

Dbanie o prywatność w internecie

Siedem sposobów ochrony prywatności w sieci

1. **Ostrożność na portalach społecznościowych** – przy tworzeniu profilu podaj minimalną, wymaganą liczbę informacji. Ustal odpowiednio zabezpieczenia prywatności w ustawieniach portalu. Im mniej danych serwis o Tobie posiada, tym więcej prywatnych informacji zachowasz dla siebie
2. **Dane w „chmurach”** – przechowywanie danych, plików, zdjęć, filmów czy dokumentów on-line jest wygodne, ale może sprowadzić na nas pewne problemy. Pamiętaj, że firmy, które przechowują te dane mają do nich dostęp. Poza tym takie usługi padają również celem ataków hakerskich. Przechowuj tam jak najmniej danych, nie przechowuj prywatnych plików, których nie chcesz pokazywać innym.
3. **Oddzielaj życie prywatne od zawodowego** – nie wykorzystuj służbowego telefonu lub komputera do przechowywania prywatnych plików. Prawdopodobnie Twój pracodawca ma dostęp do zawartości pamięci komputera oraz smartfona, może sprawdzić np. jakie strony internetowe przeglądałeś/przeglądałaś.
4. **Ustawiaj silne hasło** – ustawiaj silne, trudne do złamania hasła. Staraj się je regularnie zmieniać oraz posiadaj różne hasła do różnych serwisów.
5. **Menedżer haseł** – możesz używać menedżera haseł, czyli specjalnego programu, który wygeneruje silne hasło do serwisu, z którego korzystasz. Nie będziesz musiał pamiętać wszystkich haseł. Program dostępny jest zarówno na komputery, jak i urządzenia mobilne.
6. **Oszczędnie korzystaj z Wi-Fi i GPS na urządzeniach mobilnych** – obie usługi mogą zdradzić wiele informacji na nasz temat, np. dokładną lokalizację i szczegóły urządzenia, z którego korzystasz. Ponadto otwarte sieci wifi przeważnie nie wykorzystują szyfrowanych połączeń, zatem bardzo łatwo złodziei może przechwycić Twoje dane podczas np. logowania do banku.
7. **Prawo do bycia zapomnianym** – to prawo, które daje obywatelom możliwość usunięcia ich danych z popularnych wyszukiwarek internetowych. Jest to długi i skomplikowany proces, jednakże na przykład Google pozytywnie rozpatrzył tylko 42% dotychczasowych polskich wniosków o skasowanie danych z wyszukiwarki.

Źródło: <https://spolecznosc.ingbank.pl/-/Blog/7-sposobow-jak-chronic-swoja-prywatnosc-w-sieci/ba-p/4850>

W jaki sposób chronić swoją prywatność w sieci i czy taka prywatność w ogóle istnieje?

Prywatność w sieci jest możliwa, jednak wiąże się z koniecznością instalacji dodatkowych aplikacji i nieustannej ostrożności. Przede wszystkim nie należy korzystać z publicznych sieci wi-fi, np. w parkach, czy kawiarniach. Nawet stałe, domowe łącze nie gwarantują 100% bezpieczeństwa. Pierwszą z opcji jest tzw. VPN – Virtual Private Network. W tym przypadku prywatność w sieci jest zapewniana przez szyfrowane połączenie oraz utworzenie „tunelu” wewnątrz internetu, co zapobiega przechwyceniu danych przez inne osoby. Jedną z takich aplikacji jest USAIP. VPN jest przeważnie wykorzystywane przez firmy, rzadziej przez osoby prywatne. Możesz też wykorzystywać tzw. serwer proxy. Serwer proxy wykonuje pewne czynności za klienta, jest pośrednikiem, co umożliwia ukrycie na przykład adresu IP. Najprostszym sposobem na zapewnienie minimum prywatności w sieci jest wykorzystywanie trybu

prywatnego (incognito), w którym to trybie przeglądarka nie zapisuje historii ani plików cookies, czyli małych plików tekstowych, które gromadzą informacje na temat aktywności użytkownika w sieci. Możesz również zainstalować różnego rodzaju przeglądarki lub nakładki do najpopularniejszych przeglądarek takich jak Google Chrome, czy Mozilla Firefox. Wykorzystuj również bezpieczne skrzynki pocztowe. Google może śledzić treść Twoich maili, „na szczęście” wykorzystywane jest to głównie do personalizacji reklam. Istnieją rozszerzenia do najpopularniejszych przeglądarek lub nakładki, dzięki którym twoja poczta elektroniczna będzie szyfrowana. Jeżeli wykorzystujesz i przechowujesz dane w tzw. chmurze rozsądnie wcześniej jest je zaszyfrować. Możesz wykorzystać różne aplikacje, dostępne do pobrania za darmo w internecie. Wykorzystując portale społecznościowe nie podawaj prawdziwych danych lub podawaj tylko te najbardziej konieczne. Wydaje się, że nie da się zachować i ochronić swojej prywatności w sieci w 100%. Oprócz wykorzystywania wyżej wymienionych aplikacji, czy nakładek warto również rozsądnie decydować, które treści chcemy umieścić w internecie.

Źródło: <https://poradnikprzedsiębiorcy.pl/-jak-chronic-prywatnosc-w-sieci>

Zasady dotyczące danych przechowywanych przez Facebook – najczęstsze pytania i odpowiedzi.

- 1. Rodzaj gromadzonych informacji** – Facebook gromadzi mnóstwo informacji na twój temat. Przede wszystkim są to informacje takie jak: to, co robisz i robią inne osoby oraz informacje, których dostarczasz i dostarczają inne osoby; informacje o urządzeniach; informacje od partnerów
- 2. Korzystanie z tych informacji** – Facebook wykorzystuje te informacje, aby dostarczać, personalizować i ulepszać swoje produkty; świadczyć usługi pomiarowe, analityczne i inne usługi biznesowe; dbać o bezpieczeństwo i integralność użytkowników i danych; komunikować się z użytkownikiem; przeprowadzać badania i wprowadzać innowacje na rzecz spraw społecznych.
- 3. Udostępnianie tych informacji** – te informacje są udostępniane innym osobom i kontom, z którymi się komunikujesz i dzielisz informacjami; aplikacjom, witrynom i innym rozwiązaniom opartym na produktach Facebooka; ewentualnym nowym właścicielom; partnerom, korzystającym z usług analitycznych Facebooka; reklamodawcom; partnerom, oferującym towary i usługi w produktach Facebooka; sprzedawcom i dostawcom usług; badaczom i naukowcom; organom ścigania lub innym instytucjom prawnym na ich wniosek;
- 4. Podstawa prawna gromadzenia danych** – Facebook gromadzi dane w zakresie wymaganym do wypełnienia Regulaminu Facebooka lub Regulaminu serwisu Instagram; w stopniu niewykraczającym poza udzieloną przez użytkownika zgodę, którą można w każdym momencie cofnąć w ustawieniach Facebooka lub ustawieniach Instagrama; w zakresie wymaganym do zapewnienia zgodności ze zobowiązaniami prawnymi Facebooka; do zabezpieczenia podstawowych interesów użytkownika; w zakresie wymaganym na mocy interesu publicznego; w stopniu wymaganym przez uzasadnione interesy spółki Facebook lub innych podmiotów;
- 5. Przechowywanie danych** – Facebook przechowują dane dopóki są mu potrzebne do świadczenia usługi i dostarczania produktów Facebooka albo do usunięcia konta. Jest to ustalane indywidualnie, w zależności od charakteru danych. Na przykład w przypadku wyszukiwania czegoś na Facebooku możesz uzyskać dostęp do swojego zapytania i usunąć je z poziomu historii wyszukiwania, natomiast zapis tego wyszukiwania zostanie usunięty po 6 miesiącach. W przypadku przesłania kopii dowodu osobistego w celu weryfikacji zostanie ona usunięta po 30 dniach. W przypadku skasowania konta informacje na twój temat, udostępniane przez inne osoby nie zostaną usunięte, ponieważ nie należą do Twojego konta.

Źródło: <https://pl-pl.facebook.com/privacy/explanation>