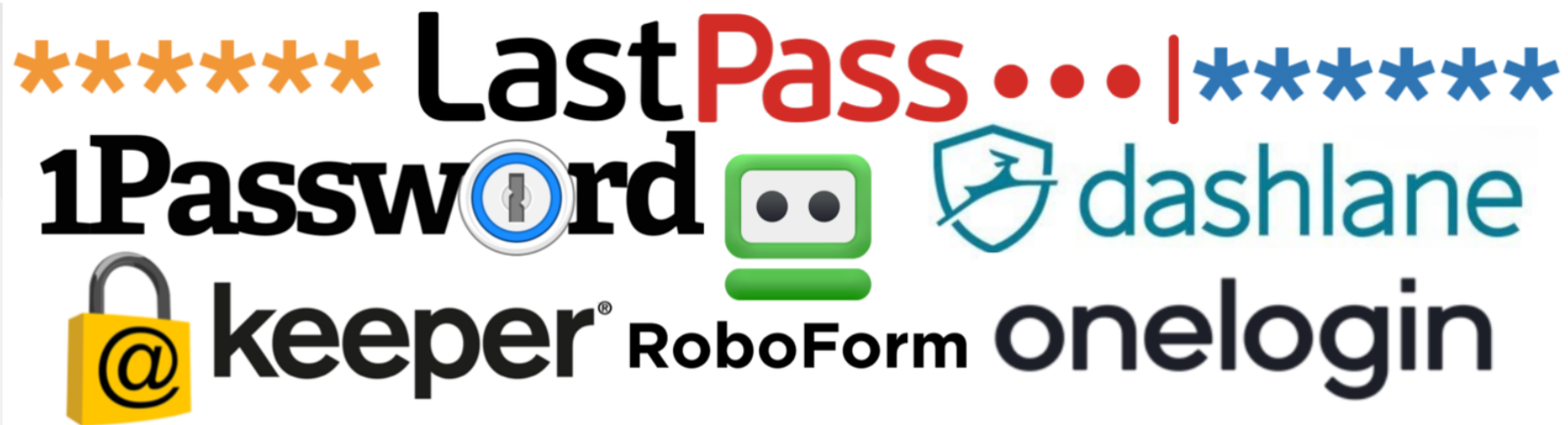
# Creepy

- <https://github.com/ChrisJohnRiley/Scythe>
- Potreban je tviter nalog

# Zaštita:

- Edukacija na prvom mestu
- [!;--have i been pwned?](#)
- Dvostepena autentifikacija
- Smanjite digitalni otisak
- Pazite koje informacije odajete
- Ako vas neko požuruje - nije dobro

# Zaštita: jake šifre i menadžeri za šifre



# Zanimljivi video snimci

- [The art of misdirection | Apollo Robbins](#)
- [Primer vishing-a](#)