

# Základy sociálneho inžinierstva

Ing. Matej Skulský

KC KB - FEI STU Bratislava

5. decembra 2025



PLÁN [OBNOVY]



- 1 Úvod do sociálneho inžinierstva
- 2 Typy útokov sociálneho inžinierstva
- 3 Praktické scenáre útokov
- 4 Ukážkové videá sociálneho inžinierstva
- 5 Ako sa brániť sociálnemu inžinierstvu
- 6 Zhrnutie a záver

# Čo je sociálne inžinierstvo?

## Definícia

Sociálne inžinierstvo je **manipulácia ľudí** tak, aby útočník získal informácie, prístup alebo vykonanie akcie, ktorú by inak človek neurobil.

### Typické ciele:

- Získať heslá, kódy, čísla kariet
- Vylákať kliknutie na škodlivý odkaz
- Donútiť človeka otvoriť prílohu alebo dvere
- Presvedčiť obeť, aby sama obišla bezpečnostné pravidlá

### Prečo funguje:

- Využíva dôveru, autoritu, strach, urgenciu
- Oslabuje našu pozornosť (stres, únava, piatok popoludní)
- Cielia na emócie, nie na logiku

- 1 **Prieskum** – zber informácií (sociálne siete, web, telefón)
- 2 **Nadviazanie kontaktu** – e-mail, telefonát, osobne pri dverách
- 3 **Budovanie dôvery** – využitie autority, známeho mena, príbehu
- 4 **Žiadosť o akciu** – heslo, kód, kliknutie, otvorenie dverí
- 5 **Zakrytie stôp** – vymazanie logov, presmerovanie viny

## Phishing:

- Masové e-maily vydávajúce sa za banku, kuriéra, cloudovú službu
- Cieľ: **získať prihlasovacie údaje** alebo prinútiť kliknúť na škodlivý odkaz

## Spear phishing:

- Cielené e-maily na konkrétnu osobu/funkciu
- Prispôsobený jazyk, mená kolegov, reálne projekty

## Smishing a vishing:

- **Smishing** – SMS/IM správy („balík na ceste“, „blokácia účtu“)
- **Vishing** – telefonáty („IT podpora“, „polícia“, „banka“)
- Často kombinované: SMS + následný telefonát

## Pretexting:

- Vymyslený príbeh: technik, kuriér, nový kolega, audit
- Cieľ: dostať sa dnu, získať informácie alebo zariadenia

## Tailgating / piggybacking:

- „Držím vám dvere- vstup za legitímnou osobou bez karty
- Zneužitie slušnosti a nechuti byť „ten nepríjemný“

## Baiting & quid pro quo:

- Baiting: USB „nájdené“ pri parkovisku, lákavý súbor
- Quid pro quo: pomoc výmenou za informácie („resetujem vám účet, len mi dajte heslo“)
- Cieľ: spustiť škodlivý kód alebo získať prístup

## Príbeh

- Piatok popoludní, používateľ chce už len dokončiť prácu a ísť domov.
- Volá „IT podpora“: tvrdí, že je problém s účtom a treba **okamžite** overiť prístup.
- Žiada meno, login, prípadne aj **dočasné heslo alebo SMS kód**.
- Používateľ nechce mať problém, tak spolupracuje.

### Príbeh

- Pri dverách stojí kuriér s veľkým balíkom, vyzerá nahnevane a v strese.
- Tvrdí, že potrebuje len „podpis a pustiť dnu na chvíľu“.
- Nemá žiadnu kartu, žiada, aby ho niekto „len rýchlo pustil“ cez turniket.
- Vnútri sa pohybuje bez dozoru, môže **odhliadnuť na obrazovky, zbierať karty, USB...**

### Príbeh

- Útočník si na LinkedIn/FB zistí, kde človek pracuje, na čom robí a kto je jeho nadriadený.
- Pošle e-mail, ktorý vyzerá ako od šéfa alebo kolegu z projektu.
- Text presne sedí na **aktuálny projekt, meeting, tému**.
- V prílohe je údajná dokumentácia, v skutočnosti škodlivý súbor.

# Video 1: Telefonát útočníka (vishing)

## Na čo sa sústrediť počas videa

- Ako sa útočník predstavuje (autorita, príbeh)?
- Aké emócie sa snaží vyvolať (strach, urgentnosť, pomoc)?
- Aké konkrétne informácie alebo akcie žiada?

## Poznámka

Počas videa si skúste **poznačiť 2–3 varovné signály**, ktoré by vás mali „nakopnúť“, že niečo nie je v poriadku.

## Profesionálny sociálny inžinier (DEF CON talk)

<https://www.youtube.com/watch?v=lc7scxvKQOo>

### Na čo sa sústrediť počas videa

- Ako útočník využíva slušnosť a tlak na rýchlosť?
- Kto si všimne, že niekto vstupuje bez vlastnej karty?
- Ako by sa dala situácia riešiť asertívne, ale slušne?

### Reflexné vesty = prístup všade ?

<https://www.youtube.com/watch?v=GyvRamX1VyA>

## Červené vlajky:

- Silná **urgentnosť** („hneď teraz“, „inak bude zle“)
- Požiadavka na **heslo, SMS kód, PIN** alebo iné tajné údaje
- Žiadosť obísť štandardný proces („len mi to pošlite e-mailom“)
- Komunikácia cez netypický kanál (súkromný mail, WhatsApp, FB)

## Ako reagovať:

- Spomaľte, **overte si** kontakt cez oficiálny kanál
- Neposkytujte heslá ani kódy – **nikdy**
- V prípade pochybností sa poraďte s kolegom alebo IT oddelením
- Radšej 10x falošný poplach, než 1 úspešný útok

## V práci:

- Nepúšťajte neznáme osoby bez karty – ani kuriéra
- Neposielajte heslá cez e-mail/IM, nezdieľajte účty
- Hlásenie podozrivých e-mailov a telefonátov (servis desk, bezpečnostný tím)
- Opatrnosť pri hovore o práci na verejných miestach

## V súkromí:

- Opatrnosť, čo zdieľate na sociálnych sieťach (rodina, práca, dovolenka)
- Nedávať kódy a heslá ani „z banky“, ani „z polície“
- Overovať si volania príbuzných z **iného** čísla („podvod na vnuka“)

- 1 **Sociálne inžinierstvo útočí na ľudí, nie na technológiu.**
- 2 **Útočníci využívajú emócie, dôveru, autoritu a urgenciu.**
- 3 **Jednoduché návyky (overovanie, nezdielanie hesiel, nepúšťanie cudzích dnu) výrazne znižujú riziko.**
- 4 **Videá a príklady z praxe ukazujú, že nikto nie je úplne imúnny – dôležité je, ako zareagujeme.**

- **Profesionálny sociálny inžinier (DEF CON talk)**

<https://www.youtube.com/watch?v=lc7scxvKQOo>

- **Reflexné vesty = prístup všade ?**

<https://www.youtube.com/watch?v=GyvRamX1VyA>

- **Rebrík = prístup všade ?**

<https://www.youtube.com/watch?v=NiEMcjSQOzg>

- **Lúpež v Louvre** <https://www.youtube.com/watch?v=ifwngc8FHZM>

<https://www.youtube.com/watch?v=h4Adz7ydeno>

- **Mr. Robot – scéna so sociálnym inžinierstvom**

<https://www.youtube.com/watch?v=s9jwOVGWWuk>

- **Jimmy Kimmel – ľudia prezrádzajú svoje heslá**

<https://www.youtube.com/watch?v=Pd7x2bHVSAAs>

- **Seclists / Passwords – wordlisty na testovanie hesiel**

<https://gitlab.com/kalilinux/packages/seclists/-/tree/0aab3b70769ed9faf79b3c1159fb32ef131c7ee6/Passwords>

Otázky?