ŠTO JE SOCIJALNI INŽENJERING?

CERT.hr

Sadržaj

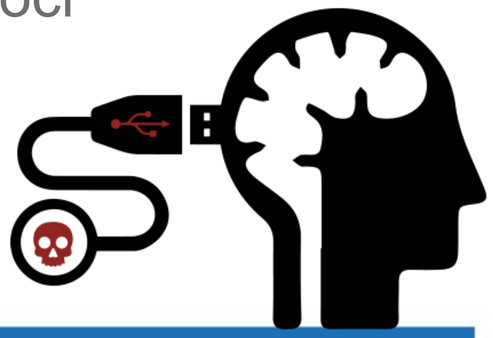
- Uvod
- Faze napada
- Mete napada
- Tehnike napada
- Uzrok i posljedice
- Zaštita od napada

Uvod

- **inženjering** = skup znanja i aktivnosti međusobno povezanih radi dobivanja određenih rezultata, ostvarenja koristi, postizanja cilja

- niz tehnika pomoću kojih pojedinac **(napadač),** iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca **(žrtvu)** kako bi ga naveo da učini nešto što nije u njegovom interesu

- najčešće se koristi u svrhu otkrivanja povjerljivih informacija ili dobivanja pristupa resursima do kojih napadač inače ne bi mogao doći



Amateurs hack systems, professionals hack people. - *Bruce Schneier*

Faze napada

1. Istraživanje
2. Odabir mete
3. Stvaranje odnosa
4. Iskorištavanje odnosa

If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology. - *Bruce Schneier*

Mete napada

- Korisnička podrška
- Tehničari
- Korisnici
- Dobavljači
- Administracija
- Uprava

Social engineering bypasses all technologies, including firewalls. - *Kevin Mitnick*

Interne prijetnje

Tko?

- Zaposlenici s visokim (računalnim) privilegijama
- Nezadovoljni zaposlenici
- Zaposlenici koji su dobili otkaz
- Zaposlenici skloni nezgodama
- Vanjski suradnici, partneri, dobavljači
- Nedovoljno osposobljeni zaposlenici

Zašto?

- Financijska dobit
- Krađa osjetljivih podataka
- Osveta
- Buduća konkurencija
- Javno priopćenje

A lot of hacking is playing with other people, you know, getting them to do strange things. - *Steve Wozniak*

Interne prijetnje

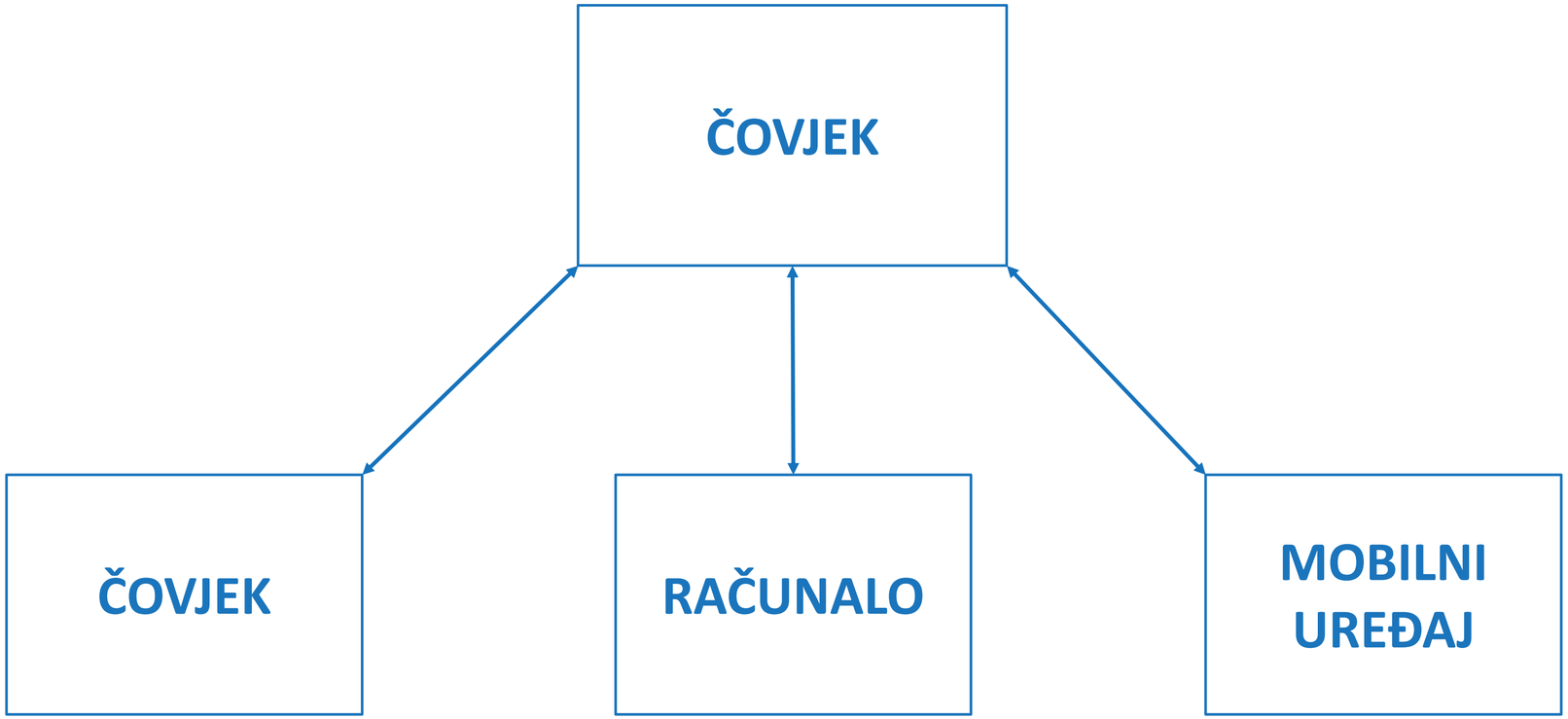
- Zlonamjerna
- Nemarna
- Profesionalna
- Kompromitirana

interna prijetnja

CERT.hr

Social engineering, the fancy term for tricking you into giving away your digital secrets, is at least as great a threat as spooky technology. - *Barton Gellman*

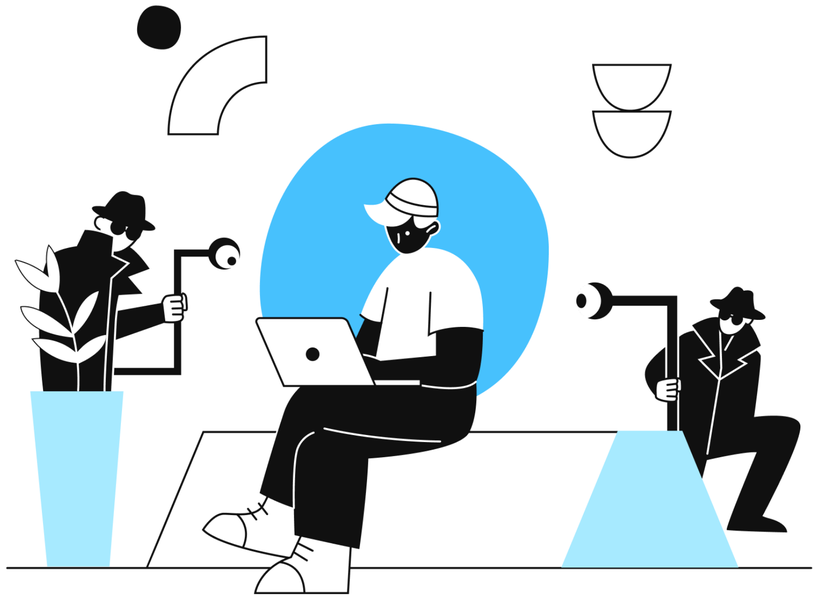
Tehnike napada



Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted; none of these measures address the weakest link in the security chain. - *Kevin Mitnick*

Čovjek - čovjek

- Lažno predstavljanje (eng. *impersonation)* kao legitimni korisnik, VIP ili agent korisničke podrške
- *Vishing* (*voice/VoIP phishing*) putem poziva
- Prisluškivanje razgovora / čitanje pisane komunikacije (eng. *eavesdropping*)
- Gledanje preko ramena *(eng. shoulder surfing)*
- Kopanje po smeću (eng. *dumpster diving*)
- *Piggybacking* vs. *Tailgating*
- *Honey trap* vs. *Catphishing*
- Bacanje mamca (eng. *baiting*)



People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. - *Bruce Schneier*

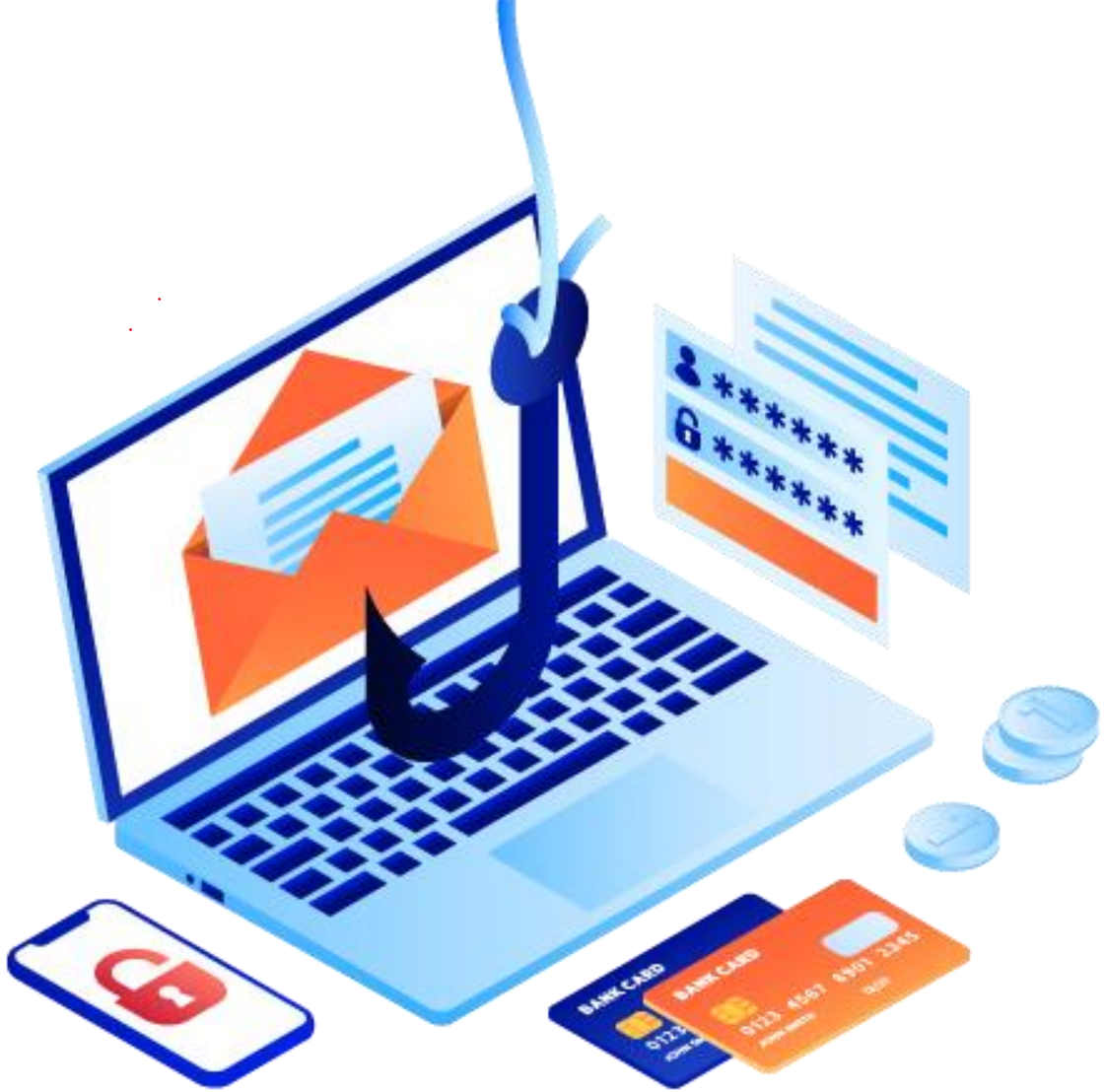
Čovjek - računalo

- Phishing
- Skočni prozori
- IM
- Hoax, scam, lanci sreće, spam

The user's going to pick dancing pigs over security every time. - *Bruce Schneier*

Phishing

- Phishing > e-pošta
- Vishing > poziv
- Smishing > SMS
- Spearphishing > određena meta
- Whaling > visokopozicionirana meta
- Pharming > malware
- Catphishing > veza
- Angler phishing > društvene mreže



The weakest link in any chain of security is not the technology itself, but the person operating it. - *A.J. Darkholme*

Šalje: E-dnevnik Potvrde <e.dnevnik.potvrde@gmail.com>
Poslano: 13. siječnja 2022. 20:34
Prima:
Predmet: E-dnevnik Potvrde

Poštovani profesori,
Radi osvježavanja sustava i ažuriranja došlo je do gubljenja podataka.
Molimo vas da što prije potvrdite vaš CARNET mail OVDJE.
Hvala!

http://e-dnevnik-potvrde.c1.biz/

A hacker is someone who uses a combination of high-tech cyber tools and social engineering to gain illicit access to someone else's data. - *John McAfee*

Cyber Security Investigator

6 TIPS to help detect a malicious email

Rialtas na hÉireann
Government of Ireland

From: William Gates <**fake123@somemail.xyz**>
To: Me <me@myemail.com>

REPLY | REPLY ALL | FORWARD

Dear Friend,

I was hoping you could **send me some money** but I need your **bank details** first.
I also need you to **reset** your email account for security reasons.
Please click **here** to download more information.

Regards,
William.

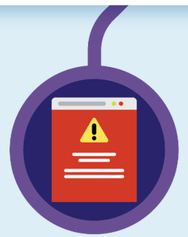
Check the displayed name against the actual email - **fraudsters often impersonate**

"DEAR FRIEND"
Beware general or impersonal greetings

"SEND ME SOME MONEY"
Fund transfer request in an email should be viewed with suspicion

"BANK DETAILS"
Any email asking for personal details should be viewed with caution

"RESET"
Beware unsolicited request asking to reset passwords



"HERE"
Always inspect a link by hovering over first. Remember, if in doubt - **Don't click!**

Čovjek – mobilni uređaj

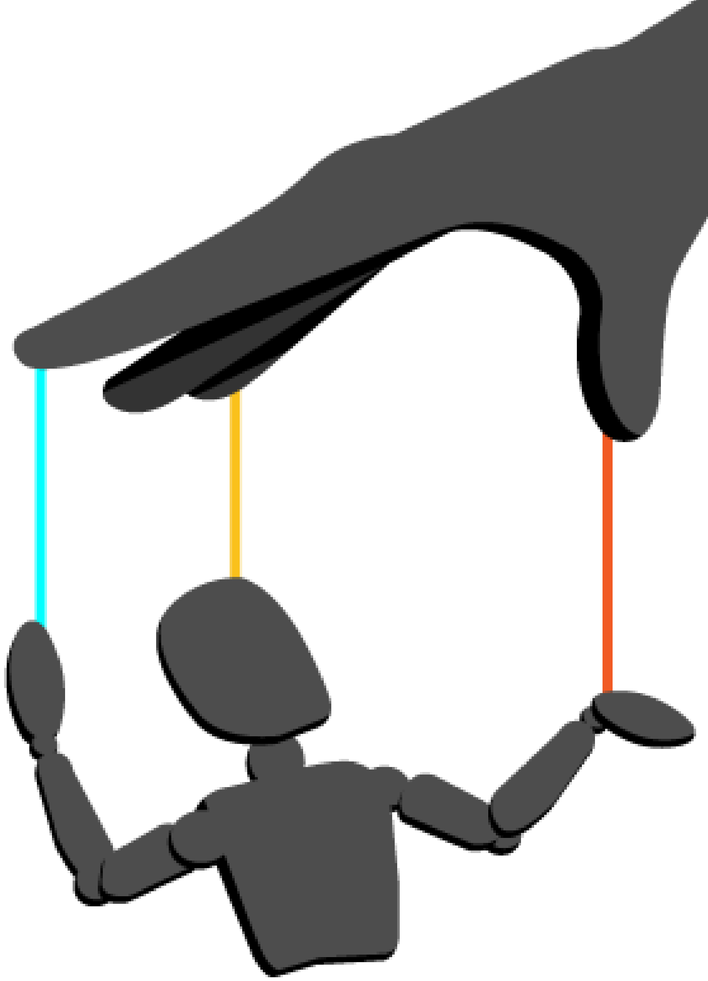
- Zlonamjerne aplikacije
- Prepakiranje legitimnih aplikacija
- Lažne sigurnosne aplikacije
- *Smishing*

Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more. - *John McAfee*

Uzrok i posljedice

- Nedovoljna svijest o kibernetičkoj sigurnosti
- Neregulirani pristup informacijama i podacima
- Nedostatak sigurnosnih politika

- Financijska/materijalna/reputacijska šteta
- Gubitak privatnosti
- Tužbe i arbitraža
- Privremeno ili trajno zatvaranje



There is no patch for stupidity. - *Kevin Mitnick*

Zaštita

- Podizanje svijesti – treninzi i edukacija
- Čitanje i kritičko promatranje
- Odgovornost i savjesnost
- Procedure i politike
- Dupla provjera
- Održavanje kibernetičke higijene

There is no technology today that cannot be defeated by social engineering. - *Frank Abagnale*

www.carnet.hr

www.naivci.hr

www.cert.hr

Kontakt:
ncert@cert.hr

Kontakt za prijavu incidenta:
incident@cert.hr

CARNET
CERT.hr
Odjel za Nacionalni CERT
Josipa Marohnića 5
10000 Zagreb
Hrvatska

Telefon: 01-666-1-650
Telefax: 01-666-1-767