Seria mythbusting

despre

DREPTURI DIGITALE

Seria de articole ApTI Digital Rights Mythbusting demaschează mituri, mentalităţi şi idei preconcepute din sfera drepturilor digitale. Vorbim despre ce înseamnă viaţa privată şi protecţia datelor personale, cum sunt ameninţate drepturile şi libertăţile online, dar şi cum te poţi proteja. Dedicăm un capitol principalelor eşecuri ale sistemului actual de drepturi de autor, oferim sugestii despre cum ar putea fi îmbunătăţit şi analizăm şi cum ne afectează propunerea de modificare a drepturilor de autor în Europa. Anumite articole sunt pregătite pe baza materialelor EDRi Privacy, Security și Freedoms, Spread Privacy şi EDRi Copyfail.

Digital rights myth:
Modul Incognito al browserului te protejează complet pe Internet

Credeai că atunci când navighezi cu browser-ul pe modul „Incognito” eşti complet protejat şi nu vede nimeni ceea ce faci? Lucrurile nu stau tocmai cum te-ai fi aşteptat.

Uite ce se întâmplă de fapt:

Punctele bune

1. Nu salvează istoricul de navigare (site-urile vizitate) după ce ai închis browserul.
2. Nu salvează informaţiile introduse în formulare (de exemplu: delogarea se produce automat, după ce fereastra de navigare a fost închisă, iar datele introduse se şterg din memorie).
3. Şterge cookie-urile https://www.apti.ro/despre-cookie-consultare instalate de site-urile vizitate, după ce închizi fereastra browser-ului.
4. Poţi să te autentifici simultan cu mai multe conturi diferite în acelaşi browser.

Punctele vulnerabile

1. Chiar dacă nu se salvează activitatea de navigare, ea este vizibilă pe serverele site-urilor accesate, pentru angajator (dacă navighezi la serviciu), pentru persoana care administrează reţeaua pe care o foloseşti, pentru motorul de căutare, pentru furnizorul tău de servicii de Internet, pentru organele de cercetare penale etc. Vezi cum aici.
2. IP-ul nu este anonimizat/ schimbat. Pentru asta, ai putea folosi un browser precum Tor. Iată mai multe metode pentru a-ţi face identitatea anonimă faţă de furnizorul tău de servicii de Internet.
3. Chiar dacă ai modul Incognito activat, site-urile pe care le accesezi tot pot face device fingerprinting (informaţiile colectate despre un dispozitiv, cu scopul identificării acelui device şi uneori chiar a persoanei deţinătoare). Vezi https://amiunique.org/ sau https://panopticlick.eff.org/.

Cum activezi funcţia privată a browser-ului tău

- Chrome → Ctrl+Shift+N (sau) dreapta sus, click pe cele trei liniuţe de meniu → New Incognito Window
- Firefox → Ctrl+Shift+P (sau) dreapta sus, click pe cele trei linuţe → Fereastră privată nouă sau Private Browsing Windows
- Safari → stânga sus, File → New Private Window
- Microsoft Edge → Ctrl+Shift+P (sau) dreapta sus, click pe cele trei puncte → New InPrivate Window
- Opera → Ctrl+Shift+N (sau) stânga sus, Meniu → New Private Window

Când e util să foloseşti modulul incognito

Deşi modul „Incognito” nu-ţi oferă anonimat atunci când accesezi un site, este foarte folositor dacă vrei să foloseşti un dispozitiv conectat la Internet care nu-ţi aparţine, fără a fi îngrijorat că cineva îţi va vedea istoricul de navigare şi că astfel poate ajunge la informaţii sensibile şi parole sau că poate deduce informaţii personale despre tine. Apropo, bookmark-urile şi download-urile vor fi în continuare păstrate, deci ai grijă să le ştergi manual după ce termini sesiunea de navigare în modul Incognito, dacă nu eşti pe dispozitivul propriu!

Digital rights myth:

Cât de sigură este parola mea?

Mit: E în regulă să folosesc aceeaşi parolă pentru toate conturile, fiindcă sigur nu o uit.

E mult mai complicat decât atât. Întâi fă un test simplu:

1. Intră pe https://howsecureismypassword.net/ şi introdu o parolă similară cu cea pe care o foloseşti pentru contul de Facebook de exemplu. Cuvântul cheie e similară: nu da nimănui parola, indiferent cât de apropiat îţi e, cât de multă încredere ai sau fiindcă ţi-a fost recomandat de ApTI şi ştii că ştim ce zicem ;P
2. Vezi în cât timp poate fi spartă de un calculator obişnuit. Atenţie: cele mai dese atacuri poate că se întâmplă de pe un calculator obişnuit din camera de cămin, în schimb atacurile cele mai puternice se întâmplă cu un echipament performant.

Bun, dacă eşti printre cei ale căror parole pot fi sparte rapid de un calculator obişnuit, gândeşte-te la următoarele idei preconcepute despre păstrarea parolelor:

Îmi notez parola pe o hârtie sau într-un fişier, deci este în siguranţă

Soluţia - Mai bine o memorezi, o notezi cu câteva caractere inversate (atenţie să ţii minte ce ai schimbat!) sau foloseşte un manager de parole (vezi un clip video despre acest lucru).

Folosesc aceeaşi parolă pentru mai multe conturi, ca să nu mă încurc

Soluţia: Inventează câte o parolă pentru fiecare cont, aşa va fi mai greu de accesat celelalte conturi atunci când unul dintre ele a fost compromis. Să nu uităm de multitudinea datelor (user şi parolă) care au fost date publicităţii de-a lungul anilor (vezi cazurile Yahoo, LinkedIn, Dropbox, SnapChat). Poţi verifica dacă parola ta a fost compromisă la https://haveibeenpwned.com/Passwords.
Ţine minte: nu permite browser-ului să îţi memoreze parola!
https://blog.livehosting.ro/gaura-de-securitate-in-browserele-google-chrome-si-mozilla-firefox/

Parola mea este formată din ceva cunoscut sau ceva ce folosesc mereu

Soluţia: Parola trebuie să îndeplinească următoarele cerinţe:
- să fie de cel puţin opt caractere;
- să conţină atât cifre şi litere (inclusiv majuscule), cât şi simboluri;
- să nu conţină date despre tine (porecle, numele animalului de companie, numărul de la maşină, elemente din adresa de acasă sau de la birou etc.);
- să nu fie alcătuită din cuvinte existente în dicţionare sau care pot fi uşor deduse (exemplu: parolamea, abcd1234);
- parola să fie greu de ghicit inclusiv de către partenerul de viaţă, de cunoscuţi, de prieteni, de familie;

Cum poţi să alcătuieşti o parolă puternică

1. Alcătuieşte o propoziţie din care iei prima literă a fiecărui cuvânt. De exemplu:
SARA **P**E **D**EAL **B**UCIUMUL **S**UNĂ **C**U **J**ALE
2. Adaugă simboluri şi o dată semnificativă (zi/lună, de exemplu: !**SPDBSCJ**20#09)
3. Ia cuvinte din titlul, primul vers sau refrenul melodiei tale preferate şi adaugă cifre, majuscule, caractere rare. De exemplu: **Billie Jean** DEVINE **@billie()JEAN19*86**.
Sau generează parola online, de exemplu la DuckDuckGo.com. De exemplu, pentru o parolă de 13 caractere, tastează **password 13**. Dacă vrei o parolă de 20 de caractere, scrie **password 20**. Copiază parola generată, DAR întotdeauna schimbă vreo 2-3 caractere.
Vezi un clip video despre acest lucru.

Pentru o mai bună protecţie, află mai multe şi despre autentificarea în doi paşi.

Digital rights myth:
Reclamele online

Mit: Nu poţi scăpa de reclamele profilate pe Internet.

Te-ai întrebat cum de ştie Google, Facebook sau un site anume că ţie îţi plac hainele dintr-un X magazin online sau de ce îţi arată noile produse ale unui magazin pe care nu l-ai accesat de ceva timp? Aceste anunţuri nu sunt nişte simple reclame standard ce îţi apar atunci când navighezi, ci se bazează pe preferinţele tale personale obţinute direct şi indirect din activitatea ta.

Cum funcţionează reclamele

De fiecare dată când vizitezi un site sau o aplicaţie, se pot stoca informaţii despre tine şi acţiunile tale, pentru a fi folosite inclusiv pentru a te profila cu anunţurile care ar putea să fie mai interesante pentru tine. Problema este nu doar proprietarul acelui site le obţine, ci deseori aceste informaţii sunt obţinute şi de alţi terţi al căror cod este integrat pe site - de la un broker de date şi până la Google sau Facebook. Vezi aici mai multe detalii despre ce firme te urmăresc pe Internet.

Într-un studiu realizat de Princeton Web Transparency & Accountability Project, se arată că gigantul Google vinde anunţuri direcţionate nu numai pe motorul său de căutare, ci şi pe alte 2,2 milioane de site-uri Web şi peste 1 milion de aplicaţii. Dar datele sunt colectate de pe mult mai multe site-uri.

Marile companii plătesc sume importante pentru a obţine date despre tine, în scopul îmbunătăţirii strategiilor de marketing pe care le utilizează. Astfel, dacă două persoane accesează acelaşi site de cumpărături, folosind dispozitive diferite, una dintre ele s-ar putea să vadă un preţ mai mare din cauza istoricului de browsing sau pentru că foloseşte un Mac, deci îşi permite să plătească mai mult.

Problema este uneori mai complicată decât pare. Pe de o parte tu nu ştii ce prespun aceste profilări despre tine. De fapt probabil nici nu ai idee exact cine te urmăreşte şi ce face cu aceste date. Pe de altă parte nu ai nici un control referitor la cum vor fi folosite aceste date. Vor fi folosite ele pentru a primi un preţ mai bun sau o reclamă relevantă? Sau vor fi folosite pentru un preţ mai mare, pentru a te face să votezi cu un anumit partid sau pentru a-ţi refuza un credit online? Habar nu ai. Şi nici noi. Dar le poţi opri.

Soluţia: Cum să scapi de reclame profilate

Instalează o extensie a browserului sau o aplicaţie mobilă, care blochează dispozitivele de urmărire ale reclamelor, printre care şi alte caracteristici de protecţie a confidenţialităţi. Poţi folosi o suită de extensii care elimină cookie-urile, trackerele şi sterge memoria cache (de ex.: Cookie AutoDelete, uBlock Origin, Empty Cache). Atenţie: accesul la Facebook şi alte conturi nu va mai fi aşa facil, deoarece dispozitivul nu îţi va mai păstra datele de acces!

Digital rights myth:
Cât de anonimizate îţi sunt datele?

Dacă atunci când navighezi pe Internet şi bifezi rubrica prin care îţi exprimi acordul ca un site să îţi colecteze datele, unele site-uri te anunţă să stai liniştit că ele sunt în totalitate dedicate protecţiei datelor personale, aşa că ţi le vor anonimiza şi nu are ce să se întâmple. Oare aşa să fie?

Cum funcţionează?

Site-ul colectează o serie de date despre tine, şi nu ne referim numai la user şi parolă, ci la întreaga ta activitate pe acel site (de exemplu: când accesezi site-ul, ce preferinţe ai etc.). Toate aceste date sunt colectate pentru a le folosi în scop de cercetare sau de stabilire a noilor politici de marketing (vezi că scrie undeva pe la politica de confidenţialitate despre asta - cum n-ai citit-o?!). În alte cuvinte folosirea datelor tale este sigură şi nu te afectează. Însă acest lucru este numai parţial adevărat. Cele mai multe companii ţin toate datele, fie ele anonimizate sau nu, în acelaşi loc. În condiţiile acestea, reidentificarea ta, chiar după ce datele ţi-au fost anonimizate se poate obţine foarte uşor. Practic, aceeaşi bază de date conţine şi datele despre tine şi identificatorul unic asociat datelor anonimizate, iar legătura dintre informaţii este uşor de făcut.

Încă dintr-un studiu din anii ‘90 realizat de către Latanya Sweeny se arată că, pe baza unor date simple (precum genul, data naşterii şi codul poştal), pot fi identificaţi 87% dintre americani prin anularea anonimizării.

Într-un alt exemplu s-a arătat că re-identificarea unor date anonimizate s-a putut realiza prin date conexe precum recomandări Netfix sau istoricul de căutări AOL.

Soluţiile

- Anonimizarea reală este lipsa datelor. Atunci când ţi se afişează ferestre prin care eşti întrebat dacă doreşti să împărtăşeşti date în mod „anonim”, mai bine alege varianta NU!
- Foloseşte servicii online care prelucrează un minim de date personale (urmează principiul *data minimization*) sau servicii care nu stochează nimic care ulterior să ajute la identificarea ta.

Digital rights myth:

Identificarea prin simpla accesare a unui site

Mit - Dacă şterg cookie-urile, nu pot fi identificat de un site pe Internet.

Hai să testăm! Accesează site-urile Nothing Private şi ClickClickClick.

Cum e posibil să interacţionezi în timp real cu aceste site-uri chiar dacă ţi-ai luat măsuri de protecţie?

Pe lângă cookie-uri, o metodă care poate fi folosită pentru identificarea şi urmărirea în mod unic a persoanelor în timpul navigării private este numită "amprentarea browser-ului". Aşa cum fiecare dintre noi are o amprentă unică, la fel se întâmplă şi în cazul unui browser.

Pe scurt, orice site poate potrivi numerele de versiune ale browserului, plugin-urile pe care le utilizează şi zeci de alte puncte de informaţii pentru a crea un cod unic (adică o amprentă), pe care îl foloseşte pentru a te urmări.

Care e soluţia?

Un prim strat ar fi folosirea unui serviciu VPN. Dar, din păcate, nu vei putea ocoli 100% monitorizarea care se întâmplă prin datele trimise de browser, iar prin instalarea mai multor extensii, dezactivarea javascript-ului şi a solicitărilor webRTC nu vei face altceva decât să-ţi creezi un browser şi mai unic, fiindcă foarte puţine persoane fac lucrurile acestea. Poţi vedea prin Am I Unique şi Panopticlick cât de unic este browserul tău.

Probabil cel mai bun sfat este separarea activităţilor publice de cele private. Citește mai multe sfaturi și explicații.