
# Заштита налога коришћењем двофакторске ауторизације

SRB-CERT

# Заштита налога коришћењем двофакторске аутентификације

Адекватна заштита онлајн налога је од изузетног значаја, јер смо често сведоци чињенице да употреба лозинке, па чак и оне која је веома комплексна, може бити недовољна за заштиту ових налога. Употребом двофакторске (2ФА) или мултифакторске (МФА) аутентификације приликом пријављивања на онлајн налог додаје се још један слој заштите који проверава нешто што корисник има и/или нешто што корисник јесте. Корисник може доказати да је у поседу:

- телефона, тако што ће примити текстуалну поруку са кодом,
- физичког токена, тако што генерише привремени код за приступ или се повезује са корисничким уређајем,
- софтвера (апликације за аутентификацију), тако што ће преко њега добити нотификацију на телефону или привремени код за приступ.


С друге стране корисник може додатно доказати да то јесте она/он кроз:

- скенирање отиска прстију,
- препознавање лица,
- препознавање гласа.

**Зашто је корисно подесити 2ФА?**

Чак и у ситуацијама када корисници пажљиво креирају своје лозинке, тако да оне буду комплексне и јединствене за сваки налог, постоји могућност да и такве лозинке буду украдене.

Нападачи, покушавају да преваре кориснике тако што им прослеђују линкове било путем е-поште, текстуалне поруке или директних порука/четова (тзв. „фишинг“ поруке) и траже од корисника да се пријаве и оставе своје податке (корисничко име и лозинку, детаље банковних картица и сл.).

За потребе неовлашћеног прикупљања лозинки нападачи често креирају малициозне интернет странице различитог садржаја и организују преваре, како би привукли кориснике да на тим сајтовима оставе своје корисничко име и лозинку.

До крађе лозинки може доћи и када организација која чува корисничке податке претрпи хакерски напад и том приликом дође до компромитовања или цурења пословних података. Нападачи затим могу користити лозинке које су украдене приликом такве компромитације како би покушали да приступе корисничким налозима, што је техника, позната као *'credential stuffing'*, која често функционише јер многи корисници користе исту лозинку за приступ различитим интернет налозима.

Како би се корисници додатно заштитили од оваквих или сличних начина одавања лозинки, потребно је користити двофакторску или мултифакторску аутентификацију као која пружа додатни ниво заштите налога корисника.

**Типови 2ФА**

Када је активирана 2ФА, од корисника ће се тражити да се поред уноса корисничког имена и лозинке, корисник додатно аутентификује и тиме потврди свој идентитет.

Доступно је неколико типова другог корака у процесу подешавања 2ФА:

- Текстуалне поруке и имејл налози

Код великог броја услуга којима корисници приступају постоји опција 2ФА преко текстуалне поруке. Током подешавања, корисник наведе свој број телефона, а услуга шаље поруку која садржи безбедносни код који треба да се користи. Такође, за исти процес корисници могу да користе имејл налоге, под условом да је то другачији имејл налог од оног који се користи за промену лозинке. Текстуалне поруке и 2ФА на бази имејл налога нису најбезбеднији тип 2ФА, али ипак коришћење било које опције 2ФА је боље, него да је уопште нема.

- Коришћење апликација за аутентификацију

Коришћење апликација за аутентификацију су главна алтернатива текстуалним порукама и употреби имејл налога. *Google Authenticator* и *Microsoft Authenticator* су примери ових врста апликација. Када се инсталирају, могу се користити на свим налозима који нуде ову могућност подешавања 2ФА. Ове апликације имају и одређене предности у односу на текстуалне поруке, попут чињенице да им није потребан сигнал за мобилни телефон или чекање да стигне текстуална порука.

- Коришћење *phishing-resistant* аутентификације

Пружаоци услуга могу понудити и опцију коришћења *phishing-resistant* аутентификације која се тренутно сматра за најбезбеднију опцију за имплементацију 2ФА аутентификације. Може се реализовати коришћењем *FIDO2/Webauthn* стандарда или помоћу инфраструктуре јавних кључева (*Public Key Infrastructure - PKI*).

*FIDO2* токени (уређаји) имају две особине које их чине отпорним на фишинг. Аутентификатор аутоматски проверава да ли је повезан са додељеном апликацијом/веб страницом. Неће се аутентификовати на лажној веб страници која посредује између захтева и одговора са легитимног сервиса. Ово је кључан елемент за превенцију фишинга. Осим путем *PIN*-а, физичка присутност се пре откључавања аутентификатора може проверавати коришћењем гестова на уређаја или биометријском провером (отисак прста, препознавање лица итд.). Такође, *FIDO2/Webauthn* доноси све предности снажне аутентификација утемељене на криптографији јавним кључем, али уз смањење комплексности њене имплементације и ширу подршку за различите уређаје и платформе. Кориснички приватни кључ никада не напушта аутентификатор и не чува се на страни сервера. Један пример оваквог уређаја је *YubiKey.*

С друге стране, PKI токен (картица) је решење двофакторске (2ФА) аутентификације базирано на технологији јавних криптографских кључева, код кога корисник поседује физички уређај (токен или картицу) у коме се налазе приватни кључ корисника и електронски сертификат корисника који је издало сертификационо тело (Certification Authority - CA), при чему се приватном кључу корисника приступа ПИН кодом који корисник треба да чува у тајности. За коришћење PKI токена (картице) потребно је да корисник на свом рачунару има инсталисан клијентски софтвер који представља међуслој (middleware) између оперативног система рачунара и PKI токена (картице). Погодности овог решења су да може да се користи не само за двофакторску (2ФА) аутентификацију, већ и за електронско потписивање и шифровање електронских

трансакција, докумената и е-писама. Када је PKI токен (картица) квалификовано квалификовано средство за креирање електронског потписа (Qualified Signature Creation Device) и на њему се налази приватни кључ и квалификовани електронски сертификат корисника, такав PKI токен (картица) се сматра средством електронске идентификације високог нивоа поузданости у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/2017 и 52/2021) и Уредбом о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости („Службени гласник РС“, бр. 60/2018 и 68/2024). Коришћењем PKI токена (картице) који је средство електронске идентификације високог нивоа поузданости и садржи квалификовани електронски сертификат, грађани Републике Србије могу да приступају електронским сервисима који су повезани са Порталом за електронску идентификацију Републике Србије (https://eid.gov.rs).

**Резервни план у случају недоступности уређаја**

Такође, добра је идеја да корисник има резервни план у случају да нема приступ уобичајеном начину другог корака аутентификације (нпр. ако се батерија на мобилном телефону испразни), и управо из тог разлога многи пружаоци услуга омогућавају корисницима да подесе више опција аутентификације и коришћење резервих (*backup*) кодова. Један резервни (*backup*) код се може искористити за аутентификацију само једном, а њихова главна предност је та што се могу користити иако корисник нема приступ свом уређају (на пример ако се испразни батерија или изгуби уређај). Резервне кодове треба чувати од других лица и изгенерисати нове уколико их све употребите.

**Како и где подесити 2ФА?**

Ако је 2ФА доступна за налог, опција за њено укључивање се обично налази у безбедносним подешавањима налога, под називом: Двофакторска аутентификација (2ФА) или Вишефакторска аутентификација (МФА).

Упутства за активирање 2ФА за одређену услугу је доступно на следећим линковима:

- Подешавање 2ФА за имејл:
  - Gmail
  - Yahoo
  - Outlook
- Подешавање 2ФА за друштвене мреже:
  - Instagram
  - Facebook
  - Twitter
  - LinkedIn
  - TikTok
- Подешавање 2ФА за друге налоге:
  - Microsoft Account

- Google Account
- Apple ID
- OpenVPN
- WhatsApp
- PayPal

Свеобухватни преглед на којим налозима и који тип двофакторске аутентификације се може применити можете пронаћи на линку https://2fa.directory/int/.

Извори:


https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv

https://2fa.directory/int/
https://smartkey.rs/?gclid=EAIaIQobChMIqunHk9LSgwMVDIpoCR3yxgfwEAAYASAAEgIwzPD_BwE

https://www.ownyouronline.govt.nz/personal/get-protected/guides/use-two-factor-authentication-to-protect-your-accounts/

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf