Безпека в мережі інтернет. Інформаційна безпека в інтернеті

Безпека в інтернеті - дуже важлива проблема нинішнього часу. І стосується вона всіх, від дітей до пенсіонерів. Вона стає все актуальнішою у зв'язку з масовим приходом в інтернет користувачів, майже, а то і зовсім, чи не підготовлених до погроз, їх чекають. Тому дана стаття і буде присвячена такого питання, як безпека в мережі інтернет. Адже страждає не один користувач, а й багато інших, об'єднані в одну глобальну структуру.

Небезпеки, що підстерігають нас в мережі.

Якщо сказати коротко, то існують дві основні можливості того, як може ваш комп'ютер стати жертвою. Перше - ви самі, мандруючи по різних сайтах або встановлюючи програмне забезпечення з неперевірених джерел, а іноді і з перевірених, заражаєте свій комп'ютер. Друге - можлива також ситуація, коли зловмисники навмисно, за допомогою, наприклад, троянських програм або вірусів, роблять ваш пристрій джерелом небезпеки.

В результаті всього цього комп'ютер, іноді навіть таємно від свого власника, починає виконувати розсилку спаму, бере участь в DDoS-атаках на різні сайти, краде паролі. Буває й так, що провайдер змушений примусово відключити такий пристрій від глобальної мережі. Виходить, що якщо користувач не обізнаний про те, що являють собою основи безпеки в мережі інтернет, доведеться йому важко.

Навіщо потрібен зловмисникам доступ до комп'ютера користувача.

Даремно звичайний користувач думає, що його комп'ютер нікому не потрібен. Це раніше хакери часто писали віруси просто заради інтересу, зараз же це робиться майже завжди з комерційною вигодою. Років 20 тому назад зловмисник отримував задоволення від того, що міг просто відформатувати жорсткий диск. Або зробити так, що при включенні комп'ютера замість стандартного робочого столу з'являться які-небудь прикольні картинки. Зараз же вони роблять все можливе, щоб власник ПК якомога довше не знав про те, що його пристрій заражено і таємно від нього виконує додаткові функції.

Для чого все це робиться? Крім того, про що було сказано вище, хакери намагаються отримати доступ до ваших електронної пошти, гаманцях, аккаунтам в соціальних мережах, форумах. Трапляється так, наприклад, що ви лягаєте спати з 20 000 рублів на електронному гаманці, а вранці отримуєте СМС-повідомлення про те, що грошей на ньому вже немає. А з пошти всі ваші контакти, та й не тільки, отримують спам-листи, а то ще й трояни. Хакери можуть об'єднати безліч заражених комп'ютерів в єдину потужну мережу, провести DDoS-атаку навіть на потужні державні сервери. З самого простого, але також приносить гроші: заблокують роботу операційної системи і вимагатимуть гроші за усунення проблеми. І, до речі, гроші візьмуть, але комп'ютер залишать заблокованим. Так що безпека в мережі інтернет повинна стати основою вашої роботи в ній.

Як зловмисники проникають у комп'ютер? Детальна інформація.

Для того щоб зламати захист ПК, навіть якщо вона є, хакери застосовують цілий ряд способів, і користувачі даремно думають, що, просто встановивши антивірус, вони позбулися небезпеки, наприклад, підчепити шкідливу програму. Тому, перш ніж шукати інформацію про те, як правильно дотримуватися безпеку в мережі інтернет, потрібно зрозуміти, а звідки беруться віруси і трояни. Зараз ми перерахуємо основні шляхи їх проникнення і методи злодійства різної інформації.

1. Перший метод називається соціальною інженерією. Завдяки різним психологічним прийомам, прийомам і довірливості користувачів хакери надсилають вам цілком нешкідливий файл або лист, а ви самі і запускаєте троянчік в ньому. Або ж на прохання нібито адміністрації сервісу видаєте всі свої паролі і явки.

2. Другий метод - пропонується різний безкоштовне програмне забезпечення, піратські диски, де заховано безліч вірусів, троянів і тому подібної гидоти.

3. В ПЗ, в тому числі і з найнадійніших перевірених джерел, постійно з'являються дірки в безпеці. Це відноситься і до операційних систем. Ось зловмисники уважно і стежать за такими моментами, намагаються їх не упустити, а використовувати у власних цілях. Зайдете на яку-небудь сторінку сто разів перевіреного сайту і - раз - ваш пристрій заражено.

4. Четвертий спосіб отримав особливе поширення останнім часом. Це фішинг, коли створюються підроблені сайти. І ви замість сторінки свого банку опиняєтеся на його підробленої копії. Про те, що може бути далі, говорити не будемо, самі здогадаєтеся.

Початковий захист комп'ютера користувача

В ідеалі, купивши ПК, користувач повинен виконати цілий ряд операцій, перш ніж кинутися борознити нескінченні простори мережі. Зараз ми представимо деякі найперші уроки безпеки в інтернеті.

1. Незважаючи на те що Windows має вбудований файрвол, рекомендується встановити більш надійний, тому що наявний - далеко не найкращий. Вибирайте платний або безкоштовний, виходячи з їхніх рейтингів.

2. Наступний крок - установка антишпигунського та антивірусного ПЗ. Потрібно відразу ж його оновити та налаштувати на автоматичне

оновлення. Також воно має запускатися автоматично, разом з ОС. І постійно, у фоновому режимі, працювати. І обов'язково перевіряйте будь-яку встановлювану програму.

3. Як тільки з'являються оновлення для Internet Explorer і інших використовуваних вами браузерів, тут же завантажуйте їх і встановлюєте.

4. Відключайте всі невживані служби на своєму пристрої, це зменшить шанси для хакерів отримати до нього доступ.

Подальші уроки безпеки

Тепер трохи інформації про те, як забезпечити безпеку роботи в мережі інтернет. Виконавши вказане в попередньому розділі, продовжуйте не забувати про щоденну захисті.

1.Видаляйте відразу ж всі листи підозрілого змісту, не здумайте відкривати файли з невідомих джерел. Ігноруйте всі пропозиції легкого заробітку, нікому не висилайте свої паролі, не переходьте за підозрілими посиланнями.

2. Використовуйте тільки складні паролі, що складаються з складного набору цифр, букв і символів. Для кожного випадку призначайте свій, оригінальний.

3. Виходячи в мережу з місць загального користування, будьте акуратні й обережні. Це ж стосується і використання проксі-серверів. Бажано не проводити ніяких банківських та інших подібних операцій з таких місць.

4. Віддавайте перевагу працювати з платіжними системами через їх власні програми, а не через сайт. Це набагато безпечніше.

5. Небажано відвідувати сайти для дорослих або подібні їм ресурси. Велика ймовірність підхопити троян.

6. Слідкуйте за інтернет-трафіком, навіть якщо він безлімітний. Якщо він без особливої причини значно збільшився, це може бути ознакою активності вірусу. Якщо будете дотримуватися цих мінімальні правила безпеки в мережі інтернет, то уникнете багатьох проблем. Це, звичайно, далеко не все. Небезпек стільки, що не можна про них забувати ні на хвилину.

Ще деякі уроки безпеки в інтернеті

Зараз коротко розповімо ще про деякі заходи обережності. Якщо з вашого банку прийшов лист з перевіркою пароля, не здумайте їм його відправляти. Банки ніколи таких запитів не роблять. Всі поштові програми мають фільтр від спаму. Довіряйте йому. Отримавши листа про виграш в мільйон рублів або спадщині в п'ять мільйонів доларів, видаляйте їх відразу ж. Рекомендуємо встановлювати комплексний захист. Вона надійніше, ніж антивірус - від одного виробника, файрволл - від іншого, а антишпигунська програма - від третього.

Віддавайте перевагу платним версіями. Так як Opera і Internet Explorer - найпоширеніші браузери, для них і вірусів існує більше всього. Використовуйте альтернативні варіанти: Apple Safari, Google Chrome і Mozilla Firefox. Не користуйтеся неліцензійним програмним забезпеченням, так як в ньому спочатку може бути встановлено шпигунське ПЗ. Якщо робіть покупки в онлайн-магазинах, то користуйтеся тільки перевіреними варіантами. Це ж відноситься і до будь-якого іншого онлайн-сервісу. Виконуйте всі ці вимоги, і тоді безпека в мережі інтернет буде більш-менш гарантована.