Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

INFORMACINIS BIULETENIS

DAR KARTĄ APIE SLAPTAŽODŽIUS IR KITAS KIBERNETINIO SAUGUMO PRIEMONES

2023 m. kovo 29 d.
Vilnius

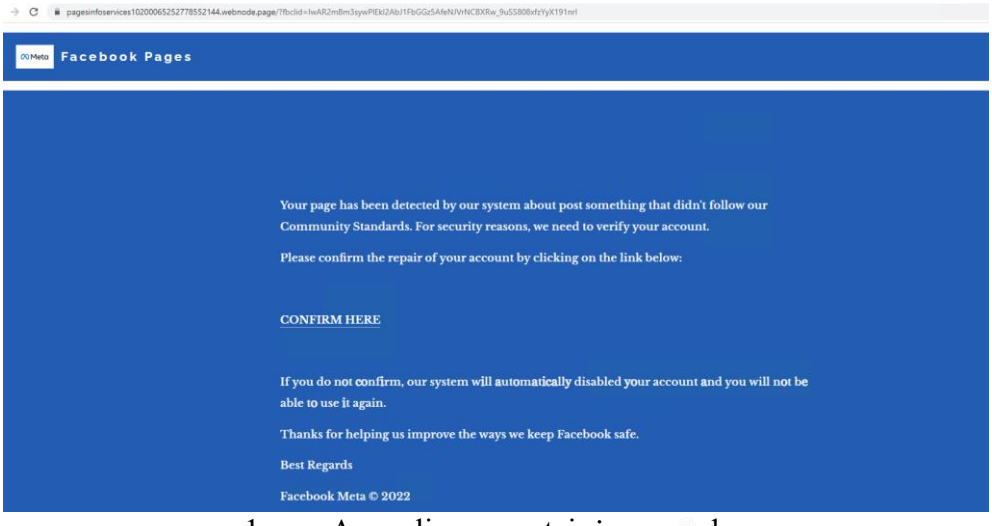
Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) nuolatos ir įvairiais kanalais primena asmenims būtinybę naudoti sudėtingus slaptažodžius, juos nuolatos keisti, akcentuoja dviejų faktorių autentifikaciją, tačiau beveik kiekvieną dieną sulaukiame pranešimų apie užvaldytas socialinių tinklų, el. pašto paskyras, nutekintą prisijungimo informaciją ar bandymus neteisėtas būdais gauti paskyrų prisijungimo informaciją.

Labai svarbu suprasti, kad socialinių tinklų ar el. pašto paskyros yra „skaitmeninis turtas“, ypač jei tai verslo paskyros. „Skaitmeniniam turtui“, kaip ir būstui ar automobiliui, reikalinga patikima apsauga. Paklauskite savęs, kodėl norėdami apsaugoti savo būstą turite šarvuotas duris, moderniausias spynas ir niekam neskolinate raktų nuo jų, o prisijungdami prie socialinių tinklų ar el. pašto paskyros naudojate lengvai atspėjamus slaptažodžius, jų niekada nekeičiate, vengiate naudoti dviejų faktorių autentifikavimą ir kitas apsaugos priemones? Žemiau primename šiuo metu dažniausiai naudojamus asmeninių duomenų išviliojimo būdus.

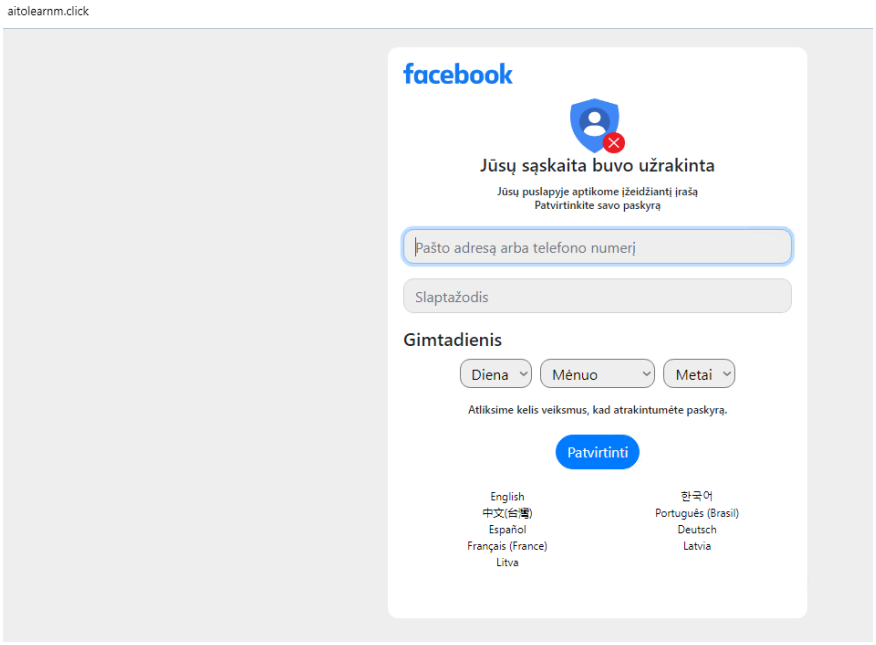
Apgaulingi interneto puslapiai

Piktavaliai paskyrų užvaldymui naudoja įvairius metodus, tačiau dažniausias jų – tai socialinės inžinerijos principais pagrįstas sukčiavimas. Potencialios aukos gauna **apgaulingus el. laiškus, žinutes** (angl. *Phishing*) ar **SMS žinutes** (angl. *Smishing*), kurios yra atsiųstos suklastojus socialinių tinklų ar el. pašto paslaugų teikėjų adresus, o kartais net ir nesivarginant to daryti, nes dalis asmenų vis dar neturi įpročio ar nemoka patikrinti informacijos apie siuntėją.

Apgaulingi el. laiškai ar žinutės nukreipia potencialias aukas į suklastotus interneto puslapius (1-2 pav.), kuriuose prašoma, o kartais ir reikalaujama, kuo skubiau pateikti ne tik savo prisijungimo informaciją, bet ir kitus asmens duomenis. Pasitaiko atvejų, kai paskyrų užvaldymui panaudojami praeityje nutekinti, tačiau vis dar aktualūs, ilgą laiką nekeisti slaptažodžiai.



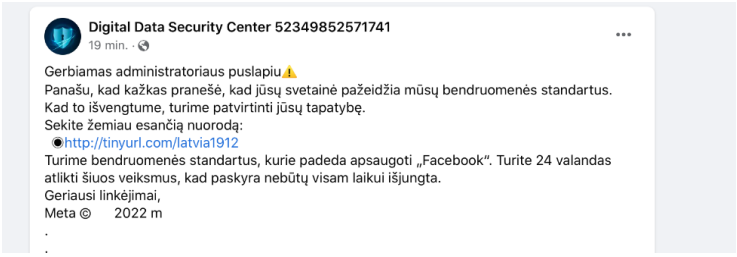
1 pav. Apgaulingos svetainės pavyzdys



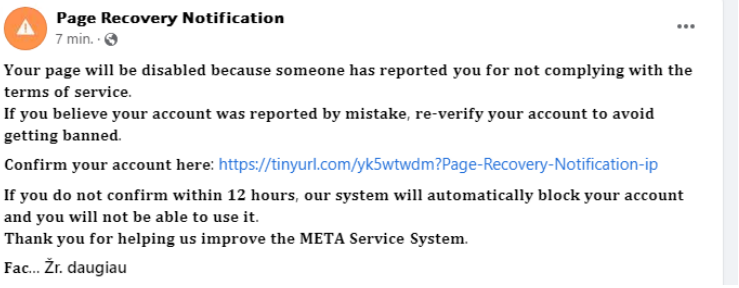
2 pav. Apgaulingos svetainės pavyzdys

Apgaulingos socialinių tinklų paskyros

Siekdami išvilioti prisijungimo duomenis, piktavaliai plačiai naudojasi ir socialinių tinklų ar el. pašto teikėjų paslaugomis (3–4 pav.). Tokiais atvejais jie sukuria paskyrą ar el. pašto dėžutę skambiu pavadinimu, apsimetant gerai žinomais skaitmeninių paslaugų tiekėjais. Paprastai naudojami tie patys metodai: bauginimas, skubinimas, manipuliavimas jausmais ar smalsumu, lengvai uždirbamais pinigais. Visi metodai yra naudojami, kol galiausiai yra paspaudžiama nuoroda į suklastotą svetainę. Užvaldytos paskyros taip pat yra naudojamos kitų apgaulingų el. laiškų ar pranešimų platinimui.



3 pav. Netikros socialinio tinklo paskyros pavyzdys



4 pav. Netikros socialinio tinklo paskyros pavyzdys

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Grasinantys el. laiškai

Senas, tačiau vis dar plačiai naudojamas sukčiavimo būdas, siekiant įbauginti naudotoją ir gauti finansinę naudą, tai grasinančio pobūdžio el. laiškų siuntimas (5 pav.). Juose piktavaliai tvirtina, kad pilnai kontroliuoja naudotojo įrenginius ir (ar) paskyras, stebi jo veiksmus bei turi surinkę kompromituojančią informaciją apie asmenį, kurią grasina paskelbti viešai. Įspūdžiui sustiprinti taip pat gali būti naudojami seni ar praeityje nutekinti slaptažodžiai, pridedama neva naudotojo kompiuterio darbalaukio / naudojamos operacinės sistemos nuotrauka. Tokio tipo el. laiškai gali būti parašyti skirtingomis kalbomis, dažniausiai anglų, rusų arba lietuvių.

I installed a virus on your system that allows me to control all your devices.
The virus software gives me access to all the controllers of your devices (microphone, video camera, keyboard, display). I have uploaded all your information, data, photos, browsing history to my servers. I have access to all your messengers, social networks, email, sync, chat history and contact list.
hp+?
I learned a lot about you!
\N0?
I thought what can I do with this data...
I recently came up with an interesting idea: to create a video clip in which you masturbate in one part of the screen and watch a porn site in the other, such videos are now at the peak of popularity!
What happened amazed me!
FXM9
With one click, I can send this video to all your friends via email, social networks and instant messengers. I can also publish access to all your emails and instant messengers that you use.
In addition, I found a lot of interesting things that I was able to publish on the Internet and send to friends.
UPW
If you don't want me to do it, send me 1400 $ (US dollar) in my bitcoin wallet.
BTC address:
1[redacted]Bp

5 pav. Grasinančio pobūdžio el. laiško pavyzdys

Šis sukčiavimo ir duomenų išviliojimo būdas buvo dažniausiai naudojamas 2018–2019 m., tačiau tokių atvejų pasitaiko ir dabar. Liūdniausia, kad tokius pranešimus gaunantys asmenys tvirtina, kad piktavaliai savo grasinimuose nurodo jų iki šiol naudojamus slaptažodžius.

Ką daryti praradus soc. tinklų naudotojo paskyrą?

NKSC kiekvieną dieną sulaukia pranešimų ir pagalbos prašymų dėl užvaldytų socialinių tinklų ar el. pašto paskyrų (6 pav.). Deja, padėti šioje situacijoje negalime. **Praradus paskyrą ją susigražinti Jums gali padėti tik konkretaus socialinio tinklo ar el. pašto teikėjo pagalbos padalinys, kuris ir atlieka priežiūros ir (ar) administravimo funkcijas.**

Pranešimas: Buvo įsilaužta į mano asmeninę pašto paskyrą[redacted]@yahoo.com, pavogta mano istagram paskyra.

Pranešimas: Laba diena,
esu Lietuvos[redacted], aktyviai naudoju savo FB paskyrą.
Tik atvykus į [redacted] mano FB paskyrą užgrobė kažkoks hotmail.com arabiškais rašmenimis ir FB ją užblokavo dėl "bendruomenei netinkamų vaizdų".

Pranešimas: Sveiki,
Kreipiuosi I Jus del isilauzimo I instagram mano paskyra, kuria galima rasti[redacted], i paskyra buvo isilauzta, pakeisti mano duomenis tokie kaip emeil ir tel, taip pat asmuo dabar valdantys mano paskyra su asmenine informacija, skleidzia melagingus pranesimus apie tariamus mano pratirtejimus ir crypto valiutas. Siuo metu neturiu jokiu galimybiu prisijungti, nes tas zmogus kuris isilauze padare 2FA apsauga. Prasau padekite🙏

6 pav. NKSC gaunamų pranešimų pavyzdžiai

Siekiant tinkamai pasirūpinti asmeninių paskyrų saugumu, rekomenduojame vadovautis šiomis paprastomis taisyklėmis:

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

1. Susipažinti su paslaugos teikėjo (socialinio tinklo ar el. pašto) įdiegtomis saugumo priemonėmis ir jas pritaikyti savo paskyros apsaugai. Populiariausi socialiniai tinklai ar el. pašto paslaugų teikėjai turi įsidiegę dviejų faktorių autentifikavimą. Taip pat galima naudotis papildomomis paskyrų apsaugos priemonėmis, pavyzdžiui, gauti įspėjimus apie prisijungimą iš neatpažinto įrenginio, peržiūrėti kada ir iš kokių IP adresų buvo prisijungta, nurodyti paskyros atkūrimo telefono numerį ar el. pašto adresą, susipažinti su naudotojo atliktais veiksmais. Informacija apie saugumo priemones dažniausiai būna pateikta naudotojo paskyroje, o jų aprašymą galima surasti paslaugų teikėjo oficialioje svetainėje.
2. Niekada ir niekam neatskleisti prisijungimo duomenų (vartotojo vardo ir slaptažodžio). Gavus pranešimą (el. laišką, SMS žinutę ar pranešimą tiesiai į savo paskyrą) su slaptažodžio keitimo nuoroda ir prašymu nedelsiant pakeisti slaptažodį arba patvirtinti paskyrą, jokiu būdu to nedaryti – nespausti atsiųstų nuorodų ir nesuvedinėti prisijungimo informacijos. Gavus tokio pobūdžio pranešimą, rekomenduojame kreiptis į socialinio tinklo ar el. pašto paslaugų teikėją arba ieškoti informacijos jų oficialiuose svetainėse. Esant poreikiui, galima pakeisti prisijungimo slaptažodį, tačiau tai reikėtų atlikti tik iš savo naudotojo paskyros.
3. Naudoti unikalius ir sudėtingus slaptažodžius. Apie slaptažodžių stiprumą, sudėtingumą ir saugą rašėme čia: https://www.nksc.lt/doc/biuleteniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf. taip pat reikėtų nepamiršti nuolatos keisti naudojamus slaptažodžius, o slaptažodžio „ziema123“ keitimas į „ziema1234“ yra bloga praktika.
4. Skirtingoms socialinių tinklų ar el. pašto paskyroms nenaudoti tų pačių slaptažodžių.
5. Atskirkite asmenines paskyras nuo verslo paskyrų, joms naudokite skirtingus prisijungimo vardus ir slaptažodžius.
6. Nesijunkite prie savo paskyrų iš tretiesiems asmenims priklausančių ar nepažįstamų ar viešų įrenginių.
7. Kritiškai vertinkite visą informaciją, kurią skelbiate apie save internete. Perteklinė informacija, gali būti panaudota prieš Jus, pavyzdžiui, socialinei inžinerijai.
8. Nesaugokite prisijungimo duomenų interneto naršyklėje.
9. Kritiškai vertinkite gautas žinutes, kuriose raginama suvesti savo asmens ar prisijungimo duomenis.

Žemiau pateikiame populiariausių socialinių tinklų ar el. pašto paslaugų teikėjų oficialias svetainių nuorodas, kuriose galėsite rasti jų teikiamų paslaugų aprašymus:

- https://support.google.com/
- https://lt-lt.facebook.com/help
- https://help.instagram.com/
- https://en-global.help.yahoo.com/kb/account
- https://help.twitter.com/en
- https://support.microsoft.com/en-us

Primename, kad NKSC nevykdo socialinių tinklų ar el. pašto paslaugų priežiūros ir (ar) administravimo funkcijų, todėl dėl prarastų ar užblokuotų paskyrų reikėtų kreiptis tiesiogiai į paslaugos teikėją.