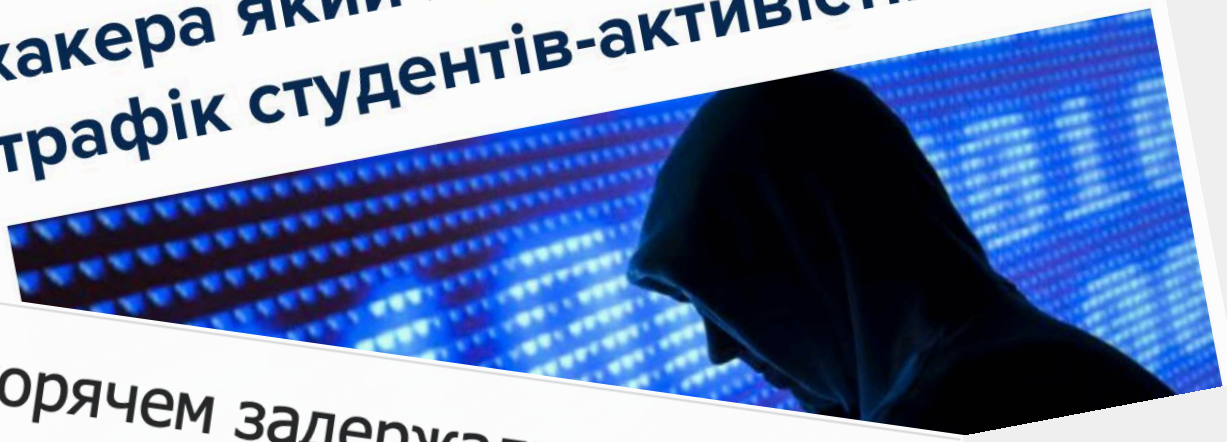
Як хакери використовують вразливості людей

План

- Як захистити домашній WiFi
- Як безпечно користуватись WiFi поза домом
- Бонус

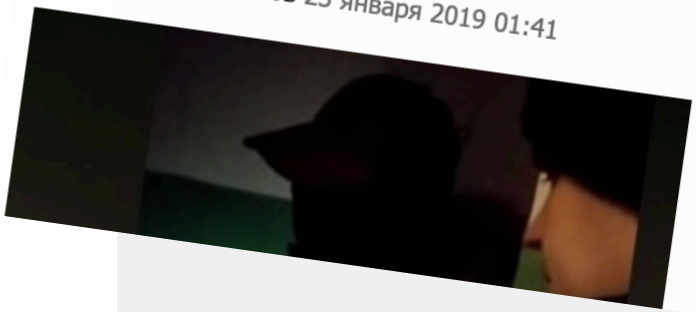
3 нещодавніх новин

Кіберполіція затримала в Києві хакера який перехоплював трафік студентів-активістів



В Киеве на горячем задержали хакера с оружием

Владимир Кондрашов 23 января 2019 01:41



Вечером 22 января, в одном из спальных районов Киева в подъезде жилого дома на горячем задержали мужчину в маске, который пытался получить доступ к сети Wi-Fi основателя общественной инициативы

Вразливість №1

Ми - безтурботні

Що зазвичай відбувається:

- Простий пароль
- Нестійкий метод шифрування
- Не змінюємо стандартні логін/пароль на роутері
- Анонсуємо SSID

Ми користуємось домашнім WiFi так, як нам його «хтось» налаштував

Що треба робити?

Пароль

Використовувати як можна складніший пароль:

- Довгий (парольна фраза)
- Цифри і спецсимволи
- Без словникових слів

- pa9ieweesuphaeRoo0eephoo2ahdohgo1leZ3QuohVoo1i thiel0ooZieng2iec
- COOK^feed&middle_shine!December

Що треба робити?

Доступ до домашнього роутеру

- Негайно змінити стандартний логін/пароль на роутері
- Оновити прошивку

1. Zyxel - *Generic Rout*

Method	Telnet
Password	1234
Level	Administrator
Doc	

8. Dlink - *DWL-900*

User ID	admin
Password	public
Level	Administrator
Doc	

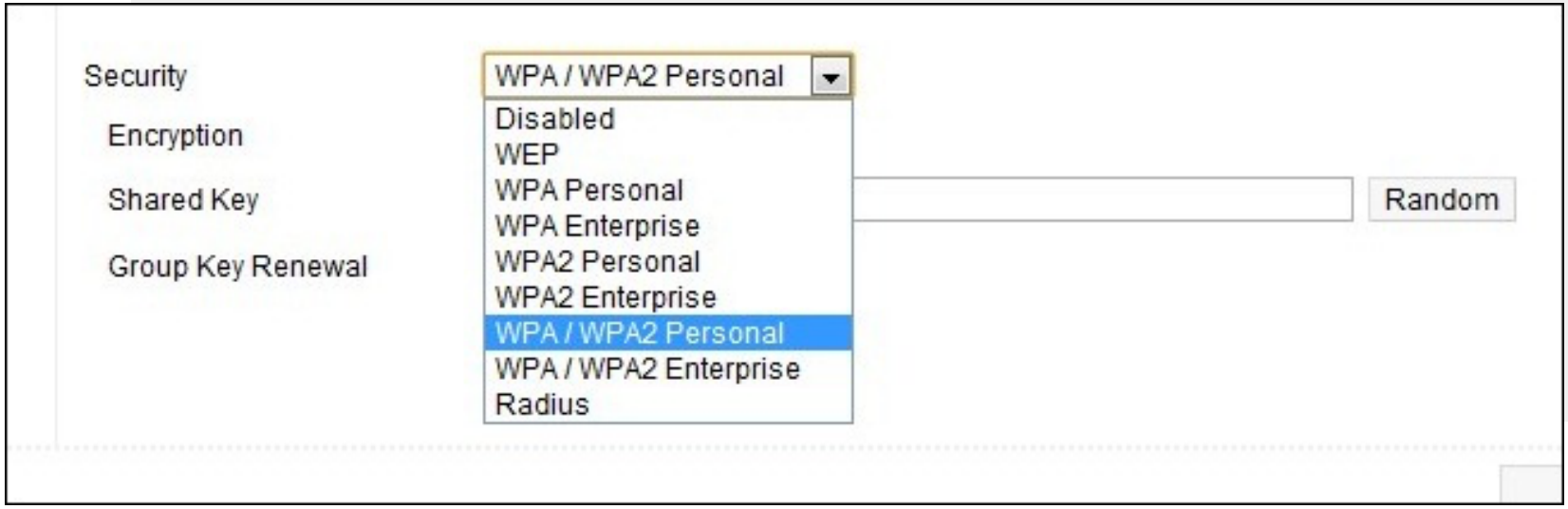
4. Asus - *RT-N16*

d	HTTP
D	admin
ord	admin
	Administrator

Що треба робити?

Протокол шифрування

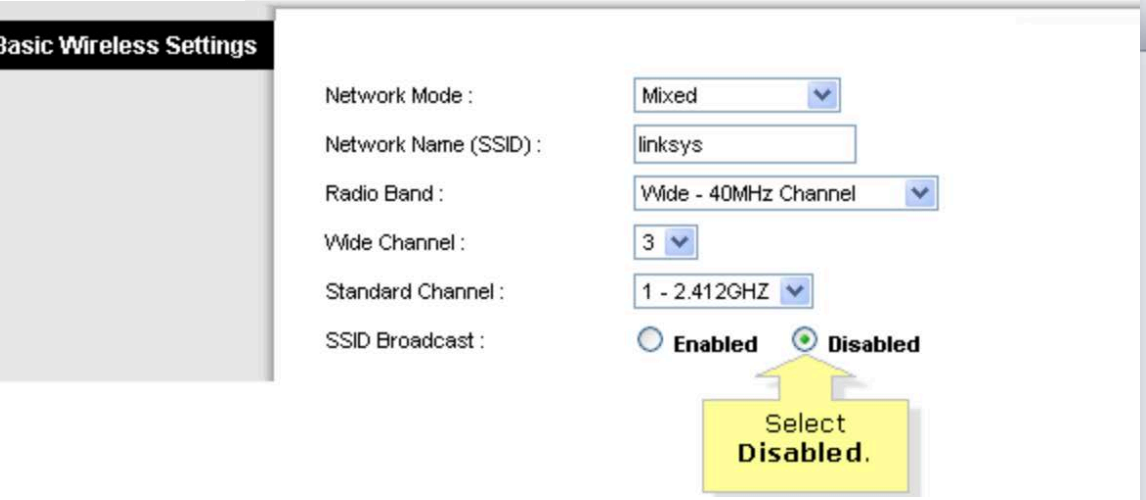
- WEP - NO
- WPA2 - OK



Що треба робити?

SSID

Змініть SSID і зробіть його непублічним



Що треба робити?

Захист домашніх користувачів на рівні DNS

Встановіть в якості DNS-адреси на роутері:

- 208.67.222.222
- 208.67.220.220

Сервіс Cisco Umbrella – безкоштовний для домашнього користувача

Вразливість №2

Ми - довірливі

Інтернет в публічних місцях

- Під'єднуємося до будь-якого відкритого WiFi
- Користуємось «як вдома»

Ваш трафік в публічній мережі може бути легко прослуханий

Що треба робити?

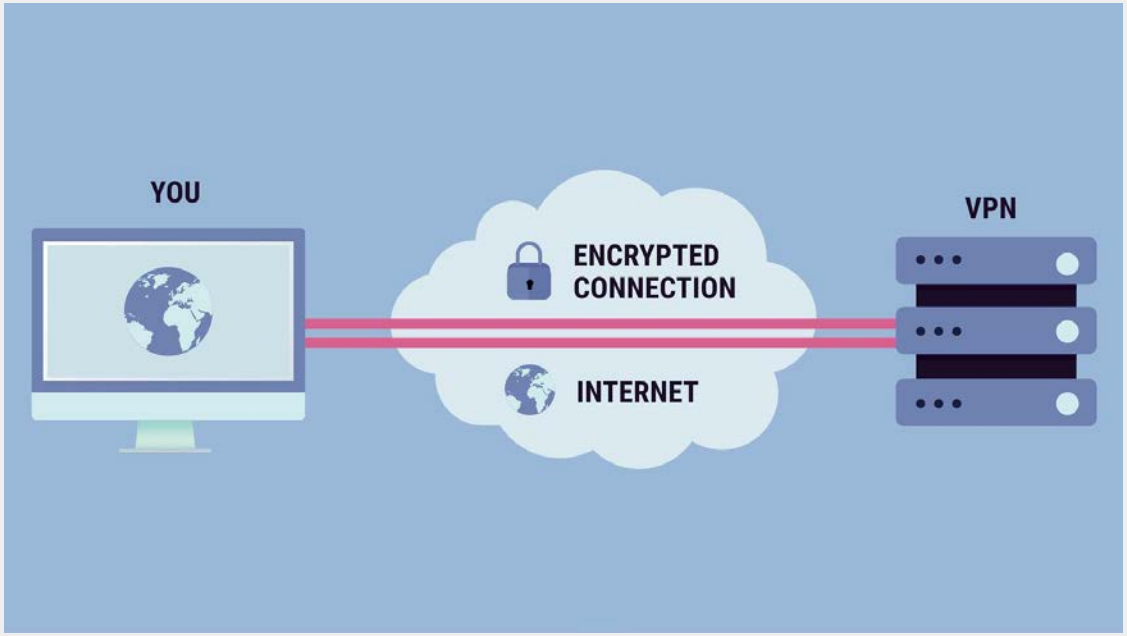
Інтернет в публічних місцях

- Тільки https
- Думайте, до кого підключаєтесь (evil APs)
- Краще використовуйте мобільний інтернет
- Вимкніть авто-підключення до WiFi Hotspots
- Двохфакторна аутентифікація

Що треба робити?

Інтернет в публічних місцях

Використовуйте VPN (можна налаштувати свій сервер – Open VPN)



Бонус

- Ви можете перевірити свій домашній WiFi на стійкість (use Google ☺)
- Пристрої Smart Home теж вразливі