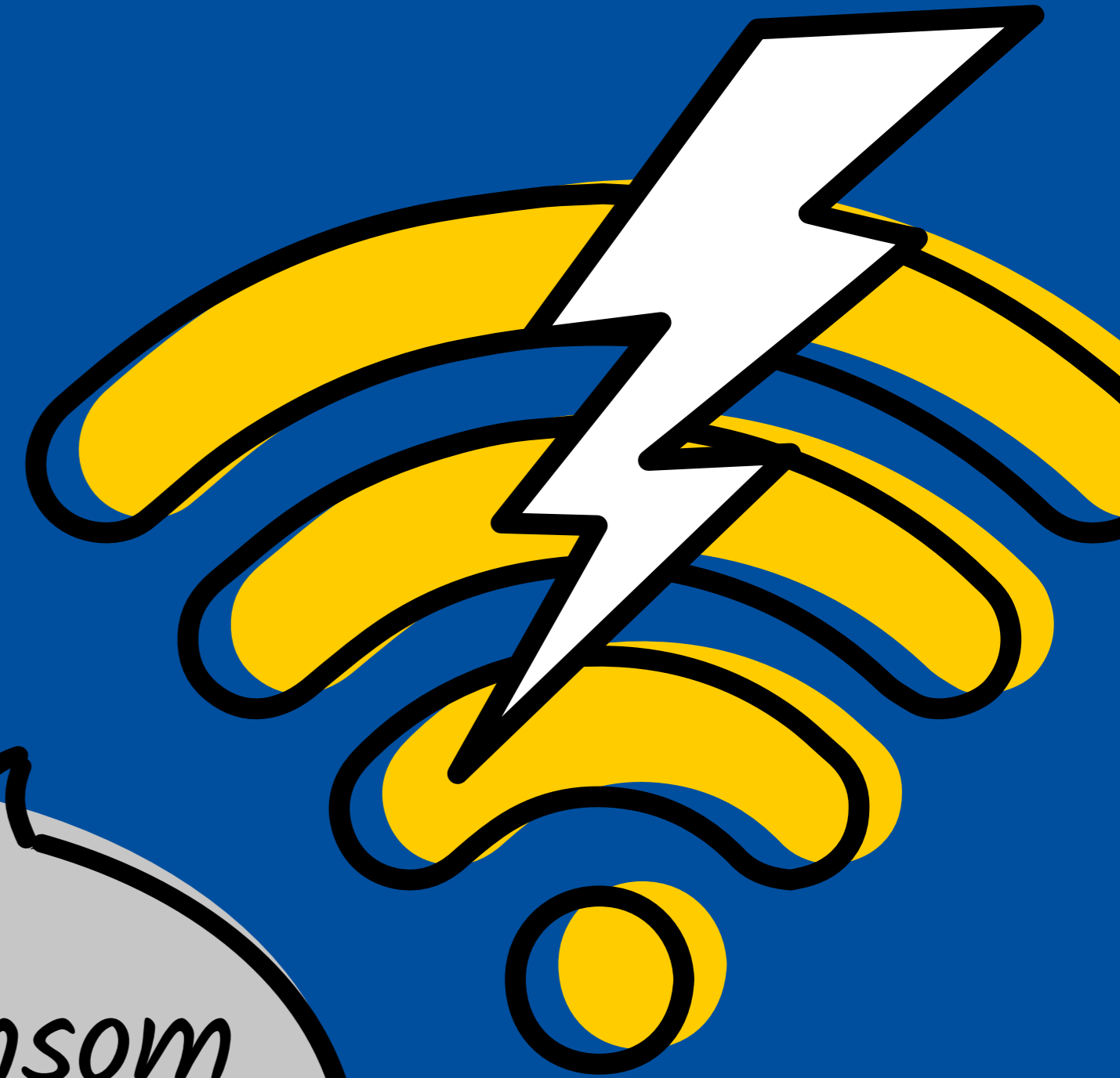




ОБЩЕСТВЕНИТЕ WI-FI МРЕЖИ МОГАТ ДА СЕ ИЗПОЛЗВАТ ЗА #RANSOMWARE

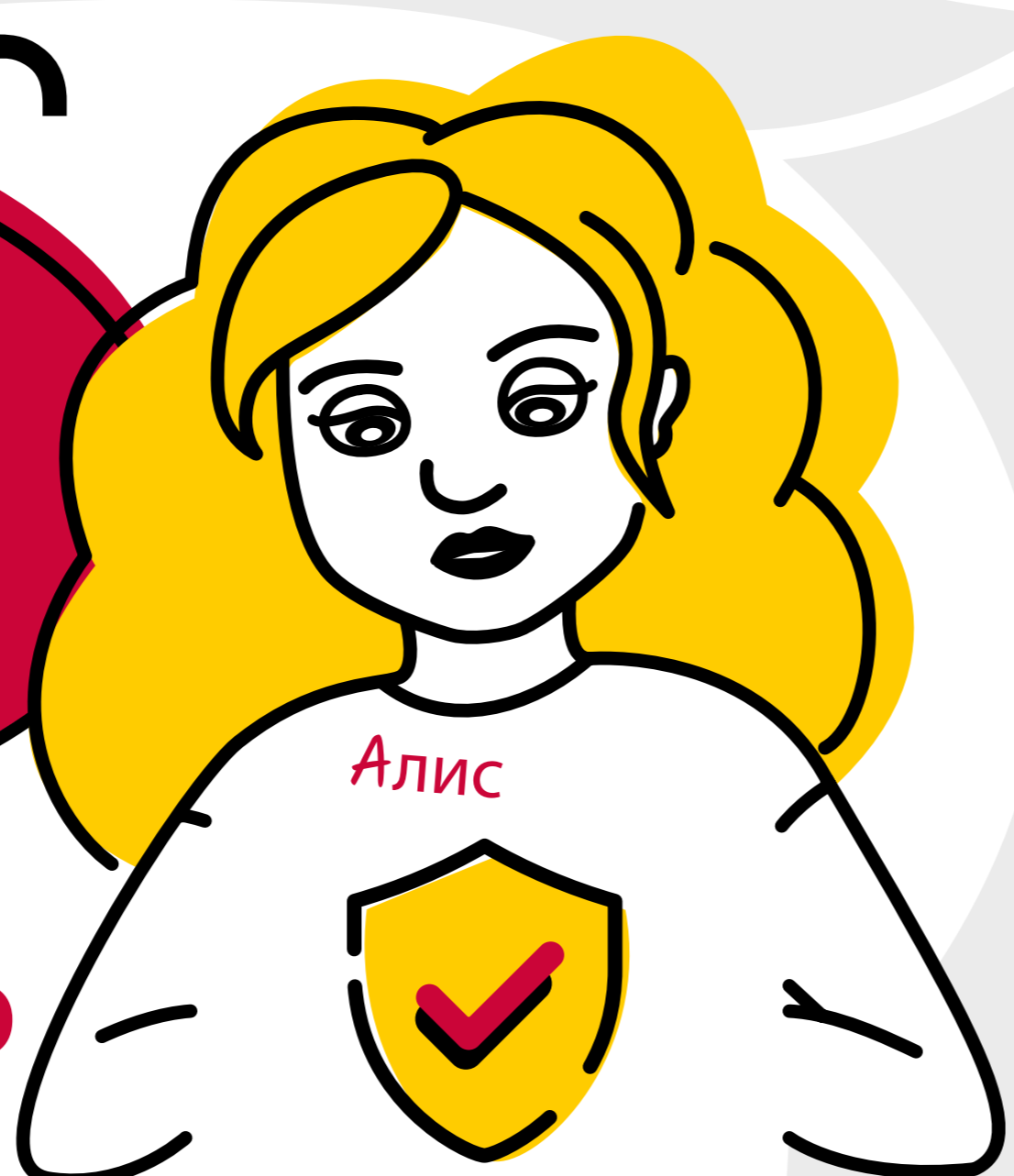


#NoMoreRansom
#CyberDialogues

Хакерът Боб работи по начини за подправяне на устройствата, свързани към обществена Wi-Fi мрежа.



#VPN PROTECTED



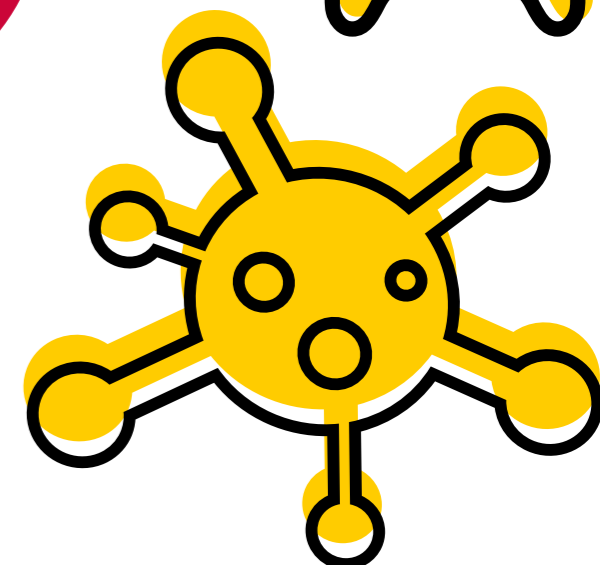
Алис пазарува онлайн, преди да хване полета си. Тя се свързва към Wi-Fi мрежата на летището.

След като дадено устройство е свързано към обществена Wi-Fi мрежа, хакерите могат да прихванат всички некриптирани данни и да ги използват, за да стартират атака с цел получаване на откуп.

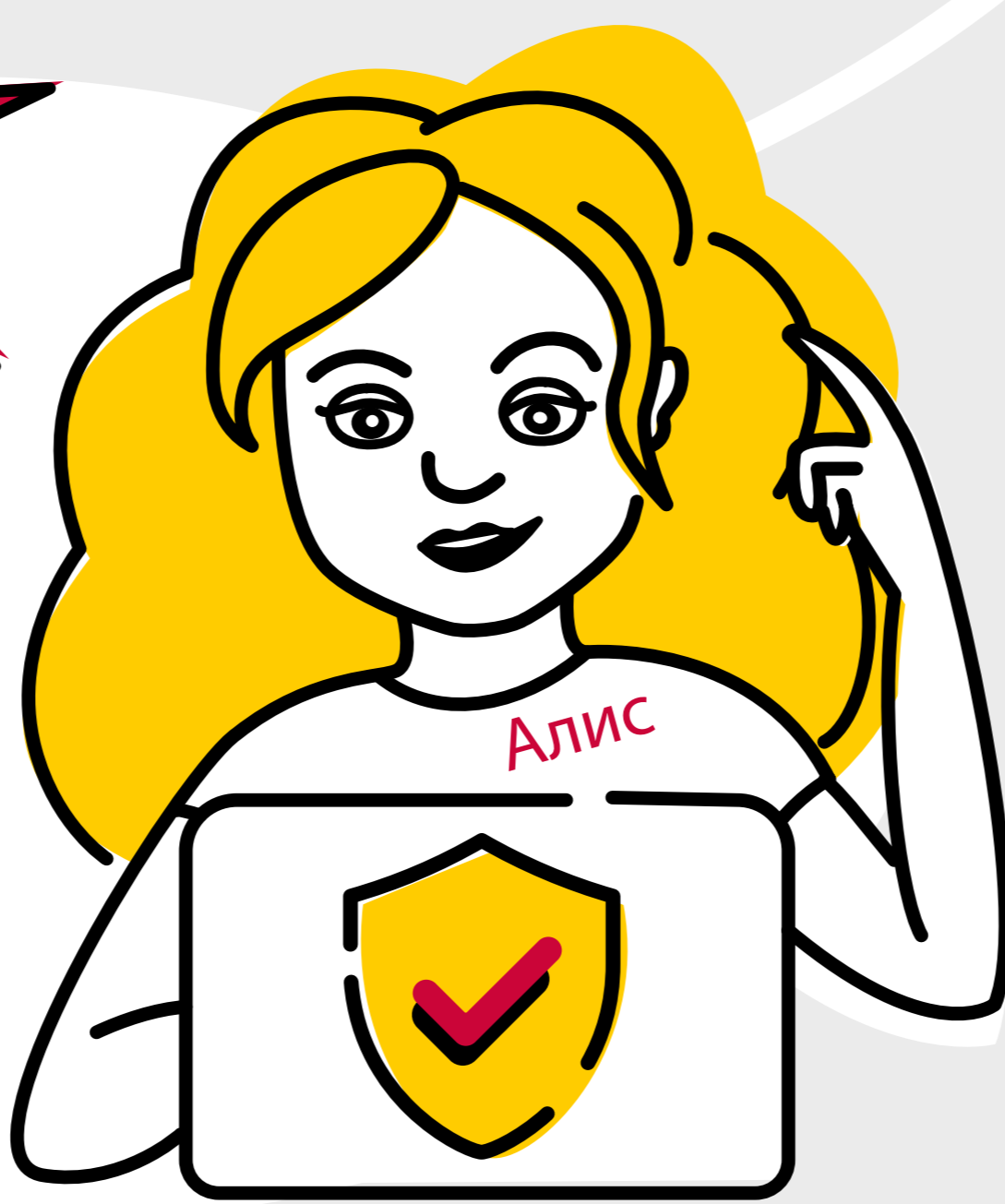
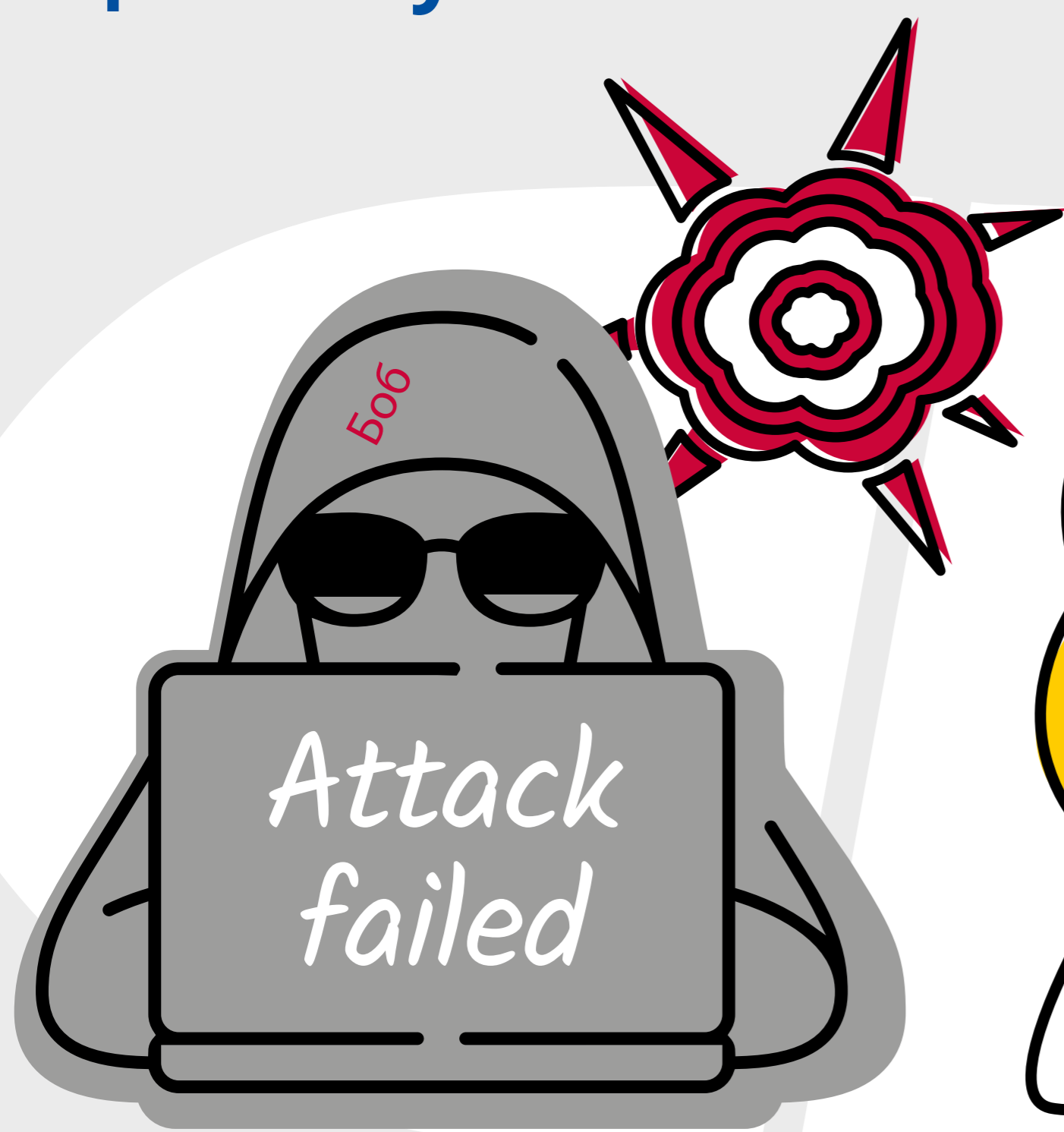


Кой се е свързал към мрежата?

SEARCH



#CYBERATTACK



Алис използва виртуална частна мрежа (VPN), за да получи достъп до уебсайта за онлайн покупки. След като приключи, тя се изключва от обществения Wi-Fi.



ЗАЩИТЕТЕ СЕБЕ СИ ОТ #RANSOMWARE

ПОВЕЧЕТО ОТ ЛИЧНИТЕ И ФИНАНСОВИТЕ НИ ДАННИ СЕ СЪХРАНЯВАТ НА МОБИЛНИТЕ НИ УСТРОЙСТВА. БЪДЕТЕ ВНИМАТЕЛНИ, КОГАТО ИЗБИРАТЕ КЪМ КОЯ МРЕЖА ДА СЕ СВЪРЖЕТЕ.

ЗА ОЩЕ СЪВЕТИ, ПОСЕТЕТЕ: <https://www.nomoreransom.org>



1. НИКОГА НЕ ПРИЕМАЙТЕ, ЧЕ ОБЩЕСТВЕНАТА WI-FI МРЕЖА Е БЕЗОПАСНА
2. АКО ТРЯБВА ДА СЕ СВЪРЖЕТЕ КЪМ ПУБЛИЧЕН WI-FI, ИЗПОЛЗВАЙТЕ VPN