Nawet fonty mogą śledzić cię online!

23 maja 2023

Jeśli korzystasz z internetu nie od wczoraj, najpewniej wiele już słyszałeś o śledzeniu użytkowników. Pliki cookie, śledzenie IP – te i inne technologie są nagminnie wykorzystywane przez firmy, by gromadzić dane o internautach. Korporacje potrafią się jednak wykazać kreatywnością. I tak oto okazuje się, że do śledzenia można wykorzystać nawet… fonty. Mowa o darmowych fontach (plikach odpowiadających za wygląd tekstu), które oferuje Google poprzez usługę Google Fonts.

Usługa Google Fonts oferuje deweloperom darmowe fonty, które mogą bez ograniczeń i opłat instalować na swoich stronach internetowych. Należą do nich takie klasyki jak Roboto, Lato czy Merriweather.

Instalowanie fontów od Googla na stronach internetowych jest korzystne z punktu widzenia deweloperów. Fonty te są bowiem stworzone w taki sposób, by wyglądać dobrze i na komputerach, i na urządzeniach przenośnych. Zapewniają więc spójny i schludny wygląd witryn, a to niezwykle ważne choćby ze względu na to, że coraz więcej osób przegląda sieć za pośrednictwem smartfonów i tabletów.

Problem jednak w tym, że gdy użytkownik łączy się ze stroną wykorzystującą googlowskie fonty, łączy się również z serwerami Googla, bo pliki są każdorazowo pobierane. Firma zyskuje przy okazji wiedzę między innymi o adresie IP użytkownika, historii przeglądania i klikniętych linkach.

Fonty to nowinka w kontekście gromadzenia danych o internautach, ale stare i bardziej znane metody są wciąż chętnie wykorzystywane przez firmy. Blokada śledzenia w sieci od lat jest tematem na topie i nic nie wskazuje na to, by

miało się to zmienić.

Co można zrobić, by uniknąć śledzenia przez fonty? Z pewnością nie ma co polegać na trybach incognito (prywatnych) w przeglądarkach. Włączenie trybu incognito nie blokuje bowiem połączenia z serwerem Google.

Niektóre przeglądarki (np. Mozilla Firefox) mają opcję pozwalającą na wyłączenie innych fontów niż tych określonych w ustawieniach. Znajdziesz je, szukając fraz „czcionki" lub „fonty" w opcjach bezpieczeństwa przeglądarki.

Dobrym pomysłem jest również łączenie się z siecią poprzez VPN. Usługa ta szyfruje dane i zmienia wirtualną lokalizację IP użytkownika, dzięki czemu firmy i reklamodawcy mają trudniejsze zadanie, próbując powiązać internautę z konkretnymi wyszukiwaniami i historią przeglądania.

Witryny, które odwiedzasz, mogą wiedzieć o tobie więcej, niż byś się spodziewał. Skąd czerpią informacje?

Adres IP to unikalny ciąg liczb, który umożliwia Twojemu urządzeniu komunikację z innymi członkami sieci. Witryny, na które wchodzisz, również mają do niego dostęp. Nie może być inaczej, bo gdyby nie adresy IP, nie byłoby wiadomo, gdzie adresować dane. Adresy IP zdradzają jednak pewne informacje o użytkowniku – na przykład jego przybliżoną lokalizację. To natomiast wystarczy, by podsuwać internautom targetowane reklamy lokalnych usług albo modyfikować cenniki na podstawie lokalizacji (np. zawyżać ceny biletów lotniczych kupowanych online).

Pliki cookie to małe pliki tekstowe zapisywane w urządzeniu przez przeglądarkę. Ich celem jest poprawianie jakości korzystania z sieci. Odpowiadają na przykład za zapamiętywanie produktów w koszykach sklepowych czy też preferencji językowych. Są więc niezbędne do tego, by surfowanie po sieci było przyjemne i wygodne. Istnieje jednak szczególny rodzaj cookies, a mianowicie: pliki cookie stron trzecich. Ten rodzaj

„ciasteczek” potrafi śledzić użytkownika po całym internecie i zbierać informacje o tym, jakie produkty ogląda i co go interesuje, by następnie posłużyć do stworzenia spersonalizowanej kampanii reklamowej.

Fingerprinting (z języka angielskiego: zbieranie odcisków palców) to metoda śledzenia użytkownika na podstawie informacji dostarczanych przez jego urządzenie. Do takich danych można zaliczyć system operacyjny i jego wersję, rodzaj przeglądarki i jej wersję, rozdzielczość ekranu, strefę czasową, język systemu i inne dane.

Można się domyślić, że gdy zbierze się wszystkie te niepozorne informacje razem, będą one bardzo dobrym identyfikatorem konkretnego użytkownika. Trudno bowiem znaleźć dwa urządzenia o dokładnie identycznej konfiguracji.

Jak chronić się przed śledzeniem w sieci?

– Korzystaj z zewnętrznych narzędzi, takich jak blokery skryptów śledzących.

– Zaktualizuj ustawienia swojej przeglądarki, szczególnie sekcję „Prywatność i bezpieczeństwo”. Wyłącz obsługę elementów śledzących i sprawdź, jakie uprawnienia ma przeglądarka (np. dostęp do lokalizacji).

– Korzystaj z sieci VPN, która zmienia adres IP i szyfruje dane, zwiększając twoje bezpieczeństwo.

– Zainstaluj wtyczkę blokującą reklamy i trackery w przeglądarce.

– Uważaj na publiczne sieci Wi-Fi, a najlepiej nie łącz się z nimi, jeśli nie musisz. Takie sieci często nie są dobrze zabezpieczone i mogą przechwytywać poufne informacje.

Źródło: MagazynFakty.pl