**Pranešimas žiniasklaidai**

2025 liepos 24 d.

**Sudėtingo slaptažodžio nebepakanka – „Google“ ragina padaryti vieną dalyką**

**Taip lengviau: greitasis skaitymas**

|  |
| --- |
| * **Sukčiavimo mastas sparčiai auga – vien pernai Lietuvoje sukčiai galėjo išvilioti apie 19 mln. eurų** * **„Google“ ragina naudotojus atsisakyti slaptažodžių ir pereiti prie saugesnio prisijungimo su prieigos raktu** * **Prieigos raktai veikia tik su vartotojo įrenginiu ir biometriniais duomenimis, todėl yra atsparesni sukčiavimui** * **„Bitės“ klientai gali stebėti pasirinktus el. pašto adresus bei telefono numerius, ar šie nebuvo nutekinti** |

**Sparčiai kintant kibernetinių grėsmių pobūdžiui, technologijų gigantai imasi ryžtingų žingsnių stiprinti žmonių apsaugą. „Google“ neseniai paskelbė įspėjimą visiems „Gmail“ naudotojams kuo greičiau atsisakyti įprasto prisijungimo su slaptažodžiu ir pereiti prie prieigos rakto (angl. passkey). Savo ruožtu ekspertai primena, kad asmeninių duomenų saugumas priklauso ne tik nuo naudojamų apsaugos sprendimų, bet ir paties žmogaus elgesio, rašoma pranešime žiniasklaidai.**

„Slaptažodžiai tampa silpniausia grandimi saugant žmonių duomenis. Juos lengva atspėti, jie dažnai naudojami kelioms skirtingoms paskyroms ir gali būti nutekinami per įvairius duomenų pažeidimus. Net ir papildomos apsaugos priemonės, kaip SMS kodai, ne visada gali apsaugoti nuo sukčiavimo atvejų, kai nuotoliniai sukčiai imituoja oficialius siuntėjus ar svetaines“, – pasakoja Mindaugas Rauba, „Bitės“ technologijų direktorius.

Pasak jo, augantį sukčiavimo mastą puikiai iliustruoja ir pastarųjų metų statistika. Vien pernai Lietuvoje sukčiai iš žmonių ir įmonių galėjo išvilioti apie 19 mln. eurų, skelbė Pinigų plovimo prevencijos kompetencijų centras. Tai beveik 66,7 proc. daugiau nei ankstesniais metais.

**Kaip apsaugoti savo „Google“ paskyrą?**

„Google“ ragina pamažu atsisakyti tradicinių slaptažodžių ir pereiti prie modernesnių prisijungimo būdų.

„Šiuo metu rekomenduojama naudoti prisijungimą su prieigos raktu (angl. passkey), kuris yra atsparesnis sukčiavimui. Jo saugumas grindžiamas tuo, kad prieigos raktas veikia tik žmogaus patvirtintuose įrenginiuose. O prisijungimui galima naudoti ne tik PIN kodą ar ekrano užrakto piešinį, bet ir biometrinius duomenis – piršto atspaudą ar veido atpažinimą (angl. Face ID). Tokios informacijos sukčiai neturi ir negali pasisavinti“, – pataria M. Rauba.

Pasak „Bitės“ technologijų direktoriaus, prieigos raktų naudojimas praverčia ir tuo, kad šis prisijungimo metodas neveikia fiktyviose svetainėse. Tad šansų nuotoliniams sukčiams išvilioti jūsų duomenis, kuriant netikras svetaines, dar labiau sumažėja.

„Prieigos raktas itin praverčia, kai su „Google“ paskyra norite jungtis prie įvairių svetainių ar socialinių tinklų. Pavyzdžiui, su „Google“ paskyra jungiatės prie „Facebook“ ar skelbimų portalo, nes nenorite kurti naujo slaptažodžio. Tokiu atveju galite būti ramūs, kad jūsų prisijungimas yra saugus, o ir nereikia prisiminti dar vieno slaptažodžio“, – pataria M. Rauba.

Visus slaptažodžius galima saugoti ir sinchronizuoti tarp skirtingų įrenginių naudojant naršyklėje veikiančią slaptažodžių saugyklą „Google Password Manager“.

**Svarbiausia – tikrinti informaciją**

Jei žmonės nenori naudoti prieigos raktų, M. Rauba rekomenduoja bent jau sustiprinti prisijungimą prie savo „Google“ paskyros su dviejų veiksnių autentifikavimu (angl. two-factor authentication).

„Dviejų veiksnių arba žingsnių autentifikavimas leidžia jums patvirtinti savo tapatybę su papildomu veiksmu. Pirma, įvedate savo slaptažodį, o tada „Google Authenticator“ programėlė jūsų telefone sugeneruoja papildomą kodą, kurį įvedę patvirtinate, kad tai tikrai esate jūs. Papildomą prisijungimo patvirtinimą verta aktyvuoti ir kituose tinklapiuose, ypač socialiniams tinklams“, – pataria vienas skaitmeninių paslaugų bendrovės vadovų.

Vis dėlto, jei taip nutiktų, kad el. pašto slaptažodis buvo nutekintas, apie tai „Bitės“ klientai, pasirinkę paslaugų planus „Saugiau“, gali sužinoti nedelsiant. Šių metų pradžioje į paslaugų planus įtraukta Kibernetinių incidentų patikros paslauga leidžia stebėti iki 5 el. pašto adresų ar telefono numerių, ar šie nepateko į nutekintų duomenų sąrašus.

„Šiuolaikinės technologijos atveria ne tik daug galimybių, bet ir naujų grėsmių. Būtina neprarasti budrumo ir atidžiai tikrinti, kur vedate savo duomenis, ar lankotės oficialiame tinklalapyje, ar gautas laiškas nėra nuotolinių sukčių ataka. Papildomos saugumo priemonės tik padeda apsaugoti savo duomenis, bet daug priklauso ir nuo paties žmogaus elgesio internete“, – sako M. Rauba.

**Daugiau informacijos:**

Jaunius Špakauskas

„Bitė Lietuva“ korporatyvinės komunikacijos vadovas

+370 682 66188, [Jaunius.Spakauskas@bite.lt](mailto:Jaunius.Spakauskas@bite.lt)