

Організація безпеки в домашній мережі

Звідки беруться загрози

Ось загальний перелік можливих загроз

- Інтернет
- заражені накопичувачі (флешки, диски та ін.)
- Заражена машина в домашній мережі (інший комп'ютер, ноутбук, планшет чи смартфон)
- Взламаний роутер
- Адміністративний доступ
- Доступ до засобів захисту

Отже по порядку, основними загрозами в інтернеті є фішингові сайти, сайти котрі розповсюджують зловмисні програми та реклама (так - реклама також [може бути заражена](#))

Способи захисту в домашній мережі

Перше коло захисту в інтернеті

Захист від зловмисних сайтів, не обов'язково покладати на [антивірус](#) ще до того як ви побачите загрозу її можна уникнути. В цьому допоможуть [DNS](#) - сервіси, вони вміють фільтрувати запити на ранніх підступах - ще до того як вони потраплять до вас.

Просто виберіть потрібний вам захист та користуйтеся



[DNS](#) - оберіть потрібний саме вам

Коло друге - реклама та частково фішинг

Плагіни для блокування майнерів, фішингу та реклами



На даний момент рекомендую [uBlock Origin](#) - який є для усіх популярних браузерів.

[Firefox/Firefox for Android](#)

[Chrome Web Store](#)

[Opera add-ons](#)

Інші варіанти:

- [AdGuard](#)
- [AdBlock](#)
- [Opera](#) - Потрапила сюди виключно тому, що має вбудований (і непоганий) блокувальник реклами та ще багато чого. Колись я напишу окрему статтю про [Opera](#)
- [Adblock Plus](#) - популярний, хоча й не ідеальний, відомий тим, що [пропускає рекламу](#) за гроші
- [Ghostery](#) блокувальник реклами з функцією приватності

Плагіни від виробників антивірусів

- [Avast Online Security "Chrome"](#) [Avast Online Security "Firefox"](#) [Avast Online Security "Opera"](#)
- [McAfee SECURE Safe Browsing "Chrome"](#)
- [Перевірка посилань від Dr.Web "Chrome"](#)

Третє коло - роутер

Основні проблеми роутерів дві:

- Дефолтні паролі, знайти їх можна на сайті <http://routerpasswords.com/>
- Старі прошивки



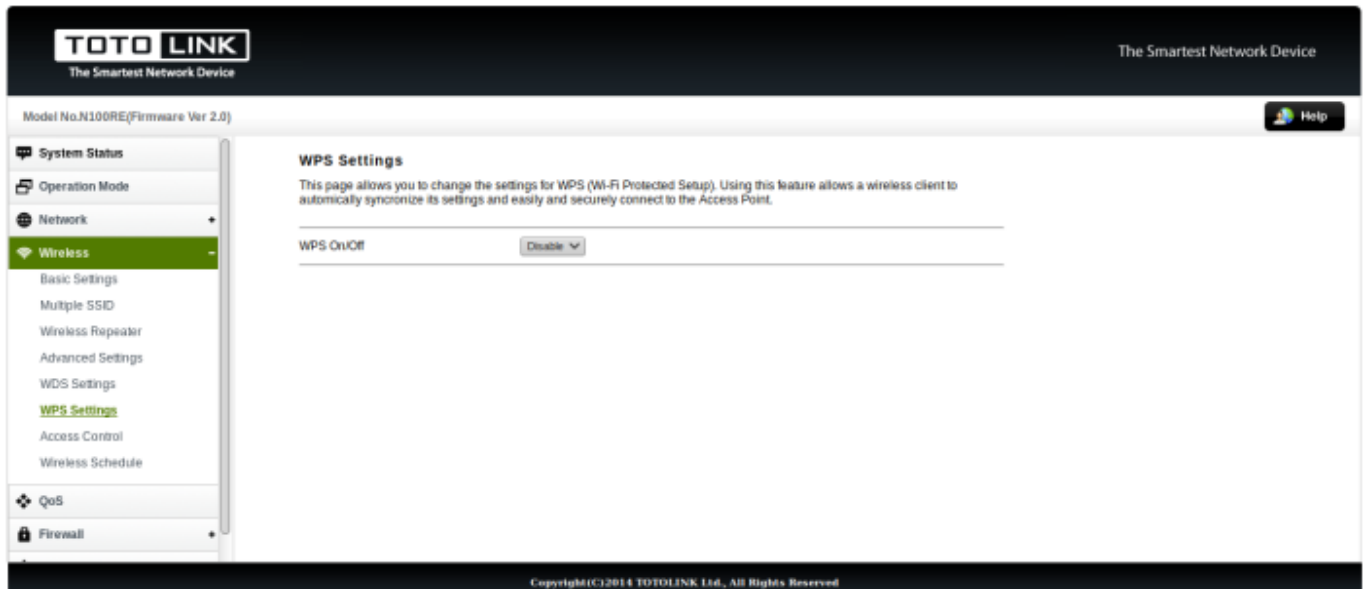
Найбільш часто логіном паролем є
admin
admin

З паролями краще відразу розібратись - деякі роутери взагалі можуть не мати паролю. Це означає, що будь-хто може робити з ним усе, що хоче.

Щодо прошивок - відразу після купівлі пошукайте на сайті виробника нові, надалі перевіряйте їх хоча б раз на рік. Саме через старі прошивки найчастіше відбувається взлам.

WPS

[WPS](#) - це та кнопка, що дозволяє підключатись без паролю. Так це зручно, але це небезпечно - буде добре, якщо ви це вимкнете.



Антивіруси - як обрати і для чого потрібен

Четверте коло - паролі

From:

<https://wiki.djal.in/> - IT - wiki

Permanent link:

https://wiki.djal.in/doku.php/howto/organizacija_bezpeki_v_domashnij_merezhi?rev=1534772515

Last update: 2018/08/20 13:41

