

Co to jest VPN i jak działa?

21 października 2022

Wirtualna sieć prywatna (VPN) szyfruje Twoje dane osobowe i ukrywa Twój prawdziwy adres IP w sieci. Jest to jedno z najpopularniejszych rozwiązań służących ochronie prywatności i bezpieczeństwa w Internecie. Oprócz korzyści związanych z prywatnością i bezpieczeństwem, VPN pozwala na dostęp do większej ilości treści w Internecie. Dzięki niemu możesz zmienić swoją wirtualną lokalizację i omijać geograficznie zablokowane strony internetowe. Czym jest VPN, jak działa i dlaczego powinieneś go używać? O tym w niniejszym artykule.

Co to jest VPN i jak działa?

VPN co to? Ustanawia on bezpieczne połączenie internetowe poprzez ukrycie adresu IP i szyfrowanie ruchu internetowego. Połączenie się z VPN pozwala również na dostęp do treści o ograniczonym zasięgu geograficznym, np. do stron zablokowanych w Unii Europejskiej.

Kiedy łączysz się z Internetem bez wirtualnej sieci prywatnej, Twój dostawca usług internetowych (ISP) jest głównym pośrednikiem między Twoim urządzeniem a Internetem. Dostawca usług internetowych przypisuje unikalny adres IP do Twojego urządzenia i śledzi wszystkie odwiedzane przez Ciebie strony internetowe. W przeciwieństwie do tego, gdy połączysz się z VPN, wszystkie żądania internetowe przechodzą przez zaszyfrowany tunel i są kierowane przez serwer VPN przed dotarciem do serwera docelowego, gdzie przechowywana jest pożądana strona internetowa. Po przetworzeniu żądania, dane wysyłane z powrotem do urządzenia (Twojego komputera, czy telefonu) przechodzą przez ten sam szyfrowany proces połączenia VPN.

Podczas korzystania z VPN połączenie internetowe Twojego urządzenia nadal przebiega za pośrednictwem Twojego dostawcy

Internetu. Ponieważ jednak jest ono zaszyfrowane i przechodzi przez serwer VPN, Twój dostawca usług internetowych nie będzie już widział stron, które odwiedzasz. Wie tylko, że jesteś podłączony do VPN i że zaszyfrowany ruch trafia z Twojego urządzenia do serwera.

Oto kilka kluczowych procesów, które wykonuje VPN, oraz ich korzyści

- Proxy. Podobnie jak zwykłe proxy, VPN ukrywa Twój adres IP i lokalizację, aby zwiększyć Twoją anonimowość online. Strony internetowe, które odwiedzasz, widzą jedynie adres IP i lokalizację serwera VPN.
- Uwierzytelnianie. Proces uwierzytelniania zapewnia, że Twój klient VPN wchodzi w interakcję tylko z serwerem docelowym, z którym chcesz się połączyć. Zapobiega to przechwytywaniu Twoich danych przez inne osoby trzecie.
- Szyfrowanie. Wiele stron internetowych, które korzystają z SSL lub TLS, szyfruje dane wymieniane między urządzeniem użytkownika a serwerem docelowym. Jednak to szyfrowanie jest ograniczone do niektórych odwiedzanych przez Ciebie stron internetowych. Tymczasem tunel VPN szyfruje cały ruch. Wiele dostawców VPN stosuje szyfrowanie klasy wojskowej, które jest prawie niemożliwe do odczytania przez osoby trzecie.

Dane osobowe, które technologia VPN może ukryć po jej uruchomieniu

- Adres IP. Adres IP jest unikalnym identyfikatorem urządzenia. Pozwala on na ustalenie wrażliwych danych, takich jak dostawca usług internetowych, kraj, miasto czy nawet adres zamieszkania. VPN ukrywa Twój adres IP za pomocą swojego

własnego.

– Położenie. Ponieważ VPN-y ukrywają Twój prawdziwy adres IP, może się wydawać, że przeglądasz strony z innej lokalizacji. Na przykład, jeśli jesteś w Polsce, ale łączysz się z serwerem VPN w USA, inni użytkownicy będą myśleć, że Twoja lokalizacja to USA.

– Historia wyszukiwania i przeglądania. Ponieważ Twoje połączenie internetowe przechodzi przez zaszyfrowany tunel VPN, Twój dostawca usług internetowych lub złośliwe strony trzecie nie będą wiedzieć, co wyszukujesz i przeglądasz online. Pomaga to uniknąć spersonalizowanych reklam i ogólnie chronić prywatność w Internecie.

Prywatność

VPN szyfruje Twój ruch sieciowy i kieruje Twoje połączenie internetowe przez zdalny serwer. Pozwala ukryć dane online, takie jak adres IP, lokalizacja, historia wyszukiwania i przeglądania oraz pobranie pliki. W związku z tym dostawca usług internetowych, odwiedzane strony internetowe i inne osoby trzecie nie mogą ich odczytać.

Niestety, w Internecie roi się od zagrożeń cybernetycznych dla stron internetowych i użytkowników. Szyfrowanie VPN i maskowanie adresów IP zasadniczo wzmacnia Twoje bezpieczeństwo w sieci. Jeśli przeglądasz Internet korzystając z niezaufanego połączenia, takiego jak publiczna sieć Wi-Fi, ryzyko, że padniesz ofiarą cyberataku jest wysokie. Połączenie z serwerem VPN zaszyfruje Twoje połączenie internetowe i ukryje Twoje IP w tych niezabezpieczonych sieciach.

W przypadku pracowników zdalnych korzystanie z VPN jest konieczne nie tylko w celu uzyskania dostępu do plików firmowych. Zabezpiecza również wrażliwe dane firmowe przed odczytaniem lub kradzieżą przez osoby trzecie.

Zyskujesz wolność

VPN zmienia wirtualną lokalizację. Ta funkcja daje użytkownikom VPN swobodę dostępu do treści zablokowanych w ich regionie. Na przykład program telewizyjny, który chcesz obejrzeć na Netflixie, może być dostępny tylko w określonej lokalizacji. Zmieniając swoją lokalizację na inny kraj za pomocą VPN, będziesz mógł uzyskać dostęp do treści geoblokowanych.

Połączenia VPN pozwalają również ominąć ograniczenia przepustowości przez dostawców usług internetowych. Wielu dostawców usług internetowych ogranicza szerokość pasma dostępnego dla szeregu zasobożernych usług internetowych, takich jak serwisy strumieniowe lub sieci peer-to-peer (P2P). Z VPN możesz to obejść, aby w pełni wykorzystywać Twoje połączenie internetowe przez cały czas.

Podobnie, niektóre sklepy e-commerce i strony z biletami wyświetlają różne ceny dla swoich klientów w oparciu o ich lokalizację, ustalając ceną na podstawie statusu społeczno-ekonomicznego. VPN może temu zapobiec i pomóc Ci uzyskać najlepszą cenę za zakupy online.

Podsumowanie

VPN to cenne i łatwe w użyciu narzędzie, jeśli zależy Ci na prywatności, bezpieczeństwie i wolności w sieci.

Autorstwo: Marcin Dyja

Źródło: [MagazynFakty.pl](https://magazynfakty.pl)

Uzupełnienie „Wolnych Mediów”

Skąd wziąć bezpłatny VPN? Przeglądarka Opera ma rutynowo wbudowany VPN, który należy włączyć w ustawieniach przeglądarki. W FireFoxie można skorzystać z wtyczek, które

znajdziesz [TUTAJ](#). Podobne wtyczki istnieją dla przeglądarek opartych na silniku Chrome – patrz [TUTAJ](#).