

OUCH!

ŠIAME LEIDINYJE...

- Apžvalga
- Slaptažodžiai
- Dviejų etapų patikrinimas

Dviejų etapų tapatybės patikrinimas

Apžvalga

Procesas, kurio metu yra nustatoma jūsų tapatybė (toliau – tapatybės patikrinimas) yra svarbiausia jūsų informacijos apsaugos dalis. Naudodami patikimą tapatybės patikrinimo būdą galite būti tikri, jog prie savo informacijos, tokios kaip el. paštas, nuotraukos ar banko sąskaitos, galėsite prisijungti tik jūs. Patvirtinti savo tapatybę galite įvairiai, pavyzdžiui, naudodami tik jums žinomą informaciją, tokią kaip slaptažodis, tik jums priklausančią dokumentą, tokį kaip vairuotojo pažymėjimas ar tik jums būdingą savybę, tokią kaip piršto antspaudas. Kiekvienas iš šių metodų turi savų privalumų ir trūkumų. Populiariausia yra naudoti slaptažodžius, t.y., tik jums žinomą informaciją. Šiame naujienlaiškyje pamokysime, kaip galite apsaugoti savo asmeninę informaciją, naudodami dviejų etapų tapatybės patikrinimą, t.y., kai ką žymiai saugesnio ir paprasčiau naudojamo už slaptažodžius. Norint geriau suprasti, kas yra dviejų etapų tapatybės patikrinimas, pirmiausiai turime pradėti nuo slaptažodžių.

Kviestinis redaktorius

Keith Palmgren informacijos saugumo klausimais yra sukaukęs virš 30 metų patirties. SANS institute jis yra atestuotas dėstytojas ir penkias dienas SANS institute trunkančio SEC301 įvadinio kurso medžiagos apie informacijos saugumą autorius. Laisvu nuo paskaitų metu, Keith teikia konsultavimo paslaugas ir rašo projektus. Keith veiklą galite sekti Twitter, įvedę [@kpalmgren](#).

Slaptažodžiai

Slaptažodžiais jūsų tapatybė yra nustatoma remiantis tik jums žinoma informacija. Tačiau slaptažodžius naudoti yra pavojinga dėl vieno jų trūkumo. Jei kažkas gali atspėti arba gauti prieigą prie jūsų slaptažodžio, tuomet jie gali apsimesti jumis ir prisijungti prie visos jūsų informacijos, kuri tuo slaptažodžiu yra saugoma. Štai kodėl esate mokomi apsisaugoti, naudojant patikimus slaptažodžius, kuriuos kitiems yra sudėtingiau atspėti, kiekvienai paskyrai naudoti vis kitokį slaptažodį arba niekada neatskleisti savo slaptažodžių kitiems. Nors tokie patarimai vis dar aktualūs, slaptažodžių nauda baigia atgyventi - šiais laikais jie nebėra veiksmingi. Naudojant naujausias technologijas, kibernetiniams nusikaltėliams dabar yra žymiai lengviau išgauti svetimus slaptažodžius. Todėl mums tereikia lengvai naudojamo, tačiau žymiai saugesnio tapatybės patikrinimo būdo. Laimei, toks būdas šiuo metu yra mums prieinamas ir jis vadinasi dviejų etapų tapatybės patikrinimu.

Dviejų etapų tapatybės patikrinimas

Dviejų etapų tapatybės patikrinimas (dar vadinamas dviejų žingsnių tapatybės patikrinimu arba anglišku trumpiniu 2FA) yra žymiai saugesnis už pavienius slaptažodžius. Čia naudojamas ne vienas, bet du asmens tapatybės patikrinimo būdai.

Dviejų etapų tapatybės patikrinimas

Pavyzdžiui, naudojant jūsų banko kortelės duomenis. Iš bankomato nusiimdami pinigų jūs iš tiesų naudojate dviejų etapų tapatybės patikrinimą. Norėdami gauti prieigą prie savo pinigų, pirmiausiai turite turėti banko kortelę (t.y., jūsų turimas daiktas) ir žinoti PIN kodą (t.y., jūsų žinoma informacija). Praradus banko kortelę, jūsų pinigai lieka saugūs. Kam nors radus jūsų banko kortelę pinigų nusiimti nepavyks, kadangi jie nežinos jos PIN kodo (nebent PIN kodą būtumėte užrašę tiesiai ant kortelės, o tai jau sukeltų problemų). Svetimas asmuo negalės nusiimti pinigų turėdamas vien tik PIN kodą, bet neturėdamas banko kortelės. Taigi nusikaltėlis, norėdamas įsilaužti į jūsų banko sąskaitą turi turėti ir žinoti abu šiuos dalykus. Štai kodėl dviejų etapų tapatybės patikrinimas yra žymiai saugesnis, be to naudodami šį būdą, jūs esate dvigubai saugesni.



Dviejų etapų tapatybės patikrinimo naudojimas

Dviejų etapų tapatybės patikrinimas yra kažkas, ką kiekvienai iš savo paskyrų nustatote individualiai. Laimei, dabar tarp daugumos internetinių paslaugų galima rasti ir šią. Labiausiai dviejų etapų tapatybės patikrinimo srityje pirmauja „Google“. „Google“ paskyros yra pagrindinis kibernetinių nusikaltėlių taikinytis, kadangi čia milijonams žmonių visame pasaulyje yra siūloma daugybė nemokamų internetinių paslaugų. Dėl šios priežasties, „Google“ reikėjo patikimesnio tapatybės nustatymo būdo ir ji buvo viena iš pirmųjų organizacijų, sugalvojusių dviejų etapų tapatybės patikrinimą daugumai savo internetinių paslaugų. Supratę, kaip veikia „Google“ dviejų etapų tapatybės patikrinimas, suprasite kaip jis veikia daugumoje visų kitų svetainių, tokių kaip Twitter, Facebook, Apple, Instagram bei daugumoje bankų.

Pirmiausiai, turite įjungti dviejų etapų tapatybės patikrinimą savo „Google“ paskyroje ir įregistruoti savo mobiliojo telefono numerį. Tai padarius, dviejų etapų tapatybės patikrinimas veiks taip, kaip aprašyta toliau. Prie savo paskyros prisijungsite kaip įprasta, naudodami vartotojo vardą ir slaptažodį. Tai bus pirmasis etapas, naudojant tik jums žinomą informaciją. Tuomet „Google“ jūsų nurodytu mobilaus telefono numeriu atsiųs SMS žinutę su unikaliu kodu, sudarytu iš šešių skaičių eilutės. Šiuos šešis skaičius kaip ir slaptažodį įveskite į svetainėje nurodytą laukelį. Tai bus antrasis etapas. Taigi, norėdami sėkmingai prisijungti prie savo paskyros, turėsite žinoti savo slaptažodį ir su savimi turėti mobilųjį telefoną, į kurio prieš tai nurodytą numerį bus siunčiami unikalūs kodai. Nusikaltėlis sužinojęs jūsų slaptažodį negalės prisijungti prie jūsų



Dviejų etapų tapatybės patikrinimas

„Google“ paskyros, nebent su savimi turėtų jūsų mobilųjį telefoną. Norint užtikrinti, kad jūsų paskyra bus tikrai saugi, kaskart prisijungiant, „Google“ jums atsiųs naują, unikalų kodą.

Štai dar vienas dviejų etapų tapatybės patikrinimo būdas, naudojamas tiek „Google“, tiek kitose svetainėse. Nepageidaujami nurodytu telefono numeriu gauti minėtųjų SMS žinučių, galite pasirinkti savo išmaniajame telefone įdiegti tapatybės patikrinimo programą. Tuomet, kaskart prisijungiant, programa sukurs unikalų kodą. Šio metodo privalumas yra tas, kad naudodami mobiliąją programą ir norėdami gauti unikalų kodą, neprivalėsite jungtis prie jokios telefono paslaugos, kadangi šį kodą jums sukurs pats telefonas. Be to, kadangi kodą kurs jūsų telefonas jo iš niekur nesiųsdamas, šis kodas negalės būti pavogtas.

Prisiminkite, dviejų etapų tapatybės patikrinimas nėra įjungiamas automatiškai, todėl jį turite įsijungti patys. Nors iš pradžių gali atrodyti, jog dviejų etapų tapatybės patikrinimo metodas yra aktualesnis darbe, labai rekomenduojame jį naudoti visur, kur tik įmanoma, ypač naudojant tokias svarbias paslaugas, kaip el. pašto paskyros, internetinė bankininkystės sistema ar internetinė failų saugykla. Dviejų etapų tapatybės patikrinimas jūsų informaciją apsaugos žymiai labiau, nei naudojant paprasčiausią slaptažodį.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę <http://www.securingthehuman.org>.

Šaltiniai

Slaptafrazės:	http://www.securingthehuman.org/ouch/2015#april2015
Svetainės palaikančios dviejų etapų patikrinimą:	https://twofactorauth.org
Sustok Galvok Prisijunk:	http://stopthinkconnect.org/2stepsahead
Google dviejų etapų prisijungimas:	http://www.google.com/landing/2step/
SANS dienos saugumo patarimas:	http://www.sans.org/tip_of_the_day.php

Licencija

OUCH! Yra leidžiamas SANS Securing The Human instituto ir platinamas pagal [Creative Commons BY-NC-ND 3.0 licencija](https://creativecommons.org/licenses/by-nc-nd/3.0/). Jums leidžiama naudoti ir platinti šį naujienlaiškį su sąlyga, kad niekas nebus keičiama. Norėdami gauti daugiau informacijos susisiekite su mumis ouch@securingthehuman.org.

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)