Kako je z varnostjo EMIL-a

Na portalu za elektronski pristop k vzajemnim skladom – **EMIL,** varnost zagotavlja uporaba sodobnih tehnologij in upoštevanje varnostnih standardov spletnega poslovanja. Pri prijavi na portal **EMIL** uporabnik vnese osebno geslo, ki ga je prejel po zaključenem postopku registracije v sistem oziroma, ki si ga je kasneje v sistemu spremenil.

Z uporabo kvalificiranega digitalnega potrdila, se verodostojnost identifikacije in s tem tudi varnost uporabe portala **EMIL** za uporabnika še poveča.

Vsa komunikacija med portalom **EMIL** in uporabnikom, je šifrirana, tako da je zagotovljena varnost pred nepooblaščenim vpogledom v podatke.

Seveda mora za varno poslovanje poskrbeti tudi uporabnik sam; v prvi vrsti z varovanjem svojih identifikacijskih podatkov, da ne bi prišlo do kraje identitete.

Kako lahko uporabnik poskrbi za večjo varnost?

Uporabnik lahko sam poveča varnost pri uporabi portala **EMIL** z upoštevanjem nekaj osnovnih pravil:

Skrbno varujte svoje identifikacijske podatke, kot so uporabniško ime, osebno geslo in kvalificirano digitalno potrdilo.

Pri uporabi digitalnih potrdil ravnajte v skladu z dobrimi praksami, ki jih predlagajo izdajatelji kvalificiranih digitalnih potrdil.

Priporočljivo je, da si v brskalniku izberete nastavitev, ki za vsako uporabo kvalificiranega digitalnega potrdila zahteva vpis gesla.

Če je kvalificirano digitalno potrdilo shranjeno na pametni kartici, je zaščiteno z geslom, ki ga sami določite. Najbolje poskrbite za varnost tako, da si geslo zapomnite, pametno kartico pa hranite na varnem mestu.

Po nešifriranih komunikacijskih poteh ne pošiljajte občutljivih zaupnih podatkov (gesla, uporabniškega imena, oznake kvalificiranega digitalnega potrdila, davčne številke ipd.).

 Pazite s kom elektronsko komunicirate. Pozorno preglejte priklicano spletno stran, ali je res takšna, kot ste je vajeni. Nepridipravi namreč lahko ponaredijo spletno stran in prek nje zahtevajo vnos vaših identifikacijskih podatkov, s pomočjo katerih se kasneje lažno identificirajo pri družbi za upravljanje ter na ta način pridejo do drugih vaših zaupnih podatkov. V primeru, da menite, da je spletna stran lažna, jo nemudoma zapustite. Zato je vedno zelo pomembno, da preverite avtentičnost spletne strani, na kateri ste, in se prepričate, da ste s portalom **EMIL** resnično povezani po zaščiteni komunikaciji – SSL. (naslov se začne z nizom https://.....)

 Skrbno ravnajte z občutljivimi podatki, ki so shranjeni na prenosnem mediju (CD, DVD, spominski ključ USB, pametna kartica ipd.), ter jih ne puščajte v računalniku ali čitalniku pametne kartice in ne posredujte tretjim osebam. Če je le mogoče, ne shranjujte svojih zaupnih podatkov na trdi disk, še posebej, če vaš računalnik uporablja več oseb (v službi ali drugje). Če posumite, da je prišlo do zlorabe vašega kvalificiranega digitalnega potrdila ali drugih identifikacijskih elementov, o tem nemudoma obvestite overitelja, ki je kvalificirano digitalno potrdilo izdal, in družbo za upravljanje, ki bosta onemogočila nadaljnjo uporabo portala **EMIL** z vašimi identifikacijskimi elementi.

 Priporoča se, da je osebno geslo sestavljeno iz kombinacije črk in številk, in naj ne vsebuje osebnih podatkov, kot so rojstni datumi ali osebna imena družinskih članov. Daljše geslo je varnejše, vendar je pri tem pomembno tudi, da si ga zlahka zapomnite.

 Vedno uporabljajte licenčno programsko opremo in jo sproti posodabljajte z najnovejšimi različicami, ki zagotavljajo najnovejše varnostne standarde.

 Pri uporabi elektronske pošte ne odpirajte pripetih datotek, če vam pošiljatelj elektronskega sporočila ni znan.

 Vklopite varnostne nastavitve spletnega brskalnika.

 Na računalnik namestite protivirusne programe, požarni zid in dodatno zaščitno programsko opremo ter jih sproti posodabljajte z najnovejšimi različicami.

 Ob okvarah računalniške opreme se za pomoč obrnite na preverjene in usposobljene servisne službe.