BlueBridge

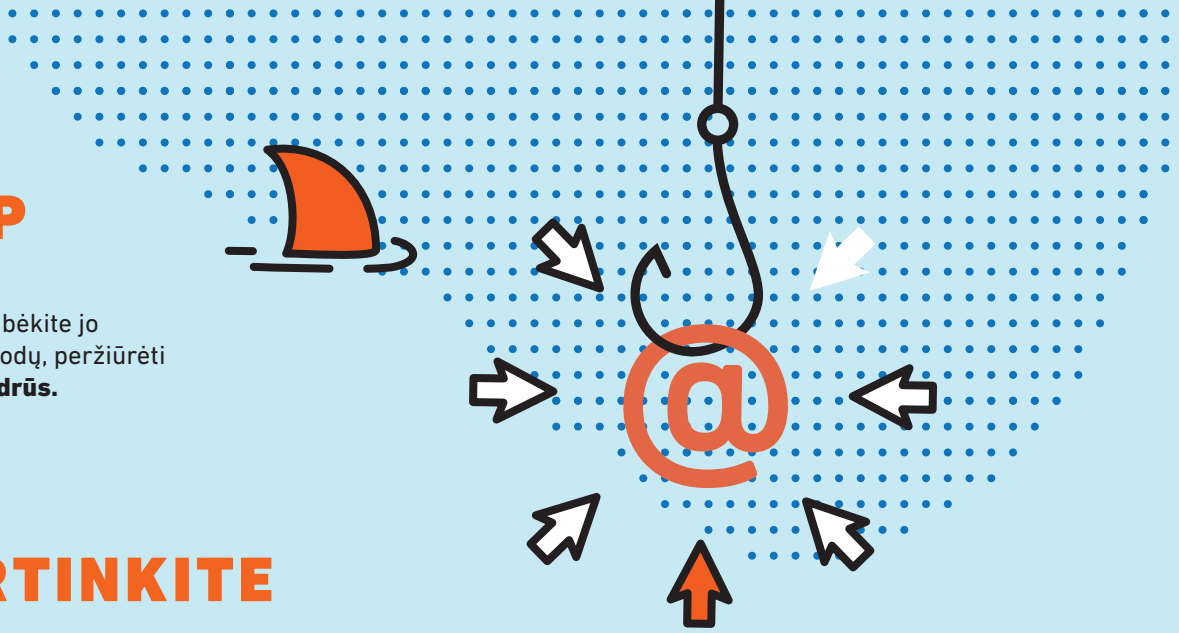
Neužkibk ant e-kabliuko

Rekomendacijos apsaugai nuo socialinės inžinerijos e-paštu

Socialinė inžinerija

Tai nusikalstamas imitavimas įvairių natūralių mūsų gyvenimo ar darbo aplinkybių, kurių metu siekiama taikinį suklaidinti, psichologiškai paveikti ir išvilioti jautrius duomenis arba išprovokuoti atlikti potencialiai žalingus IT infrastruktūrai veiksmus. Socialinės inžinerijos tikslas – išgauti konfidencialią informaciją, asmeninius, banko, finansinius duomenis. Dažniausiai taikomas socialinės inžinerijos metodas – fišingas *(angl. phishing),* duomenų „žvejojimas“ el. paštu.

bluebridge.lt



1 STOP

Gavus el. laišką neskubėkite jo atidaryti, spausti nuorodų, peržiūrėti prisegtukų. **Būkite budrūs.**

2 ĮVERTINKITE

- Ar šio laiško gavimas Jūsų nenustebino, laiško laukėte arba tikėjotės?
- Ar siuntėjo el. pašto adresas sutampa su siuntėjo vardu, o siuntėjo ir kiti matomi el. adresai nekelia įtarimo?
- Ar laiško turinys, gramatika, siuntėjo parašas/jo nebuvimas nekelia įtarimo?
- Ar laiške esate skubinamas laiko, autoriteto ar kitų sąlygų atlikti tam tikrus veiksmus, suteikti duomenis?
- Jei laiške prašoma suteikti informaciją ar duomenis – ar jie nėra konfidencialūs, jautrūs? Pvz.: asmens duomenys, prisijungimai.
- Jei laiško turinyje yra „SPAUSTI ČIA" ar kitos nuorodos – nespauskite, tačiau užveskite pelės rodyklę patikrinti, ar nuoroda logiška, suprantama.
- Jei laiškas turi prisegtukų – ar prisegtos bylos pavadinimas, plėtinys, ikona ar kita vizuali informacija nekelia įtarimo?

3 PRANEŠKITE

Visais atvejais, kai kyla pagrįstas įtarimas dėl gauto el. laiško saugumo dar neatlikus jokių veiksmų arba po galimai nesaugios nuorodos paspaudimo, bylos atidarymo, atsakomojo laiško išsiuntimo, informuokite Jūsų įmonės IT skyrių, IT administratorių arba saugos įgaliotinį.

Papasakokite, kas sukėlė Jums įtarimą ir gali būti naudinga tyrimui, pavyzdžiui: keistos nuorodos, instrukcijos laiške arba dokumente, tušti dokumento puslapiai, atsidarantys naršyklės langai, pasileidžiančios ar „nulūžtančios" programos, staigus kompiuterio greitaveikos sutrikimas, klaidų pranešimai.

4 PREVENCIJA

Būkite budrūs ir neatidarykite el. laiškų ar prisegtukų, kurie kelia įtarimą.

- **Laiškas sukėlė įtarimą?**
  Jei yra galimybė, patikrinkite laiško autentiškumą alternatyviu kanalu, pvz., telefonu.
- Neatidarykite prisegtuko su **.exe** plėtiniais.
- Neaktyvuokite tekstinių prisegtukų **Macros funkcijos.**
- Prisegtuko saugumą galite patikrinti išsaugoję jį darbalaukyje ir praskenavę turima antivirusine programa ir/arba internete esančiu nemokamu įrankiu **www.virustotal.com.**
- **Naudokite** el. pašto filtrus, naujos kartos antivirusines programas, ugniasienes ir nepraleiskite programinės įrangos atnaujinimų.
- Prisijungimams naudokite dviejų faktorių **autentifikavimą.**
- Naudokite **saugos įskiepius** naršyklėje *(angl. anti-phishing addons).*
- Stiprinkite **komandos atsparumą** socialinei inžinerijai skleisdami informaciją, organizuodami mokymus apie kibernetinį saugumą ir vykdydami praktines IT saugumo treniruotes.