Täna on Paroolipäev - sinu salasõna lahtimurdmiseks võib kuluda vaid sekund

1 aasta tagasi - 01.05.2025 Autor: AM

1. mail on rahvusvaheline **Paroolipäev**. NordPassi 2024. aasta uuringu kohaselt saab küberkurjategija lahti murda lausa 78% maailma kõige levinumatest salasõnadest ühe sekundiga.

Elisa infoturbejuhi Mai Krafti sõnul muutub küberturvalisuse ohutaset arvestades tugevad paroolid ja küberhügieen aasta-aastalt üha olulisemaks: "Salasõnade loomisel ei tohi alluda mugavusele ega rutiinile. Küberkurjategijate tööriistad muutuvad üha nutikamaks ja suudavad lihtsad mustrid hetkega ära tunda. Selleks, et enda digielu kaitsta, peaks tugeva salasõna loomine olema sama tähtis harjumus kui ukse lukustamine kodust lahkudes."

Mitmeid aastaid inimeste parooliharjumusi kaardistanud ettevõtte NordPass värske raporti kohaselt olid möödunud aastal maailma enim kasutatavad salasõnad endiselt "123456", "123456789", "12345678", "password" ning "qwerty123". Kõiki neid saab lahti murda alla ühe sekundiga. Veelgi murettekitavam on asjaolu, et ka ligi 78% maailma kõige levinumatest 200 salasõnast suudetakse lahti murda vähem kui ühe sekundiga.

Tugeva salasõna loomisel on oluline vältida kõiki lihtsasti äraarvatavaid mustreid – näiteks vältida oma nime, sünnikuupäeva, järjestikuseid numbreid (nagu 123456) või tavalisi sõnu või nimesid (salasõna, katrin), mida küberkurjategijad kõige esimesena proovivad.

Parim kaitse igal kasutajal on kasutada igal kontol unikaalset salasõna ning eelistada vähemalt 12-märgilist kombinatsiooni, kus on nii suuri kui väikeseid tähti, numbreid ja erisümboleid. Näiteks võib mõelda välja just endale tähendusliku fraasi koos suvaliste tähemärkidega, mida muudelt kohtadelt keegi ei aimaks.

Samuti tuleks vältida sama salasõna korduvat kasutamist eri kontodel – üks leke võib nii kompromiteerida korraga kogu digielu, alustades meilidest ja sotsiaalvõrgustikest, lõpetades finantsteenustega.

Selle riski maandamiseks soovitab Elisa kasutada turvalist salasõnahaldurit, mis võimaldab kõik unikaalsed paroolid turvaliselt talletada ja ise meeles pidada vaid

üht tugevamat põhiparooli, mitte kirjutada paroole lahtiselt paberile või talletada neid tekstifailina arvutisse.

Salasõna turvalisust saab lihtsasti suurendada, vahetades olulisemate teenuste (nt e-post, sotsiaalmeedia, internetipank) paroole regulaarselt, eriti juhul, kui saad teada mõnest andmelekkest või turvaprobleemist. Lisaks soovitatakse alati käivitada kaheastmeline tuvastus: see tähendab, et lisaks salasõnale tuleb sisse logides ennast kinnitada näiteks SMSi või mobiilirakenduse kaudu – nii ei õnnestu kontole pääseda ka juhul, kui salasõna on juhuslikult lekkinud.

"Paroolipäeval soovitan võtta rahulikult 15 minutit ja analüüsida, millised on olnud sinu seni kasutatud salasõnad kõige tundlikumates keskkondades – näiteks e-posti, internetipanga või sotsiaalmeedia juures. Kui mõni neist meenutab midagi liiga lihtsat või universaalset, on just nüüd õige aeg see uue vastu välja vahetada," lisas Kraft.

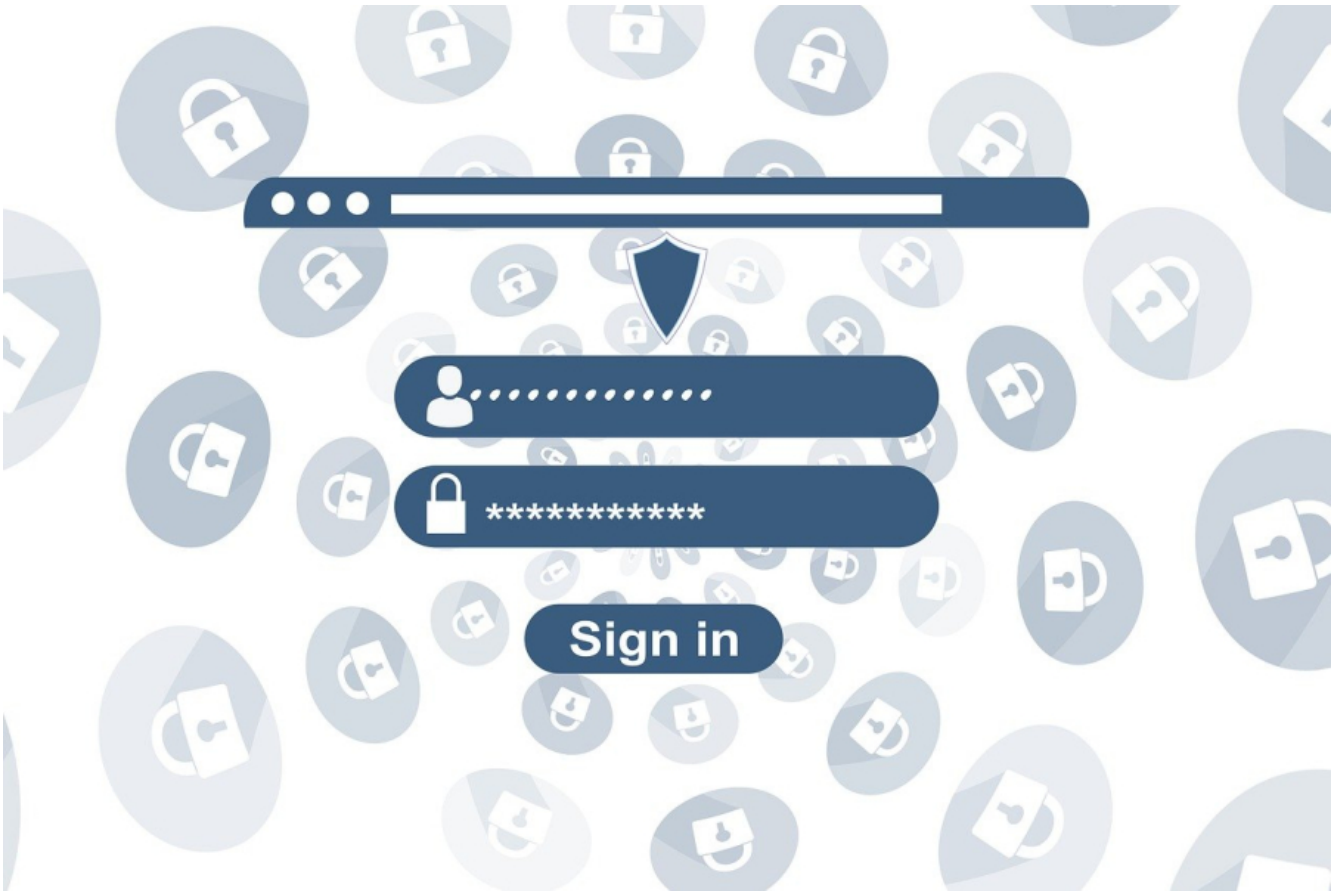
*Kuula eksperimentaalset **eestikeelset** tehisaru Podcasti sellest artiklist :)*

Helifail

- Uudised
- Lahendused

- Turvalisus

Pilt


Sign in