Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
KLASTOTĖS IR DUOMENŲ VAGYSTĖS

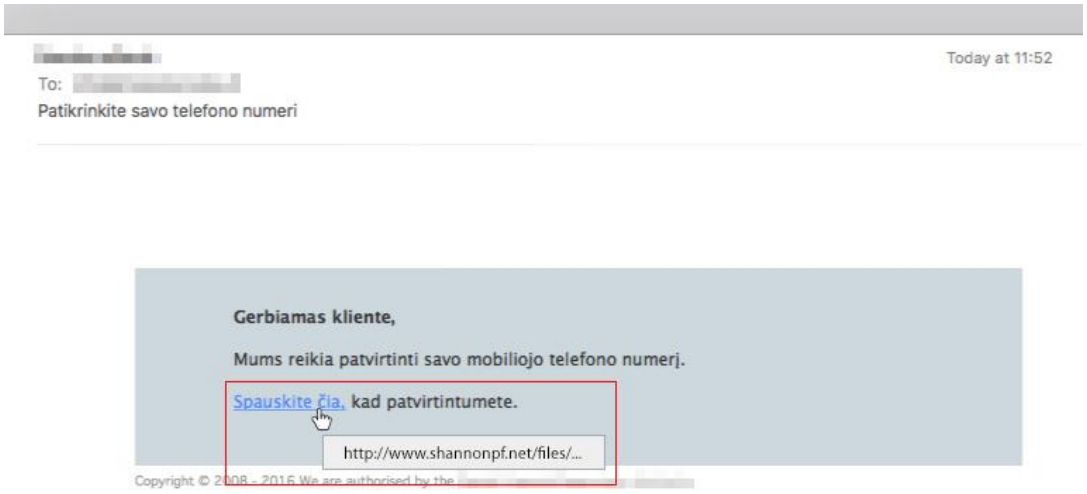
2018 m. gegužės 15 d.

Klastotės (angl. phishing) - tai įvairių formų suklastoti pranešimai (el. laiškai, sms žinutės) ir interneto svetainės, kuriomis piktavaliai, apsimesdami institucija, įmone ar asmeniu, siekia išgauti naudotojo informaciją, prisijungimo ar finansinius duomenis (banko prisijungimai, kredito kortelių duomenys) arba priversti atlikti tam tikrus veiksmus (pvz. pervesti pinigines lėšas į nusikaltėlių sąskaitas). Klastotėmis siekiama sudominti, gąsdinti ar pasitelkti kitas emocijas, kad naudotojas pats atliktų veiksmus, kurių pasekoje būtų prarasti duomenys. Dažniausiai klastotėse būna naudojamas bankų ir populiariausių elektroninių paslaugų teikėjų (PayPal, Google, Microsoft, Apple ir tt.) identitetas.

Klastočių požymiai

Pranešimas nuo banko, valtybinės institucijos ar elektroninių paslaugų teikėjo su prašymu atsiųsti ar įvesti nurodytoje svetainėje savo prisijungimo duomenis ar kitą informaciją. Laiškus siunčiantys piktavaliai informuoja apie gautą ar atliktą naują mokėjimą, apie jums priklausančią išmoką, būtinybę atlikti kokį nors veiksmą (pvz. atnaujinti tam tikrus savo duomenis) ir pan. Laiške pateikiama interneto nuoroda (adresas) ir prašoma prisijungti prie suklastotos el. bankininkystės ar kitos elektroninių paslaugų sistemos.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt



1 pav. Banko pranešimo klastotė

Pranešimas apie laimėjimą žaidime, kuriame net nedalyvavote, nežinomo asmens palikimą ar atlygį už tam tikrus veiksmus. Tokie laiškai Lietuvos gavėjus dažniausiai pasiekia anglų kalba. Juose nurodomos itin didelės – šimtus tūkstančių ar net milijonus – siekiančios sumos, į kurias neva pretenduoja pranešimo gavėjas. Tam, kad gauti nurodomą sumą, adresatas viliojamas atsiųsti arba įvesti tam tikrus savo duomenis.

Your Winning Notification

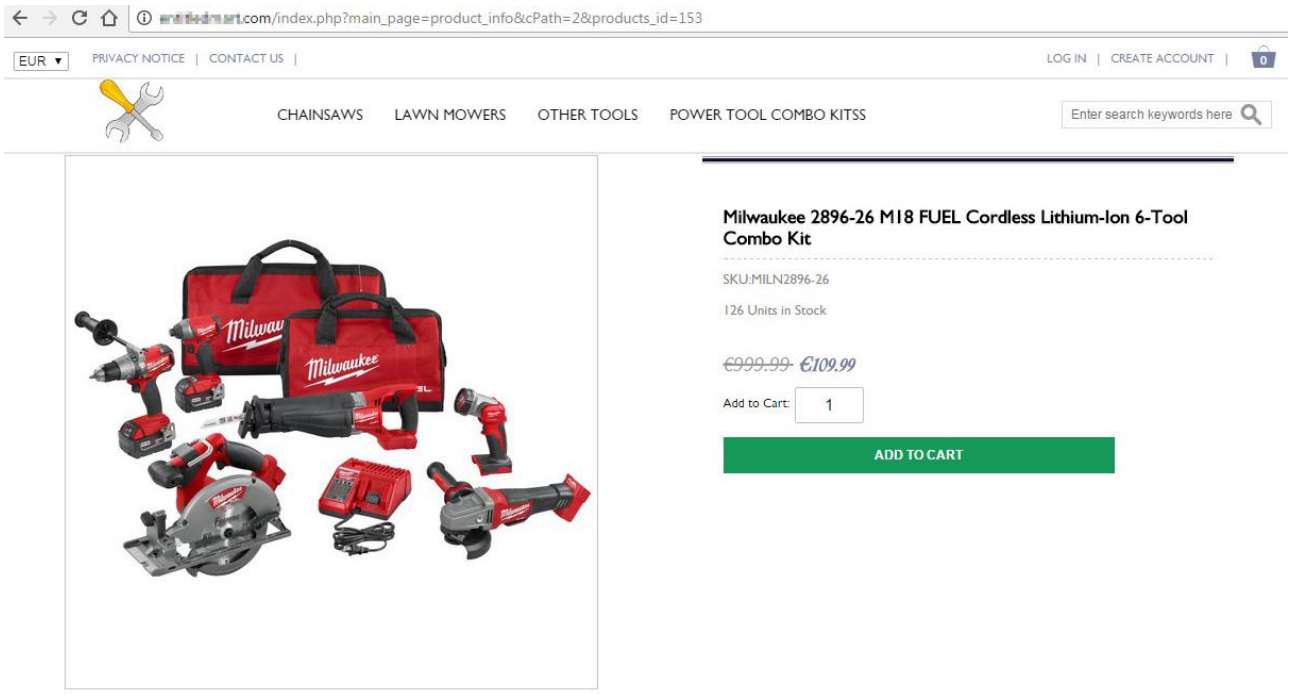
This is to inform you about the result of our Lottery DRAWS. Your e-mail address attached to ticket number 27522465896-532 with serial number 652-662 drew lucky numbers 7-14-18-23-31-45 which consequently won in the 1st category. You have therefore been approved for a lump sum pay of GBP 1.3Million (One Million Three Hundred Thousand Great British Pounds). Note that all participants in this lottery program have been selected randomly through a computer ballot system drawn from over 200,000 companies and 400,000,000 individual email addresses from all search engines and websites.

2 pav. Klastotė apie laimėjimą loterijoje

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Suklastotos elektroninės parduotuvės. Pagrindinis tokios klastotės bruožas – visos prekės parduodamos neįtikėtinai žemomis kainomis. Netikros elektroninės parduotuvės svetainės vaizdas dažniausiai nesukelia įtarimų. Svetainės adresas ar pavadinimas gali būti panašus į žinomų elektroninių parduotuvių adresus, o pirkėjai viliojami didelėmis nuolaidomis. Netikrų parduotuvių kūrėjų tikslas – per kuo trumpesnį laiką gauti kuo daugiau pinigų ir asmeninės informacijos. Tokiose parduotuvėse pirkimo procesas gali atrodyti sklandus, tačiau prekių ar paslaugų asmenys negauna.

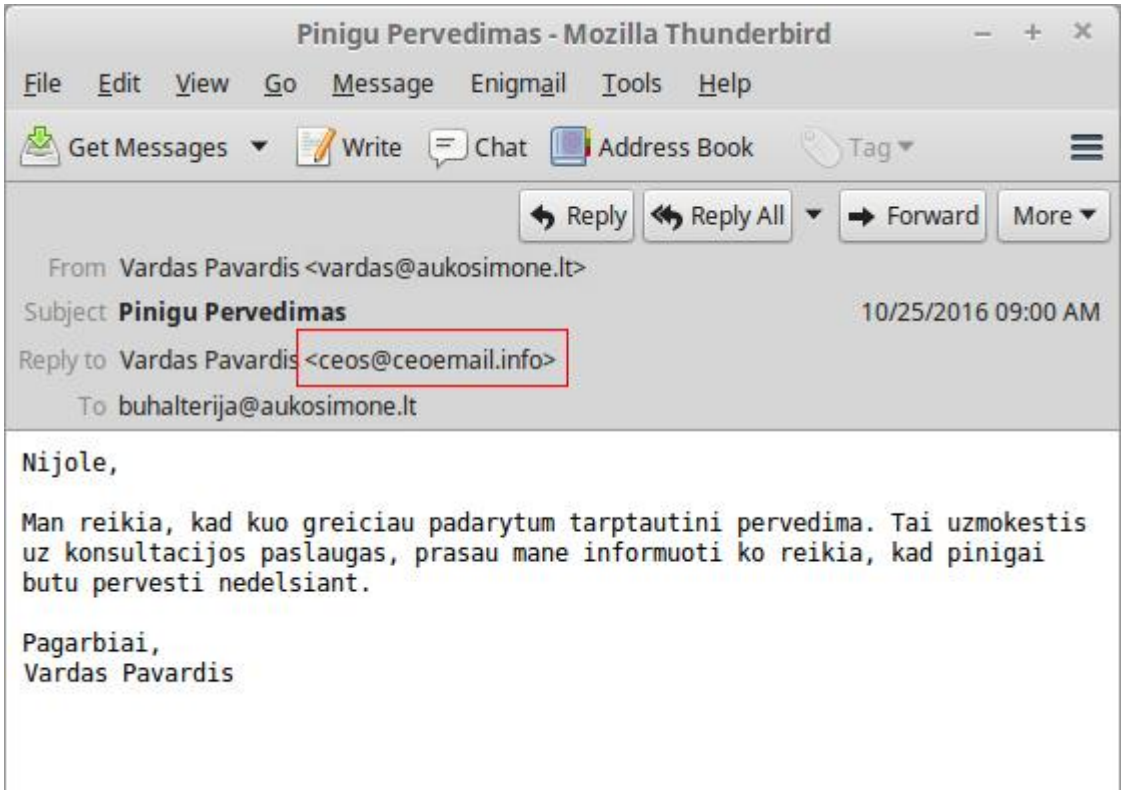
Dažniausiai tokių parduotuvių padaugėja švenčių laikotarpiu. Reklamos apie naujas el. parduotuves su „fantastiškomis kainomis“ plinta per „Facebook“, kitus socialinius tinklus arba elektroniniais laiškais.



3 pav. Suklastota el. parduotuvė. Nuolaidos siekia beveik 90%

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Prašymas atlikti veiksmus kuo skubiau. Tokie psichologinio spaudimo metodai pranešimuose siekia manipuliuoti žmogaus emocijomis ir sumažinti atakuojamojo asmens atidumą. Pranešimo adresatas verčiamas skubėti, dėl to prarandamas budrumas ir gebėjimas kritiškai vertinti gaunamą informaciją.

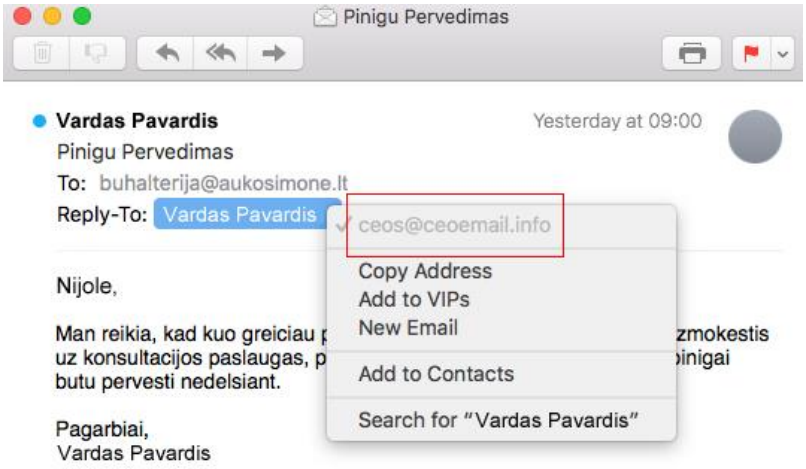


4 pav. Prašymas atlikti veiksmus kuo skubiau

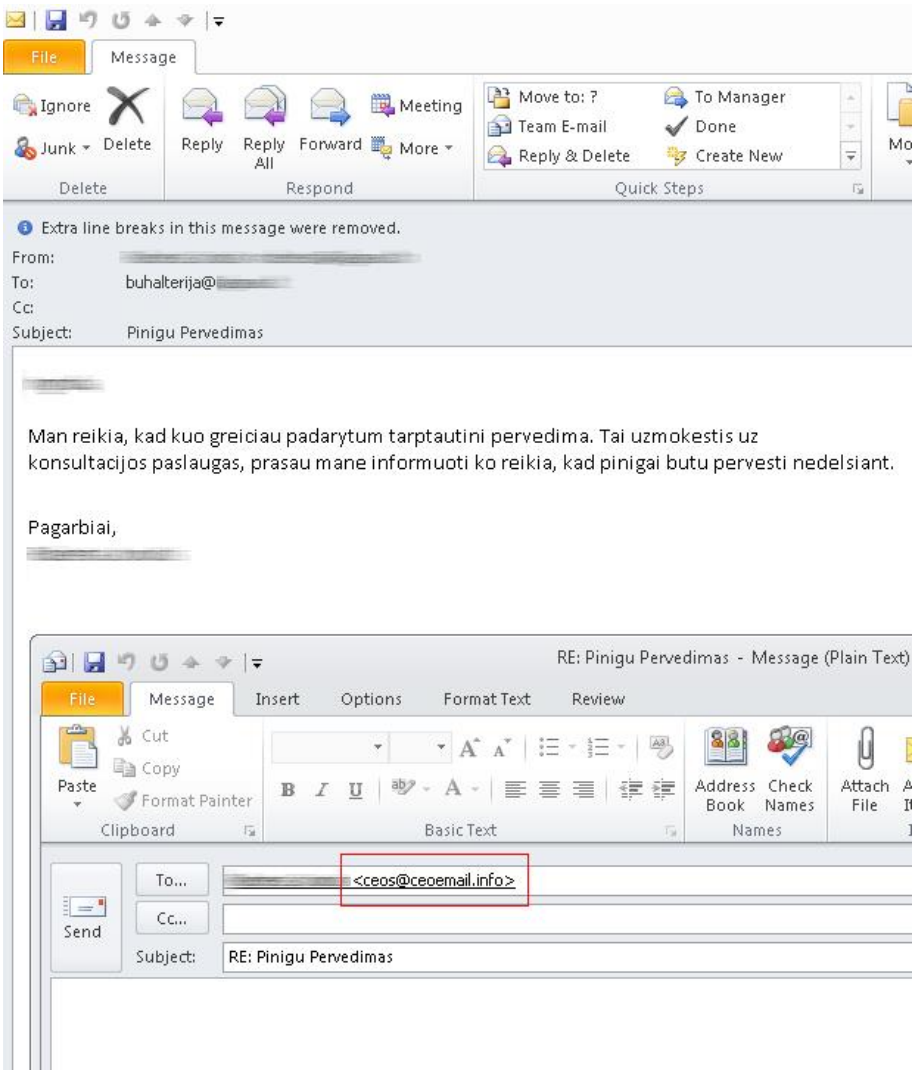
Suklastotojas siuntėjas. Tikrasis laiško siuntėjas būna ne tas, kuris nurodytas lauke „Nuo“ (angl. *From*). Tam tikrose el. pašto programose tokias klastotes atskirti paprasčiau, nes laukelyje *From* po siuntėjo vardo ir pavardės matomas tikrasis siuntėjo el. pašto adresas (pvz. Mozilla Thunderbird, pav. 4).

Kitais atvejais laiško siuntėjas vizualiai nesukelia jokių įtarimų - sunku atskirti, kad laiškas atėjęs ne nuo to siuntėjo, kuriuo prisistato piktavalis. Tik laukelis *Reply-to* (žr. pav. 5 ir 6) išduoda, kad tai yra sukčiavimo atvejis, nes el. laiško adresas jau nebėra toks pat, kaip ir siuntėjo. Jeigu *Reply-to* laukelis nematomas, siuntėjo tikrąjį el. pašto adresą galima pamatyti paspaudus „Atsakyti“ (angl. *Reply*) ir pažiūrėjus, kokiu adresu nukeliaus jūsų laiškas.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt



5 pav. Tikrasis el. laiško siuntėjas MAC OS pašto programoje



6 pav. Tikrasis el. laiškos siuntėjas Windows Live Mail pašto programoje

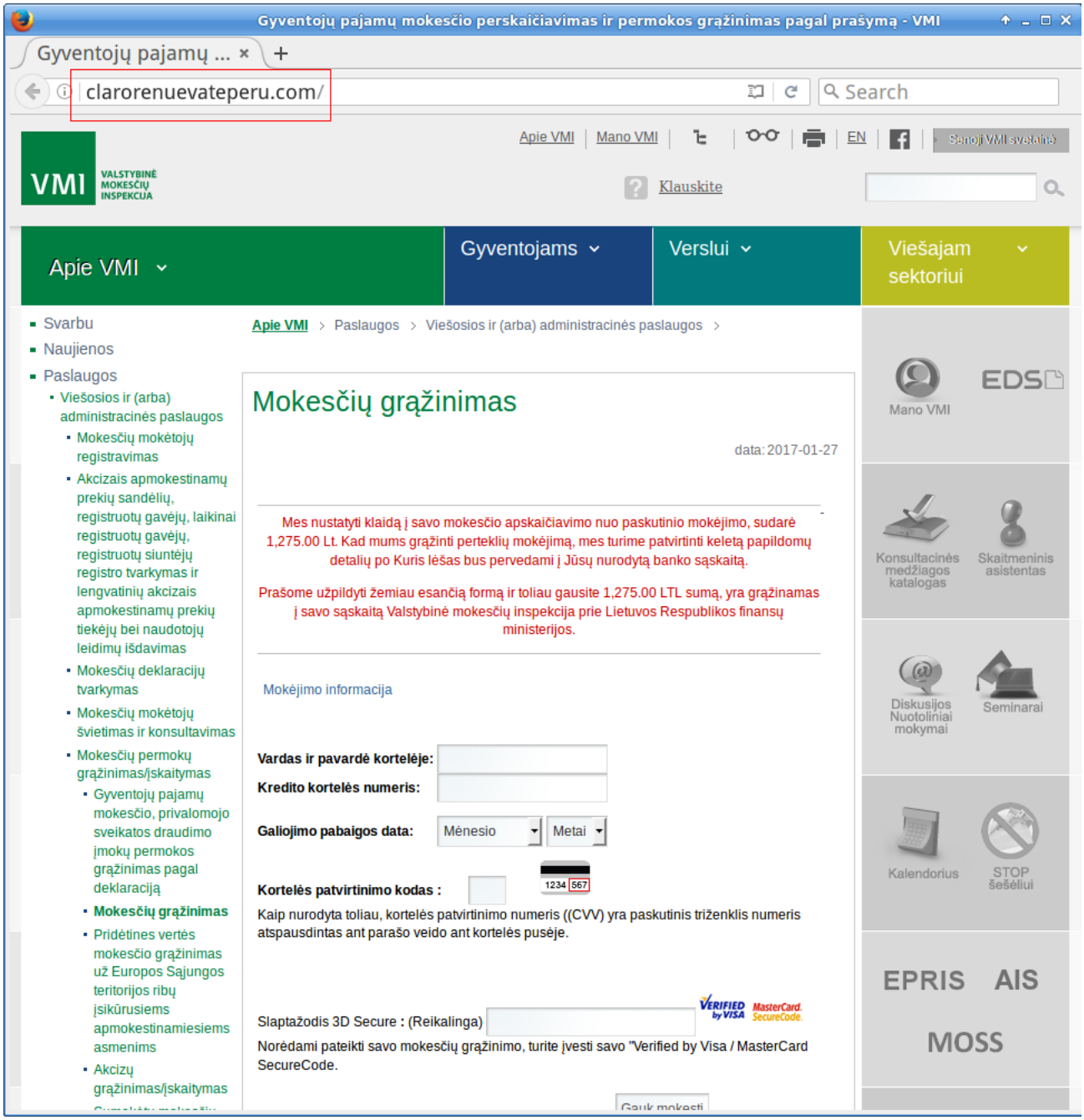
Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Netaisyklinga lietuvių kalba, lietuviškų rašmenų nebuvimas ir klaidos tekste. Tokius laiškus platina užsienio piktavaliai, kurie neturi lietuvių kalbos žinių ir tekstus verčia internetiniais teksto vertėjais, tokiais kaip Google Translate. Šiuose pranešimuose išryškėja grubios stiliaus ir sintaksės klaidos, kartais naudojama jau nebeegzistuojanti valstybinė valiuta – litai.

> ***Mokesciu grazinimas***
>
> *Mes nustatyti klaida i savo mokescio apskaiciavimo nuo paskutinio mokejimo, sudare 1,275.00 Lt. Kad mums grazinti pertekliu mokejima, mes turime patvirtinti keleta papildomu detaliu po Kuris lesas bus pervedami i Jusu nurodyta banko saskaita.*
>
> *Prasome uzpildyti zemiau esancia forma ir toliau gausite 1,275.00 LTL suma, yra grazinamas i savo saskaita Valstybine mokesciu inspekcija prie Lietuvos Respublikos finansu ministerijos.*

7 pav. Suklastotas pranešimas - grubios stiliaus ir sintaksės klaidos

Svetainės adresas skiriasi nuo tikrojo paslaugos teikėjo svetainės adreso. Jeigu ketinate įvedinėti kokius nors savo duomenis svetainėje, būtinai pasitikrinkite, ar jos adresas tikrai toks, kokį esate įpratę matyti. Jeigu turite bent menkiausių įtarimų, mėginkite naršyklės adresų juostoje įvesti tikrosios svetainės adresą arba susirasti ją interneto paieškos sistemoje.



8 pav. Klastotę galima atskirti pagal jos adresą

ES bendrasis duomenų apsaugos reglamentas ir kiti aktualūs įvykiai

Pastaruoju metu padaugėjo suklastotų elektroninių pranešimų, susijusių su gegužės 25 d. visoje Europoje, o kartu ir Lietuvoje įsigaliosiančiu bendruoju duomenų apsaugos reglamentu (BDAR, angl. *GDPR*). Piktavaliai išnaudoja išaugusį visuomenės susidomėjimą šia tema:

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

- Vilioja vartotojus į suklastotas/infekuotas svetaines;
- Laiškuose prisega kenkėjiškų bylų (informaciniai bukletai, kvietimai į mokymus);
- Prašo asmeninių/finansinių duomenų (prisijungimo duomenys, banko kortelių duomenys);
- Renka aktyvių el. pašto dėžučių adresus kenkimo arba reklamos kampanijoms.

NKSC rekomenduoja

Siekdami apsaugoti asmeninius, finansinius ar kitus jautrius duomenis nuo vagystės, visuomet išlikite atidūs jus pasiekiančiai informacijai.

- Nespauskite (neatidarinėkite) nuorodų laiškuose, gautuose iš neaiškių šaltinių;
- Įsitikinkite, kad laiško siuntėjas iš tiesų yra tas, kuris nurodytas lauke „Nuo“;
- Įsitikinkite, kad interneto svetainės adresas, kuriame įvedate savo duomenis, tikrai teisingas. Atkreipkite dėmesį, ar nėra praleistų raidžių, ar raidės nesukeistos vietomis ir pan.;
- Atidžiai įvertinkite prašymus atlikti skubius veiksmus susijusius su piniginėm perlaidom ar/ir jautrių duomenų persiuntimu/atskleidimu;
- Įsidėmėkite, kad bankai niekada neprašo klientų pateikti e-bankininkystės slaptažodžių ar mokėjimo kortelių duomenų (nei el. laiškais, nei telefonu, nei kitu būdu);
- Atidarius savo banko el. bankininkystės sistemą ar kito populiaraus elektroninių paslaugų teikėjo puslapį, pasižiūrėkite į naršyklės adreso lauką. Šios sistemos visada naudoja saugų ryšio protokolą, adreso pradžioje būtinai yra https ir galima patikrinti svetainės sertifikatą. Suklastotų svetainių adreso pradžia beveik visada būna http (be „s“).

Įvykus duomenų vagystei

Jeigu supratote, kad tapote duomenų vagystės auka, reikėtų kuo skubiau imtis veiksmų atitinkamai pagal tai, kokia informacija buvo pavogta:

- Jeigu buvo pavogti banko prisijungimo ar kreditinės kortelės duomenys arba atlikote pavedimą į nusikaltėlio sąskaitą, nedelsiant susisiekite su savo banku;

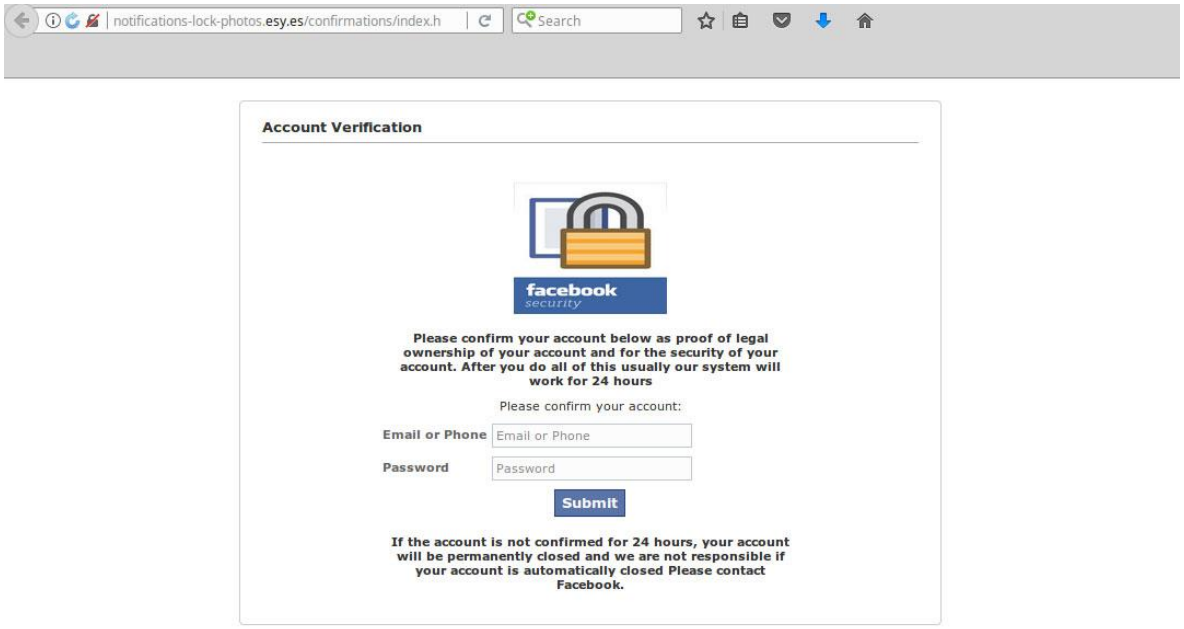
Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

- Jeigu buvo pavogti kitos informacinės sistemos duomenys, bet vis dar turite galimybę prie jos prisijungti, kuo skubiau pasikeiskite savo slaptažodį. Jeigu prisijungti prie sistemos nebegalite, kreipkitės į tos paslaugos teikėją;
- Jeigu atskleidėte konfidencialią savo įmonės/institucijos informaciją, informuokite apie tai savo vadovą, kuris turėtų nuspręsti dėl tolimesnio įvykio eskalavimo.

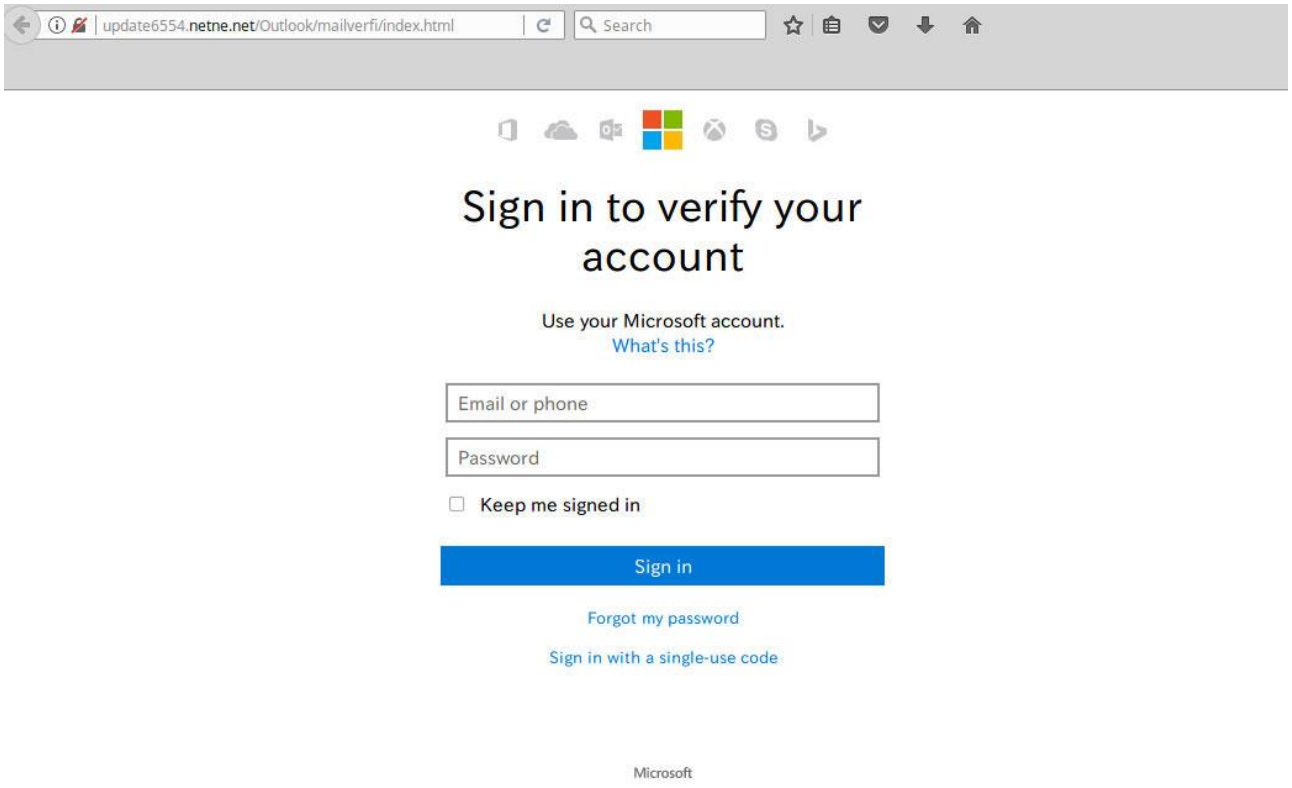
Bendros rekomendacijos el. pašto administratoriams

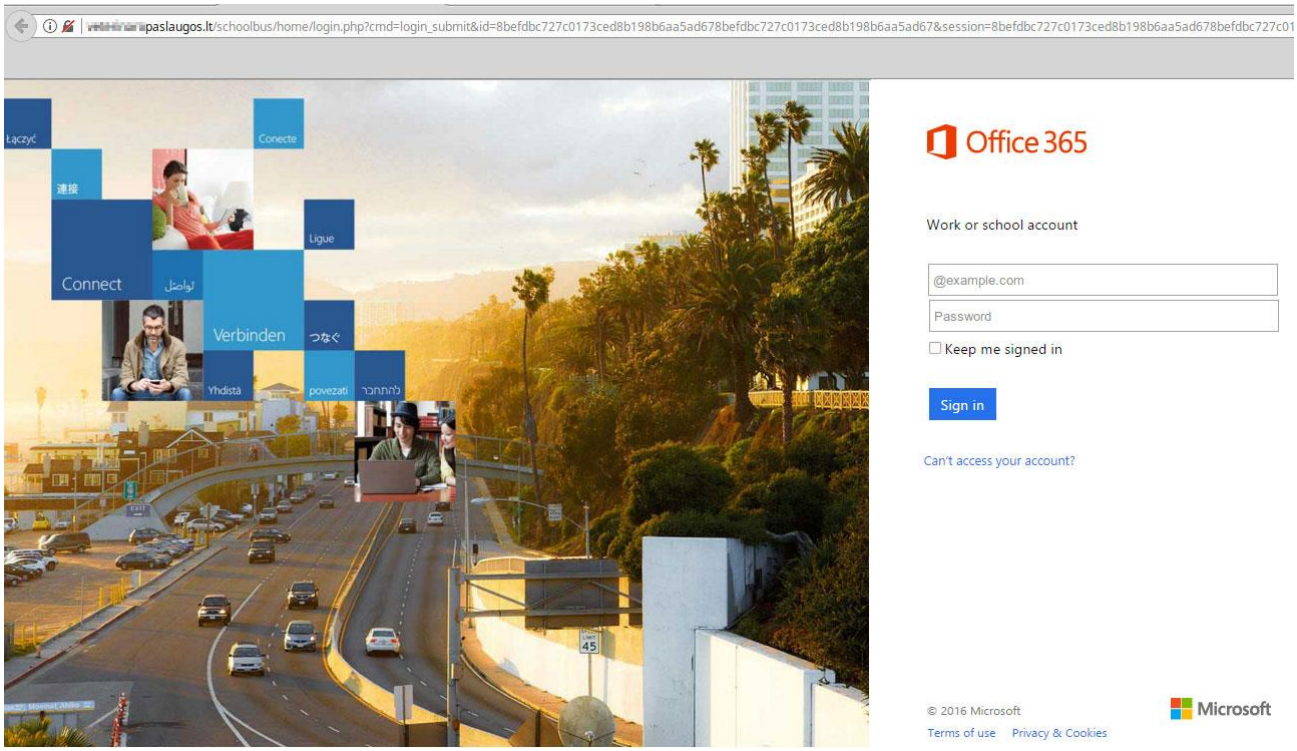
- Įdiegti siuntėjų IP adresų tikrinimą pagal RBL (angl. Realtime Block List) sąrašus;
- Įdiegti SPAM filtravimo priemones pagal turinį;
- Nustatyti siuntėjo kompiuterio vardo (hostname) tikrinimą;
- Nustatyti siuntėjo ir gavėjo el. pašto domeno tikrinimą;
- DNS zonoje pridėti SPF įrašą (sumažintų galimybę siųsti klastotes nuo jūsų domeno);
- Įdiegti autentifikavimo technologijas SPF, DKIM ir DMARC;
- Įdiegti antivirusinę programinę įrangą ir nustatyti ją el. pašto laiškams tikrinti.

Klastočių pavyzdžiai

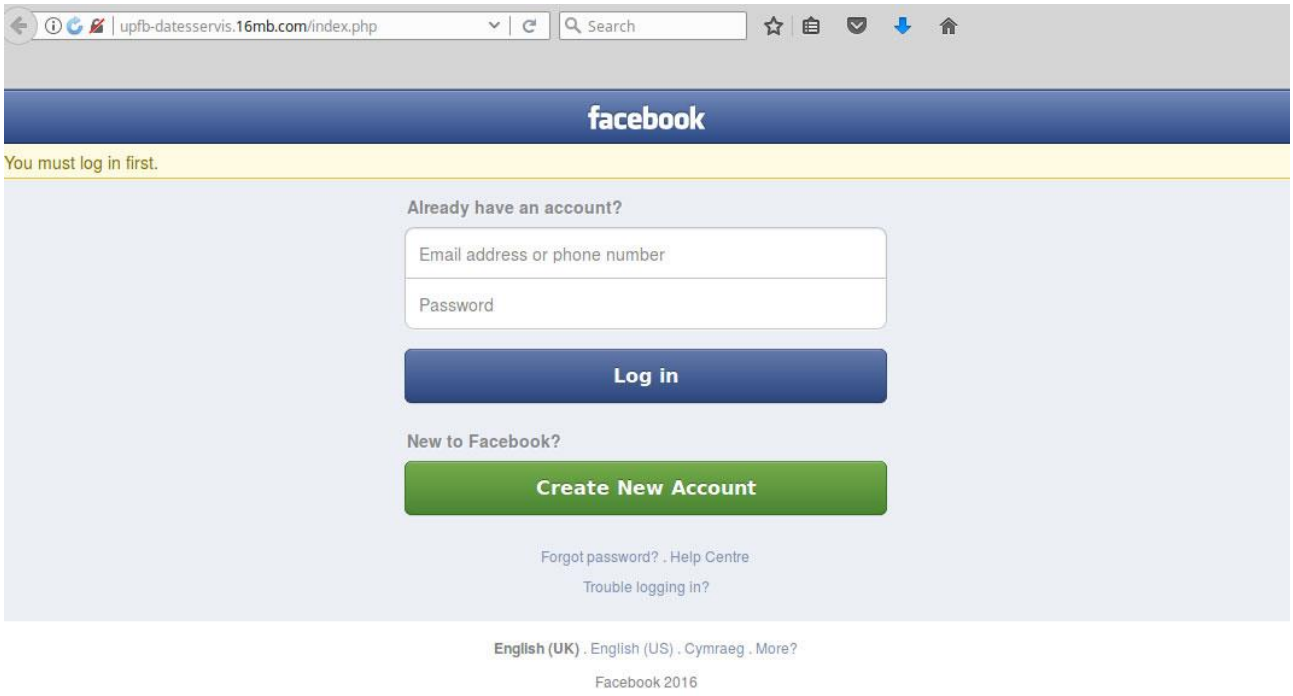


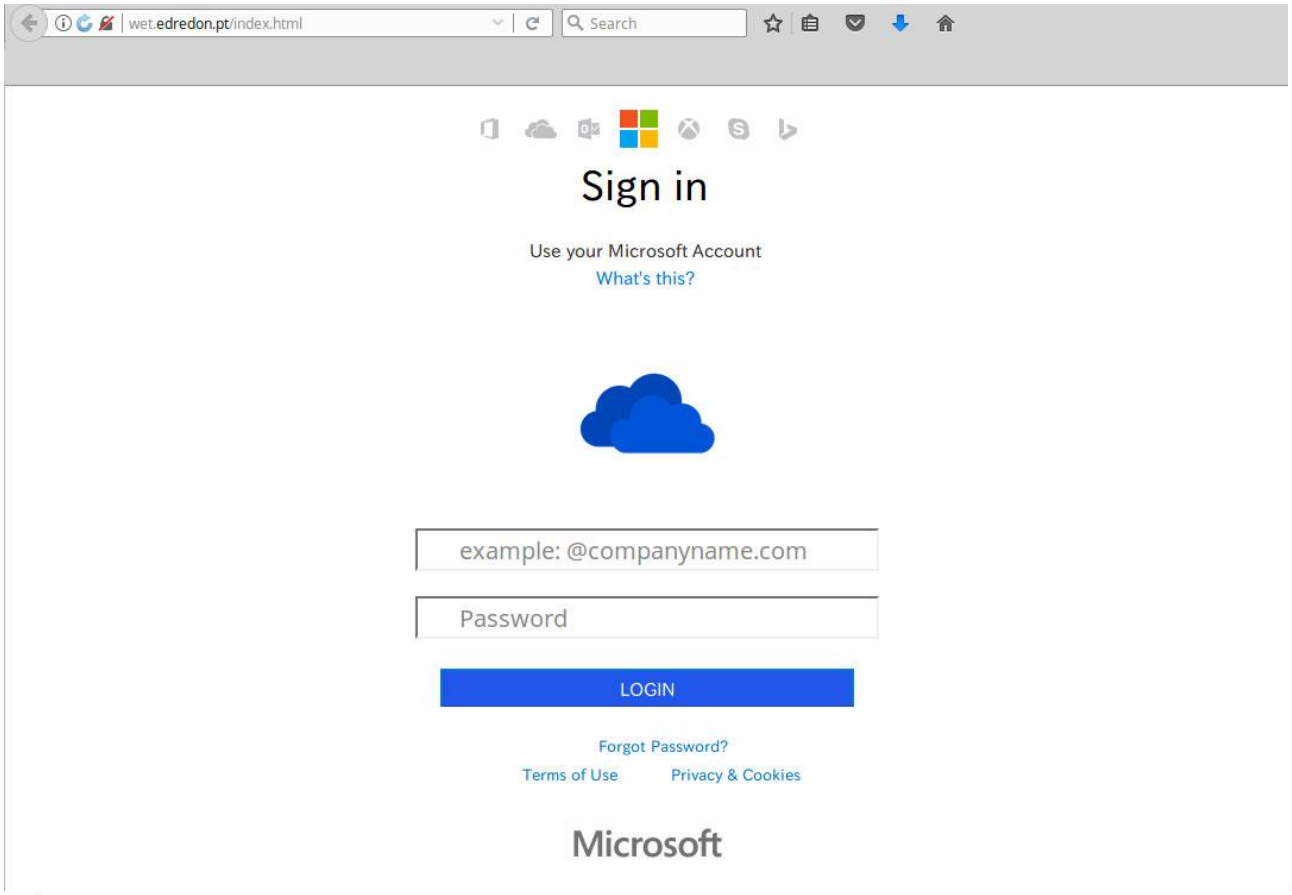
Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt



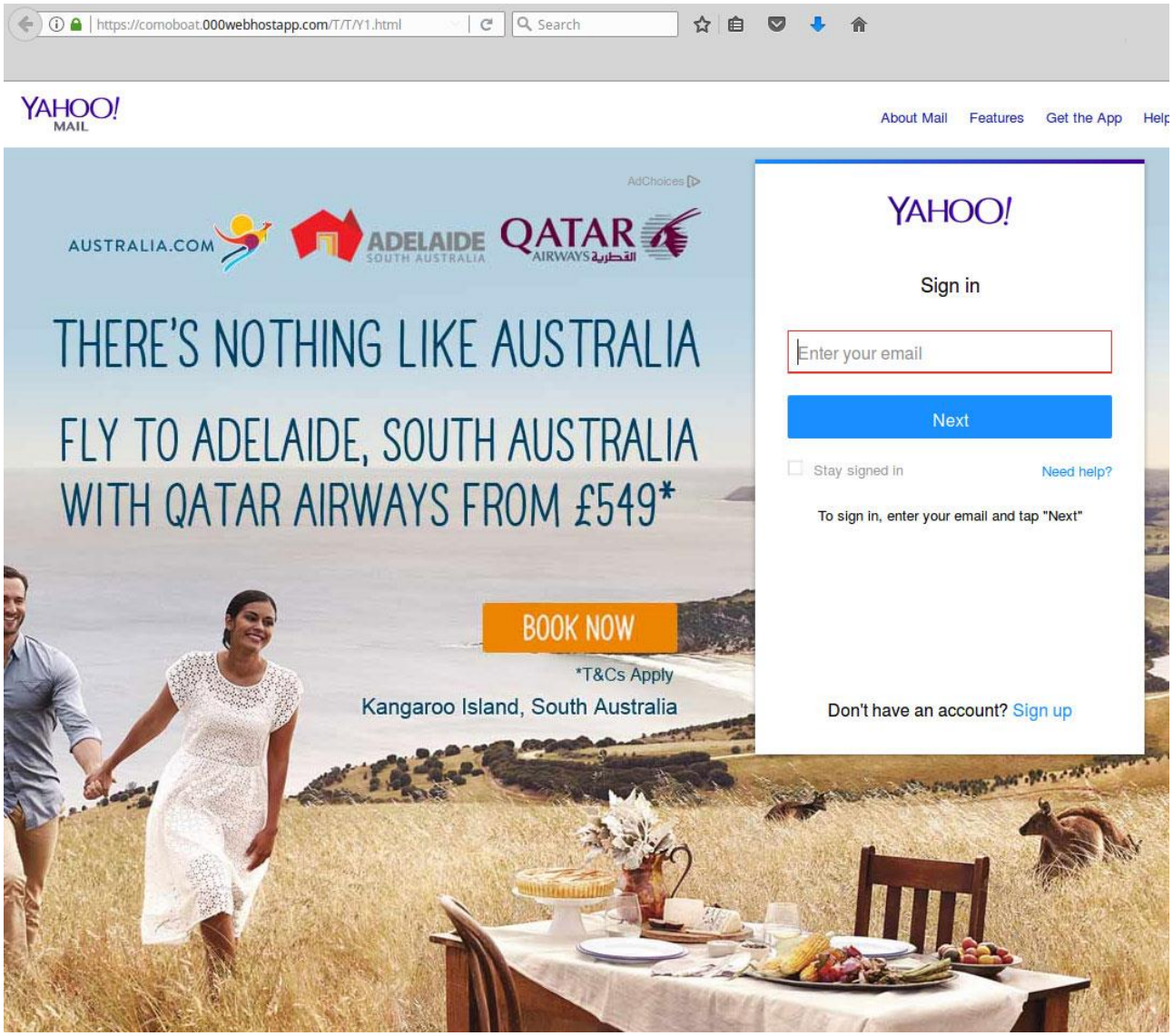


Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

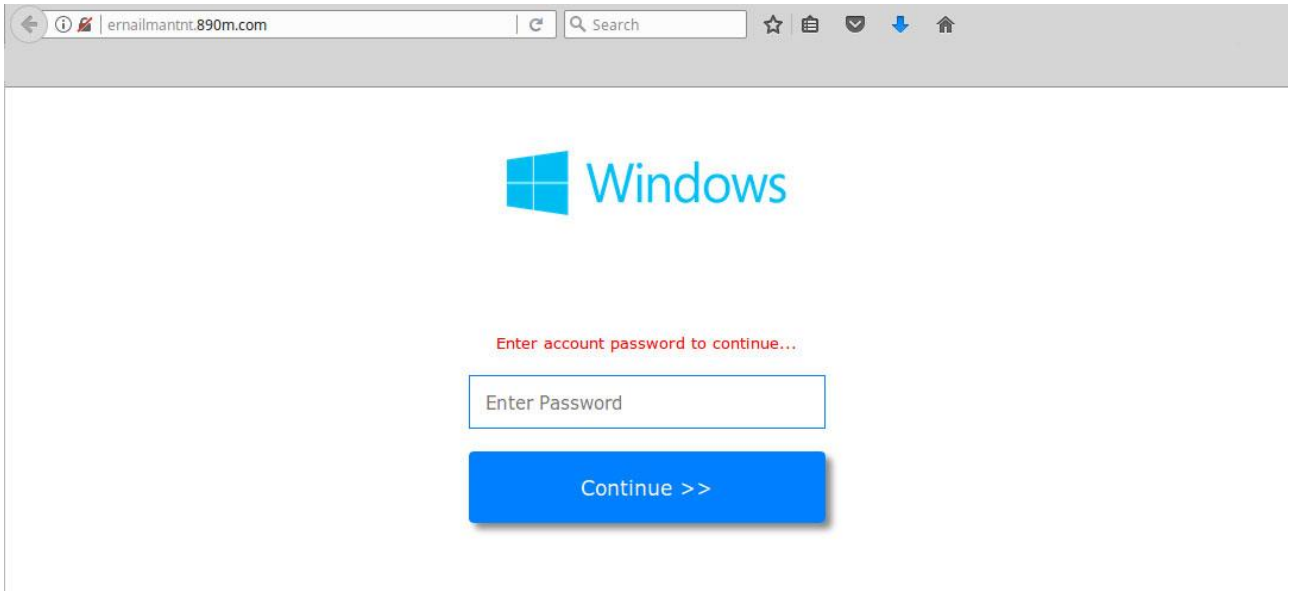


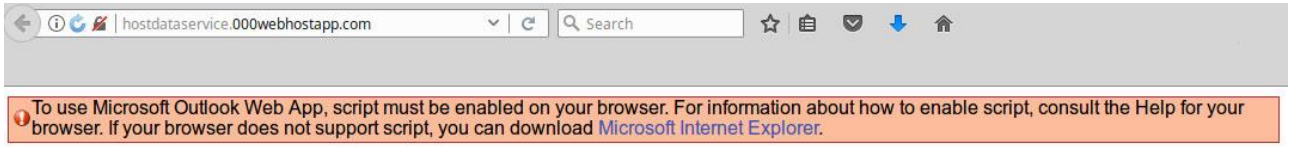


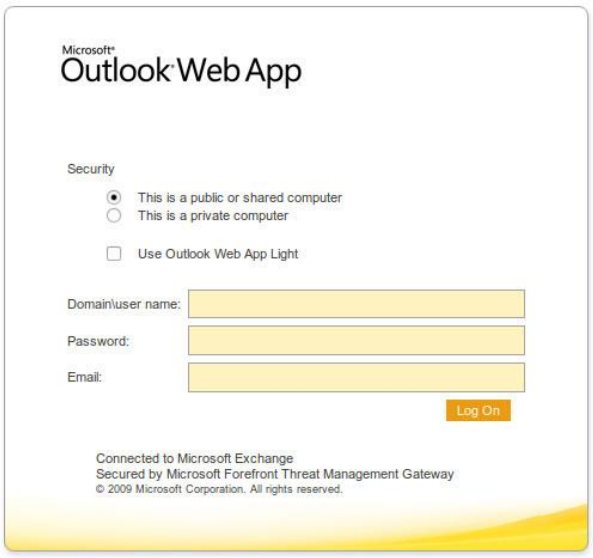
Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

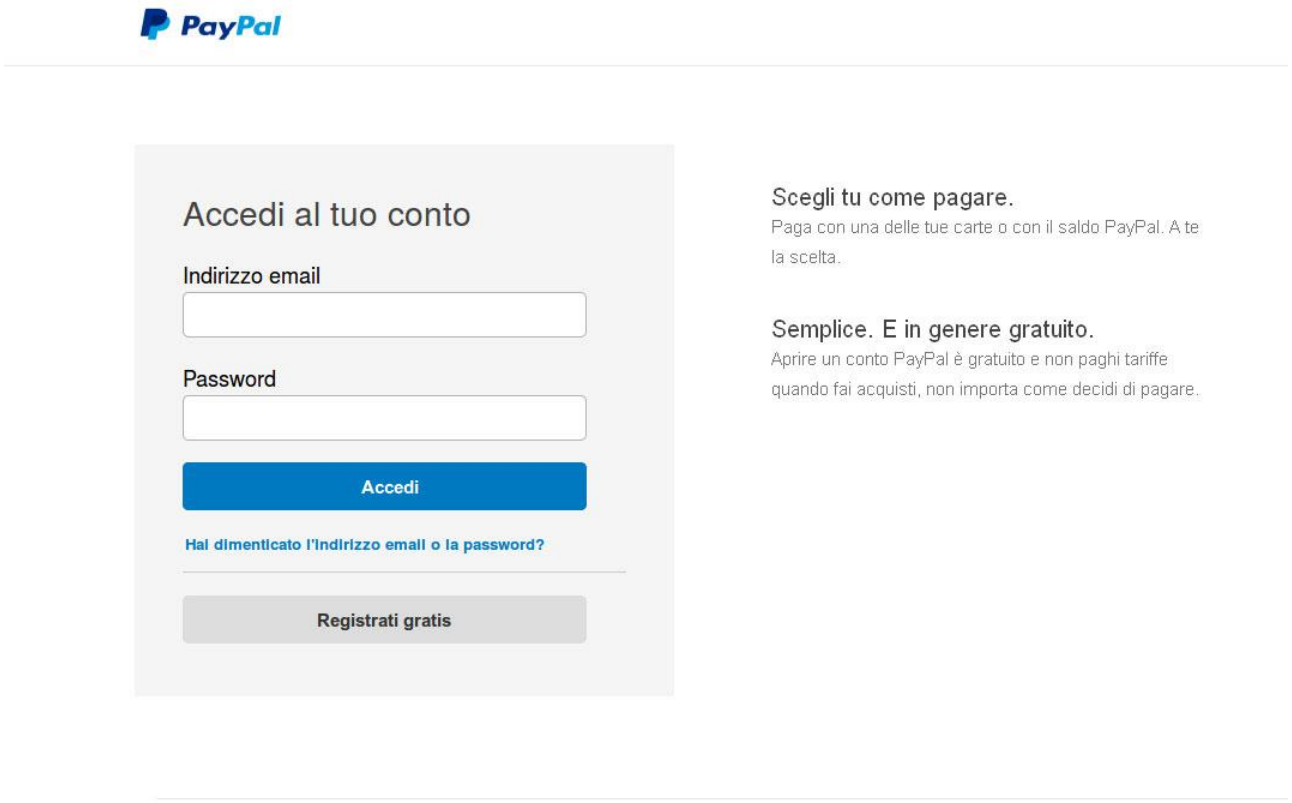


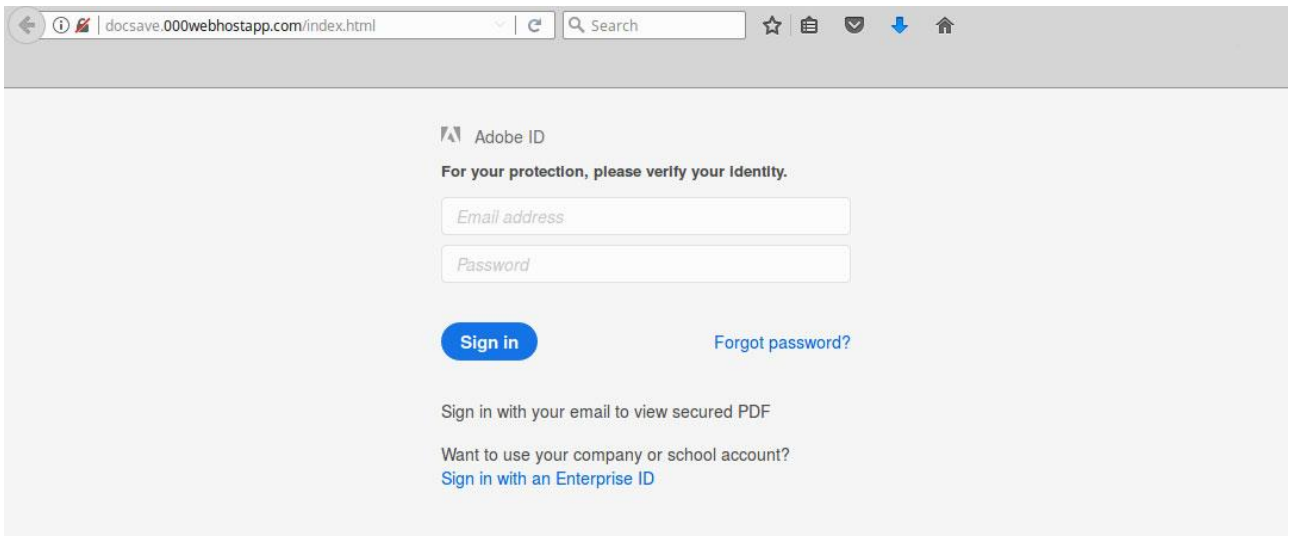
Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt








PayPal
Accedi al tuo conto
Indirizzo email
Password
Accedi
Hai dimenticato l'indirizzo email o la password?
Registrati gratis
Scegli tu come pagare.
Paga con una delle tue carte o con il saldo PayPal. A te la scelta.
Semplice. E in genere gratuito.
Aprire un conto PayPal è gratuito e non paghi tariffe quando fai acquisti, non importa come decidi di pagare.
Chi siamo | Tipi di conto | Tariffe | Privacy | Spazio Sicurezza | Contattaci | Accordi legali | Sviluppatori | PayPal Mobile | Negozi PayPal |
Copyright © 1999-2014 PayPal. Tutti i diritti riservati.


docsave.000webhostapp.com/index.html
Search
Adobe ID
For your protection, please verify your identity.
Email address
Password
Sign in
Forgot password?
Sign in with your email to view secured PDF
Want to use your company or school account?
Sign in with an Enterprise ID

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt