Презентація з інформатики

- **ТЕМА: Віртуальні приватні мережі (VPN)**

Виконала уч-ця 10-А класу ЗОШ І-ІІІ СТ. # 9
Захарченко Мілана

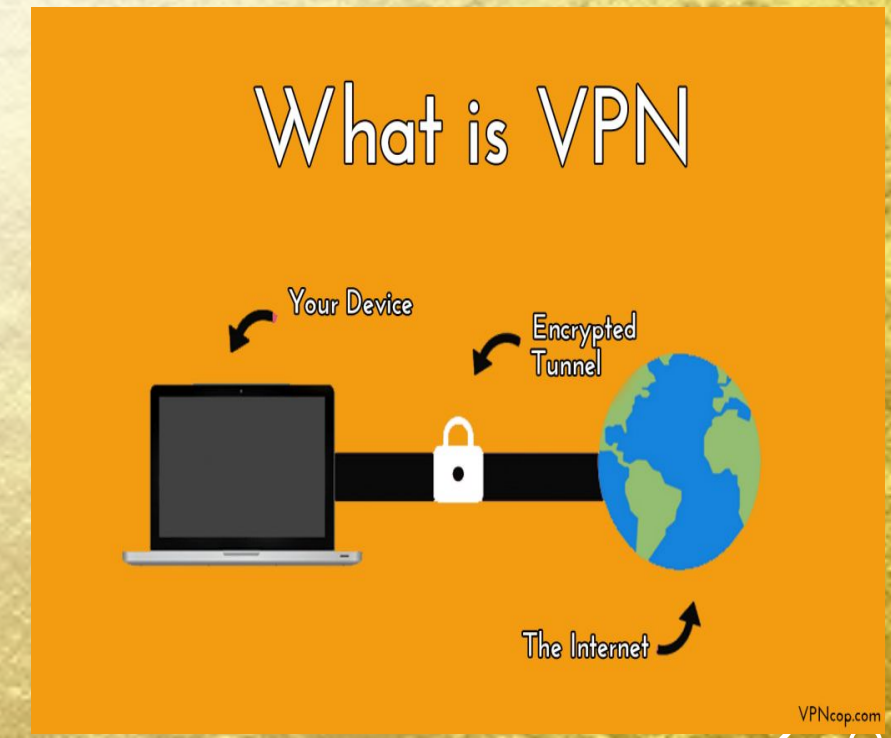
Що таке *VPN*?

VPN - це послуга, яка створює зашифроване з'єднання з вашого пристрою на сервер VPN через ваше з'єднання з Інтернетом. Подумайте про це як про тунель через гору, в якій вашим постачальником послуг Інтернету (ISP) є гора, тунель - це з'єднання VPN, а вихід - до всесвітньої мережі.

Деякі люди можуть помилково сприйняти VPN як альтернативу підключенню до Інтернету, але це неправильно.

Спочатку мережі VPN створювались для з'єднання ділових мереж для більш безпечного та зручного спілкування. Сьогодні постачальники послуг VPN наполегливо працюють, щоб перенаправити весь ваш трафік в Інтернет, минаючи моніторинг уряду чи Інтернет-провайдера, а в деяких випадках навіть примусову цензуру.

У двох словах, подумайте про VPN як про службу, яка розроблена для того, щоб допомогти вам отримати повний доступ до Інтернету та захистити вас при цьому.



Що робить VPN?

Основна мета VPN - створити захищений тунель для переміщення ваших даних до своїх серверів перед передачею в Інтернет. Однак це призвело до деяких інших переваг, таких як підробка місця.

Хоча це може здатися вам незначним, часто буває, коли підробка місцеположення допомагала людям подолати бар'єри геолокації. Візьмемо для прикладу Великий брандмауер Китаю . Китайський уряд жорстко цензурує Інтернет, і багато речей, які ми сприймаємо як належне в Інтернеті, заблоковані в Китаї . Лише за допомогою VPN користувачі з Китаю можуть отримати доступ до таких сайтів, як Google та Facebook.

Для одноранговых користувачів (P2P), крім ризику ідентифікації, ви також ризикуєте визначити свої карти портів за допомогою Torrenting. VPN допомагають замаскувати все це, щоб ваші відкриті

ЯК ПРАЦЮЄ VPN?

Трохи важко описати, як працює VPN, якщо не задіяно трохи технічних деталей. Однак для тих, хто просто хоче базової концепції, VPN створює захищений тунель від вашого пристрою до сервера VPN, а потім звідти до всесвітньої мережі.

Більш детально, VPN спочатку встановлює протокол зв'язку з вашого пристрою. Цей протокол встановить межі способу переміщення даних із вашого пристрою на сервер VPN. Є кілька основних протоколів VPN, які є загальними, хоча кожен має свої переваги та недоліки.

Загальні протоколи VPN

Хоча існує багато протоколів зв'язку, є деякі загальнодоступні, які зазвичай підтримуються незалежно від торгової марки VPN. Хтось швидший, хтось повільніший, хтось більш безпечний, інші менш. Вибір за вами, залежно від ваших вимог, тому це може бути хорошим розділом для вас, на який слід звернути увагу, якщо ви збираєтеся використовувати VPN.

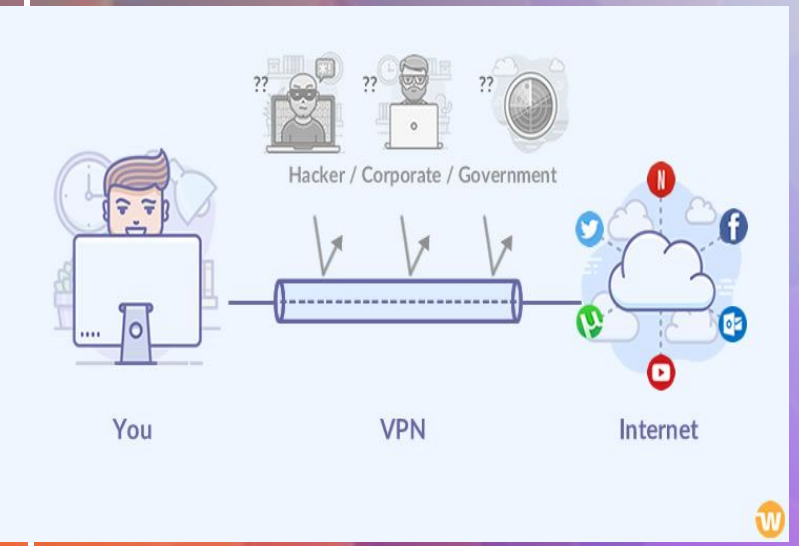
Підсумовуючи

OpenVPN : Протокол з відкритим кодом, який має середню швидкість, проте пропонує потужну підтримку шифрування.

L2TP / IPSec : Це також досить поширене явище і пропонує пристойні швидкості, але легко блокується деякими сайтами, які не надають перевагу користувачам VPN.

SSTP : Не настільки загальнодоступне, крім хорошого шифрування, не так багато рекомендацій.

IKEv2 : Дуже швидке підключення і особливо добре для мобільних пристроїв, хоча пропонує слабші стандарти



Послуги віртуальної приватної мережі (VPN) сьогодні є однією з найактуальніших тем, оскільки конфіденційність Інтернету піддається обстрілу з багатьох напрямків. Компанії намагаються зібрати більше даних про своїх користувачів настільки, наскільки це стає надмірно нав'язливим (потрібен приклад? Подивіться це , це , це і це), тоді як країни розділені щодо того, як управляти ситуацією.

Протягом багатьох років ми використовуємо такі основні продукти, як Facebook, Google, програмне забезпечення Microsoft та багато іншого, але технологія, що швидко розвивається, спокушає ці компанії вимагати від користувачів облікового запису кожної інформації, яку вони можуть, у комерційних цілях.

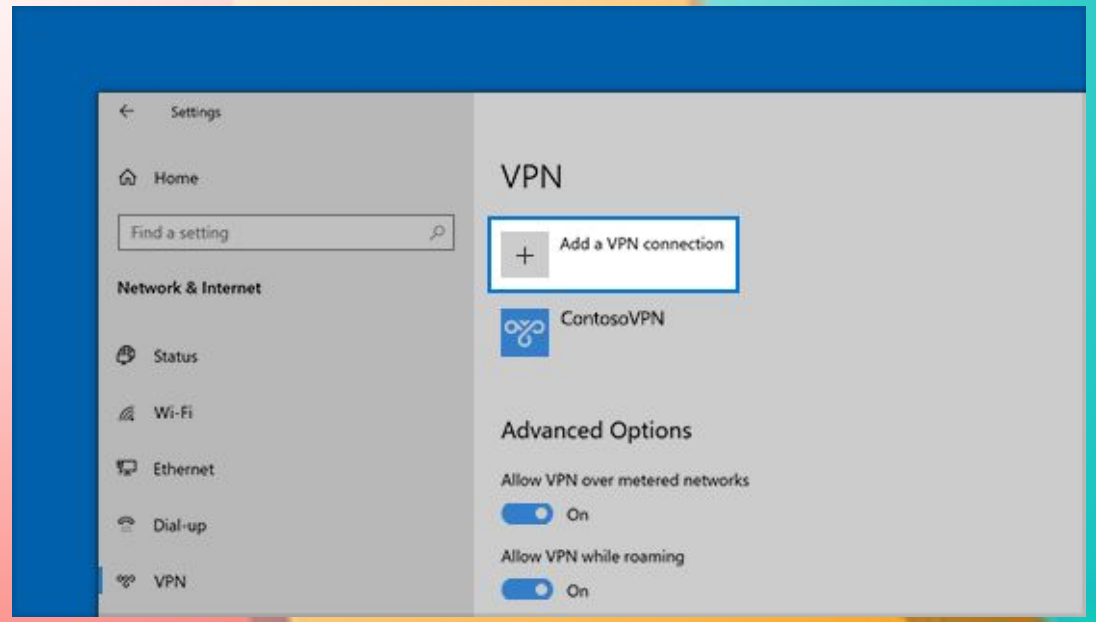
І хоча уряди можуть боротися за контроль над ситуацією, в деяких випадках саме вони винні в тих самих гріхах, за які потрапляють корпорації, - втручанні в приватне життя та незаконному збиранні приватних даних .

Отже, що ми можемо зробити для захисту приватності в Інтернеті?

ЗАПИТАННЯ ТА ВІДПОВІДІ

Чи потрібне підключення до Інтернету для використання VPN?

VPN призначений для маскування та захисту вашого місцезнаходження та даних, але вам все одно потрібне з'єднання з Інтернетом.



Скільки коштує послуга VPN?

Як і всі постачальники послуг, компанії VPN хочуть, щоб ви залишалися з ними надовго, оскільки це їхній потік доходу. Більшість постачальників послуг VPN пропонують різні умови платежів, такі як щомісячні, щоквартальні тощо. У більшості разів, чим довший план, тим дешевше буде ваш щомісячний тариф, але вам доведеться сплатити весь контракт заздалегідь. Очікуйте платити від 9 до 12 доларів на місяць в середньому за щомісячні контракти, зі знижками до 75% для довгострокових контрактів.

ЗАПИТАННЯ ТА ВІДПОВІДІ

Чи зменшить швидкість мого Інтернету використання VPN?

VPN створені в першу чергу для захисту вашої особистості та збереження ваших даних. На жаль, одним із побічних ефектів шифрування, яке використовується для захисту ваших даних, є те, що це уповільнює ваше з'єднання з Інтернетом. Як правило, сподівайтесь досягти не більше 70% від вашої фактичної швидкості лінії при використанні VPN. Інші фактори, такі як відстань від сервера VPN, навантаження сервера тощо, також впливатимуть на швидкість вашого Інтернету під час використання VPN .

Наскільки складно встановити з'єднання VPN?

По праву це повинно бути таким же простим, як встановлення програми та введення вашого імені користувача та пароля. Тоді все, що вам потрібно зробити, це натиснути кнопку, і ви під'єднаєтесь до сервера VPN. На жаль, це не завжди найкраще рішення, і для оптимальної роботи, можливо, доведеться налаштувати деякі підключення. Багато постачальників послуг VPN, такі як NordVPN , Surfshark та ExpressVPN , матимуть навчальні посібники, як це зробити, якщо не вдасться зв'язатися зі своїм персоналом служби підтримки.

На яких пристроях можна запустити VPN?

Це залежить від того, з яким постачальником послуг VPN ви зареєструвались. Майже всі провайдери підтримуватимуть Windows, MacOS та Linux разом із основними мобільними платформами. Багато хто також підтримуватиме розгортання маршрутизатора (залежно від моделі маршрутизатора), тоді як деякі обслуговують більш екзотичні пристрої, такі як Raspberry Pi.

ЗАПИТАННЯ ТА ВІДПОВІДІ

Хтось знатиме, що я використовую VPN?

Деякі веб-сайти намагаються уникати користувачів VPN і мають способи виявити, чи вхідне з'єднання відбувається з сервера VPN. На щастя, VPN знають про це і придумали контрзаходи, які допомагають. Зверніть увагу на постачальників послуг, які пропонують крадіжку або заплутування сервера.

Чи можу я просто використовувати розширення браузера VPN?

Я спробував кілька розширень для браузера VPN і виявив, що здебільшого вони поділяються на дві основні категорії. Є такі, які виступають як проксі-сервери і просто відхиляють ваше з'єднання від сервера, а деякі виконують функції керування браузером для повної програми VPN. Останнє означає, що вам все одно знадобиться встановлена програма VPN, щоб використовувати розширення. Розширення браузера VPN зазвичай не є повноцінними послугами VPN.

Чи законно використовувати VPN?

Так і ні. Хоча в більшості країн немає законів проти використання VPN, деякі прямо забороняють це. У крайніх випадках деякі країни не лише забороняють використання VPN, але й потенційно ув'язують користувачів VPN. На щастя, є лише кілька країн, де до цього часу заборонені VPN.

Я повністю відстежуваний за допомогою VPN?

Це багато в чому залежить від того, наскільки безпечно ви користуєтеся своїм з'єднанням VPN і від того, якого провайдера ви вибрали. Було багато випадків, коли користувачів VPN заарештовували після того, як вони повірили постачальнику послуг, який врешті-решт передав журнали користувачів органам влади.

ПІДСУМОК. ЧИ ПОТРІБНА НАМ VPN?

Особиста конфіденційність в Інтернеті обложена з багатьох напрямків, і, здається, це сталося за одну ніч. Пройшли ті часи, коли нам довелося турбуватися лише про кіберзлочинців, але тепер ми також маємо турбуватися про компанії та уряди, які хочуть викрасти наші дані з тієї самої причини - використовувати для своїх цілей.

Природно, що ваша потреба в VPN багато в чому залежатиме від того, в якій країні ви перебуваєте, оскільки кожна з них має різні рівні загрози. Питання не в тому, на що можна відповісти простим так чи ні.

Однак, виходячи зі швидкості зростання вартості світового ринку VPN , я скажу, що дуже ймовірно, що він вам знадобиться рано чи пізно. Минулий час окремі користувачі почали сприймати свою конфіденційність та безпеку в Інтернеті як належне і шукати способи захистити свою інформацію.

Ми самозадоволено користуємось Інтернетом майже так само, як і завжди, просто переглядаючи як можна безтурботніше. Правда, віруси та шкідливе програмне забезпечення зробили нас обережнішими, але змінилося не багато.

Існує думка, що прийняття послуги VPN має стати наступним кроком, який робить кожен користувач Інтернету. Існує нагальна потреба вирватися з мислення, що нам не загрожує те, що ми робимо в Інтернеті.


Thank you!