Nasza aktywność w internecie.

Czyli kiedy i czy widzą nas inni gdy jesteśmy on-line?

Jak internet nas śledzi?

Jakie dane są zbierane i w jaki sposób?

Techniki śledzenia i profilowania w sieci stają się coraz bardziej agresywne i zaczynają obejmować wszystkie sfery naszego życia prywatnego.

Dane dotyczące zdrowia, relacji międzyludzkich, sytuacji finansowej, słabości i marzeń milionów ludzi są zbierane, odpowiednio katalogowane, profilowane i wykorzystywane w celach komercyjnych.

W dzisiejszych czasach prawie każdy z nas ma różne konta na social mediach takich jak facebook, messenger, instagram. Ale czy jesteśmy całkowicie bezpieczni?

Każdy może wiedzieć o nas wszystko jeżeli będziemy publikować nasze ważne informacje. Każda nasza aktywność w internecie jest zapisywana.

Na początku wszyscy myśleli, że internet daje poczucie anonimowości, możliwość ukrycia swojej aktywności w sieci pod fałszywą tożsamością.

Obecnie nasza aktywność w internecie wzrosła kilkusetkrotnie, zaś narzędzia do śledzenia w sieci stały się coraz bardziej wyrafinowane, a przy tym trudniejsze do kontroli przez zwykłego użytkownika.

Punkt zwrotny w ograniczaniu prywatności w internecie nastąpił w roku 1994. Wtedy to Lou Montulli, pracownik Netscape, stworzył plik, dzięki któremu możliwe stało się śledzenie aktywności poszczególnych użytkowników na stronach internetowych. ***Dziś znamy to narzędzie bardzo dobrze – jest to oczywiście plik cookie.***

Skąd firmy wiedzą o nas to wszystko?

Historia przeglądania – historia stron, które przeglądaliśmy może być podstawą do spersonalizowanej oferty marketingowej. Na podstawie tych informacji firmy wiedzą np. że interesujemy się wykupieniem wycieczki na wakacje, remont mieszkania, zakup zabawek. W celu zdobycia informacji z naszej historii przeglądania z reguły wykorzystywane są dwie metody: śledzące pliki cookie oraz przechowywanie wewnętrzne. Dzięki ciasteczkom umieszczonym na naszym urządzeniu, a dokładniej w używanej przez nas przeglądarce, strony internetowe mogą gromadzić informacje na temat oglądanych przez nas stron.

Lokalizacja – Wiele witryn zbiera adresy IP, które są dedykowanymi numerami przypisanymi do poszczególnych komputerów w sieci określającymi lokalizację urządzenia z którego dokonywana jest aktywność. Praktycznie każdy komputer podłączony do Internetu ma adres IP

Relacje ze znajomymi, rodziną – wiele witryn korzysta z narzędzi do gromadzenia danych dotyczących naszych interakcji z innymi użytkownikami sieci. Kompleksowe programy obliczyć relacje między tobą a innymi osobami, z którymi posiadasz jakiekolwiek relacje w sieci.

Kilka sposobów jak chronić swoją prywatność w Internecie

1. Korzystaj z password managera

Przy korzystaniu z kilkudziesięciu różnych usług online, większość z nich wymaga logowania się. Po pewnym czasie trudno nam zapamiętać wszystkie hasła i zaczynamy stosować ten sam login i hasło do wielu serwisów. Jest to błąd. Lepszym rozwiązaniem jest korzystanie z password managera.

Jest to oprogramowanie dostępne wprost z przeglądarki internetowej, które zapamiętuje i gromadzi loginy i hasła do wszystkich serwisów. Manager generuje również bardzo trudne do złamania hasła i bezpośrednio wkłada je w odpowiednie okienka. Z wszystkich naszych haseł możemy korzystać również na telefonie, tablecie, właściwie wszędzie gdzie mamy dostęp do internetu. Sam dostęp do managera również jest chroniony hasłem, także musimy jedynie pamiętać jedno hasło zamiast kilkudziesięciu (jeżeli korzystamy z managera gdzieś poza domem, to nie zapomnijmy się z niego wylogować przed odejściem od komputera).

2. Wprowadź dwustopniowe logowanie

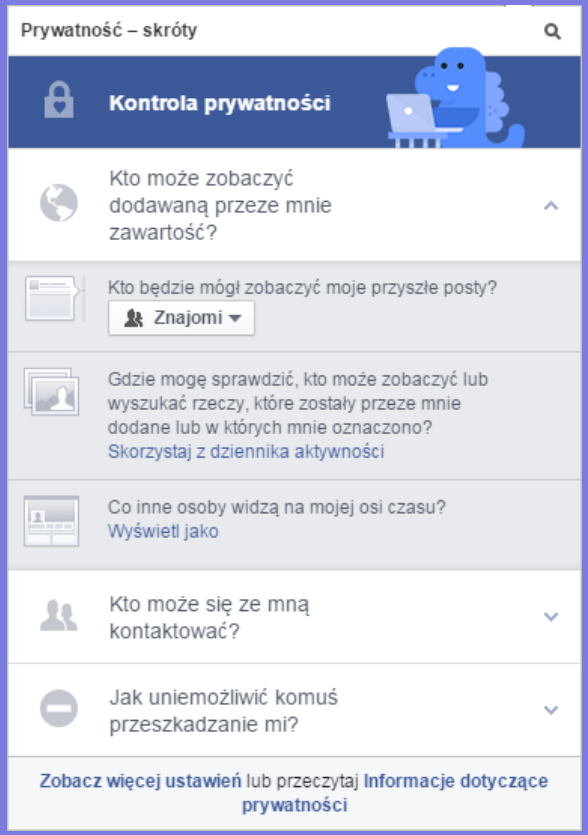
Nawet jeżeli ktoś pozna nasze hasło istnieje sposób aby się obronić. Jest to tzw dwustopniowe logowanie się. Po pierwszym wpisaniu danych pojawia się kolejne pytanie lub inne zabezpieczenie i dopiero dwukrotne wprowadzenie poprawnych danych umożliwia zalogowanie się do konta.

3. Nie podawaj numeru telefonu, daty urodzenia i adresu

Data naszego urodzenia, numer telefonu oraz adres służą często bankom i innym instytucjom do weryfikacji klientów. Starajmy się nie udostępniać tych informacji online, zwłaszcza jeżeli nie jest to wymagane.

4. Zmień ustawienia na Facebooku

Jeżeli jesteś na Facebooku sprawdź i zastanów się nad ustawieniami prywatności. Czy rzeczywiście chcesz aby nieznajomi mogli oglądać twoje fotografie, poznać imiona twoich dzieci i inne dane dotyczące życia osobistego? Zmień ustawienia tak, aby tylko osoby znajome miały dostęp do tych informacji.



5. Korzystaj z antywirusa

Zainwestuj w jakiegoś dobrego antywirusa oraz software chroniący przed atakami z sieci .

5. Zmień opcje w telefonie

Bezpieczeństwo i prywatność w sieci nie dotyczy wyłącznie komputerów. Coraz więcej osób codziennie łączy się z internetem za pośrednictwem urządzeń mobilnych (telefony, tablety, itp). Są one również narażone na różnego rodzaju ataki i próby śledzenia dlatego jeżeli nie korzystacie z sieci albo chcecie uniemożliwić śledzenie, warto wyłączyć połączenia Bluetooth, WiFi oraz opcje lokalizacji. Nie zapominajcie również o zastosowaniu specjalnego oprogramowania antywirusowego do urządzeń mobilnych.

6. Zmień co jakiś czas hasło do WiFi

Jeżeli nasze hasło dostępu do routera nie było zmieniane przez dłuższy czas, to warto je zmienić i powtarzać tą operację raz na pół roku.

7. Monitoruj jakie informacje zbierają o nas strony internetowe

Strony internetowe zbierają o nas różne informacje i zapisują różne dane w plikach cookies naszych przeglądarek. Jeżeli nam nie odpowiada to, że są zbierane dane na nasz temat możemy się bronić. Najłatwiej uruchomić funkcję *incognito* w naszej przeglądarce, która zablokuje zapisywanie ciasteczek.

8. Nie zapisuj poufnych informacji w plikach swojego komputera

Jeżeli mamy porządnego antywirusa oraz zaporę *firewall* i z komputera korzystamy wyłącznie w domu, nie powinniśmy się raczej niczego obawiać. Zapisywanie poufnych danych w plikach bez względu na okoliczności, nie jest najlepszym pomysłem. Nasz komputera może się np. zepsuć i oddając go do naprawy od razu udostępniamy go osobom trzecim.


ctrl