
OCHRANA SÚKROMIA V DIGITÁLNO M VEKU

KOMPLEXNÝ SPRIEVODCA
HROZBAMI A EFEKTÍVNOU
OBRANOU



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

- 1. Úvod do digitálneho súkromia**
 - Definícia a význam
 - Legislatívny rámec (GDPR)
 - 2. Digitálna stopa – Ako sme sledovaní**
 - Mechanizmy webového sledovania (Cookies, Fingerprinting)
 - Zber dát na sociálnych sieťach
 - 3. Krajina hrozieb – Kľúčové riziká**
 - Malware, Phishing a krádež identity
 - Nebezpečenstvá verejných Wi-Fi sietí
 - 4. Budovanie digitálnej pevnosti – Praktická obrana**
 - Digitálna hygiena a kľúčové nástroje (VPN, Správcovia hesiel)
 - Zabezpečenie účtov (2FA) a komunikácie (E2EE)
 - 5. Budúcnosť súkromia – Nové výzvy**
 - Internet vecí (IoT), AI a biometria
 - 6. Záver a zhrnutie**
 - Kľúčové obranné stratégie
-

ÚVOD: 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.

MECHANIZMUS č. 1: SÚBORY COOKIE

- **Cookies** sú malé textové súbory, ktoré webové stránky ukladajú do prehliadača.
- Ich pôvodný účel je legitímny: zapamätanie si prihlasovacích údajov, obsahu košíka alebo jazyka stránky.
- Existujú však rôzne typy s odlišným dopadom na súkromie.

TYPY SÚBOROV COOKIE

- **First-party (prvostranové):** Ukladané priamo navštívenou stránkou. Vo všeobecnosti prospešné pre používateľský komfort.
- **Third-party (tret'ostranové):** Ukladané inými doménami (reklamné siete, sociálne médiá). Ich hlavným účelom je **sledovať vašu aktivitu naprieč rôznymi webovými stránkami** na vytváranie profilov pre cielenú reklamu.
- **Zombie cookies:** Obzvlášť invazívna forma, ktorá sa dokáže **obnoviť aj po vymazaní** z prehliadača.

MECHANIZMUS č. 2: DIGITÁLNY ODTLAČOK (FINGERPRINTING)

- Oveľa sofistikovanejšia a ťažšie odvrátiteľná metóda sledovania ako cookies.
- Pasívne zbiera a kombinuje sériu technických informácií o konfigurácii vášho prehliadača a zariadenia.
- Funguje aj v
inkognito režime alebo pri pravidelnom mazaní cookies.

AKO FUNGUJE DIGITAL FINGERPRINTING?

Zbierané atribúty zahŕňajú:

- Operačný systém a jeho verzia
- Typ a verzia webového prehliadača
- Nainštalované pluginy a rozšírenia
- Systémové písmo (fonty)
- Rozlíšenie obrazovky a časové pásmo
- Informácie o hardvéri (grafická karta, CPU)
- Kombinácia týchto atribútov je **prekvapivo unikátna**. Štúdia ukázala, že až 99% používateľov Firefoxu malo jedinečný odtlačok.

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 ŠPIÓNI 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 ŠPIÓNÍ 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 ŠPIÓNÍ 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?

YouTube (Google)

- * odporúčanie videí (algoritmus)
- * zacielenie reklám
- * meranie výkonnosti videí
- * ochrana proti podvodom a botom
- * personalizácia feedu a notifikácií
- * analytika pre tvorcov

NEVIDITEĽNÍ ŠPIÓNI AKO SA ÚDAJE ĎALEJ VYUŽÍVAJÚ?

Facebook (Meta)

- * zostavenie personalizovaného newsfeedu
- * cielenie reklamy podľa záujmov, správania, kontaktov
- * odporúčanie priateľov
- * rozpoznávanie trendov a vzorcov správania
- * zabezpečenie účtu a detekcia podvodov
- * prepojenie aktivít medzi aplikáciami (Facebook, Instagram, WhatsApp)

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 ŠPIÓNÍ LEGÁLNY RÁMEC

(zjednoduše)

V EÚ platí najmä:

- * GDPR
- * ePrivacy smernica (cookies)
- * Národné zákony o ochrane osobných údajov

Tie určujú, že:

- * zber údajov musí byť oprávnený a primeraný
 - * niektoré údaje vyžadujú súhlas
 - * používateľ musí mať prístup k tomu, čo sa zbiera
 - * firma musí vysvetliť účel zberu
-

NEVIDITEĽNÍ ŠPIÓNÍ RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Veľké platformy (najmä Facebook a YouTube) dokážu kombinovať údaje o:

- * správaní (čo sleduješ, na čo klikáš, ako dlho),
- * technických parametroch (zariadenie, poloha),
- * sociálnych väzbách,
- * osobných preferenciách a názoroch.

Riziká:

- * vznik „detailných behaviorálnych profilov“ – čo ťa zaujíma, aké máš zvyky, kedy si online, čo kupuješ
- * možnosť precízneho zacielenia reklám, ktoré môžu vplývať na tvoje rozhodovanie
- * pri dostatočnom množstve dát možno odhadnúť aj citlivé informácie: politické názory, zdravotné témy, finančný stav, životný štýl

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Riziko sledovania naprieč webmi (cross-site tracking)

Mnohé stránky integrujú:

- * Facebook Pixel
- * Google Analytics
- * AdSense

Riziká:

- * vzniká globálny sledovací profil, ktorý nepatrí len jednej stránke
- * môže dôjsť k dlhodobému monitorovaniu tvojho online správania
- * ťažká možnosť kontroly – používateľ často nevie, kde všade je sledovaný

NEVIDITEĽNÍ ŠPIÓNI RIZIKO ROZSIAHLEJ PROFILÁCIE POUŽÍVATEĽOV

Firmy zdieľajú dáta s:

- * reklamnými spoločnosťami,
- * logistickými partnermi,
- * analytickými nástrojmi,
- * vývojármi externých aplikácií.

Riziká:

- * únik alebo zneužitie dát mimo pôvodnej platformy
- * ťažko kontrolovateľné šírenie – raz zdieľané údaje sa môžu dostať k ďalším subjektom
- * riziko cielených podvodov (phishing, podvodné reklamy), keď sú údaje kombinované s inými databázami

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 ŠPIÓNÍ 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.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Používaj doplnky na blokovanie sledovania

Najsilnejšia kombinácia:

- * uBlock Origin (blokovanie reklám a trackerov)
- * Privacy Badger (učí sa trackery rozpoznávať)
- * Cookie AutoDelete (automatické mazanie cookies po zatvorení tabov)
- * ClearURLs (odstraňuje sledovacie parametre z URL)

Táto kombinácia dokáže zablokovať aj 70–90 % bežného trackingu.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Vypni third-party cookies

Vo Firefoxu a Brave sú predvolene blokované.

Používaj prehliadačové kontajnery

Firefox má doplnok ****Facebook Container**** → zabráni Facebooku sledovať ťa mimo svojho webu.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Minimalizuj otlačok prehliadača (fingerprinting)

Fingerprinting dokáže identifikovať zariadenie aj bez cookies.

Vo Firefoxe aktivuj „Strict tracking protection“

Obmedzí fonty, API a prvky, ktoré fingerprinting využíva.

Používaj uBlock Origin v režime „Hard Mode“

Znižuje množstvo načítaných skriptov.

Nepoužívaj zbytočné doplnky

Čím viac doplnkov → tým unikátnejší prehliadač.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

V Android/iOS vypni „personalizované reklamy“

* Android: Nastavenia → Súkromie → Reklamy → Vypnúť personalizáciu

* iOS: Nastavenia → Súkromie → Tracking → Zakázať appkám sledovanie

Minimalizuj sledovanie zo strany Google, Facebooku, YouTube**

Google / YouTube:

* vypni soft personalizácie na myaccount.google.com

* vypni históriu polohy

* vypni históriu YouTube (vyhľadávanie aj sledovania)

* sleduj videá v anonymnom okne, ak nechceš, aby ovplyvňovali odporúčania

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Facebook:

- * vypni „Activity Off Facebook“ (sledovanie na cudzích weboch)
- * obmedz, kto ťa môže nájsť podľa telefónu/e-mailu
- * každému povoleniu v „Apps and Websites“ prekontroluj rozsah dát
- * na mobile vypni povolenia, ktoré nepotrebuje (GPS, mikrofón, kontakty)

NEVIDITEĽNÍ ŠPIÓNÍ OCHRANA

6. Minimalizuj sledovanie pri nakupovaní**

Nemaj trvalo prihlásený účet v e-shopoch

Keď si prihlásený, môžu ťa profilovať presnejšie (história, kliky).

Používaj anonymné okná pri porovnávaní cien

Niektoré obchody menia ceny podľa profilu používateľa.

Vymaž cookies pri odchode z e-shopu

Najmä ak využívajú analytické nástroje typu Hotjar/Smartlook.

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Pre oddelenie identít používaj viacero prehliadačov

Napr.:

- * Firefox (bežné prehliadanie)
- * Brave (sociálne siete)
- * Tor (citlivé veci, anonymita)

NEVIDITEĽNÍ ŠPIÓNI OCHRANA

Minimalizuj riziko únikov dát**

Používaj silné, unikátne heslá

Správca hesiel (Bitwarden, 1Password) je veľmi odporúčaný.

Zapni dvojfaktorové overenie (2FA)

Znižuje riziko prevzatia účtu.

Pravidelne čist Google/MyActivity a Facebook Activity

Odstraňovanie starých údajov znižuje dlhodobú sledovateľnosť.

HROZBA č. 3: KRÁDEŽ IDENTITY A RIZIKÁ NADMERNÉHO ZDIEĽANIA

- **Krádež identity:** Neoprávnené získanie a použitie osobných údajov inej osoby na podvodné účely.
- **Dôsledky:**
 - **Finančné podvody** (žiadosti o pôžičky vo vašom mene).
 - **Poškodenie reputácie** (vytvorenie falošných profilov, rozosielanie podvodných správ vašim kontaktom).
- **Prípadová štúdia:** Zdieľanie fotografií z dovolenky v reálnom čase je otvorenou pozvánkou pre zlodejov, ktorým signalizujete, že váš byt je prázdny.

HROZBA č. 4: NEBEZPEČENSTVO VEREJNÝCH WI-FI SIETÍ

Verejné Wi-Fi siete v kaviarňach, hoteloch či na letiskách sú často nezabezpečené a predstavujú jedno z najväčších bezpečnostných rizík.

- **Man-in-the-Middle (MitM) útok:** Útočník sa vloží medzi vás a Wi-Fi router a môže **odpočúvať** a **manipulovať** vašu nešifrovanú komunikáciu.
- **Evil Twin (Zlé dvojča):** Útočník vytvorí falošný Wi-Fi prístupový bod s názvom identickým alebo podobným legitímnej sieti. Po pripojení má plnú kontrolu nad vašou komunikáciou a môže vás presmerovať na falošné prihlasovacie stránky.

BUDOVANIE DIGITÁLNEJ PEVNOSTI

Ochrana súkromia si vyžaduje **proaktívny a viacvrstvový prístup**.

Efektívna obrana je kombináciou:

- 1. Správnych nástrojov**
- 2. Osvojených návykov (digitálnej hygieny)**
- 3. Neustáleho vzdelávania**

Je to ako zabezpečenie domu: potrebujete pevné dvere (heslo), kvalitný zámok (2FA), alarm (antivírus) a obozretnosť (rozpoznávanie phishingu).

ZÁKLADY DIGITÁLNEJ HYGIENY (CHECKLIST)

Používajte silné a unikátne heslá pre každú službu (min. 12-16 znakov, kombinácia písmen, čísel, symbolov).

Pravidelne aktualizujte softvér (OS, prehliadač, aplikácie) – aktualizácie obsahujú kritické bezpečnostné záplaty.

Pravidelne zálohujte svoje dáta – najúčinnější obrana proti ransomware.

Buďte obozretní pri klikaní a sťahovaní – sťahujte len z oficiálnych zdrojov.

Minimalizujte svoju digitálnu stopu – nastavte si profily na sociálnych sieťach ako súkromné.

Používajte bezpečnostný softvér (antivírus, firewall).

Pravidelne kontrolujte nastavenia súkromia vo svojich účtoch.

NÁSTROJ č. 1: PREHLIADAČE ZAMERANÉ NA SÚKROMIE

Štandardné prehliadače (napr. Chrome) sú často súčasťou ekosystému postaveného na zbere dát. Alternatívy ponúkajú lepšiu ochranu:

- **Brave:** Predvolene **blokuje všetky reklamy a sledovacie skripty**, čím zrýchľuje načítavanie stránok. Poskytuje robustnú ochranu proti digitálnemu odtlačku (fingerprinting).
- **Mozilla Firefox:** Vyvíjaný neziskovou organizáciou. Funkcia
 - **"Total Cookie Protection"** izoluje cookies pre každú stránku zvlášť, čím bráni sledovaniu naprieč webmi.

NÁSTROJ Č. 2: VIRTUÁLNE PRIVÁTNE SIETE (VPN)

- **Princíp fungovania:** VPN vytvára **bezpečný, šifrovaný "tunel"** medzi vaším zariadením a internetom. Vaša komunikácia sa javí, akoby pochádzala z IP adresy a polohy VPN servera.
 - **Kedy použiť VPN?**
 - **NEVYHNUTNOSŤ na verejných Wi-Fi sieťach** – chráni pred odpočúvaním a MitM útokmi.
 - **Na ochranu pred poskytovateľom internetu (ISP)**, ktorý inak vidí vašu históriu prehliadania.
 - **Na obchádzanie geoblokácie.**
VPN chráni pred poskytovateľom internetu a webmi pred štandardnou IP,
 - **ale VPN nebráni sledovaniu cez cookies a fingerprinting**
-

NÁSTROJ Č. 3: SPRÁVCOVIA HESIEL

Ľudská pamäť nedokáže spravovať desiatky unikátnych a zložitých hesiel. Správcovia hesiel tento problém riešia bezpečne.

- **Princíp fungovania:** Digitálny trezor, ktorý ukladá všetky heslá do **silne šifrovanej databázy**. Prístup je chránený jediným, veľmi silným **hlavným heslom (Master Password)**.
- **Výhody:**
 - Generujú extrémne silné heslá.
 - Automaticky vyplňajú prihlasovacie údaje.
 - Umožňujú používať **unikátne heslo pre každú službu**, čo je najdôležitejší princíp ochrany účtov.
- **Príklady:** Bitwarden (open-source), 1Password, NordPass.

ZABEZPEČENIE ÚČTOV: DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)

- Jedna z najúčinnejších metód na ochranu účtov, aj keď útočník ukradne vaše heslo.
- Pridáva **druhú vrstvu overenia** k prihlasovaciemu procesu. Vyžaduje kombináciu:
 - **Niečo, čo viete** (heslo)
 - **Niečo, čo máte** (telefón, hardvérový kľúč)

METÓDY 2FA

- **SMS kódy:** Pohodlné, ale **najmenej bezpečná metóda** kvôli riziku "SIM swapping" útokov.
- **Aplikácie na generovanie kódov (TOTP):** Aplikácie ako Google Authenticator alebo Authy generujú časovo obmedzené kódy.

Bezpečnejšia alternatíva k SMS.

- **Push notifikácie:** Aplikácia pošle na telefón notifikáciu "Pokúšate sa prihlásiť?", kde stačí ťuknúť na "Áno". Pohodlné a bezpečné.
- **Hardvérové bezpečnostné kľúče (FIDO/U2F):** Malé USB/NFC zariadenia (napr. YubiKey). Považujú sa za **najbezpečnejšiu formu 2FA**, odolnú voči phishingu.

ZABEZPEČENIE KOMUNIKÁCIE: END-TO-END ŠIFROVANIE (E2EE)

- **Princíp E2EE:** Správa je zašifrovaná na zariadení odosielateľa a dešifrovať ju dokáže **len zariadenie príjemcu**.
- Ani poskytovateľ služby (napr. WhatsApp, Signal) **nedokáže prečítať obsah správ**.
- Toto je zlatý štandard zabezpečenia súkromnej komunikácie.

PREVZATIE KONTROLY: SPRÁVA POVOLENÍ APLIKÁCIÍ

- Mobilné aplikácie často žiadajú prístup k funkciám a dátam (poloha, kontakty, mikrofón), ktoré pre svoje fungovanie **nevyhnutne nepotrebujú**.
- Pravidelná kontrola a správa týchto povolení je kľúčová.
- **Vždy sa pýtajte:** "Naozaj potrebuje táto hra prístup k mojim kontaktom a mikrofónu?"
- **Ako na to:**
 - **Android:** Nastavenia > Aplikácie > Správca povolení.
 - **iOS:** Nastavenia > Súkromie a bezpečnosť.

UZAMKNUTIE SOCIÁLNYCH SIETÍ: FACEBOOK

Dve kľúčové nastavenia na obmedzenie sledovania:

1. Aktivita mimo Facebooku (Off-Facebook Activity):

- Nastavenia > Vaše informácie na Facebooku > Aktivita mimo Facebooku.
- Umožňuje **vymazať históriu** dát z tretích strán.
- Kľúčové je **vypnúť "Budúcu aktivitu mimo Facebooku"**, aby sa nové dáta nespájali s vaším účtom.

2. Preferencie reklám:

- Centrum účtov > Preferencie reklám > Nastavenia reklám.
- **Zakážte používanie dát od partnerov** a obmedzte cielenie reklám na základe vašich aktivít.

UZAMKNUTIE SOCIÁLNYCH SIETÍ: INSTAGRAM

- **Prepnite na súkromný účet:** Najjednoduchší a najefektívnejší krok. Vaše príspevky uvidia len schválení sledujúci.
 - Nastavenia a súkromie > Súkromie účtu > Súkromný účet.
- **Namietat' voči použitiu dát pre AI:** Meta plánuje používať verejné dáta na tréningovanie AI. V centre ochrany súkromia je možné vyplniť formulár a **vzniesť námietku**.
- **Prepnite z profesionálneho na osobný účet:** Profesionálne účty sú vždy verejné. Ak nepotrebuje analytiku, prepnite sa späť.

BUDÚCNOSŤ SÚKROMIA: NOVÉ VÝZVY

Nové technológie prinášajú komplexnejšie výzvy, ktoré posúvajú hranice chápania súkromia.

- **Internet vecí (IoT):** Miliardy pripojených zariadení (inteligentné reproduktory, kamery, senzory) neustále zbierajú dáta v našich najintímnejších priestoroch.
- **Umelá inteligencia (AI):** Umožňuje z masívneho objemu dát extrahovať vzorce, robiť predpovede a automatizované rozhodnutia.
- **Biometrická autentifikácia:** Pohodlie vs. nezmeniteľné riziko.

RIZIKÁ IOT A AI

- **Extrémne detailné profilovanie:** Zariadenia v inteligentnej domácnosti zbierajú dáta o našich rozhovoroch, zvykoch, dennom režime a pohybe.
- **Automatizované rozhodovanie:** Algoritmy AI môžu na základe zozbieraných dát robiť rozhodnutia s priamym dopadom na náš život (napr. výška poistného, schválenie úveru).
- **Riziko diskriminácie:** AI modely trénované na historických dátach môžu reprodukovat' a zosilňovat' spoločenské predsudky.

RIZIKÁ BIOMETRICKEJ AUTENTIFIKÁCIE

Hlavný problém: Biometrické dáta sú neoddeliteľne spojené s našou fyzickou identitou a **nemôžeme ich zmeniť ako heslo.**

- **Nezmeniteľné riziko:** Ak dôjde k úniku databázy s biometrickými údajmi, táto **kompromitácia je trvalá.** Váš odtlačok prsta je navždy "spálený".
- **Spoofing a Deepfakes:** Útočníci môžu biometrické systémy oklamať pomocou 3D tlačiarňí alebo falošných odliatkov ("spoofing"). AI umožňuje vytvárať realistické "deepfake" videá a audio záznamy.
- **Masové sledovanie:** Technológia rozpoznávania tváre vo verejnom priestore predstavuje obrovské riziko pre anonymitu a slobodu.

ZÁVER: SÚKROMIE AKO AKTÍVNY PROCES

- Ochrana súkromia **nie je cieľový stav**, ale dynamický a nepretržitý proces.
- Pasívny prístup a spoliehanie sa na predvolené nastavenia je ekvivalentom ponechania odomknutých dverí.
- Vyžaduje si to kombináciu vedomostí, nástrojov a predovšetkým **neustálu ostražitosť**.

ZHRNUTIE KLÚČOVÝCH OBRANNÝCH STRATÉGIÍ

Efektívna obrana stojí na troch pilieroch:

1. NÁSTROJE:

- Prehliadač zameraný na súkromie (Brave, Firefox).
- Virtuálna privátna sieť (VPN).
- Správca hesiel (Bitwarden, 1Password).

2. NÁVYKY:

- Zásady digitálnej hygieny (aktualizácie, zálohy).
- Aktivácia dvojfaktorovej autentifikácie (2FA) všade, kde je to možné.

3. VEDOMOSTI:

- Schopnosť rozpoznať phishing a sociálne inžinierstvo.
- Pochopenie, ako spravovať povolenia a nastavenia súkromia.

APEL NA ZÁVER

- Hrozby sa neustále vyvíjajú. Phishing je presvedčivejší, malware sofistikovanejší.
- Najsilnejšou zbraňou a najlepšou formou ochrany je **neustále vzdelávanie a ostražitosť**.
- Zostaňte informovaní, pravidelne revidujte svoje nastavenia a kriticky pristupujte k novým službám.
- V konečnom dôsledku, najväčšou devízou je **informovaný a proaktívny používateľ**, ktorý aktívne spravuje svoju digitálnu stopu.

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde