Двофакторска автентификација

Дополнителен слој за заштита на твоите профили

MKSafeNet
IDEI Institute for Digitalization Economy and Innovation
Република Северна Македонија
Министерство за дигитална трансформација
Co-funded by the European Union

Зошто лозинката не е доволна?

Повеќето онлајн услуги се заштитени со лозинка.

Лозинката е првиот чекор за потврда на идентитетот, начин системот да препознае дека ние се најавуваме.

Но денес лозинките често не се доволни.

Причини:
- луѓето користат лесни лозинки
- користат иста лозинка на повеќе места
- некој може да ја погоди или украде
- може да се фатат преку лажни пораки (phishing)

Ако некој ја дознае лозинката, може целосно да пристапи до профилот.

Затоа современите системи користат **повеќестепена проверка на идентитетот.**

Активност:

Која ситуација е најризична?

- [ ] Иста лозинка на повеќе профили
- [ ] Различна лозинка на секој профил

Што е двофакторска автентификација?

Двофакторската автентификација (2FA) е метод за заштита кој бара два различни докази дека корисникот е вистинскиот сопственик на профилот.

Најавувањето се одвива во два чекора:

1. нешто што го знаеме (лозинка)

2. нешто што поседуваме (код, уред, отпечаток)

Само комбинацијата на двата фактори овозможува пристап до профилот.

На овој начин, дури и ако лозинката се открие, пристапот останува блокиран.

Задача

Поврзи за да биде точно:

Лозинка	Поседувам
Код од телефон	Знам

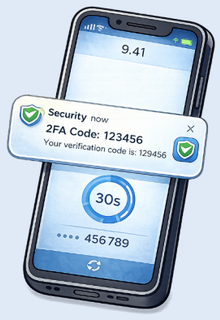
Видови на двофакторска автентификација

Двофакторската адвтентификација може да биде:

код преку SMS

апликација за двофактроски кодови

push известување



биометриска потврда (отпечаток или лице)

Секој од нив служи како дополнителна проверка дека корисникот навистина е присутен.

Важно е кодот да е временски ограничен и неповторлив.

Задача: Заокружи го точниот одговор

Што од следново не треба да се споделува?

☐ Код за најава ☐ Корисничко име ☐ Временски код

Како нè штити двојната заштита

Замисли некој ја дознал твојата лозинка.

Без двофакторската адвтентификација (2FA) → може да влезе во твојот профил

Но, со двофакторската адвтентификација (2FA) → пристапот е блокиран

Бидејќи вториот фактор го има само сопственикот, нападот запира.

Ова значително го намалува ризикот од:
- кражба на профил
- лажни објави
- злоупотреба на лични податоци

Активност

Лозинка е украдена, код нема. Дали е можно најавување?

☐ Да ☐ Не

Чести измами

Напаѓачите често се обидуваат да го добијат кодот за потврда, бидејќи без него не можат да влезат во профилот.

Понекогаш се претставуваат како:
- администратори на игра
- поддршка од апликација
- другар на кој „му треба помош“
- натпревар или наградна игра

Често може да напишат:
„Испрати го кодот за потврда“
„Проверуваме дали вие сте вистинскиот сопственик“
„Напиши го кодот и ќе добиеш награда“

Вистинските апликации и сервиси никогаш нема да ти побараат да го испратиш кодот за потврда на некој друг. Кодот е наменет само за тебе и служи за да потврди дека токму ти се најавуваш.

Ако некој ти го бара кодот преку порака, игра или социјална мрежа, тоа е обид за измама.

Активност: Што би направил

За секоја ситуација заокружи го точниот одговор:

Некој во играта ти пишува:
„Јас сум админ, прати го кодот за проверка“

☐ Го праќам ☐ Го игнорирам и пријавувам

Добиваш порака:
„Освои награда! Испрати го кодот“

☐ Го праќам ☐ Го игнорирам и пријавувам

Ти стигнува код, а не си се најавил никаде

☐ Го праќам ☐ Го игнорирам и пријавувам

Добри навики за безбеден профил

Безбедноста на интернет не зависи од една работа, туку од повеќе мали навики што ги повторуваме секој ден.

Кога внимаваме на нашите профили, ги заштитуваме нашите разговори, фотографии и игри.

Затоа е важно да:

- ☑ користиме различни лозинки за различни профили
- ☑ избираме подолги и потешки лозинки
- ☑ активираме двофакторска заштита каде што постои
- ☑ не ги споделуваме кодовите со никого
- ☑ проверуваме дали пораката е вистинска
- ☑ кажеме на родител или наставник ако нешто изгледа сомнително

Двофакторската автентификација не го прави профилот невозможен за пробивање, но го прави многу потежок за злоупотреба.

Колку повеќе добри навики, толку помалку ризици.

Активност

Замисли дека поставуваш нов профил во игра или апликација. Пополни ги чекорите за креирање на успешен профил:

Каква лозинка би избрал/а? *(Напиши пример – не ја користи вистинската лозинка)*

_____

Каде ќе ја зачуваш лозинката за да не ја заборавиш?

_____

Што ќе направиш веднаш по најавувањето?

☐ Ќе активирам двофакторска заштита ☐ Ништо, доволна е лозинката