

---

# Sajber pretnje i veb bezbednost

## Socijalni inženjering (SE)

*Univerzitet u Beogradu, Elektrotehnički fakultet  
utorak, 13. oktobar 2015.*

**Obeležavane “Evropskog meseca sajber bezbednosti “**

*Doc dr Igor Franc*

## Sadržaj:

- CIA trojstvo
- Ko nas zapravo napada?
- Socijalni inženjering - tehnike
- Kako se zaštititi?
- Dva primera iz prakse – Srbija
- Dva vodeća svetska stručnjaka iz SE oblasti
- Social Engineer Toolkit
- Serija u vezi sa tehnikama SE –Mr Robot
- Zaključak





**WHITE HAT**



**GRAY HAT**



**BLACK HAT**

# WANTED BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

## EVGENIY MIKHAILOVICH BOGACHEV



Multimedia: Images

Aliases:  
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

### DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	Hair:	Brown (usually shaves his head)
Height:	Approximately 5'9"	Eyes:	Brown
Weight:	Approximately 180 pounds	Sex:	Male
NCIC:	W890989955	Race:	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

# FBI lista sajber kriminalaca

- War dialing
- War driving
- Phishing
- Dumpster diving
- Shoulder surfing
- Eavesdropping
- Tailgating
- Impersonation
- Road apple
- Mail prevare



# War dialing



- Tehnika pronalaženja uređaja povezanih na internet
- Zastarela od kada se ne koriste modemi

# War driving / walking



- Tehnika koja je vrlo popularna u današnje vreme
- Vožnja autom sa posebnom opremom radi beleženja wi-fi mreža

# Phishing



- Phishing ili u prevodu pecanje jeste upravo to
- Prevara korisnika da bi se došlo do šifri, PIN brojeva i slično

# Dumpster diving



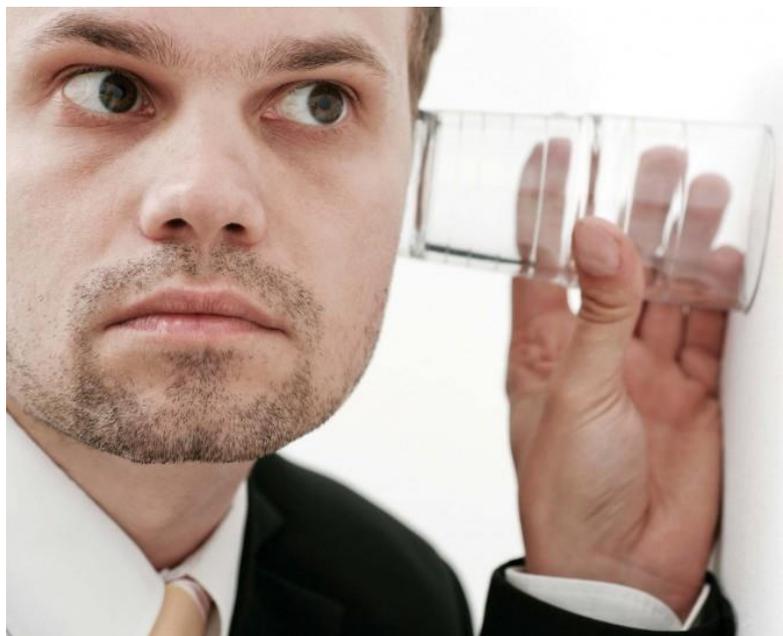
- Preturanje po kontejnerima kako bi se našlo nešto od koristi
- Uglavnom se radi o traženju papira, diskova, fascikli, uputstava i slično

# Shoulder surfing



- Gledanje preko ramena kako bi se videlo nešto korisno
- Uglavnom korisničko ime, šifra, nešto na monitoru...

# Eavesdropping



- Prisluškivanje ali se ne misli samo na obično već i na prisluškivanje prenosa podataka – Wireshark...

# Tailgating



- Tehnika koja ima za cilj neovlašćen ulazak
- Bazira se na: pridrži mi vrata molim te...

# Impersonation



- Prerušavanje u nekog drugog (rukovodioca, novog radnika)
- Ovde se uglavnom radi o navođenju čoveka na neku akciju

# Road apple



- Tehnika koja se bazira na neupućenosti ili nepažnji
- Na parkingu firme ostavljen USB koji zaposleni uzima...



- HOAX – prevare (uglavnom su bezopasne)
- SPAM – nepoželjna pošta

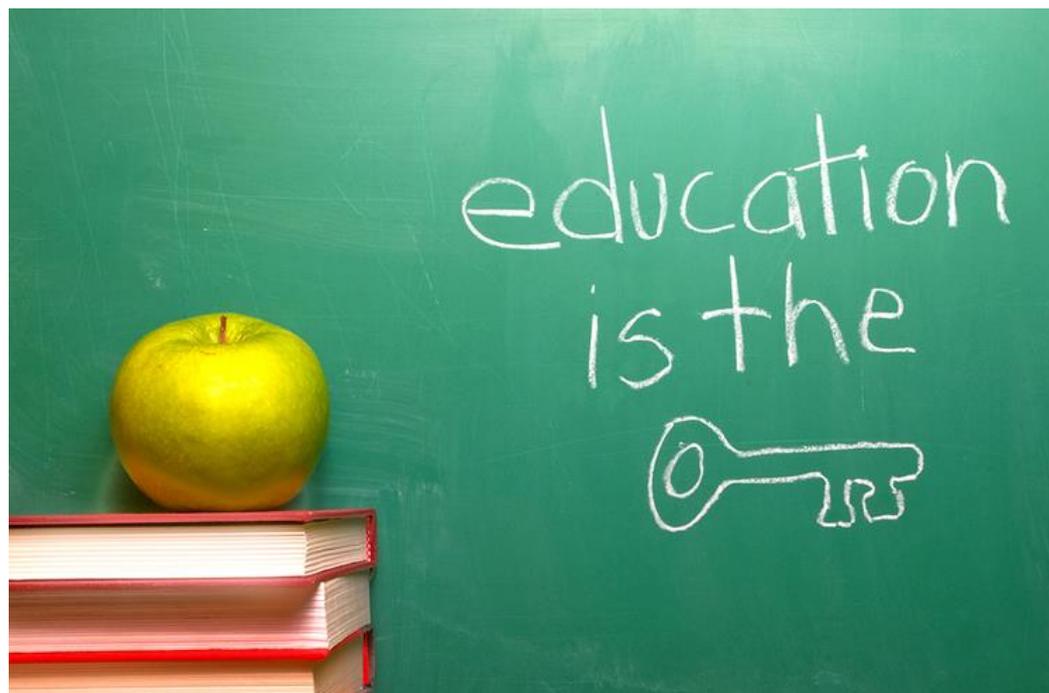
# SE na društvenim mrežama



- Tehnika novijeg datuma koja se bazira na prikupljanju informacija putem društvenih mreža
- Vodite računa kakve podatke i slike stavljate na mreže a pogotovu slike porodice ili dece
- Na žalost slučaj male Maše koji se na svu sreću dobro završio to dokazuje <http://www.dnevnik.rs/drustvo/fotke-dece-i-porodice-nisu-za-internet>

## Kako se zaštititi?

- Edukacija korisnika
- Redovni backup podataka
- Pravilno uništavanje podataka



- Najefikasnija mera zaštite od svih vrsta pretnji
- Treba je kontinualno obavljati a na periodično



- Redovno praviti rezervne kopije bitnih podataka
- System Restore – ne vraća lične podatke i nije zamena



- Pravilno uništavanje podataka je bitno

## Primer iz prakse 1



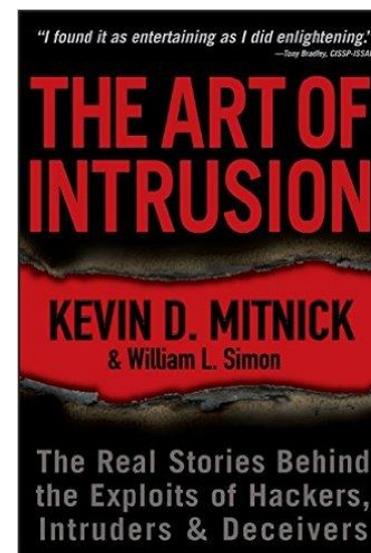
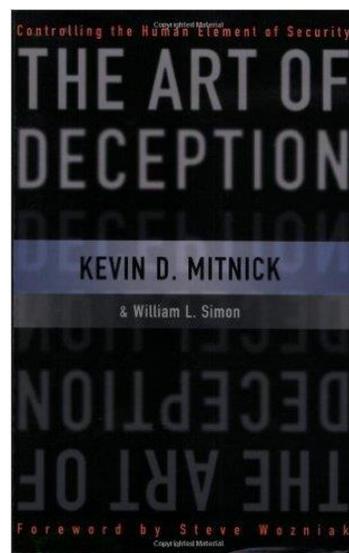
- Naručeno je 3 tone pasulja iz Kameruna
- Vrednost pošiljke je oko 28.000€
- Dodatni troškovi zbog angažovanja advokata 2.600€

## Primer iz prakse 2



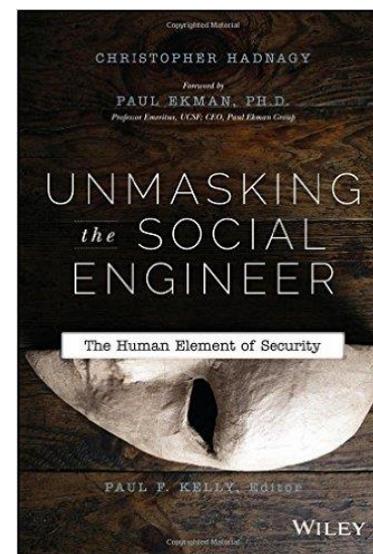
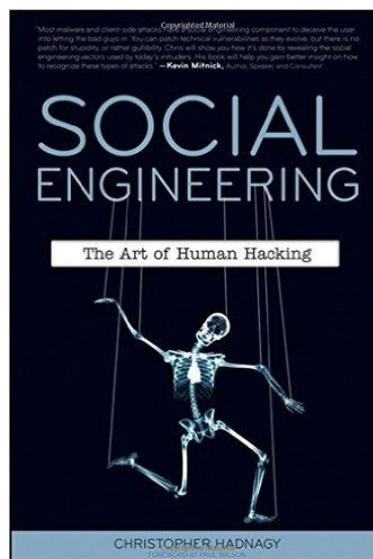
- Naručeno je više stotina vodomera iz Kine
- Vrednost pošiljke je oko 40.000€
- Vec dve godine traje sudski proces

# Kevin D. Mitnick



- Pionir socijalnog inženjeringa
- [Sajt njegove firme](#)

# Christopher Hadnagy



- Jedan od najvećih stručnjaka u ovoj oblasti
- [Njegov sajt](#)

# Social Engineer Toolkit



The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Metasploit Framework
- 5) Update the Social-Engineer Toolkit
- 6) Update SET configuration
- 7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

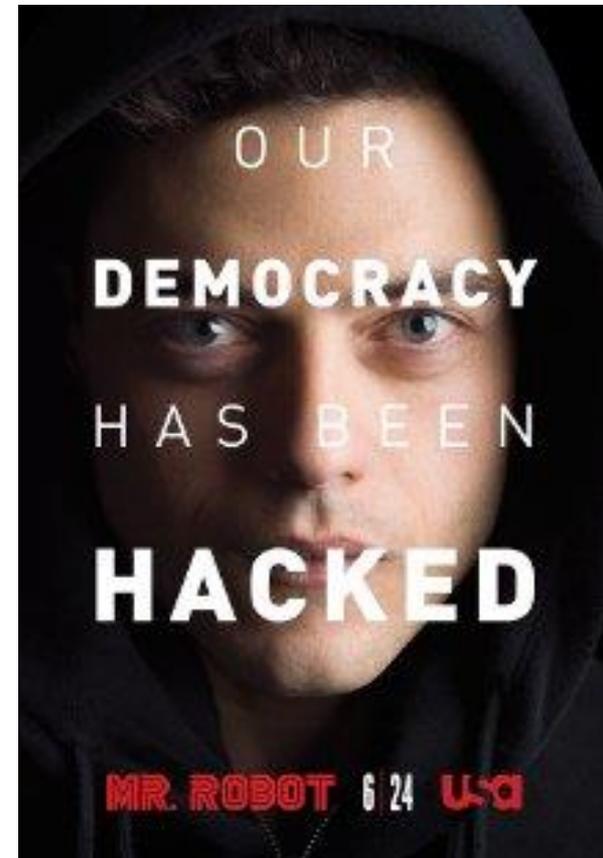
```
set> 1
```

- [Zvaničan sajt](https://www.trustedsec.com)

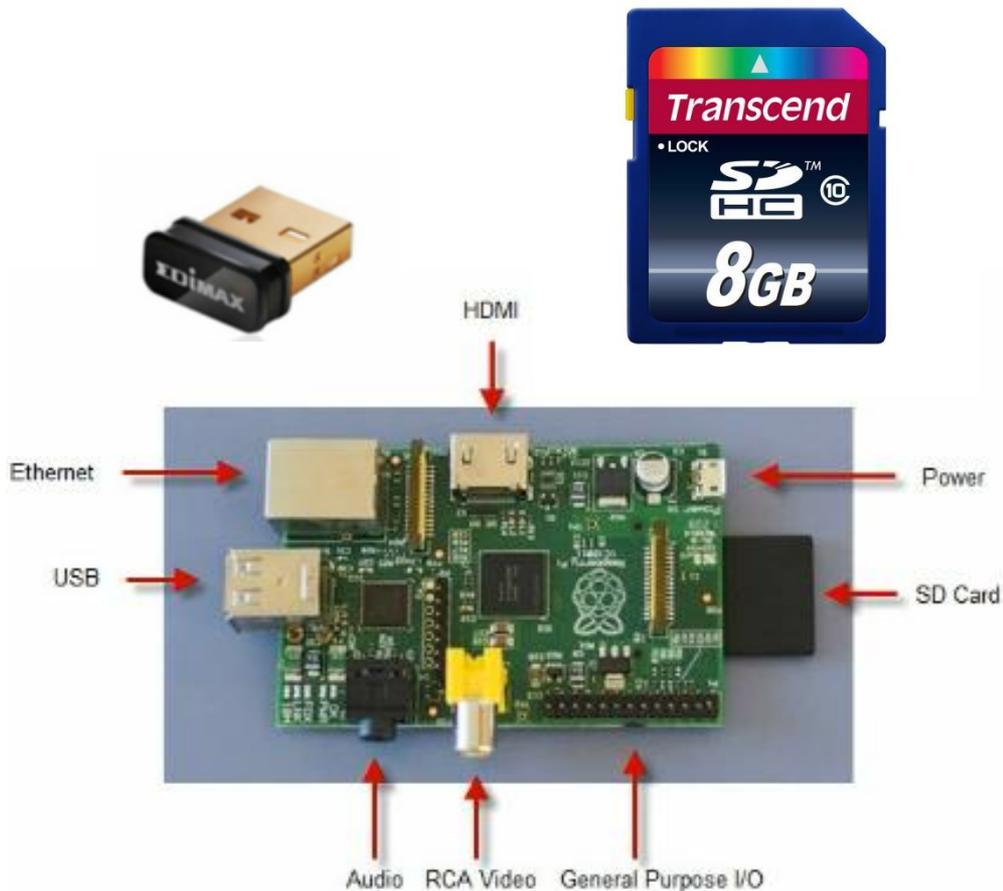
# Mr Robot



- [IMDB serije](#)
- [Trailer](#)



- Kali image arm
- Xming server
- Putty klijent



# Zaključak

- Edukacija ljudi je ključna
- Potrebno je koristiti višestruke sisteme odbrane
- Uvek budite na oprezu
- Nikada ne budite lakoverni

## Korisni linkovi:

- <http://www.informacija.rs>
- <http://thehackernews.com>
- <https://krebsonsecurity.com>
- <http://www.net-security.org>
- <http://www.wired.com/security>
- <http://www.sans.org/reading-room>
- <http://www.hackread.com/category/hacking-news>
- <http://iase.disa.mil/stigs/Pages/index.aspx>
- <http://csrc.nist.gov/publications/PubsSPs.html>
- <http://ddosattackprotection.org/blog/cyber-security-blogs>

**HVALA NA  
PAŽNJI!**



**Kontakt podaci:**

- Mail: [ifranc@secitsecurity.com](mailto:ifranc@secitsecurity.com)
- Web: <http://secitsecurity.com>
- Twitter: <https://twitter.com/francigorbg>
- LinkedIn: <https://rs.linkedin.com/in/ifranc>