

Co warto wiedzieć o śledzeniu i profilowaniu w sieci?

22 października 2014

„W Internecie nikt nie wie, że jestem psem”. Rysunek Petera Steinera opatrzony tym podpisem stał się jednym z najbardziej znanych memów i symbolem anonimowości w sieci. Faktem jest, że w Internecie można podać się za kogoś innego. Jednak ukrywanie własnej tożsamości, zainteresowań czy kontaktów jest znacznie trudniejsze niż mogłoby się wydawać na pierwszy rzut oka. I to również dla tych, których trudno zaliczyć do internetowych ekshibicjonistów. Sieć wie bowiem o nas znacznie więcej niż to, co w sposób świadomy udostępniamy. Na podstawie różnych cyfrowych śladów można odgadnąć wiek, płeć, a nawet zidentyfikować konkretną osobę. Powinien o tym pamiętać każdy świadomy użytkownik Internetu. Także dziecko.

ŚLADAMI KLIKNIEĆ

Korzystanie z Internetu nieuchronnie wiąże się z udostępnianiem informacji o sobie. Niektórymi dzielimy się świadomie, a innymi – mimowolnie, czasem nawet nie zdając sobie z tego sprawy. Już samo wejście na dowolną stronę internetową uruchamia przepływ danych. Automatycznie zostają jej przesłane: nasz adres IP oraz informacje o przeglądarce (m.in. wersja, system operacyjny, język i czcionki). Wbrew pozorom mogą to być informacje bardzo specyficzne ([Panopticlick](#) pomaga nam ocenić jak bardzo). A im bardziej nietypowe ustawienia, tym łatwiej daną osobę zidentyfikować jako konkretnego użytkownika i śledzić w sieci.

Strony, które odwiedzamy, wykorzystują różne mechanizmy służące pozyskaniu informacji o swoich użytkownikach. Najbardziej popularne są ciasteczka (ang. cookies), czyli specjalne pliki zapisywane na komputerze użytkownika. Ciasteczka mogą służyć różnym celom – część z nich jest

niezbędna do tego, by prawidłowo wyświetlać stronę bądź zalogować się. Zadaniem pozostałych jest zdobycie innych informacji cennych z punktu widzenia właściciela strony internetowej. To dzięki nim może na przykład dostosowywać wyświetlane reklamy do konkretnego użytkownika.

CIEKAWSKIE „STRONY TRZECIE”

Warto wiedzieć, że w Internecie jesteśmy śledzeni nie tylko przez strony, na które akurat wchodzimy, ale również inne podmioty. Na komputerach mogą być zapisywane również ciasteczka stron, do których stron odwołuje się strona, którą odwiedzamy (ang. third party cookies). Informacje na nasz temat mogą trafiać do baz danych firm udostępniających mechanizm do prowadzenia statystyk (np. Google Analytics) lub serwisów społecznościowych (np. Facebook, Google+). Za pomocą rozszerzenia Lightbeam (do przeglądarki Firefox) można sprawdzić, kto na poszczególnych stronach próbuje nas w ten sposób śledzić. Dość łatwo można się zorientować, że najwięksi gracze są w stanie zbierać informacje na temat ogromnej części sieciowego ruchu.

Przyjrzyjmy się, jak to działa w przypadku powszechnie instalowanych wtyczek do portali społecznościowych. Jeśli znajdują się one na stronie, z której aktualnie korzystamy, informacje na nasz temat wędrują również na serwery firmy prowadzącej portal. Co więcej, jeżeli jesteśmy zalogowani na swoim koncie (nawet jeśli w danej chwili strona portalu nie jest otwarta w oknie przeglądarki), zostaniemy zidentyfikowani jako konkretny użytkownik. To nie wszystko. Jeśli nie jesteśmy zalogowani do portalu społecznościowego, instaluje on na naszym urządzeniu ciasteczko, w którym zapisana jest nasza wizyta. Początkowo nie będzie ono przywiązane do naszego profilu, ale po zalogowaniu – o ile wcześniej nie usuniemy ciasteczka – wszystkie informacje zostaną ze sobą połączone. W efekcie administratorzy serwisów społecznościowych mogą bez większej trudności śledzić aktywność swoich użytkowników, również gdy nie jest ona związana z korzystaniem z serwisu.

W BAŃCE FILTRUJĄCEJ

Wiedza na temat naszych działań w sieci służy różnym podmiotom do różnych celów. E-marketerzy interesują się nimi, by dopasowywać określone reklamy i jak najwięcej zarobić na oferowanych produktach. Wykorzystują do tego mechanizm nazywany profilowaniem, który polega na kategoryzowaniu ludzi według cech i zachowań. Z reklamami opartymi na profilowaniu możemy spotkać się w sieci niemal na każdym kroku. Mogą być ona dobrane do nas pod kątem wieku i płci, lajków i kliknięć (np. w portalach społecznościowym), oglądanych produktów (w sklepach internetowych), wyszukiwanych słów (w wyszukiwarkach) czy treści e-maili (w usługach poczty elektronicznej).

Profilowanie w Internecie dotyczy nie tylko reklam, ale również wyszukiwanych informacji. Większość wyszukiwarek (np. Google, Bing) dopasowuje wyniki do użytkowników, bazując na historii zapytań. Oznacza to, że na przykład pasjonat gier online będzie otrzymywał od wyszukiwarki odpowiedzi dopasowane (statystycznie) do swoich zainteresowań. Na co dzień bywa to przydatne, jednak przy okazji zbierania materiałów do referatu z historii może okazać się utrudnieniem. Tak właśnie działa efekt bańki filtrującej (ang. filter bubble). Na krótką metę może ułatwiać życie, na dłuższą – zamykać we własnym świecie i ograniczać horyzonty.

INFORMACYJNA PROFILAKTYKA

Również najmłodszy powinni mieć świadomość tego, jakie cyfrowe ślady zostawiamy po sobie w sieci i zabezpieczać się przed niekontrolowanymi skutkami ich wykorzystania przez różne podmioty. Niektóre metody wymagają pewnych kompetencji technicznych i nie nadają się do samodzielnego wdrożenia przez młodsze dzieci. Tym ważniejsza jest w tej sytuacji świadomość oraz aktywna rola rodziców.

I – jak zawsze – dobry przykład. O czym warto pamiętać?

1. Dobrze się zastanów, zanim zaczniesz korzystać z portali

społecznościowych. Jeśli ich używasz, nie klikaj w nic bez zastanowienia. I pamiętaj, by wylogować się z nich po zakończeniu korzystania.

2. Jeśli używasz poczty e-mail w przeglądarce, pamiętaj o wylogowaniu się zaraz po skończonej pracy.

3. Zainstaluj kilka przydatnych wtyczek, jak np. Adblock (blokuje reklamy), Cookie Monster (pomaga zarządzać ciasteczkami), Ghostery (blokuje wybrane skrypty śledzące) oraz Better Privacy (zarządza flash cookies, umożliwia ich usuwanie przy zamykaniu przeglądarki).

4. Zadbaj o odpowiednie ustawienia obsługi ciasteczek w swojej przeglądarce (np. o wyłączeniu obsługi ciasteczek umieszczanych przez witryny inne niż odwiedzana strona). Instrukcja [TUTAJ](#).

5. Korzystaj z wyszukiwarek internetowych, które nie wykorzystują profilowania, np. [Duckduckgo.com](https://duckduckgo.com), [Ixquick.com](https://ixquick.com), [Startpage.com](https://startpage.com)

Autorka: Małgorzata Szumańska

Źródło: [Fundacja Panoptikon](#)