



Soovitused arvutikasutajale: parool, ID-kaart, mobiil-ID

18.12.2017

Arvutit era- või töötstarbel kasutades on arvutikasutaja esmaseks privaatsuse kaitseks arvutisse või arvutivõrku sisselogimise parool. Nõuetekohane parool on eelduseks kasutaja turvalisuse tagamisel.

Parool tuleb valida selliselt, et seda on võimalik meelde jätta, kuid pole lihtne ära arvata. Kindlasti ei tohiks parooli üles kirjutada ja panna näiteks töökeskkonnas sahtlisse või mis veel hullem, kleepsuga arvutiekraani külge. Samuti ei tohi parooli avaldada kolmandatele isikutele, k.a kolleegidele. Juhul, kui on tekkinud kahtlus, et kõrvalistele isikutele on parool saanud teatavaks, tuleb arvutikasutajal parool kohe ära muuta.

Soovituslikud nõuded paroolile:

Parool peaks koosnema suur- ja väiketähtede ning numbrite kombinatsioonist. Soovitav on lisaks kasutada kirjavahemärke. Veel parem, kui parooliks on fraas mõnest teile tuttavast ütlusest või laulusalmist. Kasutades seal segamini suur ja väiketähti ning sekka numbreid, on pahalastel seda tunduvalt keerukam ära arvata. Parooli pikkus võiks olla vähemalt 10 sümbolit. Mida pikem, seda parem. Parooli peab perioodiliselt muutma (nt 3 kuu tagant). Erinevates keskkondades tuleks kasutada erinevaid parooli.

Parool ei tohi olla:

- koostatud vaid ühesugustest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
- tuletatud kasutaja isiklikust informatsioonist, mida keegi võib lihtsa vaevaga ära arvata, näiteks pereliikme või lemmiklooma nimi, oma telefoni- või autonumber, enda või perekonnaliikmete sünnipäev või aadress jne;
- lihtsasti tuletatav varasemalt kasutatud paroolidest, näiteks muutes paroolis ainult ühte tähte või numbrit.

NB! Kui teenused võimaldavad nn kaheastmelist autentimist, tuleks see kindlasti aktiveerida. Levinumaks viisiks on see, et kasutaja parooliga teenusesse sisse logides saab teenus SMS-ga kasutaja mobiiltelefonile juhuslikult genereeritud lisaparooli. See aitab tagada kasutaja täiendava turvalisuse.

ID-kaart, mobiil-ID

Kõige turvalisem arvutisse või arvutivõrku sisse logimise ja autentimise viis on kasutada võimalusel ID-kaarti või mobiil-ID-d. Põhjuseks on see, et parool põhineb vaid sellel, mida kasutaja teab. Kui keegi arvab parooli ära (näiteks selle sisestamist jälgides), on ära arvajal kõik samad õigused, mis kasutajal, kelle parool teada saadi.

ID-kaart ja mobiil-ID põhinevad aga kahel turvalisuse elemendil. Esiteks, mida kasutaja teab (PIN kood) ning teiseks, mida kasutaja omab (mobiiltelefoni SIM-kaardil või ID-kaardil olev elektrooniline kiip, mis sisaldab autentimiseks vajalikke andmeid).

See tähendab, et enam ei piisa autentimiseks vaid ühest komponendist. Kui keegi varastab arvutikasutaja ID-kaardi, aga ei tea PIN koodi, ei saa ta võõra nime all arvutisse siseneda. Kui aga keegi saab teada kasutaja PIN koodi, aga ei oma tema ID-kaarti, on juurdepääs arvutisse samuti suletud.

ID-kaardi kasutamisel on kasulik meeles pidada, et pärast sisselogimist või toimingute lõpetamist tuleks ID-kaart soovitatavalt ID-kaardi lugejast välja võtta. Kui kaart on arvutiga jätkuvalt ühendatud, on võimalik ID-kaarti pahatahtlikult kasutada.



Allikas URL: <https://www.aki.ee/et/soovitused-arvutikasutajale-parool-id-kaart-mobiil-id>