

OUCH!

Вашият месечен бюлетин за информационна сигурност

Сигурност за домашната безжична мрежа

Преглед

За да направите домашната си мрежа сигурна, първо трябва да започнете с безжичната точка за достъп (понякога наричана безжичен рутер). Това е устройството, което контролира кой и какво може да се свързва с мрежата. Тук даваме пет прости стъпки, с които да подситеgurите вашата безжична мрежа, за да имате вие и семейството ви по-сигурна домашна мрежа.

Акцентируйте на основните неща

Често най-лесният начин да се свържете с безжичното си устройство и да го конфигурирате е докато сте свързани към мрежата. Отворете в уеб браузър специфичният IP адрес, документиран в ръководството на устройството (пример за това е <https://192.168.1.1>), или използвайте софтуер или мобилно приложение предоставени от производителя на устройството.

1. **Сменете паролата на Администратора:** Вашето безжично устройство най-вероятно е доставено с фабрична парола за администраторския акаунт, която ви позволява да направите първоначалните настройки. Често тези фабрични пароли са общоизвестни, а може би дори публикувани в Интернет. Уверете се, че администраторската парола е сменена с уникална и сигурна такава, така че само вие да имате достъп. Ако устройството го позволява, сменете и потребителското име на администратора.
2. **Задайте парола на мрежата:** Конфигурирайте безжичната мрежа така, че тя също да има уникална, сигурна парола (различна от тази за администратора на устройството). По този начин само доверени хора и устройства могат да се свързват с мрежата ви. Съветваме ви да използвате мениджър за пароли, за да изберете сигурна парола и да можете да управлявате всичките си пароли.
3. **Обновете фърмуера:** Включете автоматичното обновяване на операционната система на безжичното ви устройство, често наричана фърмуер. По този начин ще сте уверени, че устройството е възможно най-сигурно и с последните опции за сигурност. Ако автоматичното обновяване не е достъпно за вашето безжично устройство, периодично проверявайте дали не е публикувано ново обновление. Ако устройството ви не се поддържа вече от производителя, обмислете дали да не купите ново, което да може да бъде обновявано с най-новите средства за защита.
4. **Използвайте Мрежа за гости:** Под понятието Мрежа за гости се разбира отделна виртуална

мрежа, която може да бъде настроена на устройството ви. Това означава, че безжичната ви точка за достъп всъщност има две мрежи. От тях *първичната* мрежа е тази, към която се свързват доверените ви устройства, като например вашият компютър, смартфон или таблет. От друга страна, *мрежата за гости* е тази, към която се свързват устройства, на които нямате пълно доверие, като например тези на гости или личните ви устройства за управление на дома. Устройство, свързано към мрежата за гости, не може да види или да комуникира с никое от доверените ви персонални устройства, свързани към първичната мрежа.

5. **Използвайте сигурно DNS филтриране:** DNS е услуга на която разчита целият Интернет и отговаря за преобразуване на имената на уебсайтовете в цифрови адреси. Тази услуга помага на компютъра ви да се свърже с уебсайта, след като напишете името му. Безжичната точка за достъп обикновено използва DNS сървър предоставен от вашия доставчик на интернет, но има по-сигурни безплатни алтернативи, като например [OpenDNS](#), [CloudFlare за семейства](#), или [Quad9](#), които могат да предоставят допълнителна сигурност като блокират вредни или нежелани уебсайтове. Влезте в безжичното си устройство и сменете адреса на DNS сървър с такъв, който представлява по-сигурна алтернатива.

Подсигуряването на домашната ви безжична точка за достъп е първата и една от най-важните стъпки при създаването на сигурна домашна мрежа. За повече информация относно сигурността на вашата безжична точка за достъп се обърнете към ръководството на устройството, или ако вашият интернет доставчик ви е предоставил устройството, свържете се с доставчика за повече информация за настройките на сигурността.

Гост редактор

Джошуа Райт (Twitter @joswr1ght) е главен директор на Counter Hack Challenges, LLC, завеждащ координация и разработки на кибер предизвикателства за NetWars и Holiday Hack Challenge. Намерете Джош в LinkedIn тук:

<https://linkedin.com/in/joswr1ght>.



Ресурси

Да опростим пароли: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

Мениджъри за пароли: <https://www.sans.org/security-awareness-training/resources/password-managers-0>

Обновяване: <https://www.sans.org/security-awareness-training/resources/power-updating>

Ръководство за настройка на OpenDNS: <https://www.opendns.com/setupguide/#familyshield>

Преведено за общността от: Николай Дачев и Радослава Несторова

OUCH! се публикува от SANS Security Awareness и се разпространява под [лиценз Creative Commons BY-NC-ND 4.0](#). Можете да споделяте или разпространявате този бюлетин без промени и без да го продавате. Редакторски колектив: Уолт Скривенс, Фил Хофман, Алан Уагонър, Лес Ридаут, Принсес Йънг