

# Ochrana pred online podvodmi a dezinformáciami

## Zodpovedné správanie v digitálnom prostredí

Ing. Matej Skulský

KC KB - FEI STU Bratislava

5. decembra 2025



Financované  
Európskou úniou  
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ  
CENTRUM  
KYBERNETICKEJ  
BEZPEČNOSTI

STU

UNIVERSITA TECHNICKÁ  
BRATISLAVA

- 1 Stručné pripomenutie online podvodov
- 2 Úvod do dezinformácií
- 3 Ako fungujú dezinformačné kampane
- 4 Prečo dezinformáciám veríme
- 5 Ako rozpoznať problematický obsah
- 6 Nástroje a tipy na overovanie
- 7 Budovanie odolnosti voči dezinformáciám
- 8 Zhrnutie a praktické kroky

## Najčastejšie typy:

- Phishing (falošné e-maily, SMS, správy)
- Falošné e-shopy a investičné ponuky
- Podvody na bazároch a sociálnych sieťach
- Vydieranie (napr. sextortion)

## Spoločné znaky:

- Nátlak na **rýchle rozhodnutie**
- Emočný tlak (strach, chamtivosť, súcit)
- Snažia sa dostať **peniaze alebo údaje**
- Tvária sa ako **dôveryhodná autorita** (banka, polícia, firma)

# Prečo veríme nepravdám?

## Dezinformácie neútočia na našu logiku, ale na:

- Našu potrebu mentálnych skratiek.
- Silu emócií.
- Túžbu po sociálnej príslušnosti.

Náš mozog používa mentálne skratky (heuristiky) na rýchle rozhodovanie.

## Príklad mentálnej skratky

Pero a guma stoja spolu 1 €. Pero stojí o 90 centov viac ako guma.

**Otázka:** Koľko stojí guma?

# Prečo veríme nepravdám?

## Dezinformácie neútočia na našu logiku, ale na:

- Našu potrebu mentálnych skratiek.
- Silu emócií.
- Túžbu po sociálnej príslušnosti.

Náš mozog používa mentálne skratky (heuristiky) na rýchle rozhodovanie.

## Príklad mentálnej skratky

Pero a guma stoja spolu 1 €. Pero stojí o 90 centov viac ako guma.

**Otázka:** Koľko stojí guma?

Väčšina ľudí intuitívne odpovie **10 centov** (lebo  $1 \text{ €} - 0,90 \text{ €}$ ), ale správna odpoveď je **5 centov**: guma 0,05 €, pero 0,95 €, spolu 1 €.

## Konfirmačné skreslenie (Confirmation Bias)

Tendencia vyhľadávať, interpretovať a pamätať si informácie, ktoré potvrdzujú naše existujúce názory. Dezinformácia, ktorá rezonuje s našim svetonázorom, sa nám javí ako dôveryhodnejšia.

## Kotvenie (Anchoring)

Tendencia príliš sa spoliehať na prvú informáciu („kotvu“), ktorú o téme dostaneme. Táto „kotva“ ovplyvňuje vnímanie všetkých nasledujúcich informácií.

## Haló efekt (Halo Effect)

Náš celkový dojem z osoby alebo inštitúcie ovplyvňuje hodnotenie ich konkrétnych výrokov. Sme náchylnejší veriť autoritám, ktoré máme radi.

## Stádový efekt (Bandwagon Effect)

Tendencia prijímať názory jednoducho preto, lebo sa zdá, že ich prijíma veľa iných ľudí. V online prostredí sa to prejavuje dôverou v príspevky s vysokým počtom lajkov a zdieľaní.

## Klam preživších (Survivorship Bias)

Logický klam, pri ktorom sa sústredíme len na úspešné prípady („preživších“) a ignorujeme tie neúspešné. To vedie k skresleným a príliš optimistickým záverom.

## Dôležité

Tieto skreslenia sú **prirodené**, ale dezinformácie ich zneužívajú na manipuláciu.

# Najčastejšie logické fauly

- **Útok ad hominem:** Útok na osobu namiesto argumentu.
- **Slamený panák (Straw man):** Vyvrátenie skreslenej verzie argumentu oponenta.
- **Vytrhávanie z kontextu (Quote mining):** Zmena významu citátu jeho vytrhnutím z kontextu.
- **Falošná dilema:** Zjednodušenie voľby len na dve možnosti.
- **Ačohentizmus (Whataboutism):** Odvrátenie pozornosti protiútokom.
- **Vyberanie čerešničiek (Cherry picking):** Účelový výber dát podporujúcich vlastný naratív.

## Prečo to funguje

Tieto fauly sú ťažko rozpoznateľné, ak sa sústredíme len na emócie a nie na logiku argumentu.

# Dezinformačné kampane v priemyselnom meradle

## Astrourfing

Klamlivá praktika, kde sa organizovaná kampaň maskuje ako spontánny prejav vôle občanov.

## Trolie farmy

Organizované skupiny platených „trollov“, ktoré koordinovane šíria dezinformácie a manipulujú online diskusie.

## Boti

Automatizované softvérové programy, ktoré masovo vytvárajú a šíria obsah s cieľom umelo zosilniť dosah kampaní.

## Cieľ

Zneužiť **stádový efekt** – ak vidíme veľa „ľudí“ s rovnakým názorom, zdá sa nám, že ide o konsenzus.

# Deepfake: nová generácia dezinformácií

## Čo je deepfake?

Vysoko realistické, synteticky vytvorené audiovizuálne materiály pomocou umelej inteligencie (AI). Umožňujú zobrazit' reálne osoby hovoriť alebo robiť veci, ktoré sa v skutočnosti nestali.

## Technológia

Využíva generatívne adverzné siete (GANs) na zámenu tvárí alebo napodobnenie hlasu.

## Hrozba

Potenciál úplne zotrieť hranicu medzi realitou a fikciou.

# Prípado zo Slovenska: deepfake pred voľbami 2023

## Čo sa stalo?

Dva dni pred parlamentnými voľbami 2023, počas moratória, sa začala šíriť falošná audio nahrávka. Mala zachytávať lídra jednej zo strán a novinárku, ako sa dohadujú na manipulácii volieb.

## Dôsledky

Hoci bola rýchlo identifikovaná ako deepfake, jej načasovanie a obsah mali potenciál zasiahť pochybnosti.

## Poučenie

Tento prípad bol označený za „úsvit novej éry dezinformácií“ a varovný príklad zraniteľnosti demokratických procesov. Nešlo o izolovaný incident, ale o zbraň nasadenú na už zraniteľné informačné prostredie.

# Podvodný email (phishing)

Ahoj, mami, tohle je moje nove cislo. Muj telefon je rozbity. Posli mi zpravu na whatsapp  
+420721874184

odafone

Password Reset Request



Microsoft @microsoft.com>

To

r+n



## CONGRATULATIONS!

You have won an Apple iPhone 15 Pro!

1. Click on "OK" to visit our sponsors page.
2. Enter your address and pay \$5.95 shipping to get your iPhone 15 Pro.
3. Your Apple iPhone 15 Pro will be delivered within 3 to 5 days by the courier service.

OK

From: authenticationmail@trust.ameribank7.com  
To: johnsmith@email.com  
Subject: **A new login to your bank account**



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device.

IP address: 192.168.0.1

Location: Miami, Florida

**4 new transactions have been made with this account since you last logged in.**

**If this was not you, please reset your password immediately with the link below.**

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

## Ako sa chrániť pred online podvodmi (v skratke)

- **Nereagujte v strese** – zastavte sa, overte si informácie z iného kanála.
- **Nikdy neposielajte kódy z SMS** (bankové, overovacie) nikomu inému.
- **Nezadávajte prihlasovacie údaje** cez link, ktorý vám niekto poslal.
- **Overujte si weby a profily** (URL adresa, recenzie, oficiálne kontakty).
- Pri podozrení **komunikáciu ukončite** a poraďte sa (banka, polícia, IT oddelenie).

## Dnešná realita:

- Neustály prísun správ, statusov, videí, notifikácií
- Každý môže **publikovať** (sociálne siete, blogy, videá)
- Algoritmy nám podsúvajú **to, čo nás zaujíma a vyvoláva reakcie**

## Dôsledok:

- Ťažšie rozlíšime, čo je **overené** a čo nie
- Sme viac vystavení **manipulácii a dezinformáciám**
- Kritické myslenie je **nutná výbava**, nie luxus

## Základné pojmy

- **Misinformácia:** nepravdivá alebo zavádzajúca informácia šírená **bez úmyslu škodiť**.
- **Dezinformácia:** nepravdivá alebo zavádzajúca informácia šírená **zámerne**, s cieľom ovplyvniť alebo poškodiť.
- **Malinformácia:** pravdivá informácia použitá **vytrhnutá z kontextu** alebo v nesprávnom čase za účelom škody.

## Prečo je to dôležité

Nie každý nepresný status je hneď „dezinformácia“ - ale **všetky tieto javy ovplyvňujú naše rozhodovanie.**

## Súvisiace pojmy

- **Hoax:** Špecifický formát poplašnej, falošnej alebo žartovnej správy, širenej primárne cez internet (e-maily, sociálne siete).
- **Propaganda:** Širší pojem pre systematické ovplyvňovanie verejnej mienky. Dezinformácia je jedným z jej kľúčových nástrojov.
- **Clickbait:** Technika tvorby obsahu (najmä titulkov) s cieľom maximalizovať počet kliknutí využívaním silných emócií, často na úkor presnosti.

TEST: Určte z nasledujúcich výrokov, či ide o dezinformáciu, misinformáciu alebo malinformáciu.

### Príklad dezinformácie

- „Voľby na Slovensku sú vždy vopred sfaľované, výsledky dopredu určuje Brusel.“
- „Očkovanie proti COVID-19 bolo vymyslené na zníženie počtu obyvateľov Slovenska, vláda to pred vami tají.“
- „Ukrajinskí utečenci dostávajú od štátu viac peňazí ako dôchodcovia, lebo vláda chce Slovákom zobrať domov.“

Evokuje v nás útok (má meniť našu mienku).

TEST: Určte z nasledujúcich výrokov, či ide o dezinformáciu, misinformáciu alebo malinformáciu.

### Príklad misinformácie

- „Zajtra budú v celom Bratislavskom kraji zatvorené všetky školy kvôli štrajku učiteľov.“ (autor si zle prečítal oznámenie, týkalo sa len niektorých škôl)
- „Nový liek vylieči rakovinu u každého pacienta, čítal som o tom článok.“ (prebratá prehnaná formulácia bez pochopenia podmienok štúdie)
- „Na diaľnici bude od pondelka úplná uzávierka na mesiac.“ (v skutočnosti ide len o nočné čiastočné obmedzenie)

Neevokuje v nás zmenu mienky. Úmysel nie je poškodiť niekoho/niečo. Je to len chybná informácia.

TEST: Určte z nasledujúcich výrokov, či ide o dezinformáciu, misinformáciu alebo malinformáciu.

### Príklady malinformácie

- Zverejnenie informácií o lekároch, ktorí liečia covidových pacientov, a pracovníkoch štátu, ktorí sa podieľajú na vymáhaní pandemických opatrení.“, aby na ňu vyvolali nátlak.
- Zdieľanie starého videa z demonštrácie spred piatich rokov ako „dôkaz“, že dnes v Bratislave prebiehajú masové nepokoje.
- Zverejnenie autentických, ale vytrhnutých viet z interného e-mailu úradu bez kontextu tak, aby to vyzeralo ako dôkaz „veľkého sprisahania“.

Evokuje v nás útok (má meniť našu mienku).

## Čo sledujú tvorcovia dezinformácií:

- Oslabiť **dôveru** v inštitúcie, médiá, vedu
- Polarizovať spoločnosť (**my vs. oni**)
- Ovlplyvniť politické rozhodnutia, voľby, verejnú mienku
- Presadiť **ekonomické alebo ideologické záujmy**

## Prečo sú úspešné:

- Pracujú s **emóciami** a jednoduchými príbehmi
- Opakujú sa v rôznych formách („narratívy“)
- Zneužívajú existujúce **obavy a frustrácie**

- **Naratív „všetci klamú”** – všetky médiá a odborníci sú skorumpovaní.
- **Naratív strachu** – hrozí bezprostredné nebezpečenstvo, „oni” nám niečo zatajujú.
- **Naratív jednoduchého riešenia** – zložité problémy sa dajú vraj vyriešiť jedným jednoduchým krokom.
- **Technika čo keď?** – množstvo otázok bez zámeru nájsť odpoveď, cieľom je vyvolať pochybnosti.
- **Záplava informácií** – toľko obsahu, že je ťažké sa v ňom orientovať (*information overload*).

## Bežné skreslenia:

- **Potvrdzovacie skreslenie** (confirmation bias)
- **Efekt prvého dojmu** a titulku
- **Heuristika dostupnosti** – čo si ľahko vybavíme, to považujeme za častejšie
- **Skupinové myslenie** – prispôsobenie názoru „svojim“

## Čo z toho plynie:

- Prirodzene hľadáme informácie, ktoré **potvrdzujú náš názor**
- Sme citliví na **emotívne a jednoduché príbehy**
- Zdieľame obsah, ktorý v nás **vyvolá silnú emóciu**

## Skontrolujte:

- **Zdroj** – kto to publikoval, poznám ten web / autora?
- **Dátum** – nie je to stará správa vydávaná za aktuálnu?
- **Titulok** – je extrémne emotívny alebo sľubuje šokujúce odhalenia?
- **Autora** – je podpísaný, má kontakt, dá sa dohľadať?

## Pýtajte sa:

- Aké **dôkazy** sú uvedené? Odkazy na zdroje, dáta, odborníkov?
- **Vyváženosť** – sú spomenuté aj iné pohľady, alebo len jeden „správny“?
- **Komu to prospieva**, ak tomu ľudia uveria?

<https://ground.news/> - noviny, ktoré zbierajú správy z viacerých zdrojov a porovnávajú ich medzi sebou, a kategorizujú politické spektrum.

<https://lens.google.com/> - reverzné vyhľadávanie obrázkov.

- Extrémne silné emócie (**hnev, strach, zhnusenie**) bez konkrétnych faktov.
- Časté používanie slov ako „*pravda, ktorú vám nechcú povedať*“, „*mainstreamové médiá klamú*“.
- Žiadne alebo pochybné **zdroje** (anonýmne profily, neznáme weby).
- Výzvy typu „**zdieľajte, kým to nezmažú**“.
- Kombinácia **zrnka pravdy** s výrazne prehnanými tvrdeniami.

## Pre texty a správy:

- Skúste kľúčové tvrdenie **vyhľadať** vo viacerých zdrojoch.
- Pozrite, či sa k téme vyjadrujú **dôveryhodné inštitúcie** alebo odborníci.
- Overte si, či neexistuje **fact-check** (overovacie články).

## Pre obrázky a videá:

- **Reverzné vyhľadávanie obrázkov** (napr. Google Images, TinEye).
- Hľadajte pôvodný kontext – kedy a kde bol obrázok pôvodne zverejnený.
- Buďte opatrní pri krátkych, zostrihaných videách bez kontextu.

- Pestovať **zdravý skepticizmus** – pýtať sa, nie slepo veriť.
- **Diverzifikovať zdroje** informácií (viacero médií, rôzne pohľady).
- Učiť sa **kritické myslenie** a rozumieť základným princípom médií.
- Rozprávať sa s okolím **bez útokov**, ale s otázkami a argumentmi.
- Pri konfliktných témach si dopriať **čas na premyslenie**, nie okamžitú reakciu.

## Vo vnútri organizácie:

- Vzdelávať zamestnancov o **dezinformáciách a hoaxoch**.
- Mať nastavené **komunikačné kanály** pre dôležité informácie.
- Podporovať **otvorené otázky** a spätnú väzbu.

## Navonok:

- Transparentne komunikovať dôležité rozhodnutia.
- Reagovať na **škodlivé fámy** faktami a pokojne.
- Spolupracovať s odborníkmi a inštitúciami pri krízovej komunikácii.

- 1 Online podvody aj dezinformácie využívajú emócie a nátlak.
- 2 Nemôžeme kontrolovať informačné prostredie, ale môžeme **kontrolovať svoje reakcie**.
- 3 **Kritické otázky** a rýchly checklist pomáhajú odhaliť problematický obsah.
- 4 Jednoduché techniky overovania (vyhľadávanie, viac zdrojov, reverzné obrázky) sú dostupné každému.
- 5 Odolnosť voči dezinformáciám je **dlhodobý návyk**, nie jednorazový trik.

## Ako jednotlivec:

- ✓ Nereagovať impulzívne na šokujúce správy.
- ✓ Overiť si podozrivé tvrdenie aspoň v **dvoch** ďalších zdrojoch.
- ✓ Skúsiť reverzné vyhľadávanie obrázka aspoň raz.
- ✓ Porozprávať sa s niekým blízkym o tom, ako spoločne pristupovať k informáciám.

## Pre organizáciu:

- ✓ Zahnúť tému dezinformácií do školení (spolu s online podvodmi).
- ✓ Ujasniť si, cez ktoré kanály idú **oficiálne informácie**.
- ✓ Povzbudiť zamestnancov, aby sa **pýtali**, ak si nie sú istí.

Otázky?