

SUKČIAVIMAS, SUSIJĘS SU INVESTAVIMU

Labiausiai paplitęs investicinio pobūdžio sukčiavimas yra susijęs su esą pelningomis investavimo galimybėmis, tokiomis kaip akcijos, obligacijos, kriptovaliutos, retieji metalai, investicijos į žemės sklypus užsienyje ar alternatyvius energijos šaltinius.

KADA DERĖTŲ SUSIRŪPINTI?

- Kai sulaukiate pasikartojančių nepageidaujamų skambučių.
- Jums žadama greita grąža ir teigiama, kad investicija yra saugi.
- Pasiūlymas galioja tik ribotą laiką.
- Pasiūlymas galioja tik Jums ir Jūsų yra prašoma juo nesidalinti.

KĄ DARYTI?

- Atmeskite skambučius, susijusius su investavimo galimybėmis.
- Kitiškai vertinkite pasiūlymus, žadančius saugias investicijas, garantuotą grąžą ir didelį pelną.

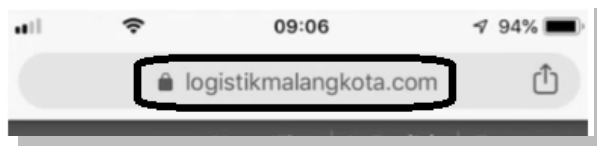
APGAULINGI ELEKTRONINIAI LAIŠKAI IŠ VALSTYBINIŲ ĮMONIŲ

Sukčiavimo žinutės su nuoroda gali būti atsiunčiamos Jūsų naudojamo banko vardu, tačiau atkreipkite dėmesį į siunčiamą nuorodą, ar ji nėra užkoduota, kaip pateikiamas pavyzdys žemiau. Bankai pranešimuose prisijungimo nuorodų dažniausiai nesiunčia.

Prašymo dėl pensijų reformos patvirtinimo kodas 4978

Gautas naujas pranešimas
<https://bit.ly/2ZOP5f0>

Prisijungdami prie elektroninio banko, įsitikinkite, kad adresų lauke yra pateikiamas tikras banko adresas, o ne fiktyvi nuoroda, kaip pateikiama žemiau. Prisijungiant prie elektroninio banko geriausia į adresų juostą adresą įvesti ranka ir po to prisijungti prie banko savitarnos.



LIETUVOS POLICIJA



LIETUVOS POLICIJA

PATARIA, KAIP NETAPTI NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE AUKA



GINTI. SAUGOTI. PADĖTI.

SUKČIAVIMAS APSIPERKANT INTERNETU

Apsiperkant internetu, neretai galima rasti patrauklių pasiūlymų, tačiau būkite atsargūs dėl galimo sukčiavimo.

KĄ DARYTI?

- Jei įmanoma, naudokitės vietiniais mažmeninės prekybos tinklalapiais - išspręsti iškilusias problemas bus tiesiog paprasčiau.
- Atlikite savo tyrimą - prieš pirkdami peržiūrėkite komentarus apie parduotuvę.
- Atsiskaitykite tik saugiu būdu. Prašoma tiesiogiai pervesti pinigus? Pagalvokite daryti!
- Mokėkite tik tada, kai esate prisijungę prie saugaus interneto ryšio, venkite nemokamų arba viešųjų bevielių tinklų.
- Saugokitės reklamų, siūlančių neįtikimas kainas ar stebuklingus gaminius. Jei pasiūlymas skamba per daug gerai, kad būtų tiesa, greičiausiai taip ir yra!
- Išliko langas, kuriame teigiama, kad laimėjote prizą? Pagalvokite daryti, galite laimėti nebent kenkėjišką programą.

APGAULINGI ELEKTRONINIAI LAIŠKAI IŠ VALSTYBINIŲ ĮMONIŲ

Apgaulingi el. laiškai iš valstybinių įmonių - vienas iš duomenų vagystės būdų. Jais siekiama iš gavėjo išgauti asmeninę, finansų ir saugos informaciją.

KAIP TAI VYKSTA?

- Šie laiškai būna labai panašūs į oficialius įmonių laiškus, tačiau juose yra gramatikos ir stiliaus klaidų.
- El. laiškuose naudojami įmonių logotipai ir kiti vizualiniai elementai.
- El. laiškuose prašoma parsiųsti pridedamą dokumentą arba prisijungti per nuorodą.

KĄ DARYTI?

- Nesuteikite „įmonei“ el. paštu prašomos slapto pobūdžio informacijos (pvz., jūsų internetinės bankininkystės slaptažodžio).
- Atidžiai peržiūrėkite el. laišką: palyginkite siuntėjo adresą su ankstesniais tikrais pranešimais iš jūsų banko. Patikrinkite, ar nėra rašybos ir gramatikos klaidų.
- Kilus net mažiausioms abejonėms, patys susiraskite įmonės kontaktus ir susisieki su jais.

„ROMANTINIS“ SUKČIAVIMAS

Sukčiai ieško aukų interneto pažinčių svetainėse, tačiau kontaktui užmegzti taip pat gali pasinaudoti socialiniais tinklais ar elektroniniu paštu.

KADA REIKĖTŲ SUSIRŪPINTI?

- Kai kažkas, su kuo neseniai susipažinote internete, prabyla apie savo stiprius jausmus jums ir prašo pradėti asmeninį susirašinėjimą.
- Žinutės dažnai yra parašytos su klaidomis, jų turinys neaiškus.
- Asmens paskyros informacija neatitinka to, ką jis jums sako.
- Jūsų gali būti prašoma atsiųsti savo intymių nuotraukų arba vaizdo įrašų.
- Pirmiausia siekiama pelnyti jūsų pasitikėjimą. Vėliau prašoma pinigų, dovanų ar jūsų banko sąskaitos duomenų.
- Nepervedę pinigų, galite sulaukti šantažo. Padarius pavedimą, pinigų bus prašoma daugiau.

KĄ DARYTI?

- Nesidalinkite jokia asmenine informacija ar vaizdais, kurie galėtų būti panaudoti šantažui prieš jus.
- Saugokitės prašymų pervesti pinigų. Niekada nedarykite pavedimų, neteikite kredito kortelių, interneto bankininkystės duomenų ar asmeninių dokumentų kopijų.

