БЕЗБЕДНО КОРИШЋЕЊЕ ОТВОРЕНОГ **БЕЖИЧНОГ ИНТЕРНЕТА (Wi-Fi)**

USAID
ОД АМЕРИЧКОГ НАРОДА

СРБ-ЦЕРТ

РАТЕЛ

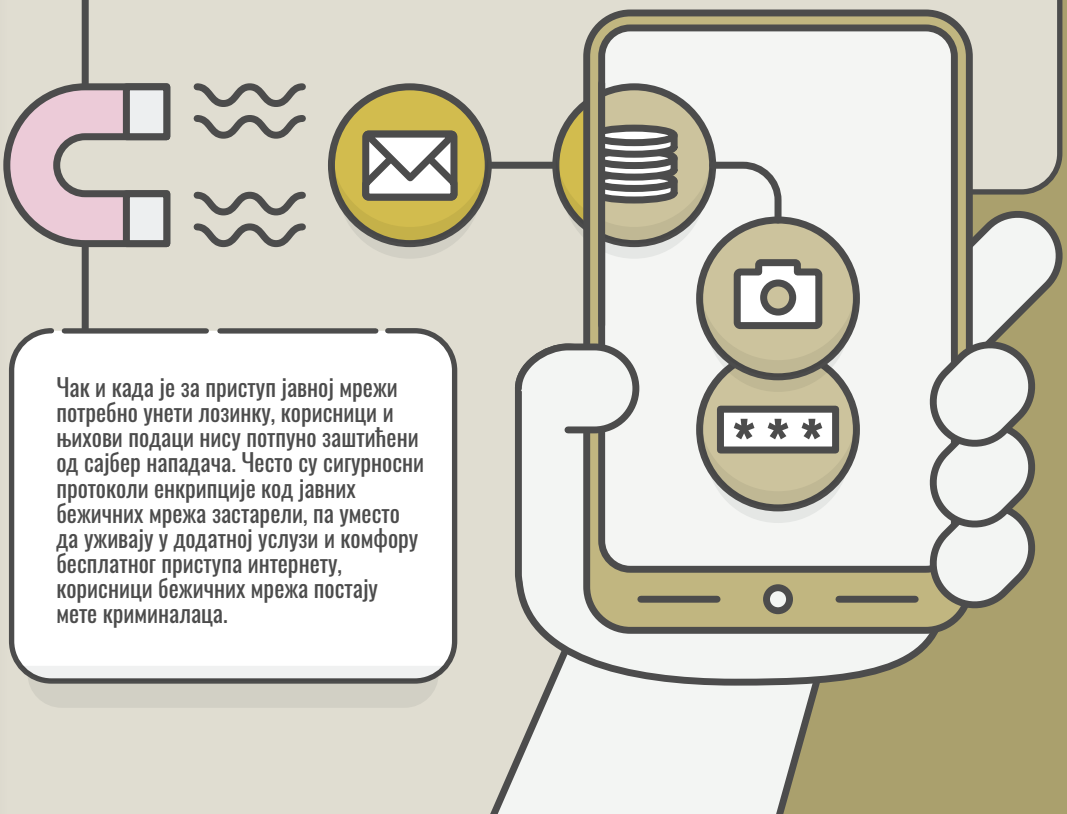
oebs Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

1. Јавне бежичне мреже

Бесплатан приступ бежичном интернету представља све распрострањенију услугу која се нуди корисницима угоститељских објеката, хотела, тржних центара, аеродрома, чак и возила јавног превоза. Број тзв. хотспотова је толико велик да већина корисника повезује своје мобилне уређаје свакодневно на њих, без икакве безбедносне провере.

Власници ресторана, туристичких објеката и сличних фирми на тај начин желе да привуку госте, који су навикнути да увек буду онлајн. Додатна корист је што гости приликом приступа јавној мрежи могу да оставе своју адресу електронске поште или се повежу са налогом на популарним друштвеним мрежама.

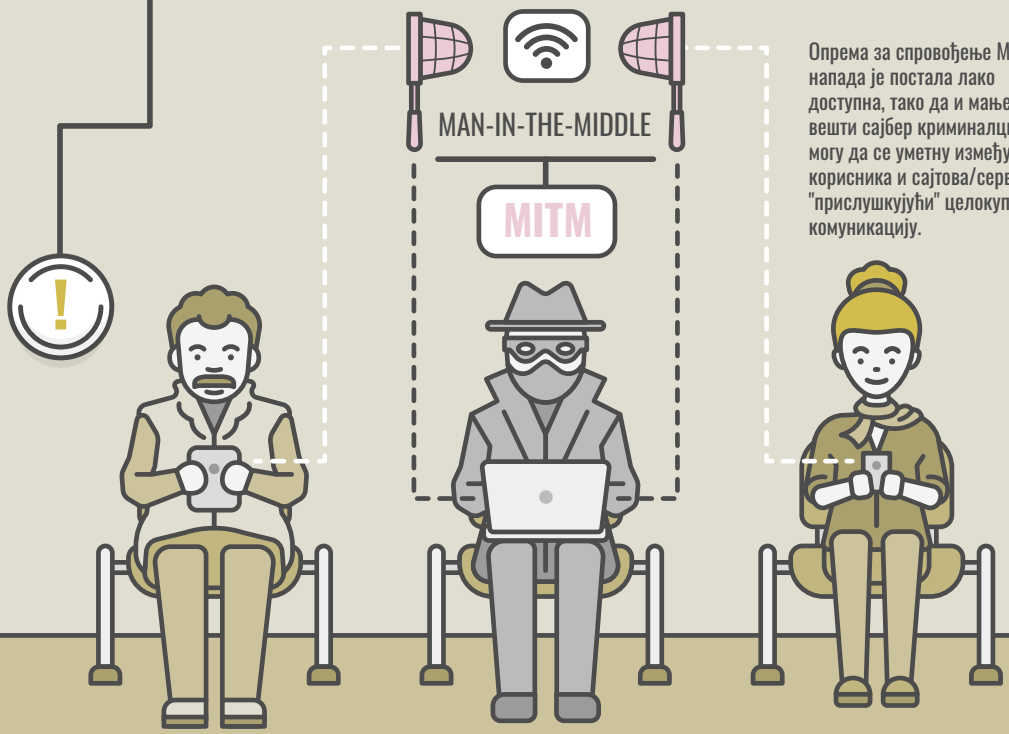
Иако могућност провере електронске поште, приступа друштвеним мрежама или "рада на даљину" из омиљеног кафића звучи привлачно, већина корисника није свесна да се на тај начин излажу значајном ризику од губитка података, као што су фотографије, поруке, лични подаци, лозинке и информације о банковним рачунима.



Чак и када је за приступ јавној мрежи потребно унети лозинку, корисници и њихови подаци нису потпуно заштићени од сајбер нападача. Често су сигурносни протоколи енкрипције код јавних бежичних мрежа застарели, па уместо да уживају у додатној услузи и комфору бесплатног приступа интернету, корисници бежичних мрежа постају мете криминалаца.

2. Сајбер напади у јавним мрежама

Веома распрострањен тип сајбер напада приликом коришћења јавних бежичних мрежа је тзв. "човек у средини" (енг. Man-in-the-middle - MITM). Циљ сајбер нападача је да буду у истој мрежи са другим корисницима и пресретну њихов приступ интернету. На тај начин добијају увид у комплетан саобраћај и могу да преузму поверљиве податке или идентитет корисника.

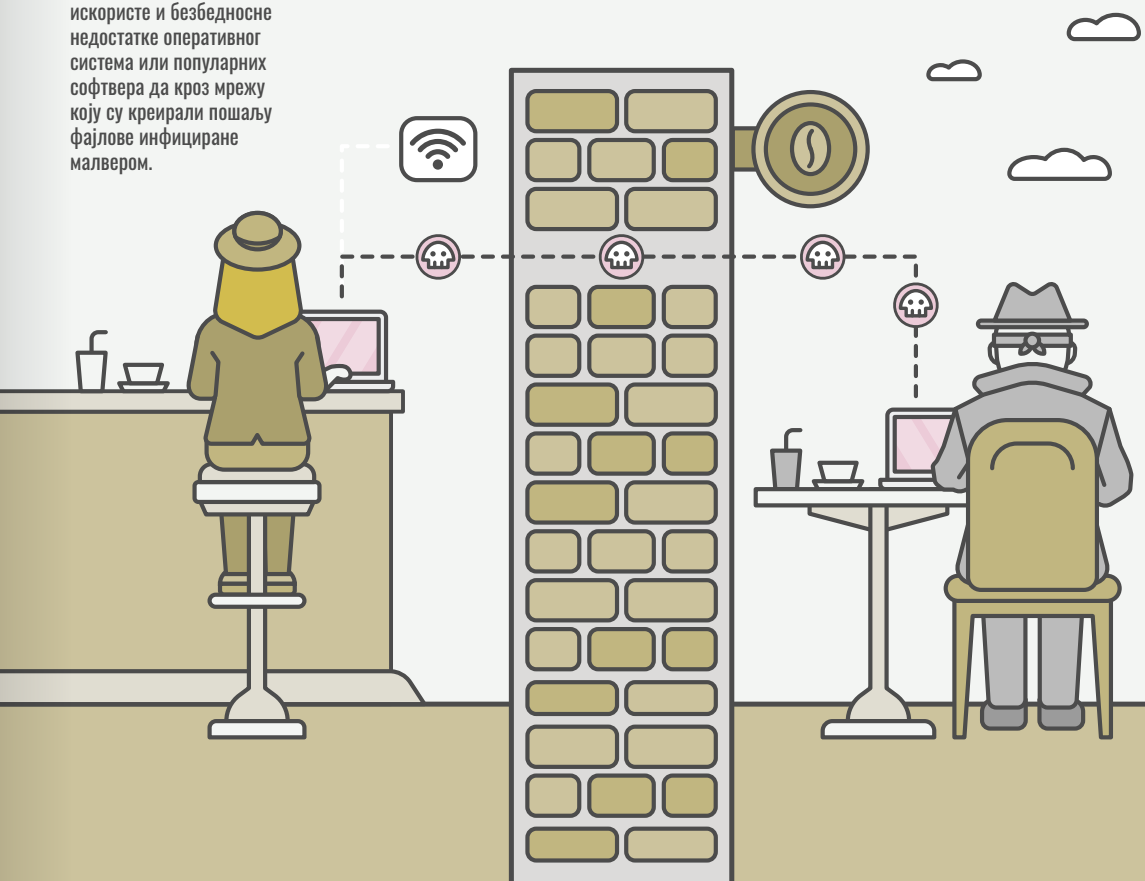


Опрема за спровођење MITM напада је постала лако доступна, тако да и мање вешти сајбер криминалци могу да се уметну између корисника и сајтова/сервиса, "прислушкујући" целокупну комуникацију.

Друга врста опасности је када сајбер криминалци креирају лажно приступно место (hotspot) за бежичну јавну мрежу, која имитира мрежу неког угоститељског или другог објекта. На таквим местима често је омогућен слободан приступ или су шифре врло лако доступне и ретко се мењају. То су идеални услови да сајбер нападач постави замку са називом мреже која личи на назив угоститељског објекта или има још очигледнији назив попут "Бесплатан Wi-Fi".

Када се повежу, корисници могу бити мета напада кроз дистрибуцију малвер садржаја. Најчешће се шаље лажно обавештење о ажурирању софтвера, чиме се покреће процес инсталације злонамерног софтвера на уређај корисника и отвара могућност за приступ личним подацима, финансијским информацијама, фајловима или корисничким налозима.

Сајбер нападачи могу да искористе и безбедносне недостатке оперативног система или популарних софтвера да кроз мрежу коју су креирали пошаљу фајлове инфициране малвером.



3. Препоруке за безбедно коришћење јавних мрежа

Најбољи начин да се заштите поверљиви подаци приликом употребе јавних бежичних мрежа је да се избегава приступање налозима електронске поште или друштвених мрежа, као и обављање финансијских трансакција. За такве активности сигурније је повезивање путем 3G или 4G модема, односно повезивање преко мобилног интернета са телефона.

Уколико користите јавну мрежу, потрудите се да то чините што безбедније:

1. Онемогућите аутоматско повезивање уређаја на отворене мреже,
2. Чим завршите коришћење, искључите се са отворене мреже,
3. Обратите пажњу на то које странице посећујете. Препорука је да то буду сигурне странице, са префиксом: https,
4. Избегавајте плаћања и проверу стања на банковном рачуну, као и унос осетљивих података и активирајте двофакторску аутентификацију,
5. Користите VPN сервис који ће криптовати саобраћај,
6. Ако сте се пријавили на налог електронске поште или друге апликације, промените шифре чим приступите сигурној мрежи,
7. Бирајте јавне мреже које захтевају унос лозинке,
8. Редовно ажурирајте систем и антивирусне програме, али не док сте на отвореним мрежама, јер нападачи могу да вам подметну инсталацију вируса.


https
VPN

БЕЗБЕДНО КОРИШЋЕЊЕ ОТВОРЕНОГ **БЕЖИЧНОГ ИНТЕРНЕТА (WI-FI)**

Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ)
Палмотићева 2, 11103 Београд, Република Србија
www.cert.rs

Ставови изречени у брошури припадају искључиво аутору и његовим сарадницима и не представљају нужно званичан став Мисије ОЕБС-а у Србији.

Израда ове брошуре омогућена је уз подршку америчког народа путем Америчке агенције за међународни развој (USAiD).
За садржај брошуре одговорни су аутори и она не мора нужно да одражава ставове USAiD-а или Владе Сједињених Америчких Држава.