

VPN płatny vs darmowy - co naprawdę chroni Twoje dane?

Konkretnie odpowiedzi na pytania, które zadaje każdy przed wyborem VPN

Tomasz Grabowski · 21.09.2026

Kilka miesięcy temu koleżanka zapytała mnie, czy może korzystać z darmowego VPN-a, który znalazła w sklepie Google Play. Miała 50 000 pobrań i cztery gwiazdki. Sprawdziłem politykę prywatności - firma sprzedawała dane użytkowników brokerom reklamowym. Zamiast chronić jej prywatność, aplikacja robiła dokładnie to, przed czym miała chronić.

To nie jest odosobniony przypadek. Według raportu Top10VPN z 2023 roku, aż 38% najpopularniejszych darmowych aplikacji VPN na Androida zawierało złośliwe oprogramowanie lub agresywne śledzenie. Dlatego zanim pobierzesz cokolwiek z napisem "VPN Free", przeczytaj ten artykuł do końca.

Czym właściwie jest VPN i co powinien robić?

VPN, czyli Virtual Private Network, to tunel szyfrowany między Twoim urządzeniem a serwerem dostawcy. Wszystko, co wysyłasz do internetu, przechodzi przez ten tunel - Twój operator komórkowy, właściciel kawiarni z Wi-Fi ani dostawca internetu nie widzą, co robisz. Widzą tylko tyle, że łączysz się z serwerem VPN.

Dobry VPN robi trzy rzeczy: szyfruje ruch, ukrywa Twój prawdziwy adres IP i nie zapisuje logów z Twojej aktywności. Brzmi prosto. Problem w tym, że "dobry" to słowo, które darmowe usługi rzadko spełniają w całości.

VPN nie jest tarczą przed wszystkim. Nie chroni Cię przed phishingiem, wirusami ani przed tym, że sam podasz hasło na fałszywej stronie. Chroni ruch sieciowy - i tylko to.

Dlaczego darmowy VPN często nie jest darmowy?

Serwery VPN kosztują. Przepustowość kosztuje. Pracownicy kosztują. Jeśli nie płacisz za usługę, ktoś inny musi - i zazwyczaj tym kims jesteś Ty, tyle że walutą są Twoje dane.

Modele zarabiania darmowych VPN-ów są różne. Część sprzedaje dane o odwiedzanych stronach brokerom reklamowym. Inne wstrzykują reklamy do stron, które odwiedzasz. Część udostępnia Twoje łącze innym użytkownikom - tak działał Hola VPN, który przez lata budował sieć z urządzeń swoich użytkowników i wynajmował ją klientom biznesowym. Twój komputer mógł być węzłem w czyjejś sieci botnet.

To nie znaczy, że każdy darmowy VPN jest złośliwy. Istnieją uczciwe darmowe opcje - ale mają poważne ograniczenia, o których za chwilę.

Najczęstsze pytania o VPN płatny vs darmowy

Czy darmowy VPN wystarczy do przeglądania internetu?

Zależy, co masz na myśli przez "wystarczy". Jeśli chcesz tylko ukryć swój ruch przed właścicielem kawiarni, w której siedzisz przy kawie, darmowy VPN może wystarczyć. Jeśli

chcesz realnej ochrony prywatności na co dzień - raczej nie.

Darmowe VPN-y najczęściej oferują limit danych (Proton VPN Free jest wyjątkiem - nie ma limitu, ale ma ograniczoną prędkość i tylko trzy lokalizacje serwerów). Windscribe daje 10 GB miesięcznie w wersji darmowej. TunnelBear - 500 MB. Przy codziennym użytkowaniu te limity kończą się bardzo szybko.

Jak sprawdzić, czy VPN naprawdę nie zbiera danych?

Szukaj audytów zewnętrznych. Poważne firmy - ExpressVPN, NordVPN, Mullvad, Proton VPN - regularnie zlecają niezależnym firmom audytorskim weryfikację swojej polityki no-logs. Wyniki tych audytów są publikowane. Jeśli VPN twierdzi, że nie zbiera logów, ale nigdy nie przeszedł audytu - masz prawo być sceptyczny.

Drugi test to jurysdykcja. Mullvad ma siedzibę w Szwecji, Proton VPN w Szwajcarii. Oba kraje mają silne przepisy o ochronie prywatności i nie należą do sojuszy wywiadowczych Five Eyes ani Fourteen Eyes. To ma znaczenie, gdy organy ścigania zwracają się do firmy z zadaniem wydania danych.

Czy płatny VPN naprawdę jest szybszy?

Tak, i to znacząco. Przetestowałem kilka opcji na połączeniu 100 Mb/s. Bez VPN pobieranie dużego pliku zajmowało mi około 8 sekund. Z Mullvadem - 11 sekund. Z NordVPN - 10 sekund. Z losowym darmowym VPN-em z Play Store - 45 sekund, przy czym połączenie kilka razy się zrywało.

Płatne usługi inwestują w infrastrukturę. NordVPN ma ponad 6400 serwerów w 111 krajach. ExpressVPN - ponad 3000 w 105 krajach. Darmowe usługi mają zazwyczaj kilka przeciążonych serwerów, bo wszyscy użytkownicy korzystają z tej samej puli.

Który VPN jest najlepszy w 2026 roku?

Nie ma jednej odpowiedzi, bo zależy od potrzeb. Zebrałem najważniejsze opcje w tabeli:

Czy VPN chroni mnie na publicznym Wi-Fi?

To jest ten scenariusz, gdzie VPN naprawdę błyszczy. Publiczne sieci Wi-Fi - na dworcu, w hotelu, w centrum handlowym - są podatne na ataki typu man-in-the-middle. Ktoś może podsłuchiwać ruch niezaszyfrowany. VPN szyfruje wszystko, zanim opuści Twoje urządzenie, więc nawet jeśli ktoś przechwyci pakiety, zobaczy tylko zaszyfrowany bełkot.

Tu nawet darmowy VPN z limitem danych może wystarczyć - jeśli korzystasz z publicznego Wi-Fi tylko przez kilka minut, żeby sprawdzić e-mail lub zrobić szybki przelew, 10 MB z limitu Windscribe zrobi robotę.

Czy VPN ukrywa mnie całkowicie?

Nie. To jeden z największych mitów. VPN ukrywa Twój adres IP i szyfruje ruch sieciowy. Ale jeśli jesteś zalogowany na Facebooku, Google lub jakimkolwiek innym serwisie, te firmy nadal wiedzą, kim jesteś i co robisz. Pliki cookie, odciski przeglądarki (browser fingerprinting), śledzenie między stronami - to wszystko działa niezależnie od VPN.

Jesli zależy Ci na pełnej anonimowości, potrzebujesz kombinacji: VPN + przeglądarka Tor + oddzielne konto bez powiązania z Twoją tożsamością. Dla przeciętnego użytkownika to przesada. VPN wystarczy, żeby Twój operator nie widział, co przeglądasz, i żeby strony internetowe nie widziały Twojego prawdziwego adresu IP.

Czy VPN spowalnia internet znacząco?

Każdy VPN spowalnia połączenie - to fizyczna konieczność, bo dane muszą przejść przez dodatkowy serwer i zostać zaszyfrowane. Pytanie, o ile. Dobry płatny VPN na szybkim łączy spowalnia połączenie o 10-20%. Przy łączy 100 Mb/s różnica jest praktycznie nieodczuwalna. Na wolniejszym łączy 20 Mb/s może być bardziej zauważalna.

Darmowe VPN-y potrafią spowalniać połączenie o 60-80% z powodu przeciążonych serwerów. Streaming wideo, wideokonferencje czy duże pobierania stają się wtedy frustrujące.

Kiedy absolutnie nie używać darmowego VPN?

Są sytuacje, gdzie darmowy VPN to zły pomysł niezależnie od wszystkiego:

- Bankowość online i płatności - jeśli VPN loguje ruch, ma dostęp do Twoich danych finansowych. Używaj tylko zaufanych, zaudytowanych usług albo wyłącz VPN na czas transakcji.
- Praca zdalna z wrażliwymi danymi firmowymi - ryzyko wycieku danych klientów lub tajemnic handlowych.
- Aplikacje z nieznanego źródła - VPN-y pobrane spoza oficjalnych sklepów lub z podejrzanych stron mogą być trojanami.
- Długoterminowe codzienne użycie - limity danych sprawiają, że darmowy VPN po prostu przestaje działać w połowie miesiąca.

Mullvad czy NordVPN - co wybrać?

To pytanie, które słyszę najczęściej od osób, które już zdecydowały się zapłacić. Mullvad to opcja dla tych, którym prywatność jest naprawdę ważna. Firma nie wymaga adresu e-mail do rejestracji - dostajesz losowy numer konta. Możesz zapłacić gotówką wysłaną pocztą lub kryptowalutą. Cena jest stała: 5 EUR miesięcznie, bez zniżek za długoterminowe plany.

NordVPN jest bardziej przyjazny dla zwykłego użytkownika. Aplikacja jest prosta, działa na wszystkich urządzeniach, ma dodatkowe funkcje jak bloker reklam i złośliwego oprogramowania (Threat Protection), a przy planie dwuletnim cena spada poniżej 4 EUR miesięcznie. Dla kogoś, kto chce VPN-a "po prostu działającego" - NordVPN to rozsądny wybór.

Czy warto używać VPN na telefonie?

Tak, szczególnie jeśli często korzystasz z sieci komórkowych w podróży lub z publicznego Wi-Fi. Aplikacje mobilne VPN działają dobrze na Androidzie i iOS. Proton VPN Free na telefonie to uczciwa opcja dla okazjonalnego użytku. Przy codziennym użyciu warto rozważyć plan płatny - szczególnie jeśli masz już subskrypcję na komputer, bo większość dostawców pozwala na jednoczesne połączenie na 5-10 urządzeniach.

Co to jest kill switch i czy jest ważny?

Kill switch to funkcja, która blokuje ruch internetowy, jeśli połączenie VPN nagle się zerwie. Bez kill switcha, gdy VPN się rozłączy, Twój ruch płynie normalnie przez Twojego operatora - bez szyfrowania, z prawdziwym IP. Możesz tego nawet nie zauważyć.

Wszystkie poważne płatne VPN-y mają kill switch. Wiele darmowych - nie. Jeśli korzystasz z VPN-a do czegoś ważnego, kill switch to nie opcja, to konieczność.

Jak wybrać VPN dopasowany do Twoich potrzeb?

Zamiast szukać "najlepszego VPN", zacznij od pytania: do czego mi to potrzebne? Poniżej trzy typowe scenariusze:

Scenariusz 1: Ochrona na publicznym Wi-Fi, kilka razy w miesiącu. Proton VPN Free lub Windscribe Free wystarczy. Limity danych nie będą problemem przy okazjonalnym użyciu. Upewnij się, że aplikacja pochodzi z oficjalnego sklepu.

Scenariusz 2: Codzienna ochrona prywatności w domu i pracy. Mullvad lub Proton VPN Plus. Koszt to 48-60 EUR rocznie - mniej niż jedna wizyta u fryzjera. Dostajesz audytowaną politykę no-logs, kill switch i sensowną prędkość.

Scenariusz 3: Rodzina lub kilka urządzeń. NordVPN lub Surfshark. Surfshark pozwala na nieograniczoną liczbę jednoczesnych połączeń w ramach jednej subskrypcji, co przy rodzinie z kilkoma telefonami i laptopami ma sens finansowy.

Nie istnieje VPN, który jest jednocześnie darmowy, szybki, bezpieczny i bez logów. Możesz wybrać maksymalnie dwie z tych cech. Darmowe usługi z reguły rezygnują z bezpieczeństwa lub prywatności.

Czerwone flagi - jak rozpoznać zły VPN?

Kilka sygnałów ostrzegawczych, które powinny Cię zatrzymać przed instalacją:

- Brak polityki prywatności lub polityka napisana niezrozumiałym żargonem bez konkretnych
- Siedziba firmy w kraju bez przepisów o ochronie danych (niektóre "VPN-y" mają siedzibę na Seszelach lub Brytyjskich Wyspach Dziewiczych - brzmi egzotycznie, ale może oznaczać brak jakiegokolwiek regulacji)
- Obietnica "100% anonimowości" - żaden uczciwy dostawca tak nie twierdzi
- Aplikacja prosi o uprawnienia, których VPN nie potrzebuje - dostęp do kontaktów, SMS-ów, aparatu
- Brak informacji o protokołach szyfrowania - uczciwy VPN zawsze podaje, czy używa WireGuard, OpenVPN czy IKEv2
- Recenzje w sklepie wyglądają na fałszywe - krótkie, entuzjastyczne, bez konkretnych

Dodatkowe zasoby i co warto przeczytać

Jeśli chcesz sprawdzić VPN przed pobraniem, zacznij od niezależnych źródeł. Strona That One Privacy Site (działa jako archiwum) zawierała przez lata szczegółowe porównania polityk prywatności. Privacy Guides ([privacyguides.org](https://www.privacyguides.org)) to aktualizowana regularnie baza rekomendacji, prowadzona przez społeczność bez powiązań z dostawcami VPN. Warto też zajrzeć na strony samych dostawców i poszukać linków do opublikowanych raportów z

audytów - Mullvad i Proton VPN publikują je otwarcie.

Jeśli interesuje Cię temat szerzej, polecam też artykuły o uwierzytelnianiu dwuskładowym i menedżerach haseł - VPN to tylko jeden element układanki. Sam bezpieczny VPN nie pomoże, jeśli używasz hasła "123456" do konta bankowego.

Jeden praktyczny krok na dziś: wejdź na stronę ipleak.net lub dnsleaktest.com i sprawdź, czy Twój obecny VPN (jeśli go używasz) naprawdę ukrywa Twój adres IP i nie wycieka DNS. Zajmuje to 30 sekund i od razu wiesz, czy płacisz za coś, co działa.