Milijardui vartotojų teks atsisakyti slaptažodžių: kaip 2025 m. pradėti su saugesniais prisijungimais?

Sakoma, kad Naujuosius reikia sutikti be nebaigtų darbų, bet tik nedaugelis prisimena apie skaitmeninius. Pagrindinis jų – seniai nekeisti ir jau sukčių rankose galimai atsidūrę mūsų slaptažodžiai, kurie lyg tiksinti bomba bet kada galia apkartinti mūsų kasdienybę. „Telia“ pasakoja, kaip ateinančių metų proga atlikti savo slaptažodžių „inventorizaciją“ ir išbandyti saugesnę jų alternatyvą.

„Slaptažodžio, kaip patikimo vartotojo identifikavimo metodo, era jau baigėsi ir apie slaptažodžių ištrynimą milijardui vartotojų jau prakalbo net pati „Microsoft“. Deja, perėjimas prie jo įpėdinio – slaptarakčio (angl. passkey) – užtruks. Todėl kritiškai svarbu pasirūpinti, kad pereinamuoju laikotarpiu mūsų slaptažodžiai būtų kuo saugesni. Šį darbą reikėtų pradėti nuo „nulaužtų“ prisijungimų patikros „haveibeenpwned.com“ svetainėje ir jų pakeitimo, o pratęsti – įjungiant dviejų žingsnių autentifikaciją bei pasinaudojant slaptažodžių tvarkyklėmis“, – teigia „Telia“ išmaniųjų įrenginių ekspertas Marijonas Baltušis.

Pirmas žingsnis – pasitikrinti

Kad ir kaip būtų gaila, paskyrų saugumas nėra vien mūsų rankose. Net sugalvojus sudėtingiausią ir ilgiausią slaptažodį nėra garantijos, kad programišiams jo „ant lėkštutės“ nepatieks aplaidus paslaugos teikėjo požiūris ar ydingos duomenų saugumo praktikos. Visgi, nors visiškai eliminuoti šios rizikos neįmanoma, ją galima reikšmingai sumažinti.

Tokiose svetainėse, kaip „databreach.com“, suvedę savo elektroninio pašto adresą ar telefono numerį, galima pasitikrinti, kokių paslaugų prisijungimai yra patekę į programišių rankas. Jei norite patikrinti tik konkretaus slaptažodžio saugumą, tą siūlo „haveibeenpwned.com/Passwords“.

Dar patogiau tą padaryti leidžia „Google Chrome“ naršyklė ir „Passwords“ programėlė „Apple“ įrenginiuose. „Chrome“ atveju reikėtų nukeliauti į nustatymus, atverti slaptažodžių skiltį ir spustelėti „Tikrinti“, o atvėrus „Passwords“ aplikaciją – paspausti ant langelio „Saugumas“. Abu šie įrankiai automatiškai patikrins išsaugotus slaptažodžius ir praneš, kurie iš jų yra nutekėję.

Šiai informacijai paaiškėjus, reikėtų prisiminti, ar tų pačių el. pašto adreso bei slaptažodžio kombinacijų nenaudojote jungdamiesi prie kitų sistemų ir šiuos duomenis pasikeisti kaip įmanoma skubiau.

„Kiekvienai paskyrai reikia sukurti unikalų slaptažodį, kuriame būtų derinamos didžiosios ir mažosios raidės, skaičiai bei simboliai. Jame jokiu būdu negalima naudoti savo gimimo

datos, artimųjų vardų ar kitos lengvai atspėjamos informacijos. Vis dėlto dar svarbiau visur, kur įmanoma, įjungti dviejų žingsnių autentifikaciją (2FA), kuri kiekvieną kartą jungiantis papildomai pareikalaus SMS žinute ar specialios programėlės sugeneruoto kodo. Net jei slaptažodis būtų nutekėjęs, 2FA užkerta kelią neteisėtam prisijungimui“, – priduria M. Baltušis.

Prie alternatyvos turės pereiti milijardas vartotojų

Prieš didžiąsias šių metų šventes „Microsoft“ paskelbė apie itin paaštrėjusią slaptažodžių saugumo problemą. Per 2024 m. į slaptažodžius nukreiptų atakų skaičius išaugo dvigubai – šiuo metu kas sekundę užblokuojama net 7 000 tokių išpuolių. Atsižvelgdama į šią statistiką, bendrovė paskelbė, kad tradicinių slaptažodžių era baigiasi, o milijardas jos vartotojų anksčiau ar vėliau turės ištrinti savo dabartinius slaptažodžius ir pereiti prie slaptarakčių.

Slaptaraktis – tai modernus ir saugus prisijungimo sprendimas, kuriame naudojamas biometrinis identifikavimas arba įrenginyje saugomas šifravimo raktas. Skirtingai nei slaptažodžiai, slaptarakčiai nėra perduodami internetu ir negali būti pavogti ar panaudoti „phishing“ atakoms.

„Slaptarakčiai ne tik didina saugumą, bet ir siūlo patogumą, kurio vartotojai ilgai laukė. Jie panaikina poreikį prisiminti sudėtingus slaptažodžius, mažina klaidų riziką ir leidžia be streso pasiekti savo paskyras. Bet svarbiausia, kad ši technologija yra atspari įprastoms grėsmėms. Net jei nusikaltėliai pavogtų jūsų el. pašto adresą ar kitą informaciją, jie negalėtų pasinaudoti jūsų paskyromis fiziškai neturėdami jūsų įrenginio ir nenuskaitę jūsų “, – detalizuoja „Telia“ atstovas.

Išbandyti slaptarakčio veikimą jau galima tokį prisijungimo būdą aktyvavus „Google“, „Apple“, WhatsApp“, „LinkedIn“ ir daug kitų garsiausių skaitmeninių paslaugų paskyrų.

Padėti gali slaptažodžių tvarkyklės

Norint užtikrinti slaptažodžių saugumą ir supaprastinti jų valdymą, verta išbandyti slaptažodžių tvarkykles. Tokios programėlės kaip „Apple Passwords“ ir „Google Password Manager“ leidžia automatiškai sugeneruoti stiprius, sunkiai atspėjamus slaptažodžius bei juos išsaugoti. Šie įrankiai taip pat sinchronizuoja slaptažodžius visuose vartotojo įrenginiuose, todėl prisijungti prie įvairių paskyrų tampa greita ir paprasta.

Nenorintiems prisirišti prie vieno gamintojo ekosistemos, galima išbandyti universalias slaptažodžių tvarkykles, tokias kaip „NordPass“, „1Password“ ar „LastPass“. Jos leidžia

vartotojui prisiminti tik vieną pagrindinį slaptažodį, kuris suteikia prieigą prie visos tvarkyklės. Be to, šios programėlės dažnai turi papildomų funkcijų, tokių kaip slaptažodžių bendrinimas su šeimos nariais ar kolegomis.

„Slaptažodžių tvarkyklės yra puikus įrankis tiems, kurie nori naudoti stiprius slaptažodžius, tačiau nenori prisiminti daugybės skirtingų kombinacijų. Jos ne tik padeda užtikrinti vartotojo paskyrų saugumą, bet ir ženkliai palengvina prisijungimo procesą kasdien naudojant skaitmenines paslaugas. Pasirinkę slaptažodžių tvarkyklę, galite pradėti Naujuosius metus su gerokai stipresniu skaitmeniniu „imunitetu“ ir atsikratę rūpesčių dėl dažnai pamirštamų slaptažodžių“, – pataria „Telia“ išmaniųjų įrenginių ekspertas.