

**Keičiasi metai, keičiasi dešimtmečiai, o saugumui internete koją kiša ta pati sena problema - apmaudžiai prasti žmonių slaptažodžiai. Anonimiškai atliktos internetinės apklausos rodo, kad daugybė žmonių naudoja skaičius 12345 ar tiesiog žodį „password“ - kodus, kuriuos nulaužti programišiams yra vienas juokas. Kas patenka tarp prasčiausių interneto slaptažodžių ir ar įmanoma susikurti tokį, kurio nenulauš niekas?**

**Jei matote čia savo slaptažodį - nedelsdami jį pasikeiskite**

12345, 123456 ir 123456789. Štai tokius slaptažodžius turi mažų mažiausiai 6,3 mln. interneto vartotojų. Statistiką pateikia duomenų nutekėjimus ir anonimines apklausas ištyrusi „NordPass“ platforma, išvis analizavusi 500 mln. skirtingų paskyrų slaptažodžių. Tad maždaug procentą visų slaptažodžių sudaro vien šios elementarios skaičių sekos, nedaug nuo jų atsilieka tokie variantai kaip „asdf“ arba „qwerty“

„Svarbu nuraminti, jog Lietuvos vartotojų naudojamų slaptažodžių dažnumo patikrinti neįmanoma, tačiau tikėtina, kad pasaulinėms tendencijoms – nesipriešiname ir čia“ –, akcentuoja bendrovės „Bitė Lietuva“ korporatyvinių reikalų ir ryšių su visuomene vadovas Jaunius Špakauskas.

„Niekas negali sužinoti jūsų slaptažodžio, tad vieninteliai būdai įvertinti, kurių jų populiariausi, yra didelės apimties anoniminės apklausos. Iš globalios statistikos matyti, kad daugelis vartotojų renkasi skaičių ar raidžių kombinacijas, kurias prisimintų vos pažvelgę į klaviatūrą. Taip pat mėgstami vardai, ypač moteriški, taip pat sporto šakos, pavyzdžiui, žodžiai „futbolas“ ir „krepšinis“ yra vieni populiariausių pasaulio slaptažodžių“, – pastebi J. Špakauskas.

10 populiariausių slaptažodžių pasaulyje:

1. 12345
2. 123456
3. 123456789
4. test1
5. password
6. 12345678

7. zinch

8. g\_czechout

9. asdf

10. qwerty

### **Kodėl slaptažodžių mados nesikeičia?**

Blogiausia, jog panaši informacija apie elementarių slaptažodžių populiarumą pasklinda jau nebe pirmus metus – nesvarbu, kiek žmonės perspėjami apie pavojus, tendencija nelabai keičiasi. Komunikacijos specialistas pastebi dvi svarbiausias priežastis, kurios abi, deja, tiesiogiai susijusios ir su asmeninės informacijos saugumu.

„Pirma ir paprasčiausia priežastis – vartotojas neprisimena sudėtingų slaptažodžių. Jei turėtume tik vieną socialinį tinklą ir vieną elektroninio pašto dėžutę, išimintume dvi unikalias kombinacijas ir nepatirtume sunkumų. Vis tik šiandien daugelis turime dešimtis paskyrų, kurių dalis dar ir reikalauja reguliariai slaptažodį keisti. Todėl dalis vartotojų numoja ranka ir pasirenka vieną žodį, kurio su niekuo nesupainios. Bet vadovaujantis tokia logika rizikuojama, kad nulaužę vieną vartotojo paskyrą, programišiai iškart turės priėjimą prie jų visų“, – sako „Bitė Lietuva“ atstovas.

Anot jo, antroji priežastis susijusi su dvejone, ar išvis verta gaišti laiką galvojant apie slaptažodžius – juk daugelio svetainių paskyros net į jas įsilaužus neduos ilgapirščiams daug naudos.

„Šis požiūris pasikeičia palyginus interneto vartojimą su asmeniniu gyvenimu – juk net jei žinotume, jog pašalinis žmogus nieko nepavogs, ar leistume jam savavališkai stebėti, ką mes veikiamo ar dar blogiau – lankytis mūsų namuose? Be to, surinkus asmeninius duomenis juos galima panaudoti išgaunant prieigą prie kitų mūsų duomenų, o taip pamažu kyla rizika netekti kažko išties svarbaus“, – pabrėžia J. Špakauskas.

### **3 žingsniai, kaip susikurti (beveik) tobulą slaptažodį**

1. Užuoat galvoję su hobiais ar šeima susijusį slaptažodį, pasinaudokite vienu nemokamų internetinių slaptažodžių generatorių – tuomet jūsų kombinacija bus atsitiktinė ir niekaip neatspėjama net jus pažįstantiems. Tą patį pakartokite su kiekviena paskyra.

2. Šiuos naujus slaptažodžius bus itin sudėtinga prisiminti ar atspėti (juk tam juos ir

naudojate) – tam galite parsisiųsti vieną iš daugybės slaptažodžių valdymo programėlių, kurios prisimena už jus: „LastPass“, „1Password“, „Keeper“, „KeePass“ ir kt. O jums tereikės prisiminti tik vieną, pačios programėlės, slaptažodį.

3. Visose svetainėse, kurios turi tokią galimybę, būtinai naudokite dviejų faktorių autentifikaciją (vadinamąją 2FA), tuomet prisijungiant kompiuteriu reikės tą patvirtinti telefonu ir atvirkščiai. Tikimybė, kad kam nors pavyks nuotoliniu būdu perimti dviejų jūsų prietaisų kontrolę yra labai maža, tad svetainėse, kur naudojate šį prisijungimo būdą greičiausiai būsite saugūs.

„Vis tik kaip nėra tobulo saugumo sprendimo namams ar automobiliui, taip jis vargu ar egzistuoja ir internete. Vis dėlto svarbu, jog savo paskyrų saugumą internete galite dešimteriopai sustiprinti dėl to nepatirdami nei išlaidų, nei gaišdami brangų savo laiką, o tiesiog įsiminę kelis svarbiausius patarimus“, – rekomenduoja J. Špakauskas.

