ADWISERY
wise solutions

KIBERNETINIO SAUGUMO MOKYMAI

Lektoriai:
Kibernetinio saugumo ekspertas
Arnoldas Judinas

Vilnius, 2024-12-05

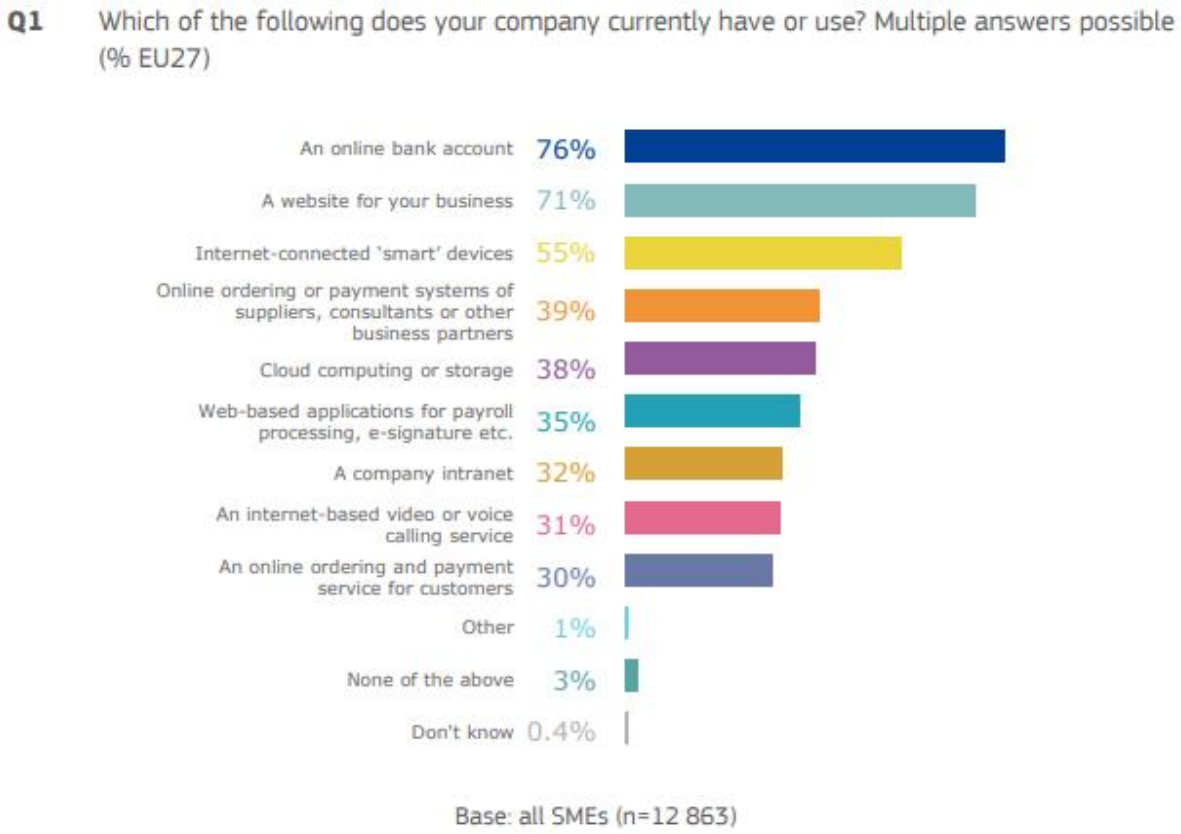
ADWISERY
wise solutions

Informacijos saugos problematika, tikslai, principai, priemonės

ADWISERY
wise solutions

Šiuolaikinių organizacijų veikla paremta IT priemonių ir (ar) paslaugų naudojimu, įskaitant:

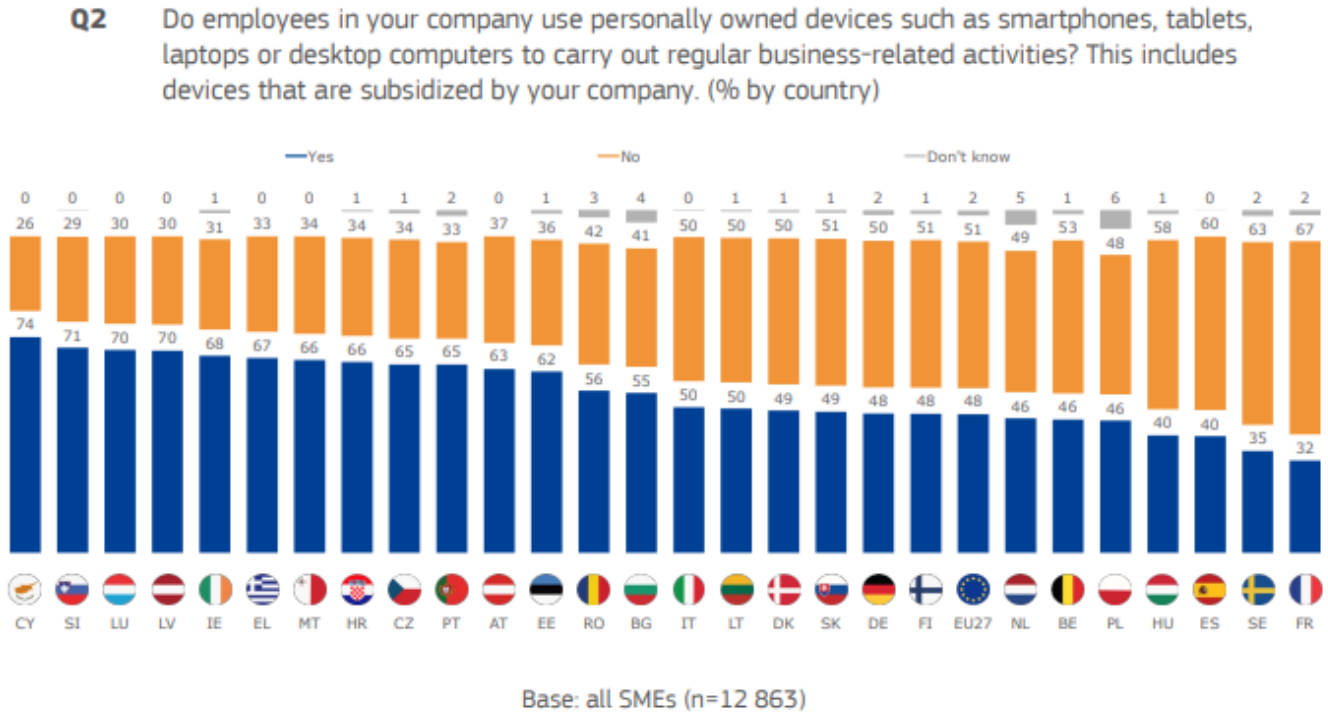
- Online banko sąskaitas;
- Organizacijų internetinius tinklapius;
- Išmaniuosius įrenginius;
- Debesijos paslaugas;
- WEB aplikacijas ir kt.



Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

ADWISERY
wise solutions

Didelė dalis darbuotojų darbo reikmėms naudoja asmeninius įrankius, kurie galimai nėra tinkamai apsaugoti ir gali turėti pažeidžiamumų.



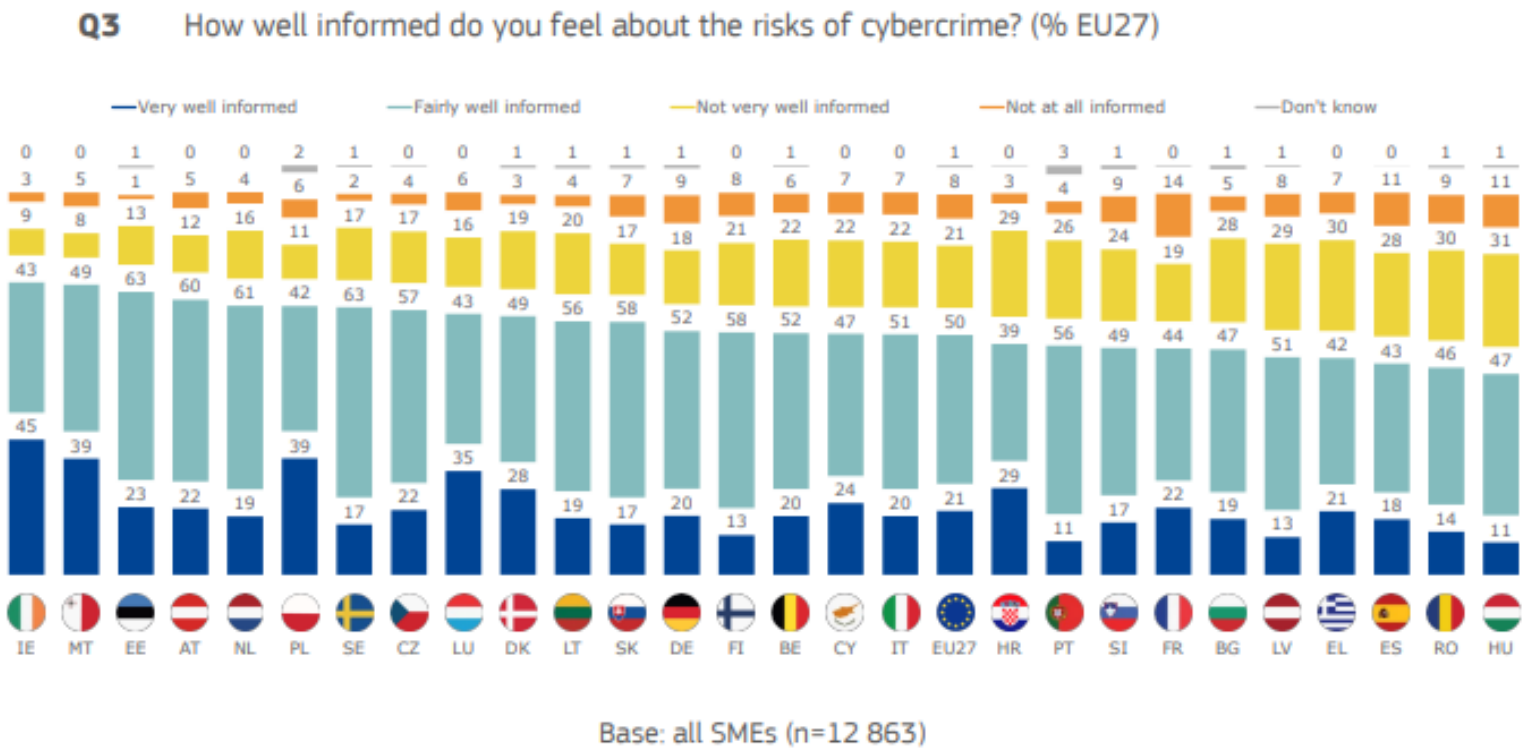
Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

ADWISERY
wise solutions

Darbuotojai nėra labai gerai informuoti apie kibernetinius incidentus, todėl greičiausiai nesugebėtų jų atpažinti ir nuo jų tinkamai apsisaugoti.

LT – labai gerai informuoti jaučiasi 19%;

EU - labai gerai informuoti jaučiasi 21%.



Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

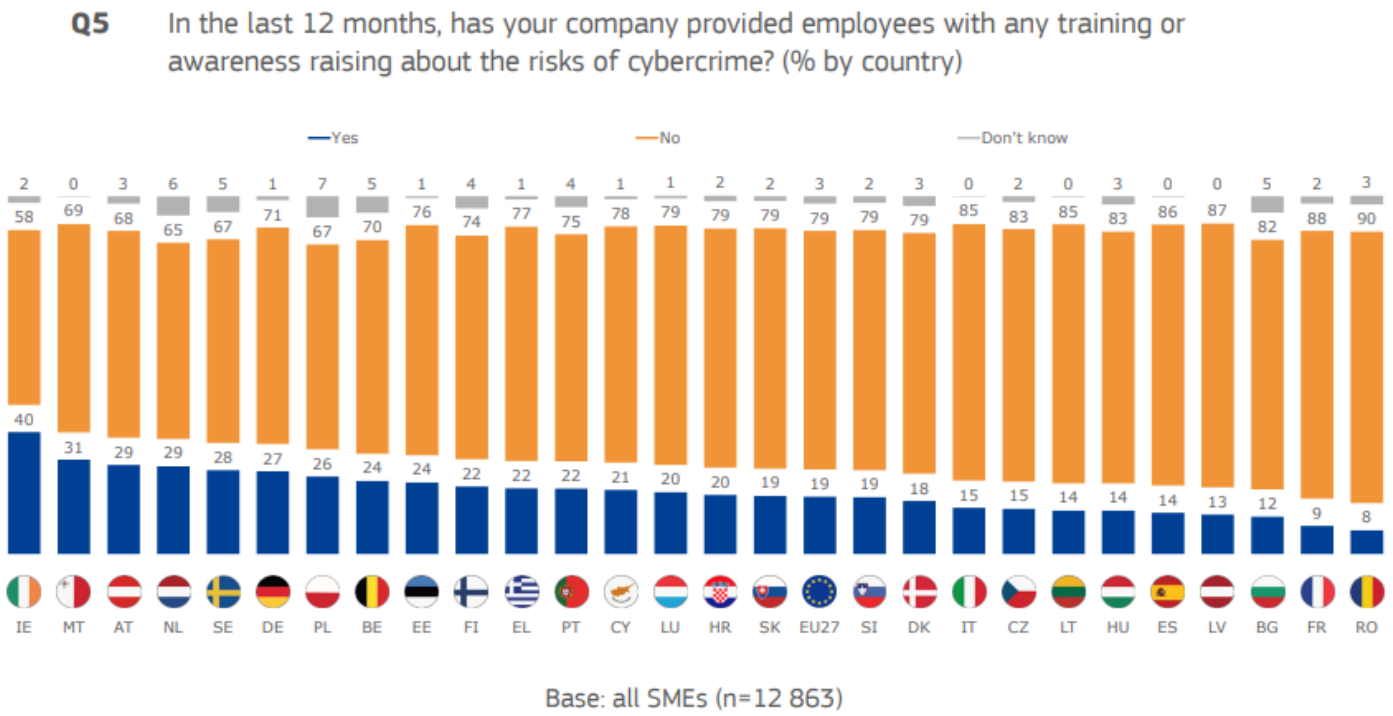
ADWISERY
wise solutions

Darbuotojai nėra reguliariai mokomi, informuojami apie kibernetinio saugumo rizikas.

Per paskutinius 12 mėn.:

LT – 14% įmonių organizavo mokymus darbuotojams;

EU - 19% įmonių organizavo mokymus darbuotojams.



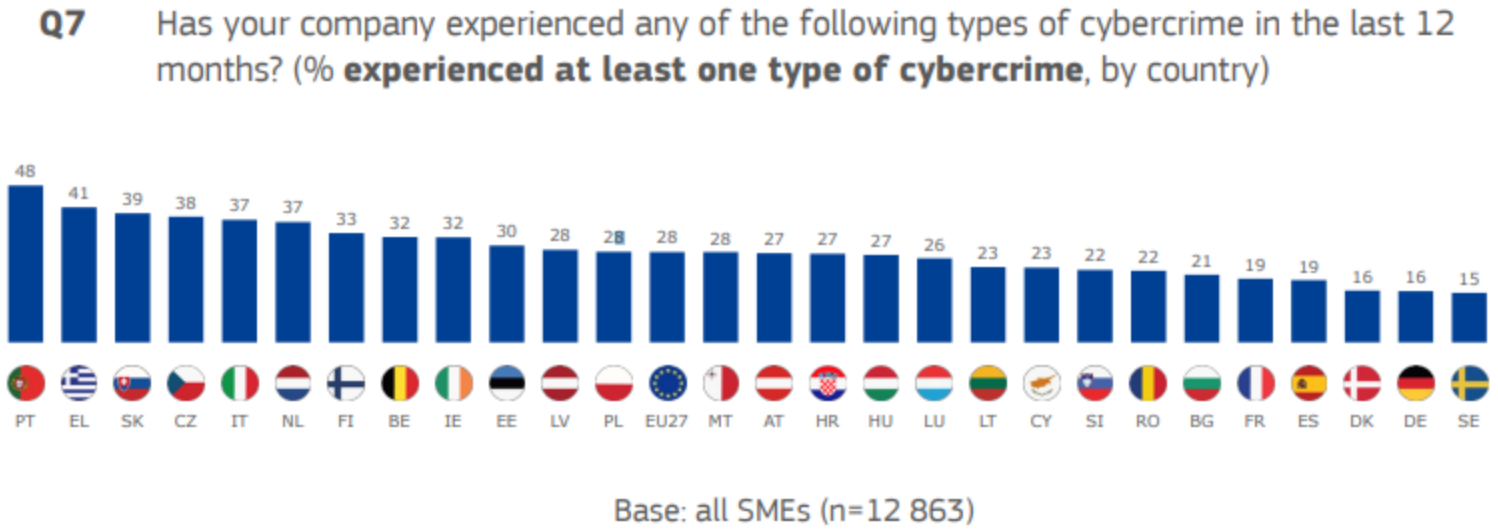
Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

ADWISERY
wise solutions

Per paskutinius 12 mėn.:

LT – 23% įmonių susidūrė su kibernetiniu nusikaltimu;

EU - 28% įmonių susidūrė su kibernetiniu nusikaltimu;



Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

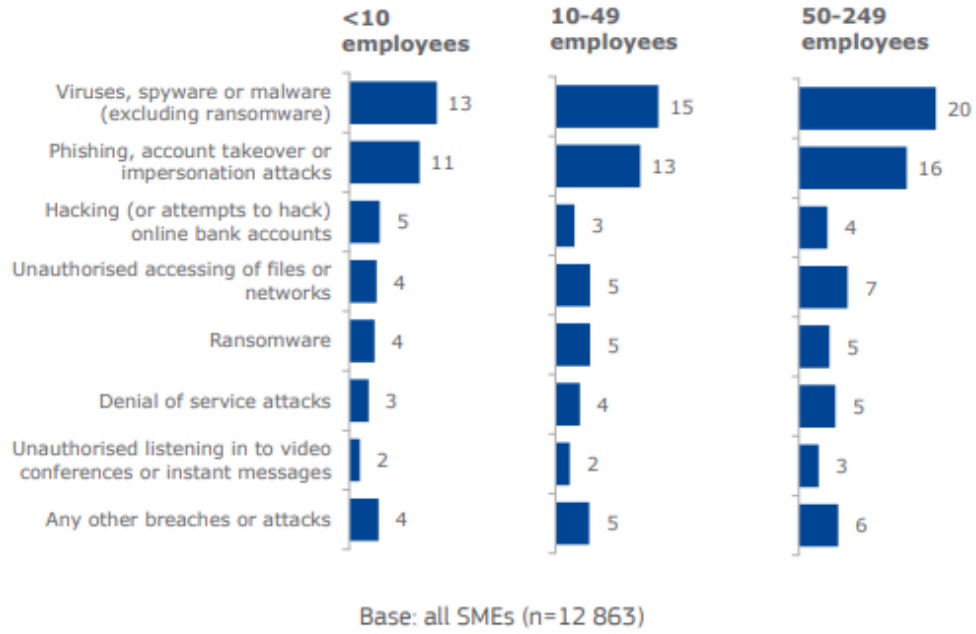
ADWISERY
wise solutions

„Mes maži, niekam neįdomūs..“

„Iš mūsų nėra ką pavogti...“

Rizika tapti kibernetinio nusikaltimo auka nepriklauso nuo įmonės dydžio.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% by company size)



Base: all SMEs (n=12 863)

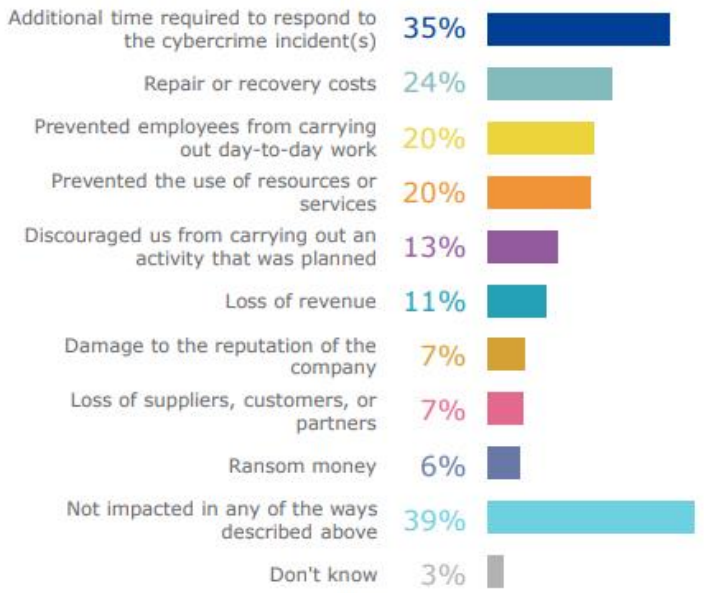
Šaltinis: *Eurobarometro apklausa 496 “Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas“, 2022 m. gegužė*

ADWISERY
wise solutions

Incidentų pasekmės:

- Reikėjo skirti papildomo laiko reaguoti į incidentą;
- Darbuotojai negalėjo atlikti kasdienio darbo;
- Išlaidos veiklos atstatymui;
- Pajamų praradimas;
- Reputacinė žala;
- Klientų, partnerių, tiekėjų paradimas ir kt.

Q9 Still thinking about the most serious incident, how was your business impacted? Multiple answer possible (% EU27)



Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

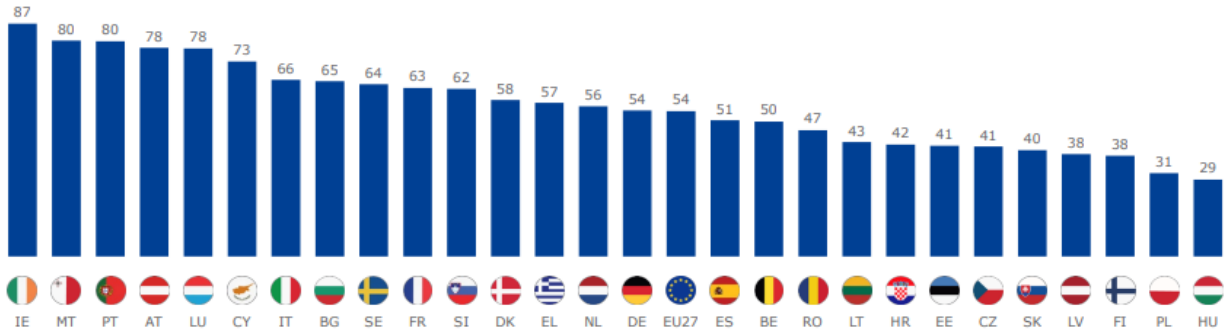
Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

ADWISERY
wise solutions

Apie kibernetinius incidentus retai pranešama.

Apie incidentą buvo pranešta:
LT – 43% atvejų;
ES – 54% atvejų;

Q10a Who, if anyone, did you report this incident to? Multiple responses possible
(% **Total 'Reported to someone'**, by country)



Pranešimas apie kibernetinius nusikaltimus

q10 Ar kam nors pranešėte apie šį incidentą? (GALIMI KELI ATSAKYMAI)

Šaltinis: *Eurobarometro apklausa 496 "Smulkiosios ir vidutinė įmonės ir kibernetinis nusikalstamumas", 2022 m. gegužė*

ADWISERY
wise solutions

- **Konfidencialumas**

Informaciją gali gauti tik tas, kam ji yra siunčiama.

- **Vientisumas**

Niekas negali pakeisti dalies arba visos žinutės turinio.

- **Prieinamumas**

Visada prieinama tam, kas ją turi gauti.

CIA triada

ADWISERY
wise solutions

Kiti informacijos saugos uždaviniai

- **Autentiškumas**

Gavėjas gali būti tikras nuo ko gavo žinutę.

- **Negalėjimas atsisakyti**

Siuntėjas ir gavėjas vėliau negali paneigti, kad jie siuntė ir gavo būtent šią žinutę.

- **Prieinamumo kontrolė**

Informacijos šaltinis yra pilnai kontroliuojamas to, kam jis priklauso.

ADWISERY
wise solutions

Informacijos saugos principai

- Mažiausių privilegijų / Minimalaus duomenų kiekio;
- „Gilios“ apsaugos (organizaciniai, techniniai, fizinės saugos reikalavimai);
- Principai kontrolės požiūriu:
  - Leista viskas, kas nėra uždrausta;
  - Leista tik tai, kas yra oficialiai leista;
- Principai sudėtingumo požiūriu
  - Paprastumo;
  - Saugumo per neaiškumą;

ADWISERY
wise solutions

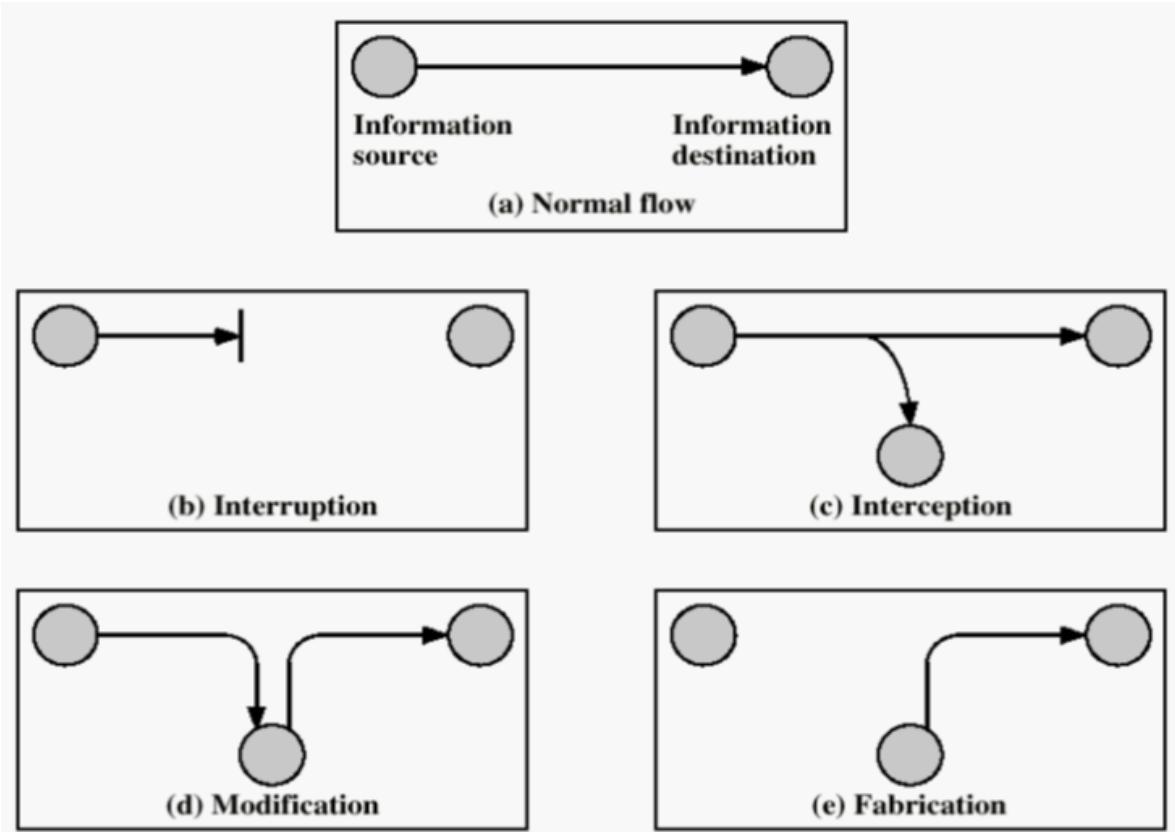
Kas mus puola?

- Script-kiddies – nepatyrę (lengva apsisaugoti), bet jų daug;
- Karderiai – banko kortelių vagystės, klastojimas;
- Programišiai – asmens duomenų vagystė, resursų išnaudojimas;
- Aktyvistai – grupės veikiančios kartu (politiniai, socialiniai motyvai);
- Valstybės / Specialiosios tarnybos – sabotažas, šnipinėjimas;
- Įmonės / organizacijos darbuotojai – duomenų, paslapčių nutekinimas ir pardavimas.

ADWISERY
wise solutions

Atakų rūšys

- Nutraukimas (angl. Interruption);
- Perėmimas (angl. Interception);
- Modifikavimas (angl. Modification);
- Klastojimas (angl. Fabrication).



ADWISERY
wise solutions

Atakų metodai

- Papirkimas;
- Sudėtingi technologiniai būdai / įsilaužimai;
- Kenksmingas programinis kodas / Nuotolinis šnipinėjimas;
- DDoS atakos;
- Socialinė inžinerija.

ADWISERY
wise solutions

Informacijos saugos sprendimai

- Technologiniai sprendimai
- Organizaciniai sprendimai
- Fizinės saugos sprendimai

ABSOLIUTAUS SAUGUMO NĖRA!

Tik priemonių kompleksas leidžia užtikrinti priimtiną saugos lygį.

ADWISERY
wise solutions

Technologiniai sprendimai

- Antivirusinės sistemos;
- Duomenų šifravimas;
- Ugniasienės / Tinklų zonavimas / Produkcinių ir testinių aplinkų atskyrimas;
- IDS/IPS (Intrusion detection/prevention) sistemos;
- Prieigos stebėjimas (logging) ir analizė (SIEM);
- DLP (data loss prevention) sistemos;
- Atsarginių kopijų kūrimo įrankiai;
- Infrastruktūros / įrangos dubliavimas patikimumo didinimui.

ADWISERY
wise solutions

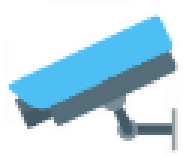
Organizacinės / valdymo priemonės

- Rizikos analizė ir valdymas / veiklos tęstinumo parametrų nustatymas (RTO / RPO);
- Saugumo politika, procedūros;
- Saugos standartų pritaikymas įmonės veikloje;
- Veiklos tęstinumo ir atsako į incidentus planai;
- Personalo / tiekėjų valdymas iš saugos perspektyvos;
- Teisinės aplinkos stebėjimas / atitikties užtikrinimas;
- Reguliarus auditas ir pažeidžiamumų paieška.

ADWISERY
wise solutions

Fizinės saugos užtikrinimo priemonės

- Prieigos kontrolė;
- Patalpų apsauga;
- Signalizacija;
- Vaizdo stebėjimas;
- Duomenų centro patalpų įrengimas;
- Priešgaisrinės sistemos;
- Darbo vietų ir nešiojamų kompiuterių, mobilių įrenginių apsauga.



ADWISERY
wise solutions

Kibernetinio saugumo reglamentavimas Lietuvoje

ADWISERY
wise solutions

Kibernetinio saugumo įstatymas

KSĮ detalizuoja pagrindinius kibernetinio saugumo principus, kibernetinio saugumo subjektų pareigas. KSĮ taikomas ne visiems ūkio subjektams, o tik tiems, kurie užsiima specialia veikla – valdo ir prižiūri valstybės informacinius išteklius, ypatingos svarbos informacinę infrastruktūrą, teikia viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas, teikia elektroninės informacijos prieglobos (angl. hosting) paslaugas ir skaitmenines paslaugas.

Bendrasis duomenų apsaugos reglamentas

BDAR nustato asmens duomenų tvarkymo, saugumo užtikrinimo reikalavimus, asmens duomenis tvarkančių (ar valdančių) subjektų teises ir pareigas bei duomenų subjektų – fizinių asmenų, kurių duomenys tvarkomi, teises. Reglamentas taikomas visiems ūkio subjektams, tvarkantiems (ar valdantiems) asmens duomenis.

ADWISERY
wise solutions

Kiti teisės aktai reglamentuojantys informacijos saugą ir kibernetinį saugumą:

- Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;
- Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;
- Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“

ADWISERY
wise solutions

Rizikos ir atitikties vertinimai, pažeidžiamumai ir grėsmės

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (Patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimu Nr. 818), **nustato organizacinius ir techninius kibernetinio saugumo reikalavimus** kibernetinio saugumo subjektams.

Kibernetinio saugumo subjektų ryšių ir informacinių sistemų rizikos vertinimas (II skyrius):

„Kibernetinio saugumo subjektų ryšių ir informacinių sistemų kibernetinio saugumo **organizacinių ir techninių priemonių užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimu..“**,

ADWISERY
wise solutions

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (III skyrius):

- Ne rečiau kaip **kartą per metus** arba po esminių organizacinių ar sisteminių pokyčių turi būti atliekamas **rizikos vertinimas**.
- Ne rečiau kaip **kartą per metus** turi būti atliekamas **atitikties** Reikalavimams **vertinimas**.

ADWISERY
wise solutions

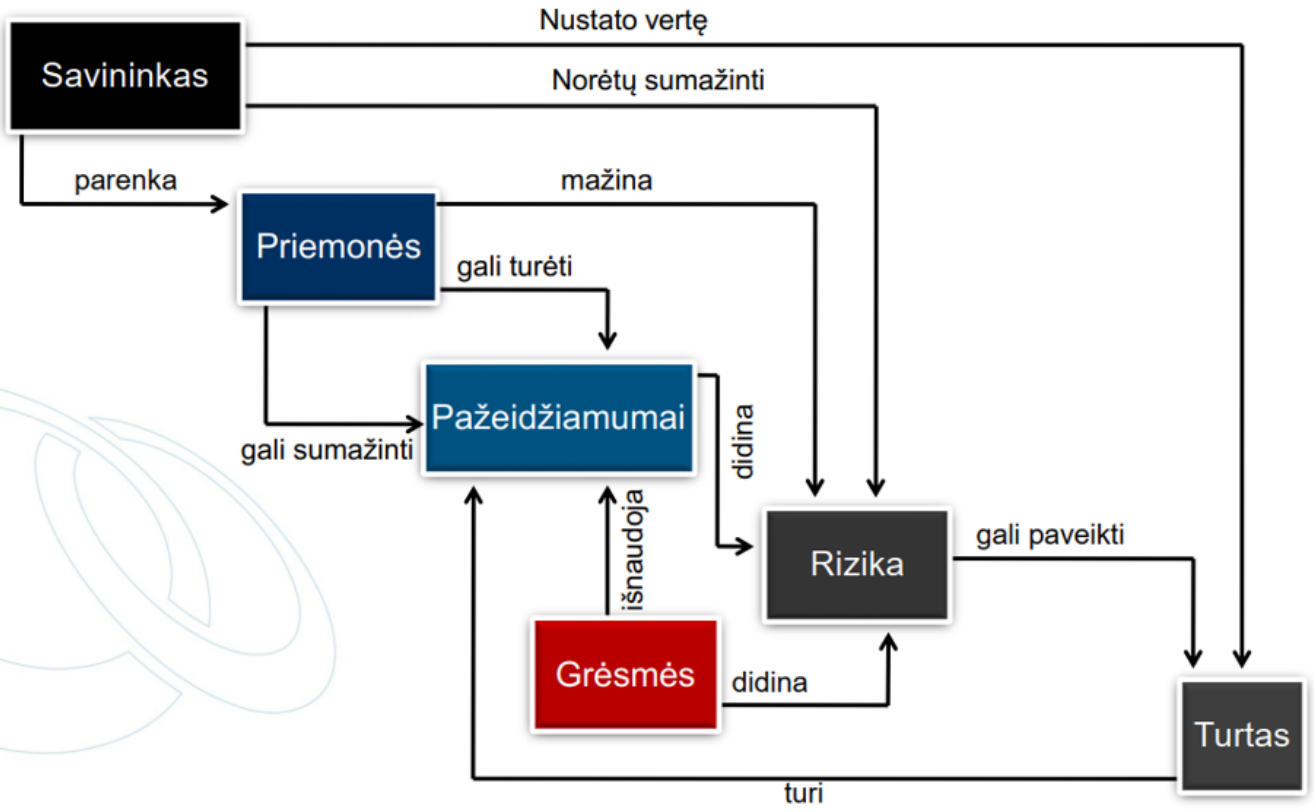
Kibernetinio saugumo subjektų ryšių ir informacinių sistemų rizikos vertinimas (II skyrius):

Kibernetinio saugumo subjektai, organizuodami ryšių ir informacinių sistemų rizikos vertinimą:

- Paskiria atsakingą asmenį;
- Nustato reikalavimus rizikos vertinimo procesui;
- Nustato grėsmes ir pažeidžiamumus;
- Įvertina grėsmių tikimybę ir pasekmes, nustato rizikos lygį;
- Atsižvelgdami į atliktą rizikos vertinimą, rengia bei peržiūri patvirtintus teisės aktus, nustato, kuriuos iš reikalavimų būtina atnaujinti ar įgyvendinti.

ADWISERY
wise solutions

Ryšiai tarp informacijos saugumo sąvokų



ADWISERY
wise solutions

Kuo skiriasi šios sąvokos?

- Grėsmės
- Pažeidžiamumai
- Rizika

ADWISERY
wise solutions

Grėsmė

Potenciali nepageidaujamo incidento, galinčio sukelti žalos sistemai ar organizacijai galimybė

Grėsmės tipas	Pavyzdys
1. Fizinė žala	Gaisras
	Vandens žala
2. Gamtinė nelaimė	Žemės drebėjimas
	Potvynis
3. Pagrindinių paslaugų praradimas	Oro kondicionieriaus gedimas
	Elektros tiekimo nutrūkimas
4. Spinduliavimas	Elektromagnetinis spinduliavimas
	Šiluminis spinduliavimas
5. Informacijos nutekėjimas	Pasiklausymo įranga
	Dokumentų vagystė
6. Techninis gedimas	Įrangos gedimas
	Per didelis tinklo apkrautumas

ADWISERY
wise solutions

Pažeidžiamumai

Saugumo priemonės silpnumas, kurį gali išnaudoti grėsmė

Pažeidžiamumo tipas	Pavyzdys
1. Aparatinė įranga	Nepakankama priežiūra
	Nešiojama įranga
2. Programinė įranga	Nėra registracinių įrašų
	Komplikuota vartotojo sąsaja
3. Tinklas	Duomenys nešifruojami
	Prieiga per vieną tašką
4. Personalas	Nepakankami mokymai
	Priežiūros stoka
5. Pastatas	Nestabilus elektros tiekimas
	Pastatas gali būti užlietas potvynio
6. Organizacinė struktūra	Pareigos nėra atskirtos
	Nėra pareiginių instrukcijų

ADWISERY
wise solutions

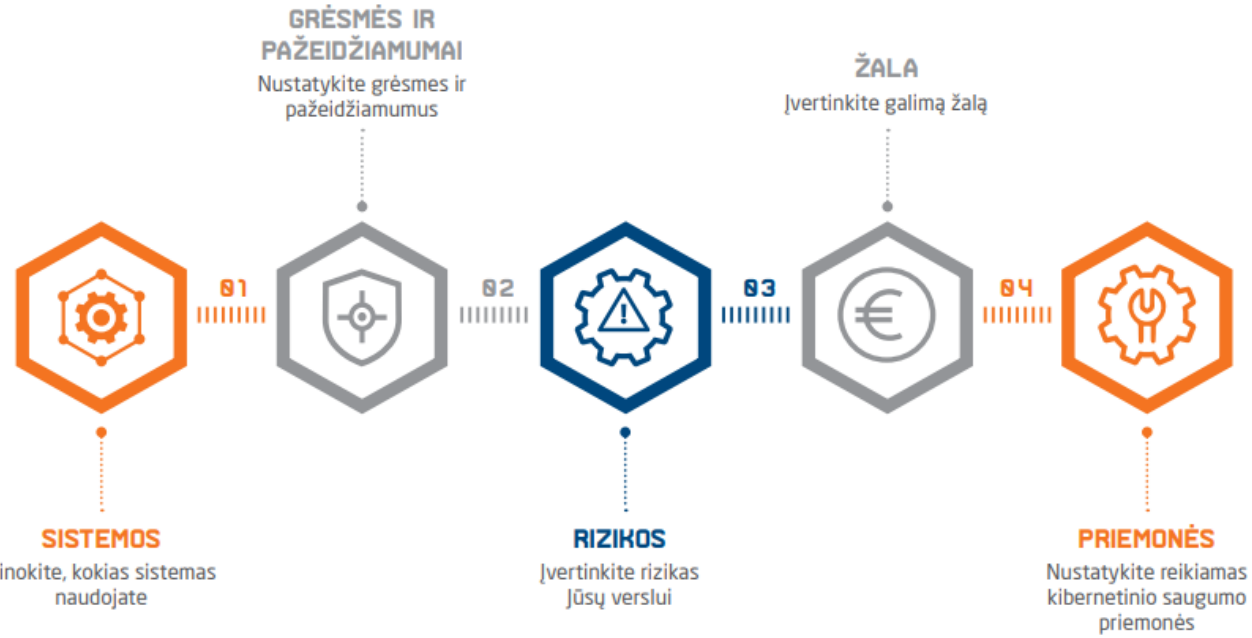
Informacijos saugumo rizika

Galimybė, kad konkreti grėsmė išnaudos pažeidžiamumus ir taip pakenks organizacijai.

ADWISERY
wise solutions

RIZIKŲ VERTINIMAS

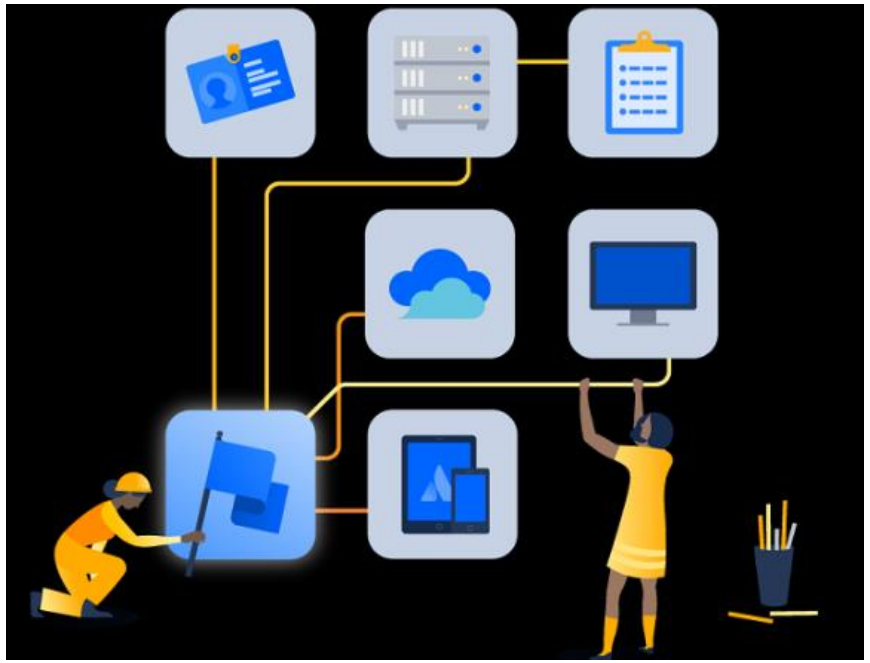
Kaip įvertinti ir valdyti rizikas?



ADWISERY
wise solutions

1) Žinokite, kokias sistemas naudojate ir su kokia informacija dirbate

IT sistemos gali būti naudojamos iš išorės arba iš vidaus.



ADWISERY
wise solutions

2) Nustatykite grėsmes, jų šaltinius ir pažeidžiamumus

Įvertinkite ir nustatykite, kokiais būdais įsilaužėliai gali gauti prieigą prie įmonės tinklo ar duomenų.

ADWISERY
wise solutions

46 grėsmės, Federalinis informacijos saugumo biuras (Vokietija)

• Gaisras • Nepalankios oro sąlygos • Vanduo • Tarša, dulkės, korozija • Stichinės nelaimės • Aplinkos nelaimės • Dideli įvykiai aplinkoje • Elektros tiekimo gedimas ar sutrikimas • Ryšių tinklų gedimas ar sutrikimas • Magistralinio tiekimo gedimas ar sutrikimas • Paslaugų teikėjų patiriamas gedimas ar sutrikimas • Įsiterpianti spinduliuotė • Informatyvi spinduliuotė • Informacijos perėmimas / Šnipinėjimas • Slaptas klausymasis • Įrangos, duomenų laikmenų ir dokumentų vagystė • Įrangos, duomenų laikmenų ir dokumentų praradimas • Netinkamas planavimas arba suderinamumo trūkumas • Konfidencialios informacijos atskleidimas • Informacija ar produktai iš nepatikimų šaltinių • Manipuliavimas aparatine ir programine įranga • Informacijos klastojimas • Neleistina prieiga prie IT sistemų • Įrangos ar duomenų laikmenų sunaikinimas • Įrangos ar sistemų gedimas • Įrangos ar sistemų sutrikimas • Išteklių trūkumas • Programinės įrangos pažeidžiamumai ar klaidos • Teisės aktų ir taisyklių pažeidimai • Nesankcionuotas įrangos ir sistemų naudojimas ar administravimas • Netinkamas įrangos ir sistemų naudojimas ar administravimas • Piktnaudžiavimas įgaliojimais • Darbuotojų stygius • Ataka • Prievarta, plėšimas arba korupcija • Tapatybės vagystė • Veiksmų išsižadėjimas • Piktnaudžiavimas asmens duomenimis • Kenkėjiška programinė įranga • Paslaugos atkirtimas • Sabotažas • Socialinė inžinerija • Pranešimų persiuntimas • Neleistinas patekimas į patalpas • Duomenų praradimas • Svarbios informacijos vientisumo praradimas

ADWISERY
wise solutions

ENISA grėsmių žemėlapis 2022

Grėsmės duomenų saugumui
Socialinė inžinerija
Dezinformacija
Kenksminga programinė įranga
Išpirkos reikalaujantys virusai
DDoS atakos
Ir kita.

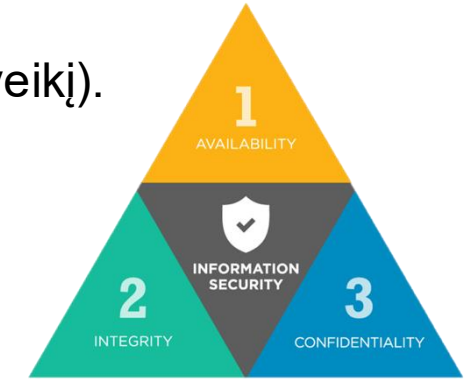
ADWISERY
wise solutions

3) Įvertinkite grėsmių riziką Jūsų veiklai

Rizika gali būti apibrėžiama kaip bet kokia aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui.

Kibernetinio saugumo rizikos gali būti skirstomos pagal minėtas kategorijas: **grėsmė informacijos konfidencialumui, vientisumui arba prieinamumui**.

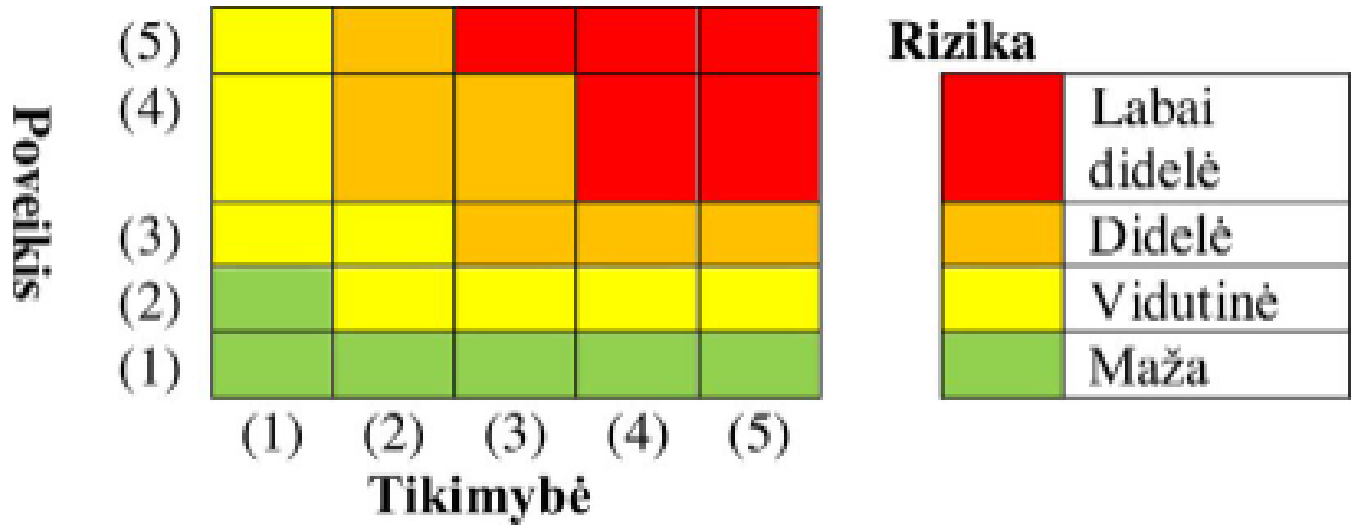
Rizikos turėtų būti suskirstytos pagal saugos pažeidimo tikimybę ir įtakos kriterijus (poveikį).



Rizikų visiškai pašalinti neįmanoma.

ADWISERY
wise solutions

Kokybinė rizikos laipsnio matrica



ADWISERY
wise solutions

4) Įvertinkite galimą žalą

Kibernetinio saugumo incidentai gali sukelti įvairialypę žalą Jūsų veiklai. Dėl to būtina įvertinti, kokią žalą gali sukelti vieno ar kito tipo incidentas.

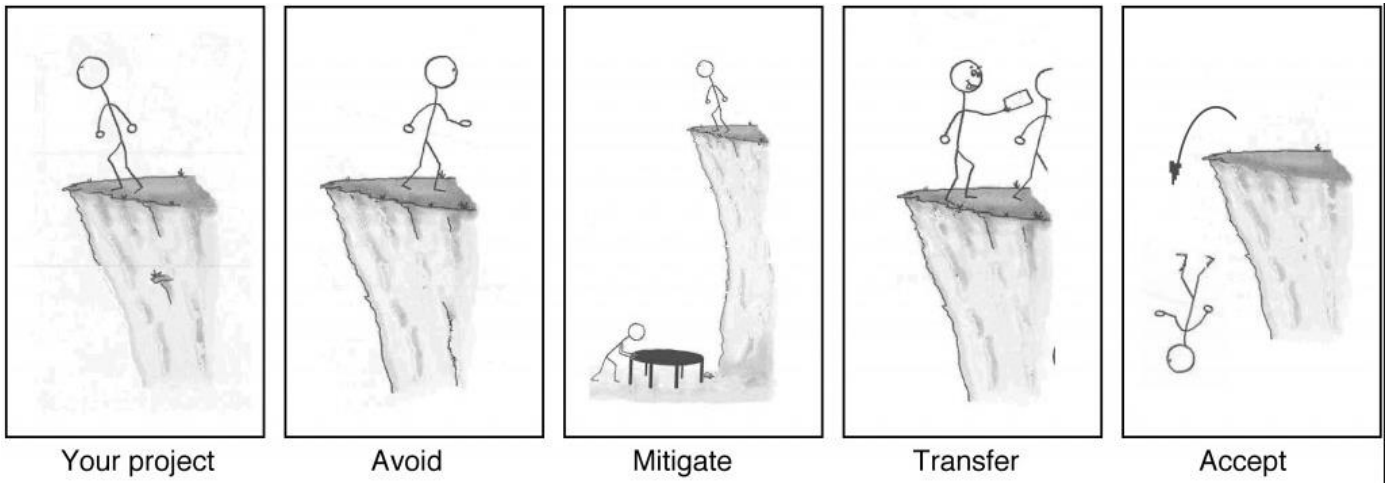
ADWISERY
wise solutions

5) Nustatykite reikiamas kibernetinio saugumo priemones

Nustatę ir įvertinę galimas kibernetinio saugumo rizikas bei galimus nuostolius Jūsų veiklai, galėsite sukurti planą, kaip valdysite nustatytas rizikas ir kokių priemonių reikėtų imtis nustatytoms rizikoms valdyti.

Rizikų vertinimas nėra vienkartinis veiksmas, o bene svarbiausias, nuolat kartojamas procesas.

ADWISERY
wise solutions



Rizikų valdymo strategijos

- Sumažinimas (angl. *Risk Mitigation*).
- Perdavimas (angl. *Risk Transference*).
- Priėmimas (angl. Risk *Acceptance*).
- Vengimas (angl. Risk *Avoidance*).

ADWISERY
wise solutions

Kibernetinio saugumo situacija Lietuvoje, kibernetiniai nusikaltimai

ADWISERY
wise solutions

Kibernetinis saugumas – visuma **teisinių, informacijos sklaidos, organizacinių ir techninių priemonių**, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėms sistemoms (toliau - RIS) ir joje tvarkomai informacijai, RIS netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę RIS veiklą.

Lietuva yra tarp lyderių pagal nacionalinį kibernetinio saugumo indeksą (NCSI).

Rank	Country	National Cyber Security Index
1.	Belgium	94.81
2.	Lithuania	93.51
3.	Estonia	93.51
4.	Czech Republic	92.21
5.	Germany	90.91
6.	Romania	89.61
7.	Greece	89.61
8.	Portugal	89.61
9.	United Kingdom	89.61
10.	Spain	88.31

ADWISERY
wise solutions

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

NKSC, atsižvelgdamas į būtinybę incidentus klasifikuoti pagal poveikį, nuo 2019 m. **kibernetiniais incidentais traktuoja atvejus, kada specialistai įvykius apdoroja betarpiškai** – priskiria poveikio reikšmę bei nustato incidento kategoriją. Nuo 2019 atskiriami **automatinėmis priemonėmis ir programomis apdoroti procesai, kurie traktuojami kaip kibernetiniai įvykiai.**

Tokia klasifikacija, kai kibernetiniai įvykiai atskiriami nuo kibernetinių incidentų, įvesta siekiant suvienodinti klasifikavimą pagal ES kibernetinio saugumo agentūros bei kitų šalių kibernetinių incidentų valdymo komandų taksonomiją.

ADWISERY
wise solutions

Kibernetinius incidentus tiriančios / valdančios institucijos

- Nacionalinis kibernetinio saugumo centras (NKSC).
- Valstybinė duomenų apsaugos inspekcija.
- Lietuvos policija.

VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

Kibernetinių incidentų valdymas – procedūros, kurių tikslas – **aptikti, analizuoti** kibernetinius incidentus ir **reaguoti** į juos, taip pat **atkurti** įprastinę ryšių ir informacinių sistemų veiklą.

ADWISERY
wise solutions

Kibernetinių incidentų poveikis

Nereikšmingas (bent vienas iš kriterijų) • RIS trikdoma < 1 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 % • Paslauga teikiama, bet trikdoma • Nuostoliai < 250 000 Eur.	**Vidutinis** (bent du iš kriterijų) • RIS trikdoma ≥ 1 val., bet < 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 % • Paslauga trikdoma dalyje šalies teritorijos • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas • Nuostoliai ≥ 250 000, bet < 500 000 Eur.
Didelis (bent du iš kriterijų) • RIS trikdoma ≥ 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 % • Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas • Nuostoliai ≥ 500 000 Eur.	**Pavojingas** (bent vienas iš kriterijų) • RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % • Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše

ADWISERY
wise solutions

Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N)	Vidutinis (V)	Didelis (D)	Pavojingas (P)
Informacijos rinkimas (angl. *information gathering*) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. ***social engineering***), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	3.1. RIS paketų / informacijos perėmimas		V	D	P
	3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant **socialinės inžinerijos** principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)		V	D	P
	3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N	V		
	3.4. Naudojami **socialinės inžinerijos** metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją	N	V		

Šaltinis: Nacionalinis kibernetinių incidentų valdymo planas patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“

Socialinės inžinerijos incidentas, priklausomai nuo pogrupio ir poveikio kategorijos, **gali būti priskiriamas nereikšmingam, vidutinio, didelio arba pavojingo svarbumo incidentui**.

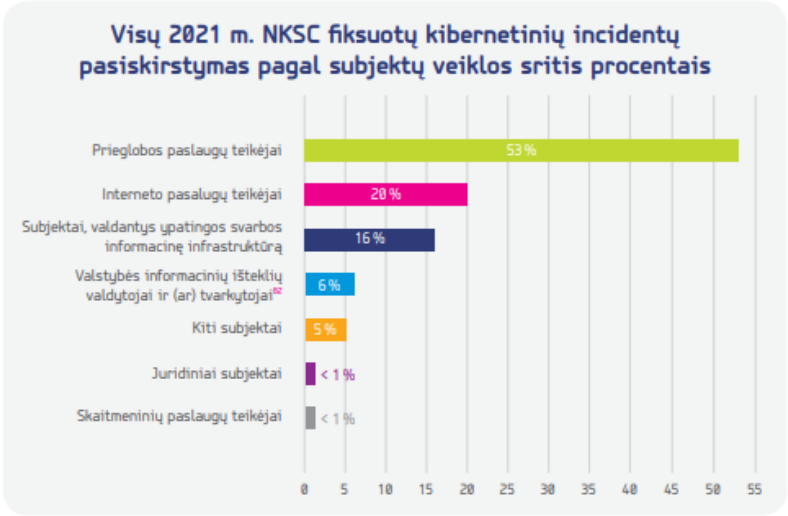
Nevaldomas arba netinkamai valdomas, priklausomai nuo pogrupio ir poveikio kategorijos, **nereikšmingas socialinės inžinerijos incidentas gali tapti vidutiniu, o vidutinis – dideliu arba pavojingu**.

ADWISERY
wise solutions

2021 m. **NKSC** iš viso registravo **4088** kibernetinius incidentus (5% mažiau nei 2020 m.)

- Kenkimo PĮ išliko pagrindine kibernetinių incidentų grėsme;
- Stipriai augo informacijos rinkimo (phishing) incidentų skaičius;
- Daugiausia kibernetinių incidentų fiksuota prieglobos paslaugų bei interneto paslaugų teikėjų ryšių ir informacinėse sistemose.

Nr.	Kibernetinio incidento grupės	2021 m. kiekis	2020 m. kiekis	Pokytis vnt.
01	Kenkimo PĮ	1 890	1 966	↓ 76
02	Informacijos rinkimas (angl. *phishing*)	1 187	962	↑ 225
03	Nepageidaujamų laiškų, klaidinančios informacijos platinimas	399	739	↓ 340
04	Mėginimas įsilaužti	278	171	↑ 107
05	Neteisėta veikla, sukčiavimas	136	85	↑ 51
06	Sėkmingas įsilaužimas	125	61	↑ 64
07	Paslaugų trikdymas (angl. DDoS)	43	75	↓ 32
08	Kiti incidentai (atskiri, neatitinkantys nė vienos iš nurodytų grupių aprašymų)	22	271	↓ 241
	Iš viso:	4088	4330	↓ 242



Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

Hibridiniai incidentai

- Naudojami įvairūs kibernetinių incidentų elementai;
- Nauja tendencija – melagingos informacijos platinimas nevykdant kibernetinių įsilaužimų;
- NKSC prognozuoja, kad tokio pobūdžio hibridinių incidentų bus vykdoma ir ateityje, išnaudojant žemą viešojo sektoriaus kibernetinio atsparumo lygį ir siekiant nustatyti atsakingų institucijų veikimo ribas bei efektyviausius eskalacijos būdus bei šaltinius Lietuvai jautriais naratyvais.

Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

Kibernetinių incidentų valdymo planas ir veiklos tęstinumas

Kaip ir gyvenime, taip ir versle – įvykus neplanuotam ar netikėtam įvykiui, visada yra svarbu nepanikuoti ir gebėti valdyti krizines situacijas.

Įmonė turėtų pasiruošti incidentų valdymo ir veiklos tęstinumo planą.

Pirmieji veiksmai, kurių imamasi įvykus kibernetiniam incidentui ar duomenų pažeidimui, yra labai svarbūs, nes dažnai nulemia, koks bus poveikis įmonei, gebėjimą atstatyti verslo veiklą ir ateities įsilaužimų tikimybę.

ADWISERY
wise solutions

Kibernetiniai nusikaltimai plačiąja prasme

Nusikalstamumą elektroninėje erdvėje labiausiai lemia sukčiavimo atvejai, jie 2021 m. sudarė dominuojančią 71 proc. dalį visų elektroninėje erdvėje padarytų nusikalstamų veikų. 2021 m. vyravo tokie sukčiavimo elektroninėje erdvėje būdai:

- telefoninis sukčiavimas (apgaulingi skambučiai ir apgaulingos SMS žinutės, angl. vishing, smishing) sudarė 70 proc. visų tokių sukčiavimų;
- investicinis sukčiavimas – 17 proc.;
- sukčiavimas panaudojant bendravimo programėles – 8 proc.;
- sukčiavimas perimant susirašinėjimą elektroniniu paštu, apgaulingi elektroniniai laiškai (angl. phishing) – 5 proc.

Rekomendacijos, kaip apsisaugoti nuo sukčių:

Naudingų patarimų pateikiama Lietuvos policijos interneto svetainėje (skiltyje „Sukčiavimo būdai") **https://policija.lrv.lt/lt/policija-pataria**.

Vienas svarbiausių patarimų – kritiškai vertinti ryšio ar kitomis priemonėmis gaunamus ar skelbiamus pasiūlymus ir įvairią informaciją.

Įsidėmėkite:

- kuo ilgiau kalbate su sukčiumi, tuo didesnį nerimą jaučiate ir tampa vis sunkiau atpažinti apgavystę;
- nepriimkite žaibiškų sprendimų, neatskleiskite asmens duomenų, neperveskite pinigų į svetimas banko sąskaitas;
- nesuteikite nepažįstamiems asmenims nuotolinės prieigos prie Jūsų kompiuterio ar kito įrenginio;
- teisėsaugos pareigūnai, bankų ir kitų įstaigų darbuotojai neturi teisės ir niekuomet telefonu neprašo pateikti (padiktuoti) asmens duomenų, banko kortelių, generatorių, elektroninės bankininkystės prisijungimo kodų, slaptažodžių ir kt.;
- teisėsaugos pareigūnai, bankų ir kitų įstaigų darbuotojai netarpininkauja tarp nukentėjusiojo ir pažeidėjo sprendžiant piniginius klausimus;
- kritiškai vertinkite pasiūlymus įsigyti prekes už mažesnę negu rinkos kainą. Susigundę patraukliu prekybiniu pasiūlymu, įvertinkite pardavėjo patikimumą ir galimas rizikas.

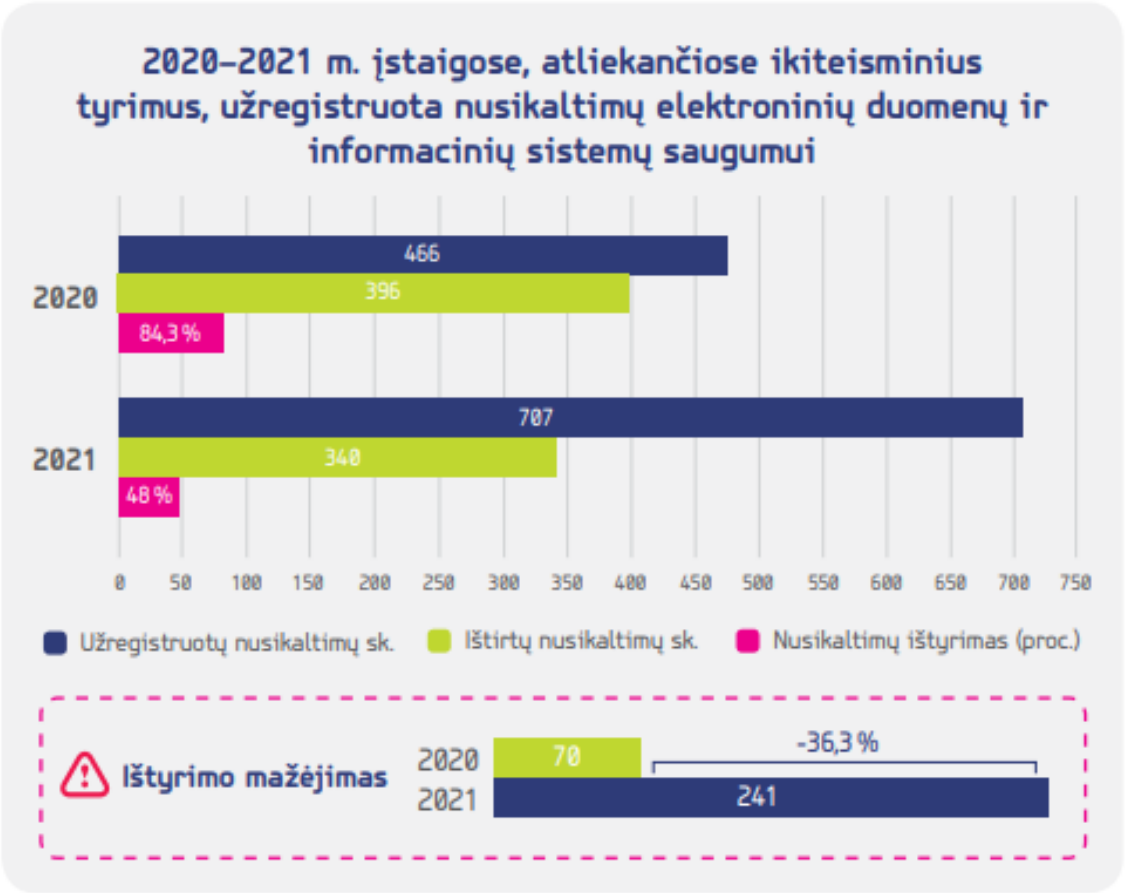
Kilus įtarimui, kad susidūrėte su sukčiumi ar jį pastebėjote, nedelsdami praneškite policijai telefonu 112. Kodėl? Pranešę policijai, padėsite efektyviau ir greičiau išaiškinti sukčius – visi gauti pranešimai yra registruojami, analizuojami, gretinami ir susiejami pagal bendrus požymius.

Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

Kibernetiniai nusikaltimai siaurąja prasme

- 2021 m. Lietuvoje buvo užregistruota 39 718 nusikalstamų veikų. Bendroje nusikalstamumo struktūroje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196–198²str.) 2021 m. sudarė 2 proc. (707 vnt.)
- Palyginti su 2020 m., šių nusikaltimų užregistruota 241 atveju, arba 51,7 proc., daugiau, o šių nusikaltimų ištyrimas sudarė 48 proc.



Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

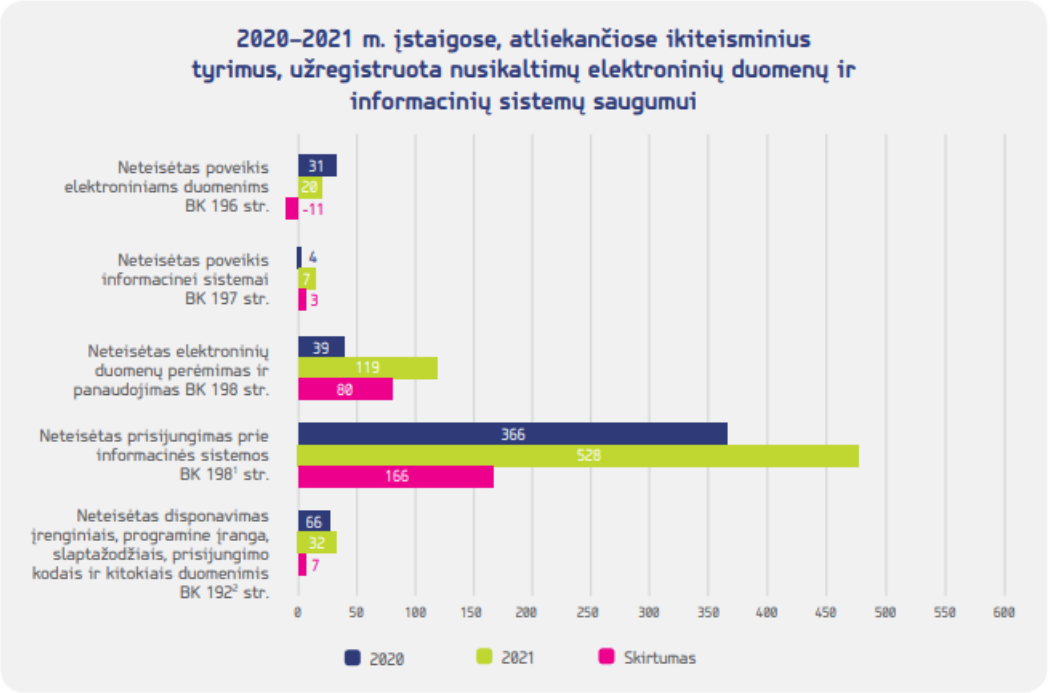
Detalesnė informacija apie kiekvieną iš LR BK 196–198 str. nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui

Pagal LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims“ 2021 m. buvo užregistruota 20 nusikaltimų (2020 m. - 31). 2021 m., palyginti su 2020 m., šių nusikaltimų užregistruota 11 atvejų, arba 35,5 proc., mažiau.

Pagal LR BK 197 str. „Neteisėtas poveikis informacinei sistemai“ 2021 m. užregistruoti 7 nusikaltimai (2020 m. - 4). 2021 m., palyginti su 2020 m., šių nusikaltimų užregistruota 3 atvejais, arba 75 proc., daugiau.

Pagal LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ 2021 m. užregistruota 119 nusikaltimų (2020 m. - 39). 2021 m., palyginti su 2020 m., šių nusikaltimų užregistruota 80 atvejų, arba 205,1 proc., daugiau.

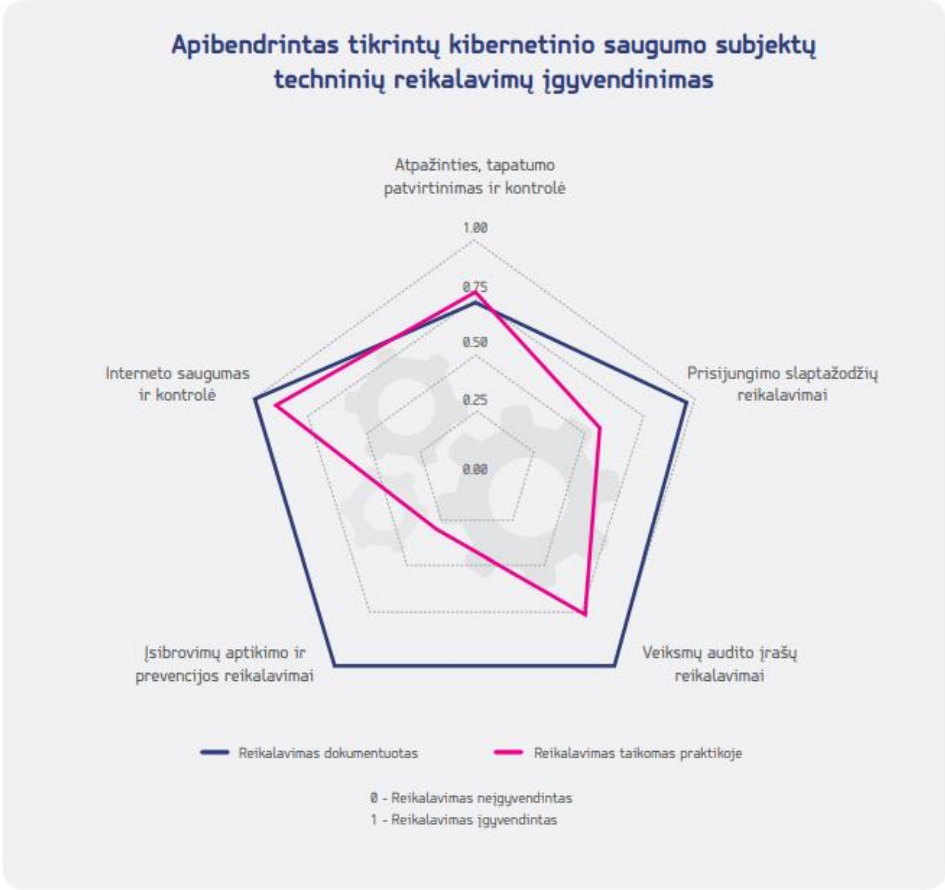
Pagal LR BK 198[1] str. „Neteisėtas prisijungimas prie informacinės sistemos“ 2021 m. užregistruoti 528 nusikaltimai (2020 m. - 366). 2021 m., palyginti su 2020 m., šių nusikaltimų užregistruota 162 atvejais, arba 44,3 proc., daugiau.



Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

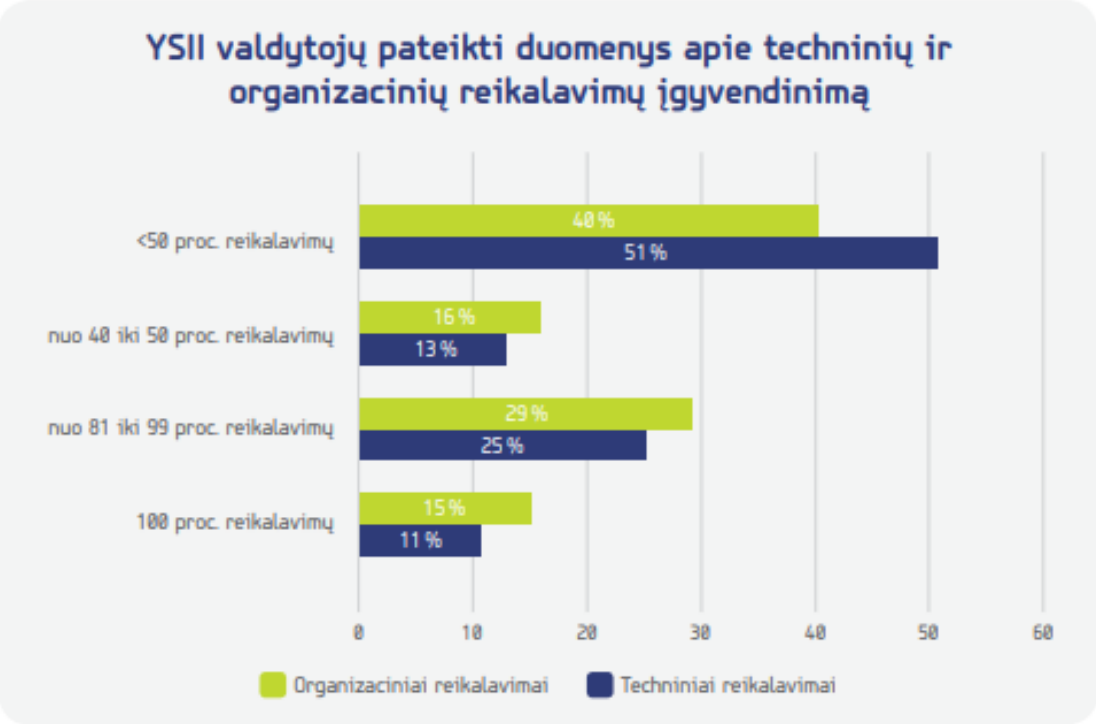
ADWISERY
wise solutions

NKSC atliktų patikrinimų rezultatai - reikalavimai daugeliu atvejų yra įgyvendinami formaliai: dokumentai periodiškai neatnaujinami, nesuderinti su atsakingomis institucijomis, nėra aiškiai priskirtų atsakomybių ir kontrolės.



Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions



NKSC 2021 m. atliktos apklausos duomenimis:

- visiškai arba beveik visiškai (nuo 81 iki 100 proc.) organizacinius kibernetinio saugumo reikalavimus teigia įgyvendinę 44 proc. valdytojų, o techninius kibernetinio saugumo reikalavimus – 36 proc. valdytojų;

Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

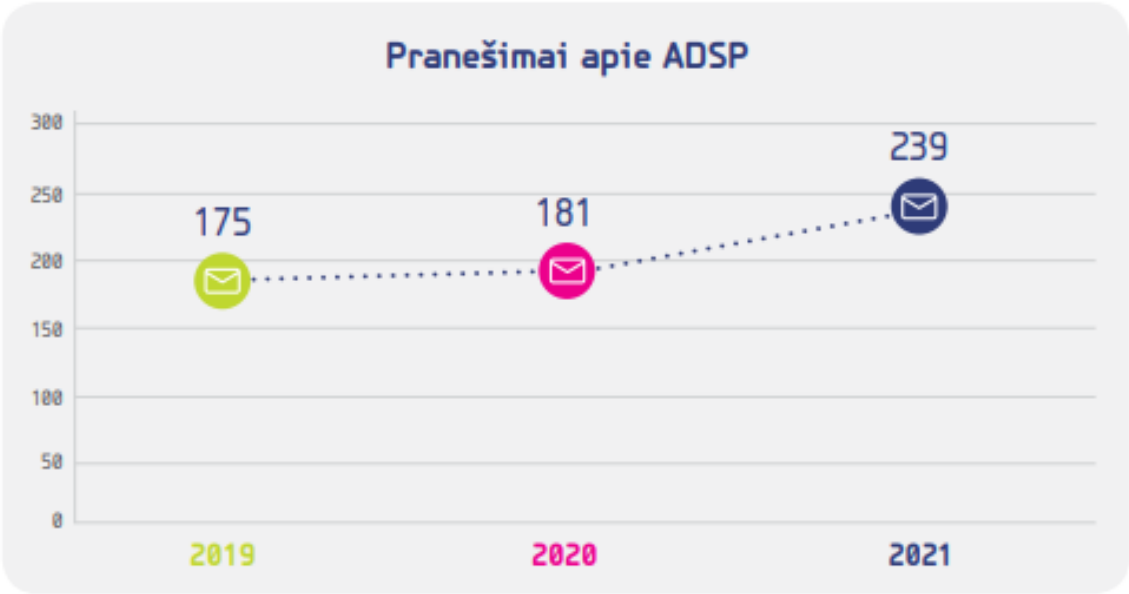
Atsakingas spragų atskleidimas

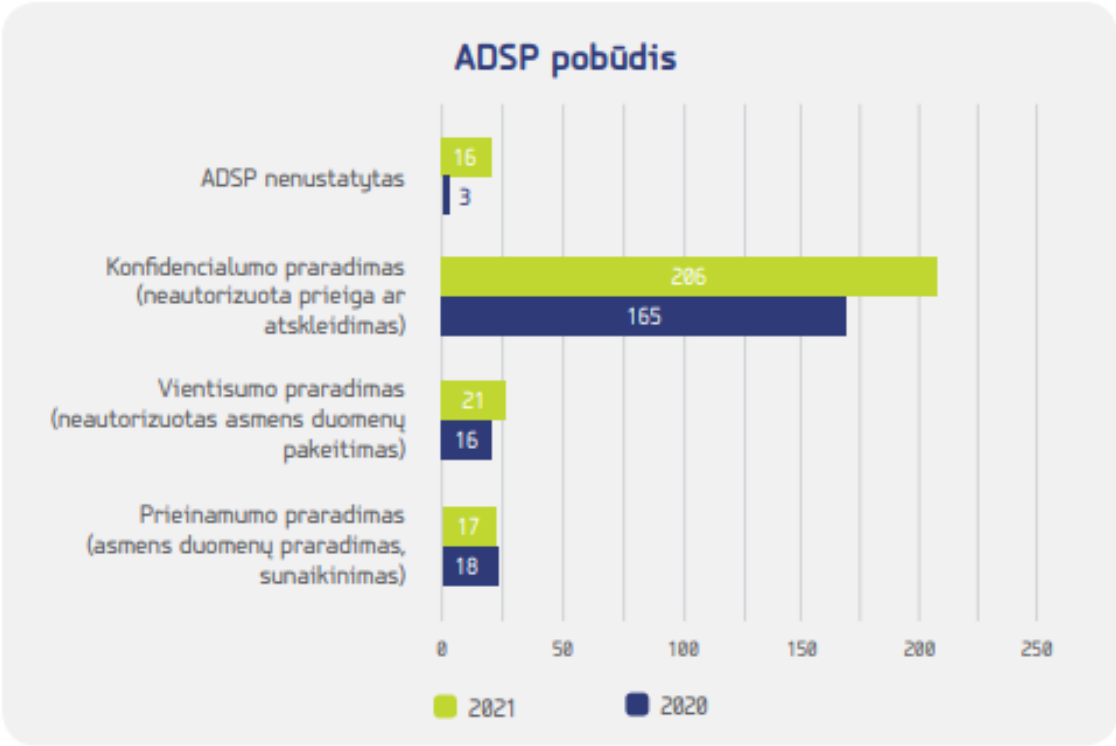
- 2021 m. birželio mėn. Lietuvos Respublikos Seimui patvirtinus Kibernetinio saugumo įstatymo pataisas, buvo reglamentuotas ir įsigaliojo atsakingo ryšių ir informacinių sistemų spragų atskleidimo procesas;
- Atsakingas spragų atskleidimas – informacija apie aptiktas spragas visų pirmiausia pateikiama pačiai organizacijai, kurios sistemose ar produktuose jos buvo aptiktos, ir (ar) spragų atskleidimo procesą koordinuojančiai institucijai (NKSC);
- NKSC 2021 m. gavo 81 pranešimą apie įvairias kibernetinio saugumo spragas.
- Daugiausia pranešimų sulaukta apie interneto svetainių ir žiniatinklio sistemų spragas. Taip pat buvo gauta keletas ypač svarbių pranešimų apie kritines spragas valstybinėse informacinėse sistemose bei plačiai naudojamoje programinėje įrangoje

Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

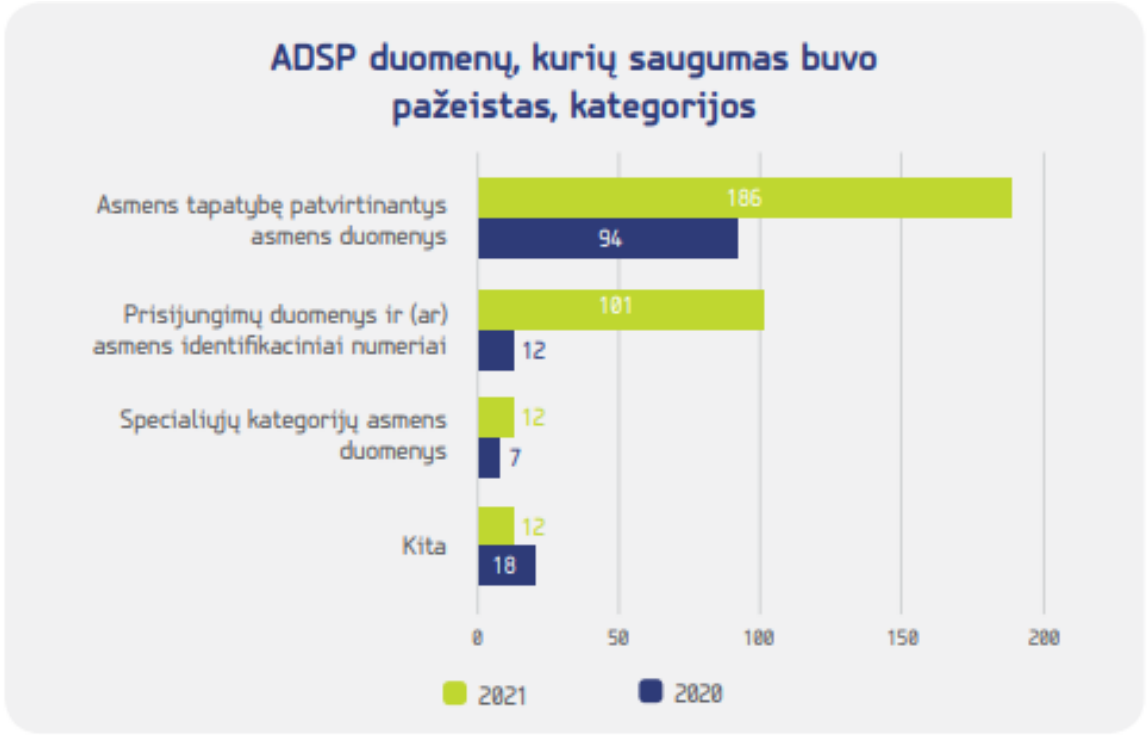
Per 2021 m. VDAI gavo 239 pranešimus apie ADSP Lietuvoje. Palyginti su 2020 m., ADSP pranešimų padaugėjo trečdaliu.

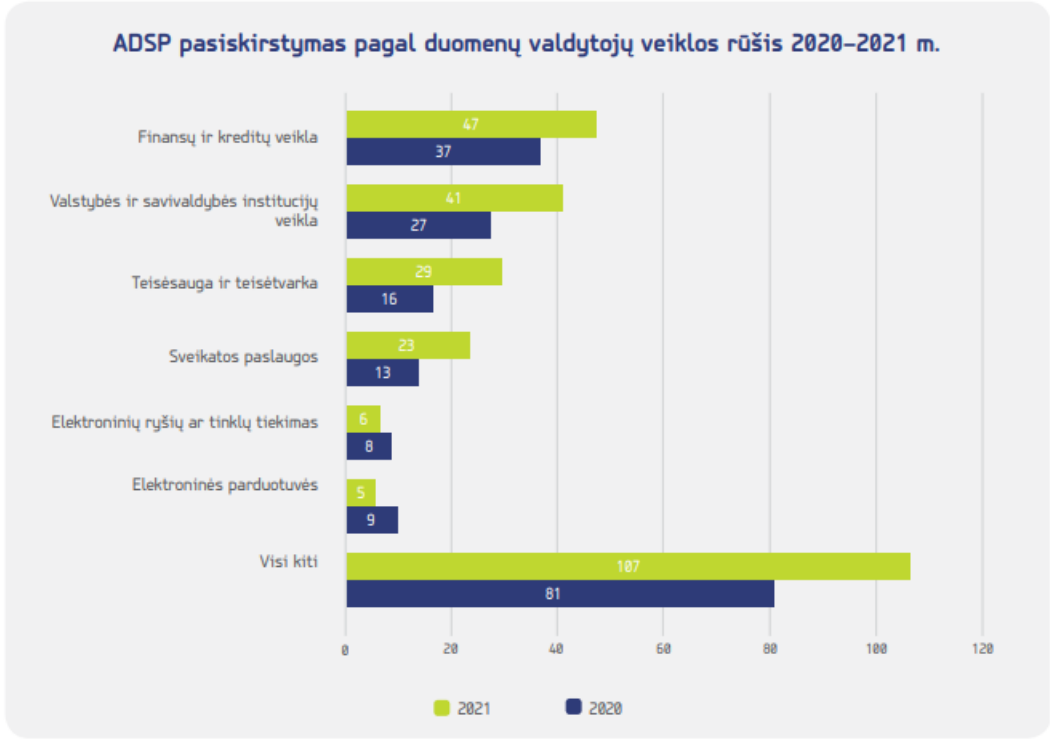




Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

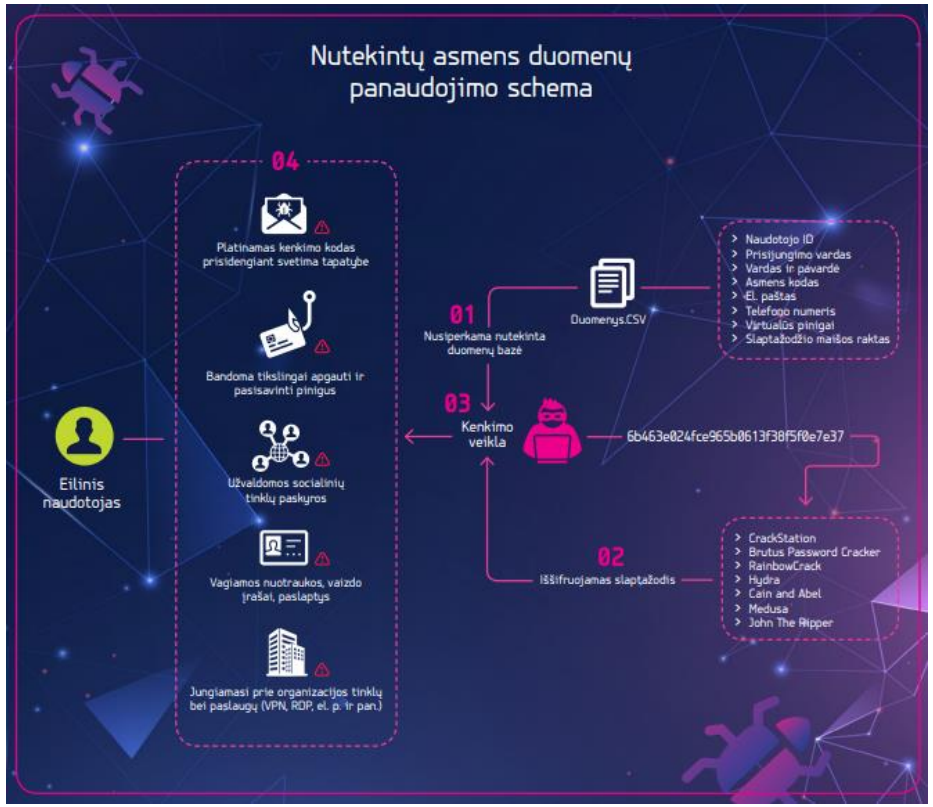
ADWISERY
wise solutions





Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions



Asmens duomenų nutekėjimo atvejai

- Pvz.: CityBee atvejis
- Nutekintais naudotojų slaptažodžiais ir prisijungimų duomenų sąrašais dažniausiai naudojamasi vykdant automatizuotus slaptažodžių spėjimus ar socialinės inžinerijos atakoms vykdyti pvz.: per el.pašto paskyras platinti kenkimo kodą ar užvaldyti socialinių tinklų paskyras.

Šaltinis: Nacionalinė kibernetinio saugumo būklės ataskaita už 2021 metus

ADWISERY
wise solutions

Švaraus stalo politika

ADWISERY
wise solutions

Darbuotojai turi laikytis švaraus stalo politikos:

- Darbo vietoje laikyti tik tuos dokumentus, kurie reikalingi atliekant jų darbo užduotis.
- Baigę darbą, nepalikti ant stalo dokumentų ar informacijos laikmenų su konfidencialia informacija. Ypač negali būti paliekami prisijungimo prie informacinių sistemų paskyrų duomenys (prisijungimo vardai ir slaptažodžiai).
- Dokumentus ar informacijos laikmenas su konfidencialia informacija saugoti rakinamuose stalčiuose ar tam skirtose spintose bei seifuose.
- Nebereikalingi ypač svarbūs dokumentai (konfidencialios informacijos) turi būti ne išmetami, o sunaikinami dokumentų naikikliu (nesant galimybės, smulkiai suplėšomi).
- Dokumentus, kuriuose pateikiama ypač svarbi, konfidenciali informacija, spausdinimą inicijavęs asmuo iš spausdintuvų turi išimti nedelsiant.

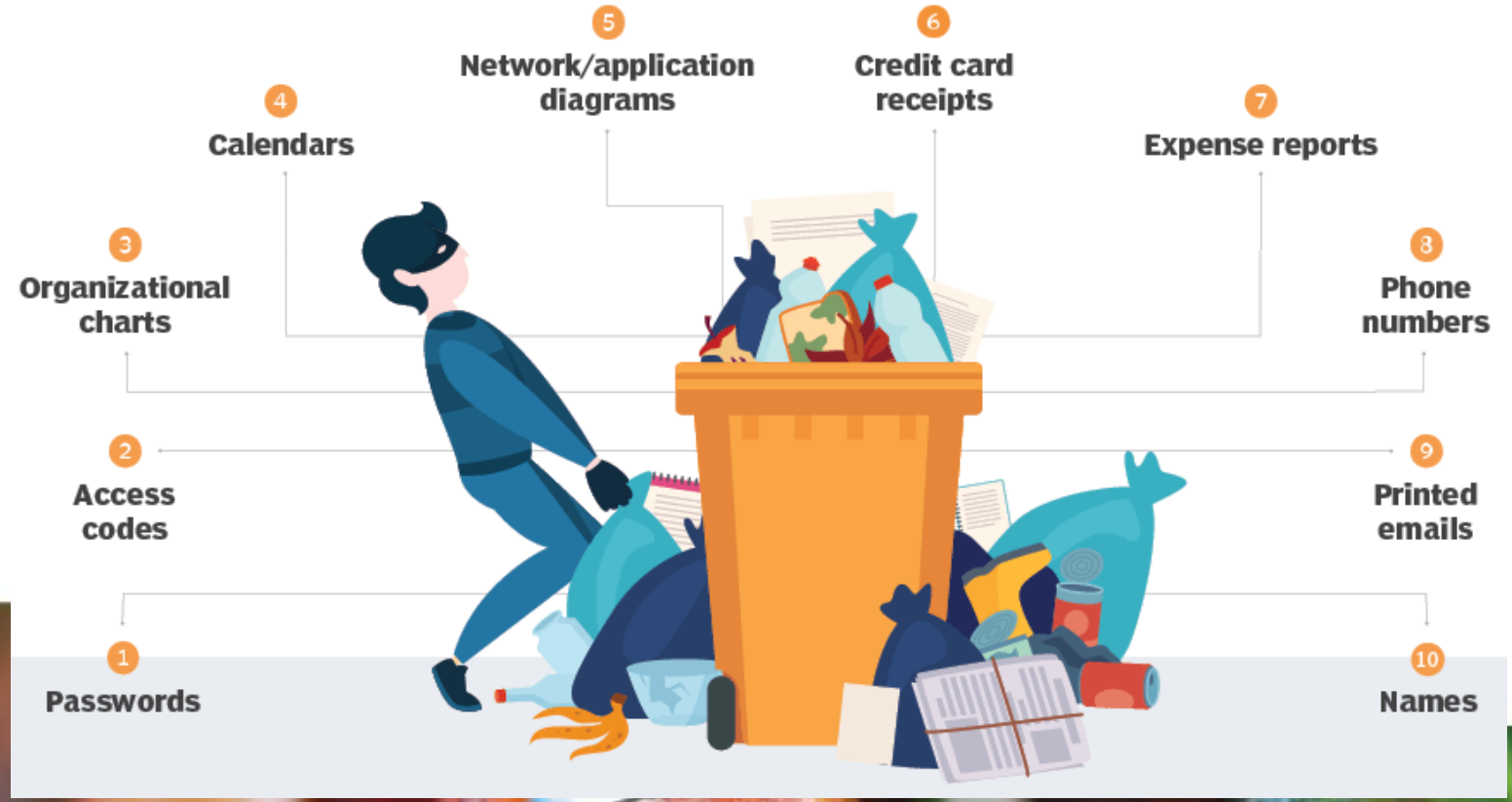
.

ADWISERY
wise solutions

„Nardymas šiukšlėse“ (angl. *Dumpster diving*)

Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



ADWISERY
wise solutions

Šnipinėjimo „per petį“ atakos viešumoje

Šnipinėjimo „per petį“ atakos apibūdina situaciją, kai užpuolikas gali fiziškai stebėti įrenginio ekraną ir klaviatūrą, kad gautų asmeninės informacijos. Tai vienas iš nedaugelio atakos būdų, kai užpuolikas turi būti fiziškai arti aukos.

Kai kurie užpuolikai šnipinėdami savo aukas gali naudoti miniatiūrines vaizdo kameras. Tikslas yra gauti tokią informaciją, kaip naudotojų vardai ir slaptažodžiai, asmenį identifikuojanti arba neskelbtina informacija.

ADWISERY
wise solutions

Darbuotojai turi laikytis švaraus ekrano politikos:

- Kompiuterio **darbalaukyje nelaikyti** konfidencialios informacijos.
- Nors trumpam palikdami darbo vietą, **įjungti kompiuterio darbalaukio užsklandą** su slaptažodžiu.
- Baigus darbą, uždaryti programų langus ir tinkamai **išjungti kompiuterį**.

CYBER RISKS FROM EMPLOYEE BAD HABITS

A company's commitment to data security must start with formal, and visible, security policies and procedures.
A cluttered workplace can lead to information breaches caused by human error.

25%

of workers said that they leave their computer unlocked and unattended.

63%

of confirmed data breaches involved weak, default or stolen passwords.

2016 Data Breach Investigations Report

1 in 3

Android smartphones are not secured with a lockscreen passcode, the most basic level of protection!

Data Labs data

£120,000

Fine for Heathrow Airport in 2018 after an employee lost a memory stick containing sensitive information about 60 people.

9%

of small business qwners have no policy in place for storing and disposing of confidential documents.

2017 Shred-it Information Security Tracker survey

Šaltinis: https://www.goldphish.com/post/how-a-clean-desk-and-clear-screen-helps-reduce-your-cyber-risk

ADWISERY
wise solutions

Kodėl darbuotojai nesilaiko švaraus stalo ir ekrano politikos:

- Tai reikalauja laiko ir pastangų;
- Darbuotojai tai suvokia kaip antraeilį dalyką ir todėl koncentruojasi į pirmo būtinumo darbus;
- Tiesiog nežino, kas yra švaraus stalo ir ekrano politika;
- Tai suvokia, kaip papildomas darbo funkcijos, kurios jų manymu jiems nepriklauso;
- Tingi arba piktybiškai to nedaro;

Švaraus stalo ir ekrano politikos įpareigoja laikytis informacijos saugumo standartas **ISO 27001** ir Bendrasis duomenų apsaugos reglamentas (toliau - **BDAR**) bei kiti teisės aktai. Ši politika turėtų būti patvirtinta organizacijos vidaus teisės aktuose. Už politikos nesilaikymą gali būti skiriamos drausminės nuobaudos.

ADWISERY
wise solutions

Kokios rizikos kyla nesilaikant švaraus stalo ir ekrano politikos:

- Kibernetinio incidento rizika.
- Asmens duomenų pažeidimo rizika.
- Konfidencialios informacijos atskleidimo rizika.

BDAR

ADWISERY
wise solutions

Asmens duomenų apsaugos pagrindai

ADWISERY
wise solutions

Duomenų gavėjas

Asmens duomenų saugumo pažeidimas

Asmens duomenys

BDAR sąvokos

Duomenų valdytojas

Priežiūros institucija

Duomenų subjekto sutikimas

Duomenų tvarkytojas

Duomenų tvarkymas

Duomenų apsaugos pareigūnas

BDAR duomenų tvarkymo principai

ADWISERY
wise solutions

Teisėtumo, sąžiningumo ir skaidrumo

Asmens duomenys duomenų subjekto atžvilgiu turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu

Tikslo apribojimo

Asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu

Duomenų kiekio mažinimo

Asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi

Tikslumo

Asmens duomenys turi būti tikslūs ir prireikus atnaujinami

Saugojimo trukmės apribojimo

Asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi

Vientisumo ir konfidencialumo

Asmens duomenys turi būti tvarkomi tokiu būdu, kad, taikant atitinkamas technines ar organizacines priemones, būtų užtikrintas tinkamas asmens duomenų saugumas

Atskaitomybės

Organizacija yra atsakinga už tai, kad būtų laikomasi duomenų tvarkymo principų, ir turi sugebėti įrodyti, kad jų laikomasi

ADWISERY
wise solutions

Duomenų tvarkymo teisėtumas

Sutartis | Teisinė prievolė | Gyvybinių interesų apsauga | Viešasis interesas | Teisėtas interesas | Sutikimas

Būtinas galiojančio sutikimo pagal BDAR aspektas yra reikalavimas, kad duotą sutikimą būtų galima lengvai atšaukti.

Privalomi sutikimo pagrindo elementai:

- Laisva valia duotas.
- Konkretus.
- Pagrįstas informacija.
- Nedviprasmiškas duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi jo asmens duomenys.

ADWISERY
wise solutions

Duomenų apsaugos pareigūnas

- Informuoja duomenų valdytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal **BDAR** ir konsultuoja juos šiais klausimais;
- Rengia ir tvarko organizacijos asmens duomenų politiką reglamentuojančius dokumentus;
- Sudaro ir tvarko duomenų tvarkymo veiklos įrašus;
- Padeda duomenų subjektams įgyvendinti jų teises;
- Atlieka kontaktinio asmens funkcijas, priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais.

Darbuotojas **sužinojęs apie galimą asmens duomenų**, tvarkomų automatizuotomis arba neautomatizuotomis priemonėmis, **saugos pažeidimą**

praneša savo

Darbuotojo vadovas, gavęs informaciją apie galimą asmens duomenų saugos pažeidimą, **informuoja duomenų apsaugos pareigūną**

ADWISERY
wise solutions

Pranešimas apie incidentus

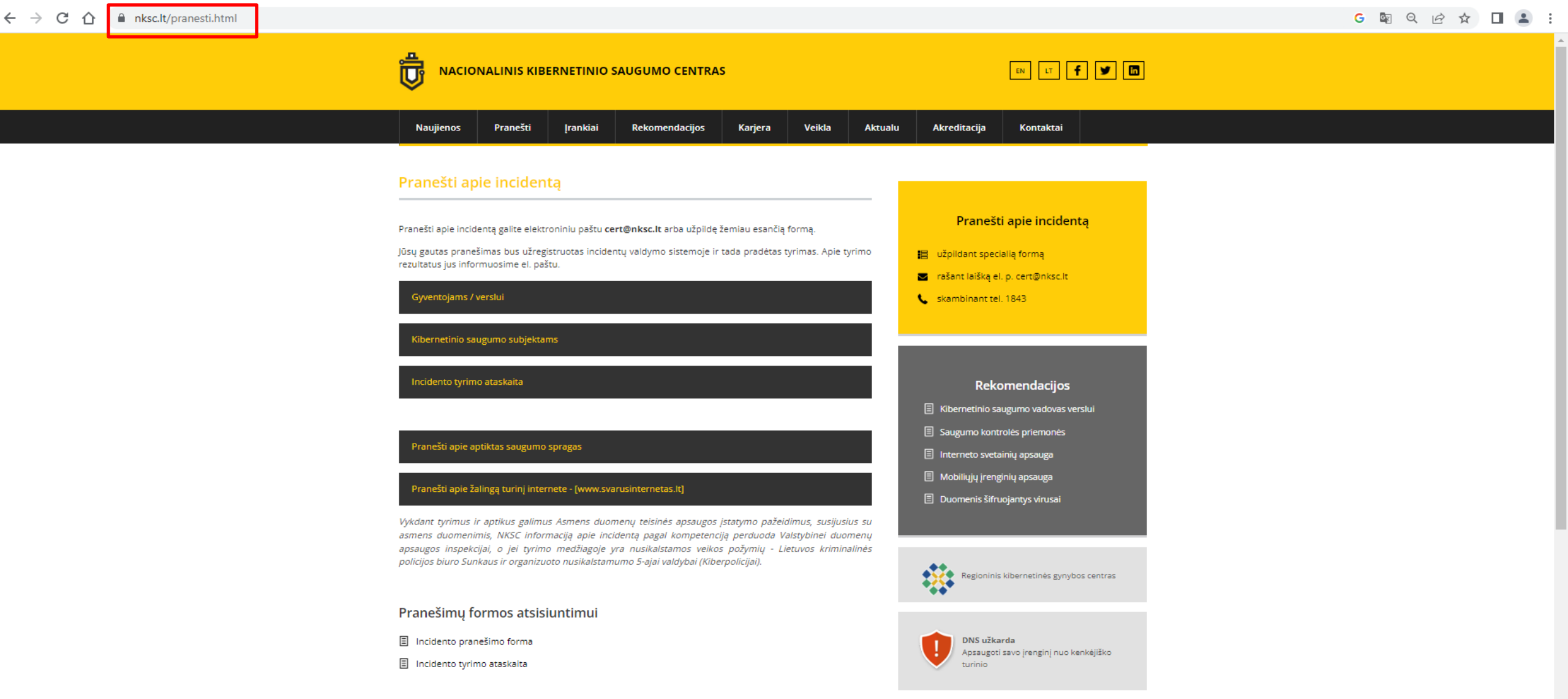
ADWISERY
wise solutions

Nacionalinis kibernetinio saugumo centras

Pranešti apie patirtas atakas, incidentus:

- užpildant specialią formą https://www.nksc.lt/pranesti.html
- rašant laišką el. p. cert@nksc.lt
- skambinant tel. 1843

ADWISERY
wise solutions



ADWISERY
wise solutions

Organizacija informuoja apie incidentą NKSC:

- **didelio poveikio** kibernetinius incidentus – **nedelsiant, bet ne vėliau kaip per 1 (vieną) valandą** nuo jų nustatymo,
- **vidutinio poveikio** kibernetinius incidentus – **ne vėliau kaip per 4 (keturias) valandas** nuo jų nustatymo,
- **nereikšmingo poveikio** kibernetinius incidentus – **periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną** teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

Asmenys, kuriems teisės aktuose nėra nustatytos pareigos apie kibernetinius incidentus pranešti NKSC, turi teisę tai padaryti savanoriškai. Tinkamas reagavimas į kibernetinius incidentus sumažina galimą patirti žalą, siekiant užtikrinti kibernetinį saugumą.

ADWISERY
wise solutions

Lietuvos Respublikos administracinių nusižengimų kodeksas

479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatų dėl pareigos teikti informaciją pažeidimai

KEISTA:
1. 2017 12 19 įstatymu Nr. XIII-922 (nuo 2018 01 01)
(TAR, 2017, Nr. 2017-21594)
2. 2018 06 30 įstatymu Nr. XIII-1427 (nuo 2018 07 12)
(TAR, 2018, Nr. 2018-11734)

1. Informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

2. Nacionalinio kibernetinio saugumo centro nurodymų kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, ir kibernetinio saugumo būklei įvertinti, nevykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

3. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamų veikų požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

4. Šio straipsnio 1, 2, 3 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki vieno tūkstančio keturių šimtų keturiasdešimt eurų.

ADWISERY
wise solutions

Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 5-oji valdyba

Pranešti jei kibernetinis incidentas gali turėti nusikalstamos veikos požymių:

- užpildant specialią formą https://www.epolicija.lt/report
- rašant laišką el. p. cyberpolice@policija.lt
- skambinant tel. 112

ADWISERY
wise solutions

ePolicija.lt

Pranešimas policijai | El. paslaugos | PRISIJUNGTI | LT

Pranešimas policijai

Ar šiuo metu reikalinga skubi pagalba?

Jeigu Jums ar kitiems žmonės yra reali grėsmė gyvybei, sveikatai ar saugumui, Jūsų turtui kyla reali grėsmė (kėsinamasi pagrobti Jūsų automobilį, kėsinamasi sugadinti ar sunaikinti Jūsų turtą), šiuo metu matote vykstančias muštynes, **skambinkite 112**.

Pagalba nukentėjusiems nuo nusikaltimo >

Pagalba patyrusiems smurtą >

Kokiu būdu pranešite?

- (•) Pateiksiu savo duomenis — Rekomenduojama
- ( ) Pranešiu anonimiškai

Kas atsitiko?

- ( ) Pažeistos Kelių eismo taisyklės
- ( ) Įvykdyta vagystė, sukčiavimas, turto sunaikinimas, sugadinimas
- ( ) Įvyko smurtas artimoje aplinkoje
- ( ) Padarytas kūno sužalojimas, sukeltas fizinis skausmas, įvyko muštynės
- ( ) Vyko triukšmas, konfliktas ar kitas viešosios tvarkos pažeidimas
- ( ) Radau ar pamečiau daiktą
- ( ) Nei vienas iš išvardintų

Įspėjimas dėl melagingų pranešimų

Pranešimas apie nebūtą nusikaltimą ar administracinį nusižengimą užtraukia baudžiamąją atsakomybę (**Lietuvos Respublikos baudžiamojo kodekso 236 straipsnis**) arba administracinę atsakomybę (**Lietuvos Respublikos administracinių nusižengimų kodekso 224 straipsnio 2 dalis**).

BDAR

Valstybinė duomenų apsaugos inspekcija

Pranešti jei kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais:

- užpildant specialią formą https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima
- rašant laišką el. p. ada@ada.lt
- Dokumentą pateikiant registruotu paštu ar įteikiant vietoje VDAI patalpose

ADWISERY
wise solutions

2018 m. gegužės 25 d. pradėjus taikyti BDAR apie duomenų saugumo pažeidimus Valstybinei duomenų apsaugos inspekcijai privalo pranešti visi duomenų valdytojai, ne tik tvarkantys valstybės informacinius išteklius ir viešųjų ryšių tinklus bei bendrovės viešųjų elektroninių ryšių paslaugų teikėjos, tais atvejais, jei kyla didelis pavojus duomenų saugumui.

Apie asmens duomenų saugumo pažeidimus privaloma pranešti Valstybinei duomenų apsaugos inspekcijai per **72 valandas** nuo tada, kai ji sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša Valstybinei duomenų apsaugos inspekcijai.

Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus asmenų teisėms ir laisvėms, duomenų valdytojas nedelsdamas turi pranešti apie tai ir patiems žmonėms.

ADWISERY
wise solutions

vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima

Pranešimas apie asmens duomenų saugumo pažeidimą

2018 m. gegužės 25 d. pradėjus taikyti Bendrąjį duomenų apsaugos reglamentą (BDAR) visos organizacijos, patyrusios duomenų saugumo pažeidimus, privalo ne tik imtis veiksmų pažeidimams pašalinti, bet ir informuoti apie tai Valstybinę duomenų apsaugos inspekciją.

Kokiu būdu galima pateikti Valstybinei duomenų apsaugos inspekcijai pranešimą apie duomenų saugumo pažeidimą:

1. Užpildant **El. paslaugos formą El. valdžios vartuose**.
2. Naudojantis **El. siuntų sistema E.pristatymas** (siuntos pristatymas E.pristatymo sistemoje turi teisinę ir įrodomąją galią, atitinkančią registruotojo laiško įteikimą).
3. **El. parašų pasirašytų** dokumentų siuntimas el. paštu ada@ada.lt.
4. Dokumento pateikimas **registruotu paštu ar įteikimas vietoje** VDAI patalpose.

Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojama forma (Aktuali redakcija su 2022-07-25 Nr. 1T-105 (1.12.E) pakeitimais)

Informuojame, kad Jums kreipiantis į Valstybinę duomenų apsaugos inspekciją su pranešimu apie asmens duomenų saugumo pažeidimą Jūsų asmens duomenis Valstybinė duomenų apsaugos inspekcija tvarkys tikrinimų (prevencinių, ES informacinių sistemų (Šengeno, Muitinės, Vizų, Eurodac), pranešimų apie asmens duomenų saugumo pažeidimus, kt.) ir auditų atlikimo ir, kai taikoma, tarptautinio bendradarbiavimo, įskaitant įgyvendinant nuoseklumą, užtikrinimo tikslais. Daugiau informacijos apie Jūsų asmens duomenų tvarkymą (teisinius pagrindus, saugojimo terminus, duomenų subjekto teises ir kt.) skaitykite prie šio laiško prisegtame **Privatumo pranešimas**

ADWISERY
wise solutions

Socialinės inžinerijos teoriniai aspektai

ADWISERY
wise solutions

Socialinė inžinerija – tai manipuliavimas žmonėmis, jų silpnybėmis, siekiant apeiti informacijos apsaugos sistemas bei pagrobti ir užvaldyti konfidencialią informaciją.

Socialinė inžinerija – tai piktavalio ir potencialios jo aukos kontaktas, manipuliuojant pastarojo emocijomis, siekiant įgyti asmeninę informaciją, prieigą prie duomenų ar kito skaitmeninio turto.

Pagrindinės socialinės inžinerijos taikymo sritys:

- Įvairaus tipo kritinių duomenų vagystės,
- Pramoninis šnipinėjimas,
- Finansinės machinacijos,
- Sukčiavimas,
- Šantažas,
- Informacijos rinkimas.

ADWISERY
wise solutions

Pagrindiniai socialinės inžinerijos principai:

- Įtikinėjimas - Apsimetama pažįstamais žmonėmis, imituojamos interneto svetainės, el. p. adresai, pateikiami naudotojui žinomi faktai;
- Konsensusas - Bandoma pagrįsti, kad prašomi atlikti veiksmai yra veikiantys, autorizuoti bei nekenksmingi. Patikimumui pateikiami pavyzdžiai;
- Stygius - Bandoma paveikti auką, kad šiam skubiai neatlikus veiksmų jis praras pinigus, galimybes įsigyti prekę;
- Familiarumas - Referuojama į artimą ryšį, apsimetama pažįstamais žmonėmis, bendradarbiais ir pan.;
- Pasitikėjimas - Kuriamas pasitikėjimas, apsimetama autoritetais;
- Skubumas - Prašoma atlikti veiksmus kuo skubiau.

ADWISERY
wise solutions

Socialinės inžinerijos tikslas – vartotojui nesuvokiant **išgauti** iš jo privačią **informaciją**, sužinoti, tai, ko jis realiame gyvenime nenorėtų atskleisti tretiesiems asmenims.

Daug paprasčiau apgaulės būdu priversti vartotoją atskleisti savo slaptažodį, negu sugaišti daug laiko bandant įsiskverbti į vartotojo programinę arba techninę įrangą.

Deja, ir toliau yra laikomasi nuomonės, kad kibernetinis saugumas yra **informacinių technologijų specialistų kompetencijos ir techninės įrangos** klausimas. Įvykus kibernetiniam incidentui, atsakomybė dažniausiai yra perkeliama naudotojui, kuris iki įvykio dažniausiai deramai neinformuojamas ar nešviečiamas, kaip valdyti su kibernetiniu saugumu susijusias rizikas

ADWISERY
wise solutions

Informacijos konfidencialumo kriterijai:

Slapta

- nėra vieša ir negali būti atskleista, o prireikus galėtų būti atskleista tik tokia apimtimi, kiek to reikalauja organizacijos interesai.

Vertinga

- kuria organizacijai pridėtinę vertę, yra svarbi jos veiklos tęstinumui, kai galimas tokio pobūdžio informacijos konfidencialumo praradimas sukeltų organizacijai veiklos sutrikdymo, finansines, reputacines, kitokio pobūdžio grėsmes.

Saugoma

- taikomos protingos, pakankamos pastangos tokios informacijos apsaugai ir organizacija ir darbuotojai deda tinkamas ir adekvačias pastangas tokią informaciją apsaugoti.

Konfidencialiai informacijai priskiriama:

I. ŽINIOS APIE PERSONALĄ IR VALDYMO STRUKTŪRĄ,

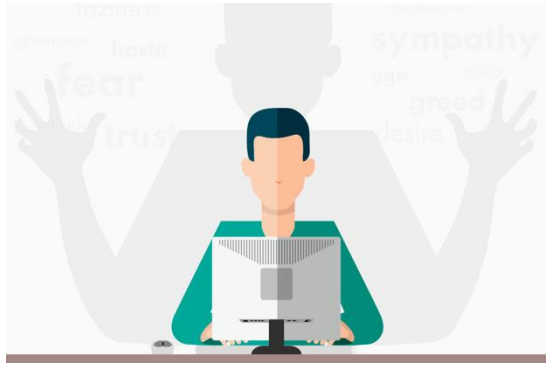
II. ŽINIOS APIE VALDYMO PROCESUS,

III. FINANSINĖ – EKONOMINĖ INFORMACIJA,

IV. KITA INFORMACIJA (bet kokia informacija, kuri darbuotojui buvo atvirai pateikta arba atskleista nurodant, kad tokia informacija turi būti laikoma konfidencialia ir/ar **kurios atskleidimas galėtų padaryti žalą organizacijai** ar ją pateikusiems asmenims).

ADWISERY
wise solutions

Socialinės inžinerijos psichologiniai įtakos veiksniai (I)



Socialinis programavimas. Įtakos instrumentas, kuriuo siekiama paveikti žmonių elgesį, kad jie **pradėtų elgtis pagal piktavalio primestą elgesio modelį**.

Pripažinimas (atlygis). Sukuriama iliuzija, kad bus gaunama kažkokia nauda.

Smalsumas. Įdomiai suformuluotas žinutės tekstas arba netikėtas, tačiau pažįstamas šaltinis sudomina. Išnaudojamas žmonių **noras pirmauti**, norėdami parodyti savo vertę, be svarstymų **išduos piktavaliui jo prašomą informaciją**.

Baimė. Piktavaliai, žinodami, kad žmogaus **emocijos** ir **protas ne visada bendradarbiauja**, siekia įbauginti, paskatinti priimti skubų ir gerai neapgalvotą sprendimą.

ADWISERY
wise solutions

Socialinės inžinerijos psichologiniai įtakos veiksniai (II)

Pasitikėjimas. **Daug lengviau yra patikėti gauta informacija, nei ją tikrinti ir kritiškai įvertinti**. Žmonėms gali būti tiesiog nepatogu kažkam prieštarauti ir išreikšti tam tikras abejones, ypač jei kalba visuomenėje labai gerai žinomas veikėjas. Svarbiausias faktorius – autoritetas.

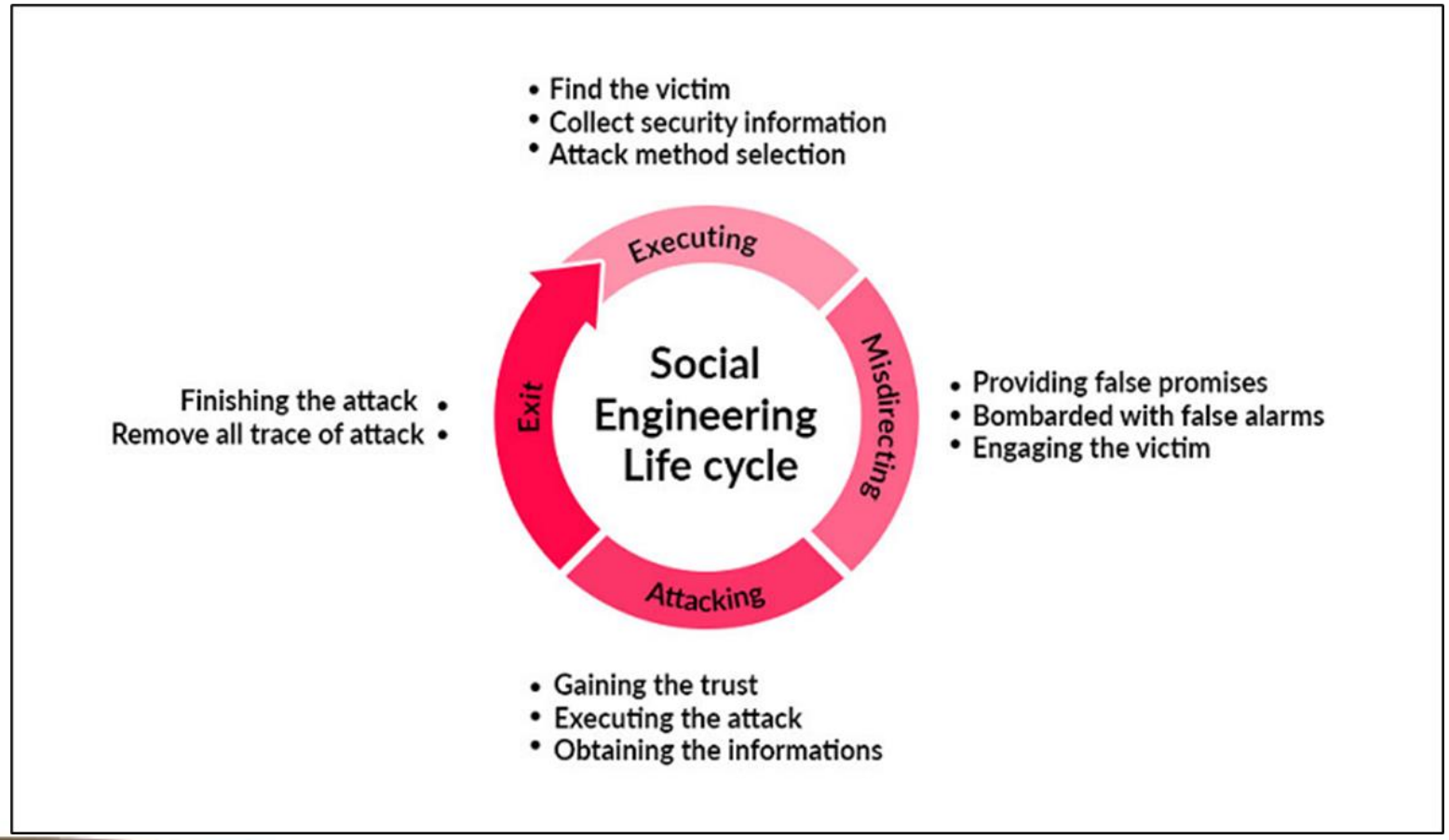
Pranašumas. Būsena, kai jautiesi **daugiau žinančiu ir turinčiu didesnę vertę** lyginant su kitais. Sukčiavimo aukai ypač svarbi kitų nuomonė, ji gali būti perdėtai giriama.

Empatija. Socialinės inžinerijos metodą naudojantis apgavikas gali manipuliuoti **aukos emocijomis** – pagalba, užuojauta, globa, motinystė ir tėvystė.

Skubėjimas. Priimami **skubūs ir neapgalvoti sprendimai**, gavus laišką neatkreipiamas dėmesys į jo šaltinį ir turinį.

ADWISERY
wise solutions

Socialinės inžinerijos gyvavimo ciklas



ADWISERY
wise solutions

Socialinės inžinerijos metodai (I)

Pretekstas (angl. *Pretexting*). Kibernetinis nusikaltėlis didelį dėmesį skiria patikimo scenarijaus kūrimui, kurį panaudoja kaip pretekstą bandydamas pavogti savo aukų informaciją ar asmeninius duomenis. Sukuriamas melagingas pasitikėjimo jausmas, gali būti apsimetama – bendradarbiu, privačios arba valstybės įmonės darbuotoju. Pavogti asmens duomenys yra panaudojami tapatybės vagystėms ir antriniams išpuoliams įvykdyti.

Panika (angl. *Scareware*). Kibernetinių nusikaltėlių aukos atakuojamos melagingais pavojaus signalais ir fiktyviais grasinimais. Pavyzdžiui, interneto naršyklės lange iššoka reklaminės juostos įspėjančios apie pavojų jūsų kompiuteriui, kuriose rašoma „Jūsų kompiuteris užkrėstas virusais, išvalyti“, „Jūs turite virusų, paspauskite šią nuorodą“ ir t. t. Paspaudus tokią reklamą nukreipiama į užkrėstą svetainę arba pradedama siųsti kenkėjiška programinė įranga**.**

ADWISERY
wise solutions

Masalas (angl. *Baiting*). Apgavystei panaudojamas melagingas pažadas, išnaudojant sukčiavimo aukos godumą ar smalsumą. Aukos įviliojamos į spąstus, pavagiama jų asmeninė informacija arba užkrečiamos informacinės sistemos kenkėjiška programine įranga.

Pavyzdžiui, kibernetiniai nusikaltėliai matomose vietose palieka masalą – kenkėjiškų programų užkrėstą USB raktą, tikėdamiesi, kad auka jį ras ir juo pasinaudos. Masalo efektui sustiprinti, USB raktas gali būti išskirtinės išvaizdos, taip pat panaudojamas žinomos įmonės logotipas ir užrašomas tekstas „konfidencialu“, „neskaityti“, „privatu“ ir t.t.

Sukčiavimas nebūtinai turi būti vykdomos fiziniame pasaulyje, internete viliojančios reklamos sukčiavimo aukas nukreipia į kenksmingas svetaines arba siūlo atsisiųsti įvairaus skaitmeninio turinio kartu su kenkėjiška programine įranga**.**

ADWISERY
wise solutions

Sukčiai socialinės inžinerijos metodais bando išvilioti naudotojų pinigus prašydami **atlikti pinigines perlaidas, apsimesdami organizacijų vadovais, siūlydami įsigyti prekes suklastotose interneto svetainėse.**

Tai neapsiriboja:

- elektroninių laiškų,
- suklastotų interneto svetainių kūrimu
- žinučių socialiniuose tinkluose siuntimu
- piktavaliai gali paskambinti telefonu,
- bandyti susisiekti kitais būdais.

Socialinės inžinerijos incidentų padaugėja **šventiniais periodais**, kai naudotojai yra viliojami **nuolaidomis**, ir **vertingai atrodančiais pasiūlymais** ir pan.

ADWISERY
wise solutions

„***Vishing***“ yra sukčiavimo praktika, kai siekiama gauti informacijos ir/ar išvilioti pinigų, apsimetus kitu asmeniu paskambinus telefonu aukai, pvz.:

- IT paslaugų teikėju.
- Banko darbuotoju.
- Kokios nors valstybės institucijos darbuotoju.
- Ir t.t.

ADWISERY
wise solutions

Kaip apsisaugoti:

- Išlikite skeptiškas, jei sulaukiate netikėto ar neprašyto skambučio iš nepažįstamo asmens, jums nereikėtų skubėti atskleidžiant jam dominamą informaciją (dažniausiai vidinis balsas sako, kad kažkas yra negerai).

- Saugokitės, klausimų kurie jums užduodami. Jei skambinantis asmuo teigia, kad jis yra iš įmonės ar pardavėjo, su kuriuo glaudžiai bendradarbiaujate, bet jo vardo neatpažįstate, neatsakykite į jo klausimus. Vietoj to, įsiminkite jų vardą ir informuokite, kad dabar kalbėti negalite. Baigę pokalbį paskambinkite tiesioginiam tos įmonės ar pardavėjo kontaktui ir paklauskite apie prieš tai skambinusį asmenį.

- Atkreipkite dėmesį, jei jūsų prašo eiti į svetainę, kurioje paprastai nesilankote, arba ji šiek tiek skiriasi nuo tos, prie kurios paprastai prisijungiate. Sukčius gali bandyti atsiųsti jums el. laišką su nuoroda; atkreipkite dėmesį į el. pašto adresą (gali skirtis tik vienas ar du simboliai nuo to, kurį paprastai atpažįstate). Nespauskite jokių nuorodų ir neatidarykite jokių priedų, kurių nesitikėjote.

ADWISERY
wise solutions

Sukčiai niekada neišnyks; jie tiesiog keičia savo metodus, kad atitiktų besikeičiančias technologijas. Apsisaugokite nuo šios taktikos:

- **Būkite atsargūs**, kai kas nors jums skambina, kurių neatpažįstate.
- Jei kyla klausimų, kokią informaciją ką tik kam nors suteikėte, nedelsdami **informuokite savo vadovą ar kitus už saugumą atsakingus asmenis** - saugos įgaliotinį, IT administratorių, saugos įmonę ir t.t.
- **Būtinai pakeiskite visus slaptažodžius**, kuriuos galėjote netyčia arba tiesiogiai kam atskleisti.
- **Išlikite ramūs**. Jei įtariate, kad tai vyksta, nediskutuokite su įmone susijusių dalykų be aiškaus įmonės leidimo. Užduokite klausimų, prašykite patvirtinimo.

ADWISERY
wise solutions

„*Fišingas*“ (angl. *Phishing*) – tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis.

Daugybei žmonių siunčiami suklastoti laiškai su kenksmingu programiniu kodu prisegtuke arba nuorodoje, pranešantys netikėtą *loterijos laimėjimą, programinės įrangos gedimą, neapmokėtą sąskaitą*, kurią neva siunčia jūsų vadovas arba programinės įrangos teikėjas.

Sukčiai išsiunčia tūkstančius vienodo turinio žinučių ir tikisi, jog keli ar keliolika vartotojų „*užkibs ant kabliuko*“. Beasmenės žinutės tampa vienu iš pirmųjų pavojaus signalų.

Dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis.

Nr.	Pavojaus signalas
1	Beasmenė žinutė
2	Žinutė iš paslaugų teikėjo kurio paslaugomis niekada nesinaudojote
3	Laiške nurodytos neaiškios nuorodos
4	Laiške prisegti neaiškūs priedai (failai)
5	Įtartinas tinklapio adresas
6	Nenaudojamas „https“ protokolas

ADWISERY
wise solutions

Šaltinis: Nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2022“ ataskaita

Pratybų metu tikrintas personalo atsparumas suklastotiems laiškams (phishing):

- Išsiųsta virš **56 tūkst.** Laiškų dalyvaujančių organizacijų darbuotojams;
- 4,7% (**2,6 tūkst.)** iš jų paspaudė nuorodą, bet duomenų nesuvedė;
- 8,1% (**4,5 tūkst.)** iš jų atidarė nuorodą ir įvedė duomenis.

Rezultatai rodo, kad **būtina stiprinti** kibernetinio saugumo subjektų personalo **atsparumą** suklastotiems laiškams, nuolat **vykdyti** personalo **švietimą** ir **simuliacijas**.

ADWISERY
wise solutions

Spear-phishing – sudėtingesnė nei reguliari *phishing* ataka, piktavaliai analizuoja potencialių aukų asmeninę informaciją ir pagal ją formuojamas *phishing* laiškas. Tokie laiškai yra sunkiai identifikuojami naudojant *phishing* filtrus.

ADWISERY
wise solutions

Socialinės inžinerijos rizikų valdymo rekomendacijos

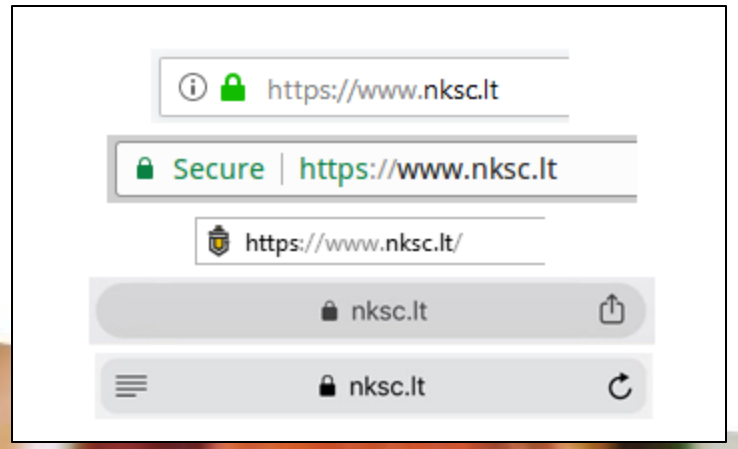
Nr.	Grėsmė	Rekomendacija
1	Naudotojas paspaus nuorodą, vedančią į kenkėjišką puslapį.	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar rodomas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
2	Naudotojas įves savo slaptažodį suklastotoje interneto svetainėje.	Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. naudojamas SSL sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių faktorių autentifikavimo įrankius (pavyzdžiui, slaptažodis, mobilusis įrenginys, piršto antspaudas).
3	Naudotojas pats atskleis savo prisijungimo slaptažodžius piktavaliui.	Naudoti mažiausiai dviejų faktorių autentifikavimą, saugoti savo prisijungimo slaptažodžius, jokiais būdais nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone.
4	Naudotojas atliks piniginę perlaidą piktavaliams.	Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas); prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pavyzdžiui, pasitikslinti aplinkybes paskambinus telefonu.
5	Naudotojas įdiegs kenkimo PĮ.	Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pavyzdžiui, iš nelegalių PĮ platinimo šaltinių).
6	Naudotojas pasiduos piktavalio manipuliacijoms.	Neatlikti skubotų veiksmų, nepasiduoti emocijoms, detaliai išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.

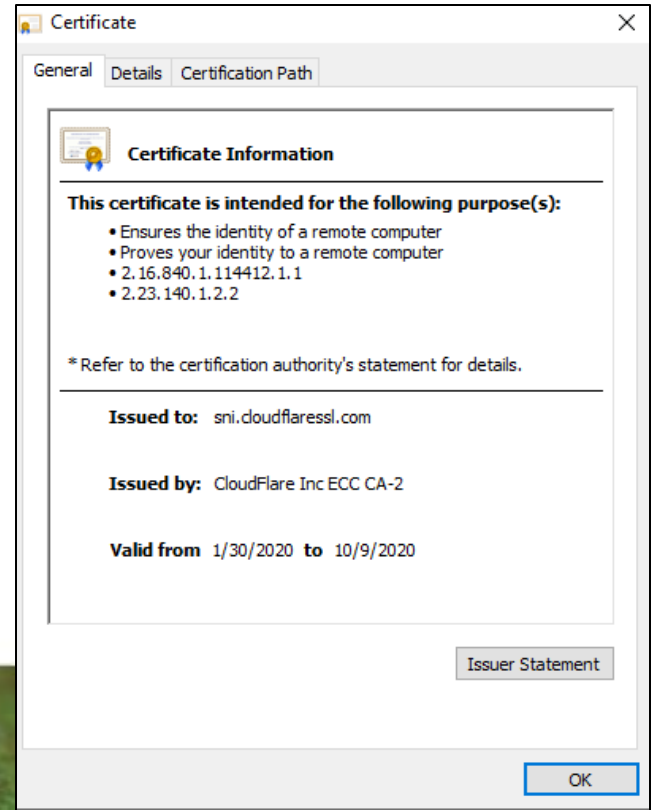
Šaltinis: Nacionalinis kibernetinio saugumo centras

ADWISERY
wise solutions

- Jeigu jungiatės prie interneto svetainės, kuria bus perduodami svarbūs duomenys, įsitikinkite, kad ji pasiekiama saugiu SSL sertifikatu. Tokį saugumo lygį parodo svetainės adreso pradžioje esantis trumpinys ***https*** arba **pavaizduotas spynelės** simbolis. Paspaudus spynelės simbolį galima sužinoti daugiau informacijos apie *išduotą saugumo sertifikatą, svetainės savininką ir pan*.

- Įsitikinkite, kad interneto svetainės adresas, kuriame įvedate savo duomenis, *tikrai teisingas* - atkreipkite dėmesį, ar nėra praleistų raidžių, ar raidės nesukeistos vietomis ir pan.





ADWISERY
wise solutions

Saugus naršymas. El. paštas ir socialiniai tinklai (I)

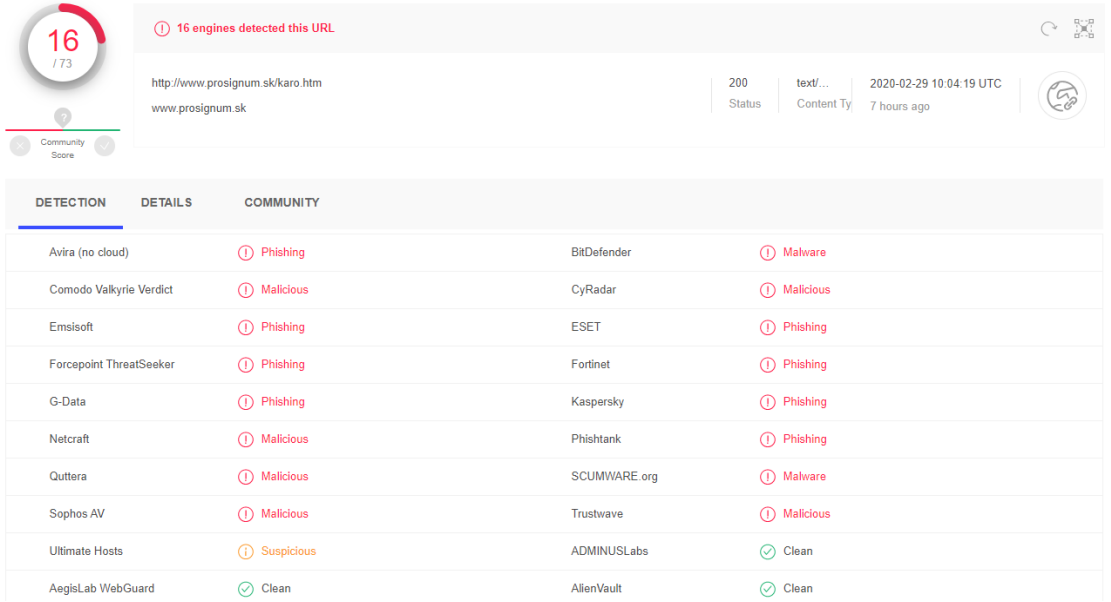
- Nespauskite ir neatidarinėkite nuorodų e. laiškuose ar žinutėse, kurias gavote iš nepažįstamų asmenų, nežinomų šaltinių. Įsitikinkite, kad laiško siuntėjas iš tiesų yra tas, kuris nurodytas lauke „Nuo“.

- Jeigu gavote įtartiną el. laišką ar žinutę nuo pažįstamo asmens, pasiskambinkite arba kontaktuokite su juo kitais kanalais ir įsitikinkite, kad asmuo iš tiesų Jums kažką siuntė.

ADWISERY
wise solutions

- Prisijungimus prie e-bankininkystės, el. pašto ir kitų paskyrų atlikite iš pagrindinio žinomo paslaugų teikėjo puslapio, o ne spausdami nuorodas, gautas el. laiškais ir žinutėmis.

- Gautus įtartinus failus galite savarankiškai pasitikrinti VirusTotal svetainėje.



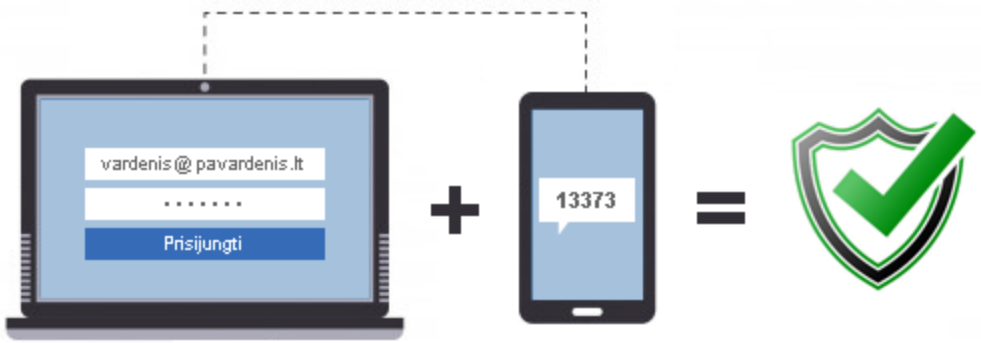
Šaltinis: https://www.virustotal.com/gui/home/upload

Kelių veiksnių autentifikacija

Naudokite kelių veiksnių (faktorių) autentifikaciją. Vis daugiau internetu pasiekiamų paslaugų teikėjų suteikia galimybę naudoti šį papildomą apsaugos lygmenį.

3 pagrindiniai autentifikacijos būdai:

- Tai, ką žinote: jūsų slaptažodis, PIN, paskyros numeris ar betkokia kita skaitmenų ar raidžių seka;
- Tai, ką turite: USB saugos raktas, telefonas ar betkokia kita technologija kurią galite turėti fiziškai;
- Tai, kuo esate: jūsų pirštų antspaudas, akies, veido atvaizdas arba tiesiog – biometriniai duomenys.



Dviejų veiksnių autentifikacijos veikimo principas

Saugūs slaptažodžiai (I)

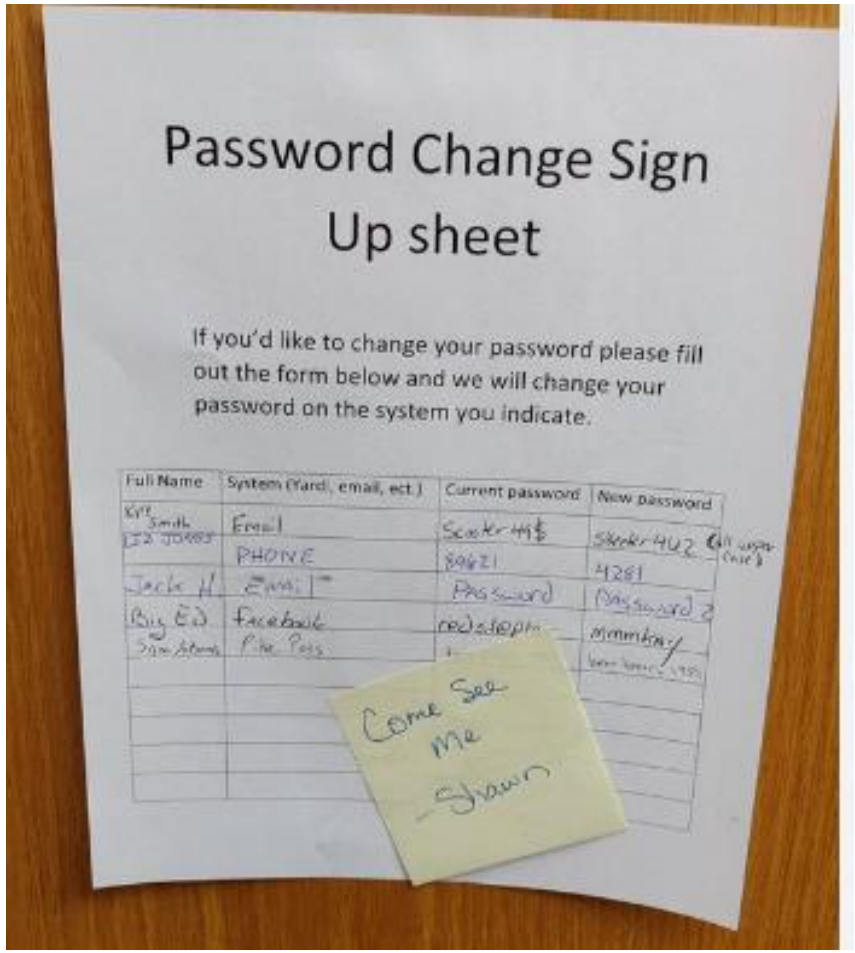
ADWISERY
wise solutions

Reikalavimai slaptažodžiui
Sudėtingas slaptažodis yra tas, kurį sudarant laikomasi šių kriterijų:

- Slaptažodis netrumpesnis nei **12 simbolių** (jei leidžiama – pageidautina 14 ir daugiau);
- Naudojamos **didžiosios** raidės, **mažosios** raidės, **skaitmenys** bei **specialieji simboliai**;

Bendri principai

- Naudokite skirtingus unikalius slaptažodžius, skirtinguose interneto svetainėse, paskyrose, programėlėse;
- Tinkamai saugokite savo slaptažodžius – jeigu juos užsirašote, tuomet šalia nerašykite kam jie skirti, arba užsirašykite nevisą slaptažodį;
- Neatskleiskite savo slaptažodžių kitiems bei neįvedinėkite jų kam nors stebint.
- Nesiųskite slaptažodžių el. paštu ar nesakykite ir jų girdint kitiems.



ADWISERY
wise solutions

Saugūs slaptažodžiai (II)

Ko reikėtų vengti?

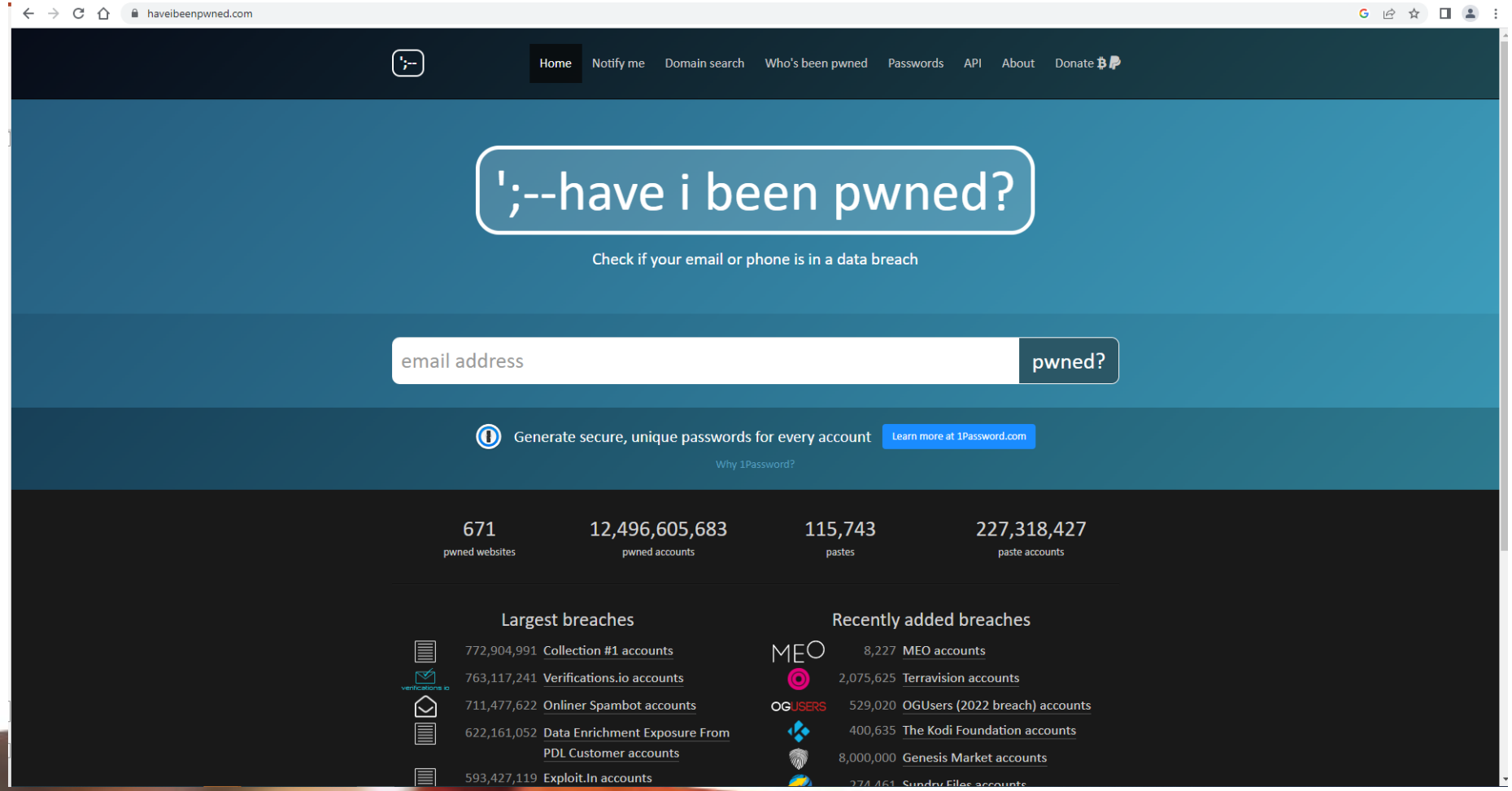
- Nesirinkite slaptažodžio, skelbiamo viešai ar pavyzdžio pavidalu. (pvz., „slaptazodis“, „password“)
- Nenaudokite slaptažodžio, kurį žino tretieji asmenys (pvz., stebėję kaip jūs jį įvedate).
- Nenaudokite slaptažodžio, susidedančio iš asmeninės informacijos (vardai, gimtadieniai ar datos, lengvai susiejamos su jumis).
- Nenaudokite klaviatūros šablonų (pvz.. „qwerty“, „wasd“, „zxcvb“) ar nuoseklių skaičių (pvz. „12345“, „09876“).

REITINGAS	SLAPTAŽODIS	LAIKAS IKI NULAUŽIMO	SKAIČIUS
1	**123456**	< 1 Sekundę	912
2	**kilobaitas**	6 Dienos	629
3	**123456789**	< 1 Sekundę	347
4	**lopas123**	4 Sekundžių	196
5	**labas123**	9 Sekundžių	163
6	**123123**	< 1 Sekundę	152
7	**Matttt24**	2 Valandos	143
8	**nesakysiu**	7 Sekundžių	142
9	**samsung**	< 1 Sekundę	139
10	**kompas**	5 Sekundžių	133

Šaltinis: *https://nordpass.com/lt/most-common-passwords-list/*

ADWISERY
wise solutions

Žinojimas. Ar mano duomenys buvo nutekinti? (I)



ADWISERY
wise solutions

Žinojimas. Ar mano duomenys buvo nutekinti? (II)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

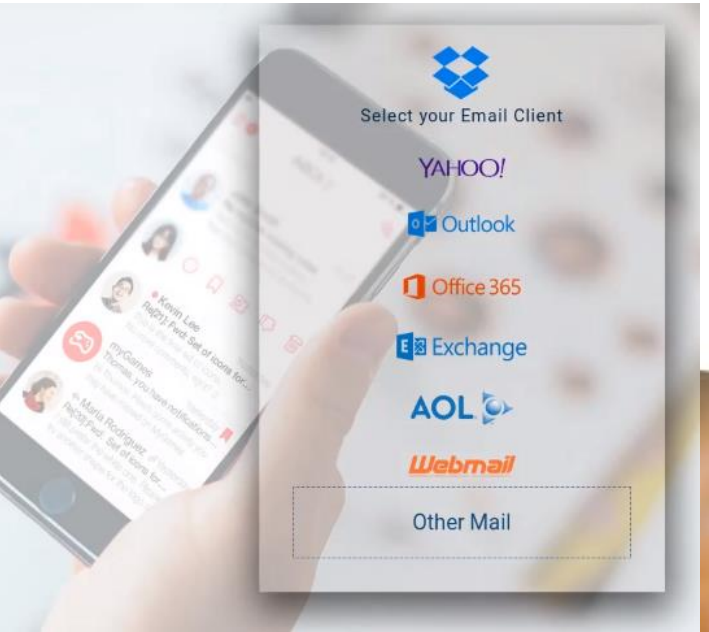
Facebook: In April 2021, a large data set of over 500 million Facebook users was made freely available for download. Encompassing approximately 20% of Facebook's subscribers, the data was allegedly obtained by exploiting a vulnerability Facebook advises they rectified in August 2019. The primary value of the data is the association of phone numbers to identities; whilst each record included phone, only 2.5 million contained an email address. Most records contained names and genders with many also including dates of birth, location, relationship status and employer.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, Names, Phone numbers, Relationship statuses

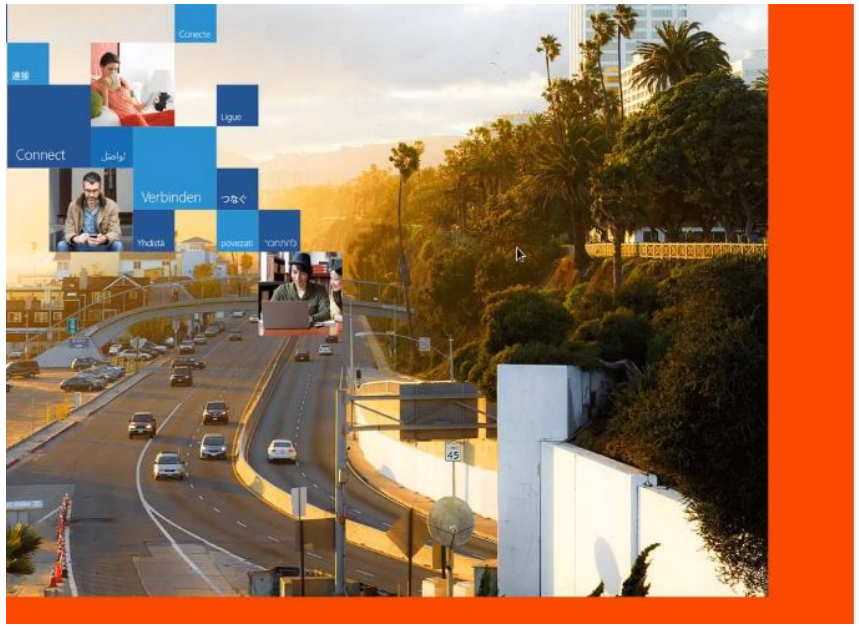
ADWISERY
wise solutions

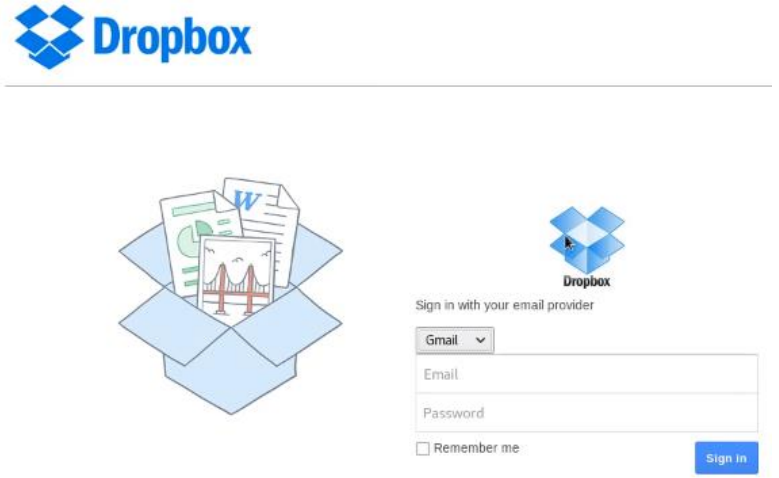
Socialinės inžinerijos praktiniai pavyzdžiai

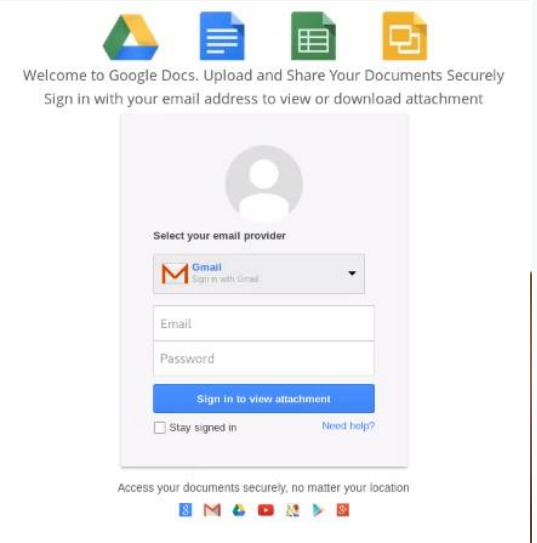
Phishing svetainių pavyzdžiai (I)

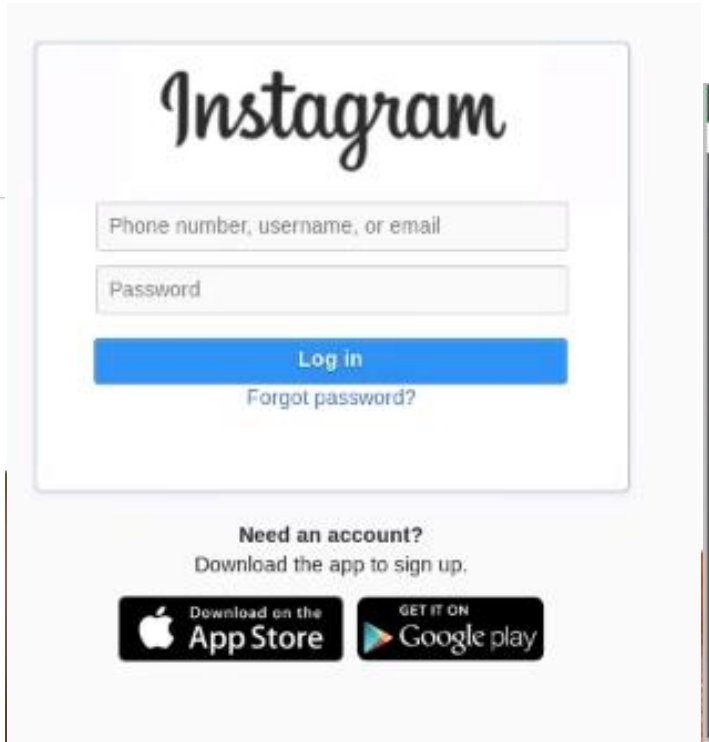


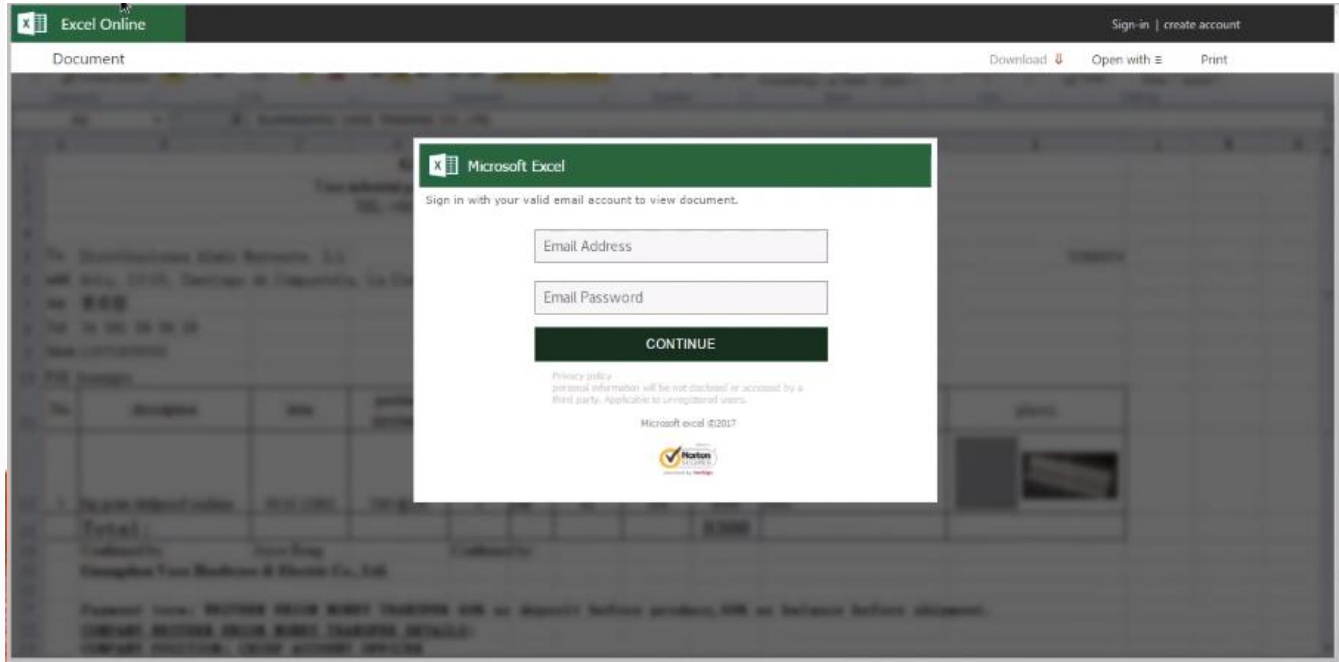
Phishing svetainių pavyzdžiai (II)





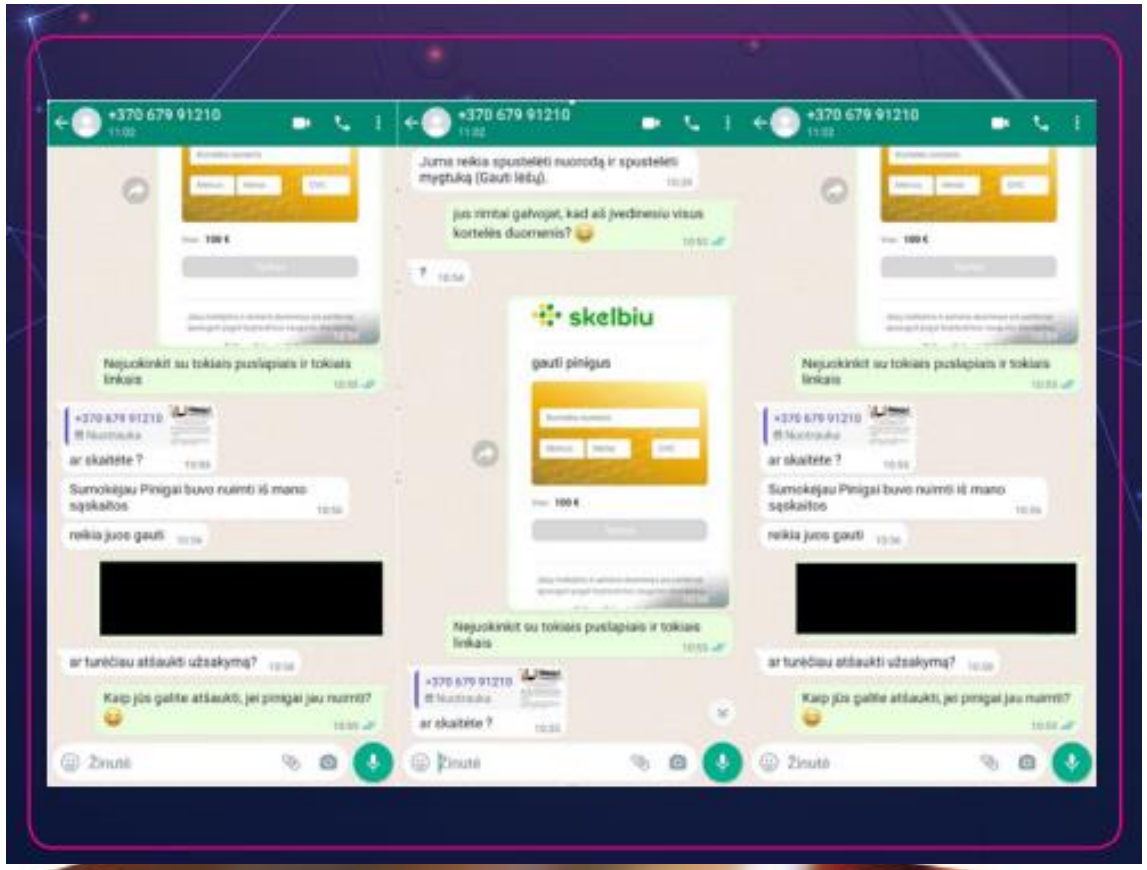


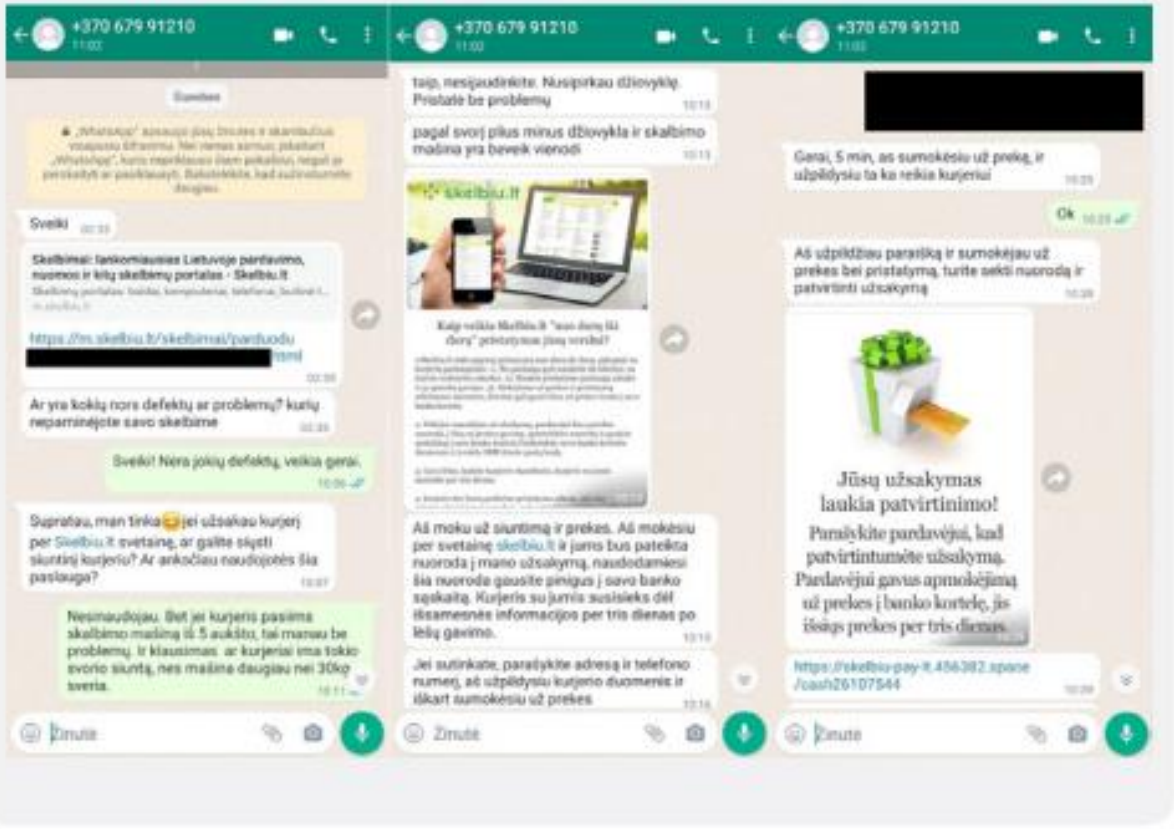




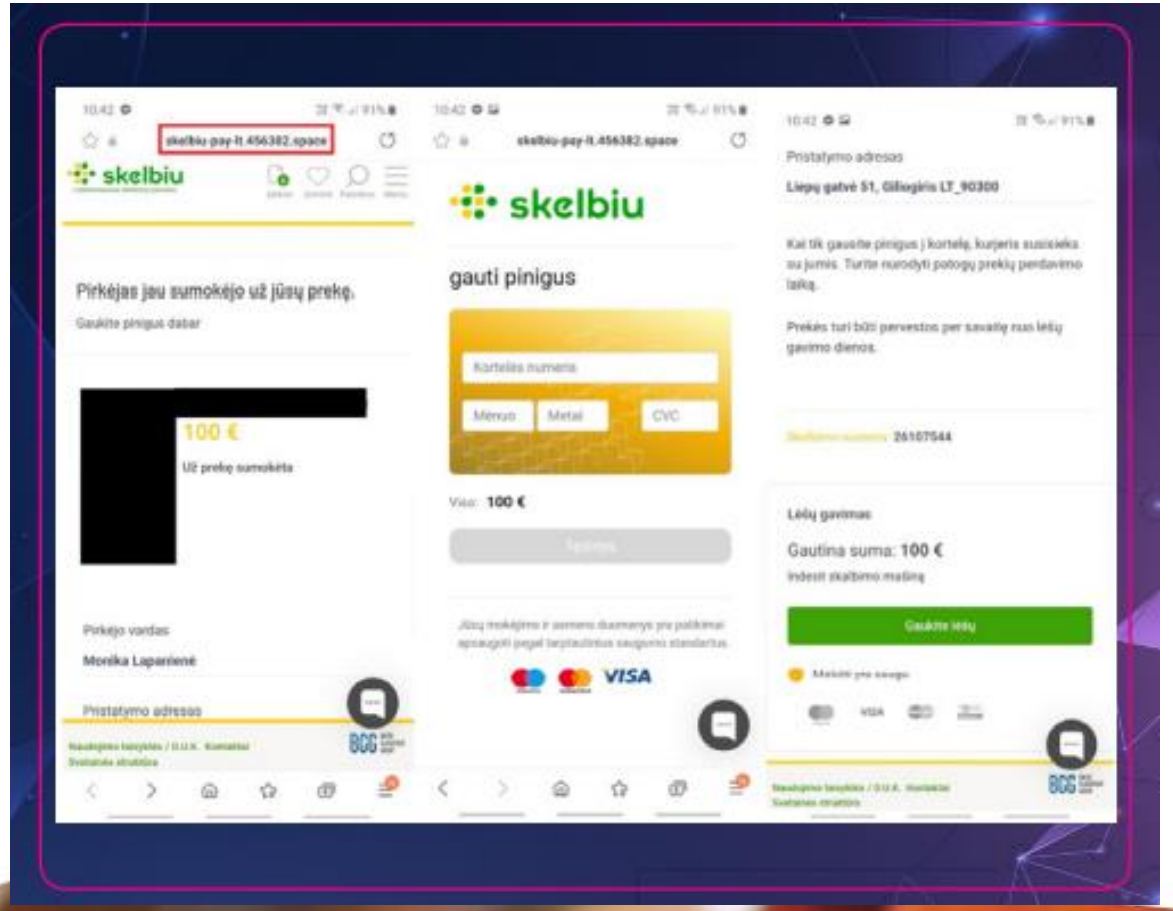
ADWISERY
wise solutions

Phishing svetainių pavyzdžiai (III)





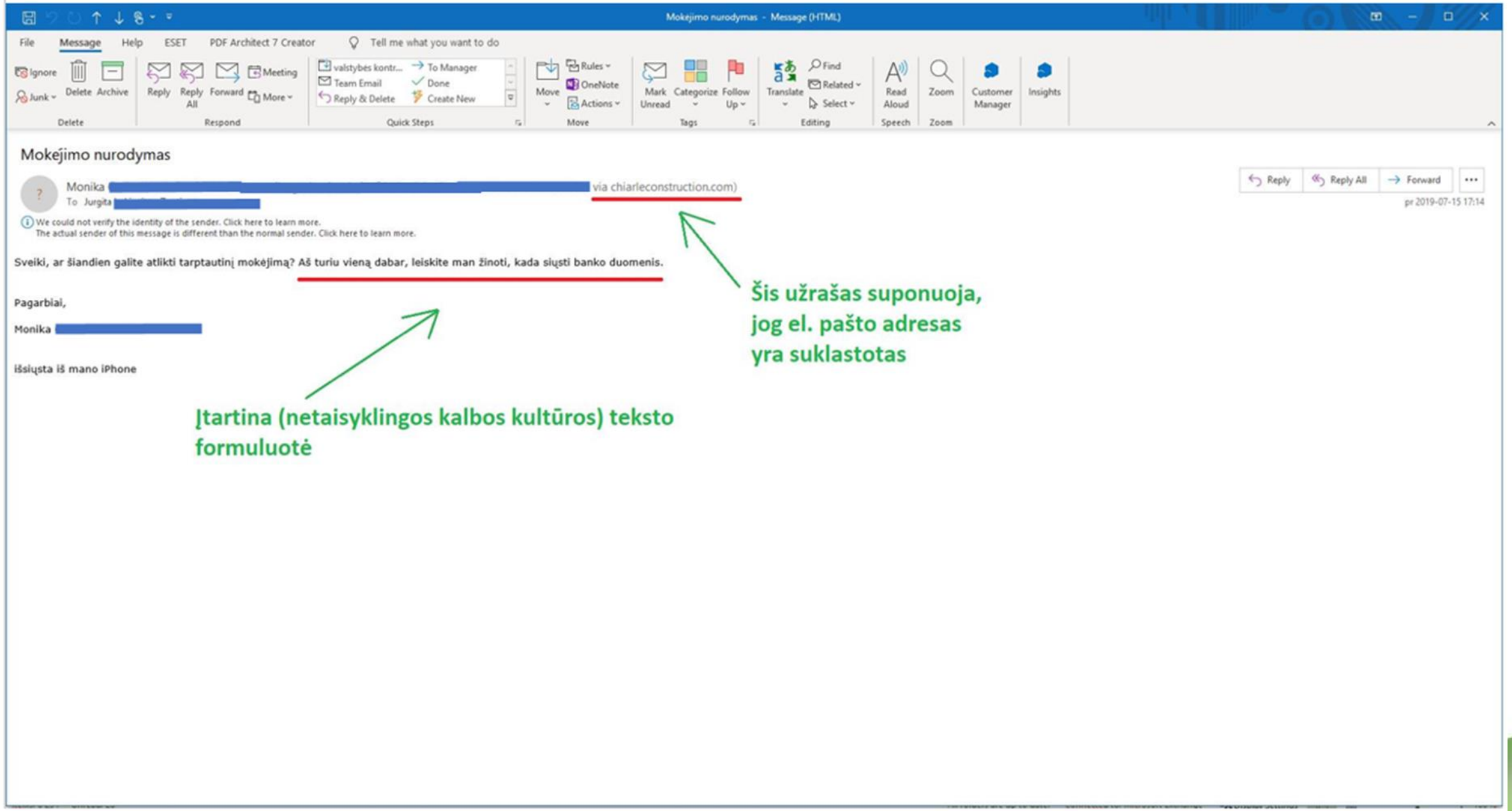
ADWISERY
wise solutions



Naudojami socialinės inžinerijos principai:

- Įtikinėjimas – imituotas skelbiu.lt domenas, kuris iš tikrųjų yra skelbiu-pay.lt.456385.space. Atvaizduojamas realus dizainas, taip pat pateikiama nuoroda į iš tikro parduodamą prekę;
- Pasitikėjimas – nurodoma, kad mokėti yra saugu, pateikiamas realus prekių pristatymo adresas;
- Stygius – mokėjimo kortelė atvaizduojama patrauklia auksine spalva. Įspūdžiui sustiprinti nurodoma, kad kurjeris susisieks gavus piniginę perlaidą.

Phishing e. laiškų pavyzdžiai (I)



Phishing e. laiškų pavyzdžiai (II)

From: UAB Trukme <trukme@trukme.lt>
Date: Wednesday, 18 September 2019 at 15:08
To: Recipients <trukme@trukme.lt>
Subject: Saskaitos fakturos patvirtinimas, V/0435

Labas rytas,

Peržiūrėkite pridėtą sąskaitą faktūrą ir atlikite koregavimus, jei to reikia.

Atsiųskite mums savo banko duomenis, kad galėtume sumokėti 2019 09 19, penktadienį.

Laukiu malonių atsiliepimų

Pagarbiai / Best regards,

Lina [redacted]
Buhalterė/ Accountant

UAB / JSC "Trukmė"
J.Šimkaus g. 21, Garliava
Kauno raj. LT-53204
Lietuva / Lithuania

Company code: 159898440,
VAT code: LT598904418
AS LT75 7044 0600 0316 3082
Tel +370 62966011
Fax +370 37 393049
www.trukme.lt

THINK BEFORE YOU PRINT!

Identifikatorius kuris išduoda, kad laiškas nebuvo skirtas konkrečiam adresatui

Siuntėjo ir gavėjo e. pašto adresai sutampa

Nelogiškas sakinys (kalbos kultūra)

Phishing e. laiškų pavyzdžiai (III)

ADWISERY
wise solutions

kt 2018-09-06 09:49

Monika [redacted] <officemail1302@naver.com> 1

Mokėjimas

To Odeta [redacted]

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk E-mail filter.
We converted this message into plain text format.

Ar galime šiandien sumokėti 28 705,58 eurus? 2

Pagarbiai
Monika [redacted] 3

išsiųsta iš mano iPhone

<https://mail.naver.com/readReceipt/notify/?img=n9%2B0Mr04p4YmKqJn16JRKonYa6EXMrudpo2%2FFxMqKxU9axMdKxUZFzuqp4J0pAUlaEIo%2BrkSKxt5W4d5W4C5bX0q%2BzkR74FTWx%2FsWr30%2Bzu5MNiTpzJrbrR0tzwZ%2BVln%2Bg%3D%3D.gif> 4

Pavojaus signalai, įspėjantys apie „phishing“ ataką:
- netikras (suklastotas) siuntėjo el. laiško adresas (kartais gali būti labai panašus į tikrą);
- nėra pasisveikinimo, iškart rašomas įtartinas tekstas;
- nėra lietuviškų raidžių;
- neaiški nuoroda.

Phishing e. laiškų pavyzdžiai (IV)

From: Monika [redacted] <monika [redacted] @ [redacted] lt>
Sent: Tuesday, October 22, 2019 10:56 AM
To: Asta [redacted] <Asta [redacted] @ [redacted] lt>
Subject: Skubus mokėjimas

Koks yra mūsų sąskaitos likutis?
Ar galime šiandien sumokėti 41 290 eurų?

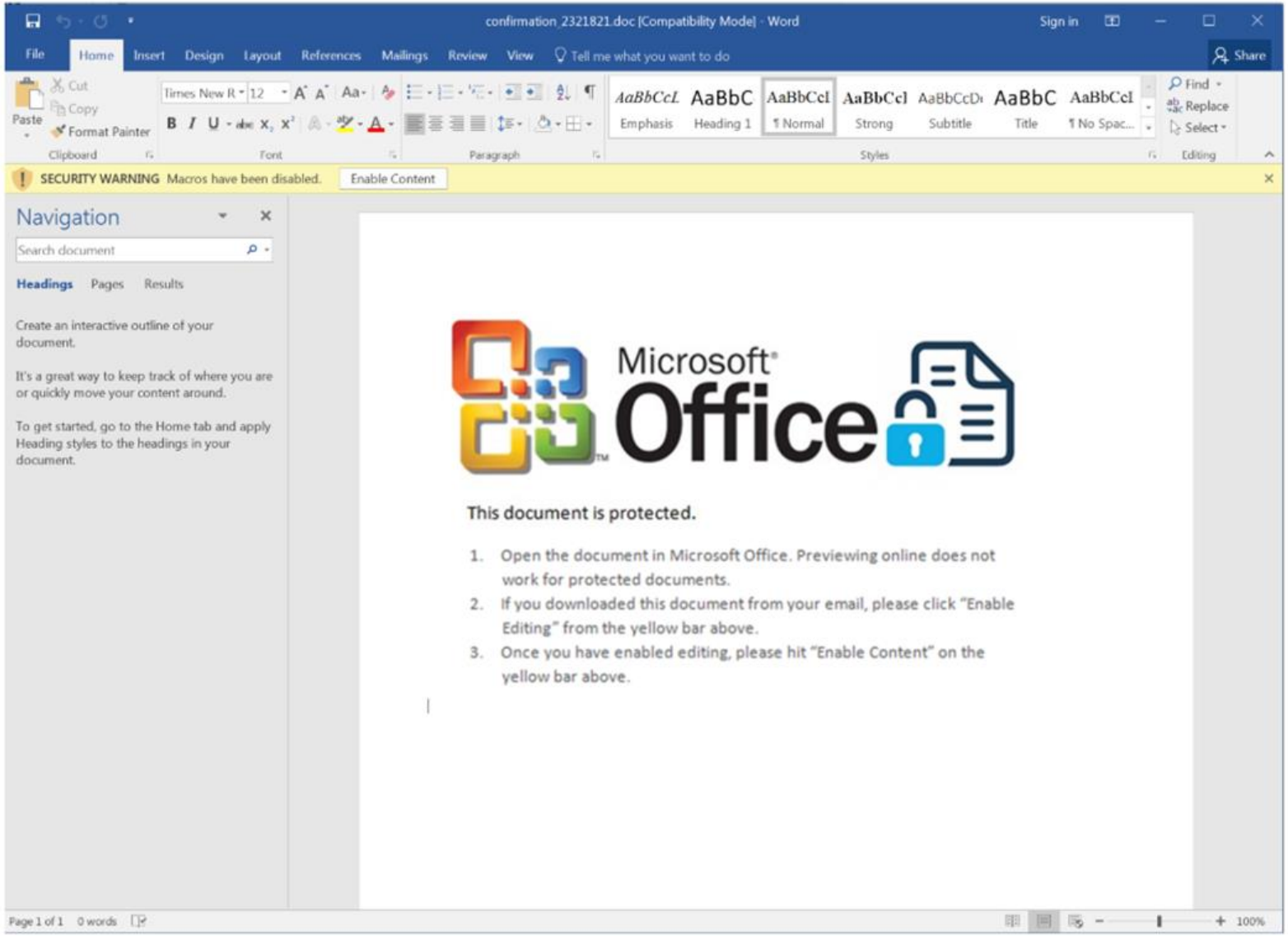
Pagarbiai
Monika

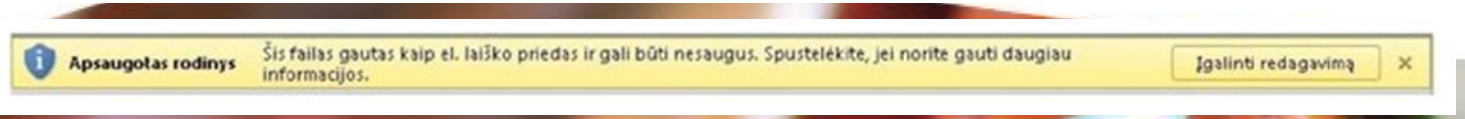
Teksto turinys įtartinas.

This email has been checked for viruses by Avast antivirus software.
www.avast.com

Ši programinė įranga organizacijoje nenaudojama.

Phishing e. laiškų pavyzdžiai (V)



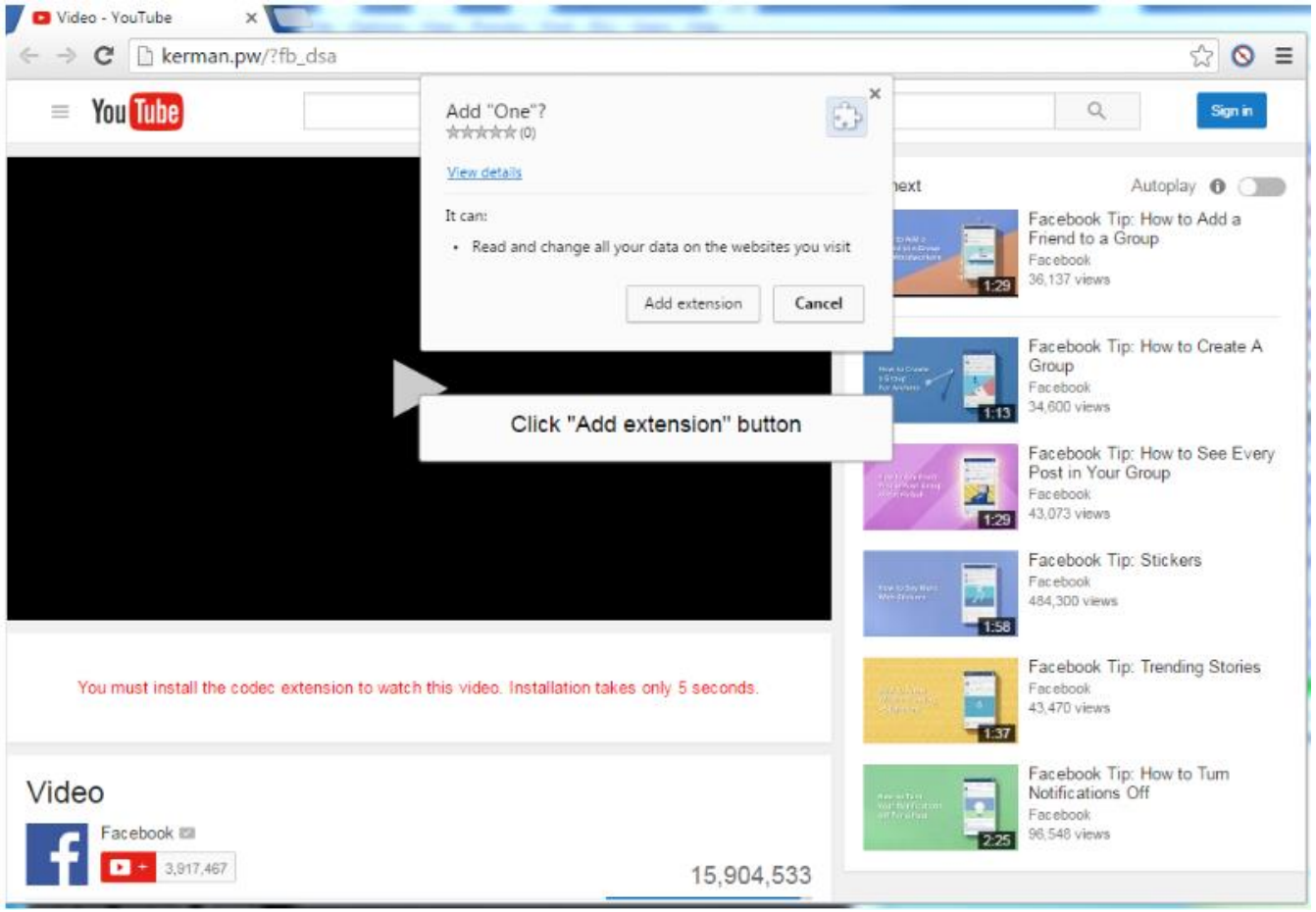


Kenkėjiškos makrokomandos sukčiavimo el. laiškuose per pastaruosius metus tapo vis labiau paplitusiu būdu teikiant išpirkos programas. Šie dokumentai **pernelyg dažnai praeina antivirusines programas** be jokių problemų.

Jei vartotojams nepavyksta įgalinti makrokomandų (angl. ***Enable Content***), ataka nesėkminga.

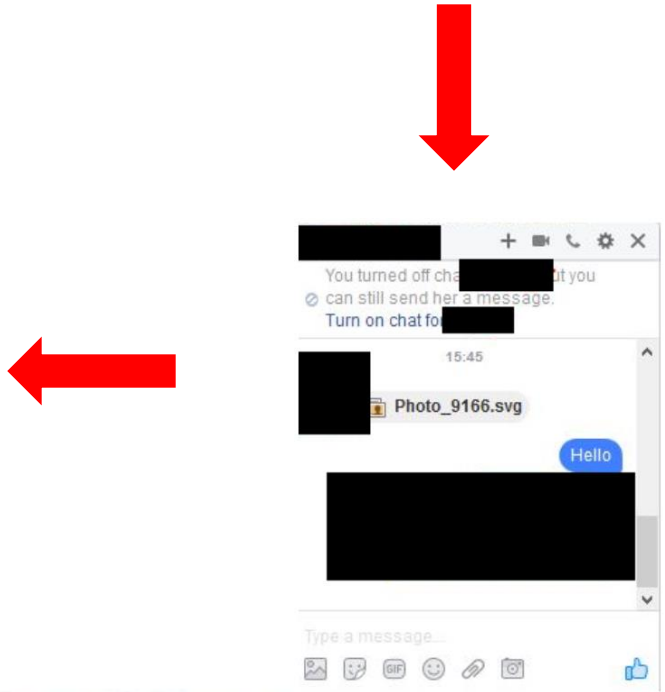
El. laiškais platintų dokumentų antraštė, kurią paspaudus yra aktyvuojama „macro“ komanda, atsisiunčiama kenkimo PĮ.

Phishing socialiniame tinkle pavyzdžiai (VI)



Naudotojai, kurie spustelėjo failą, kad jį atidarytų, buvo nukreipti į **fiktyvų Youtube** puslapį, kuris paragino vartotojus **įdiegti du Chrome plėtinius**, kurie tariamai reikalingi (neegzistuojančiam) vaizdo įrašui puslapyje pamatyti.

Facebook vartotojai į savo Messenger paskyras gavo žinutes iš kitų jiems jau pažįstamų vartotojų. Pranešimą sudarė vienas .SVG (angl. *Scaleable Vector Graphic*) vaizdo failas, kurio neužfiksavo Facebook failų plėtinių filtras.



Phishing e. laiškų pavyzdžiai (VIIa)

El. laiškas yra nuasmenintas, nėra jokios kontaktinės informacijos klausimams

El. laiško turinys nėra logiškas, t. y. LR finansų ministerija nevykdytų apklausos apie darbuotojų darbo krūvį ir gaunamą atlygį

Suklastotas siuntėjo el. pašto adresas apklausos@**finmin.group**, kuris neatitinka LR Finansų ministerijos el. pašto domeno.

Siunčiamas smalsumą žadinantis ir pareigingumą vertinantis el. laiškas

El. laiške pateikta nuoroda į suklastotą internetinę svetainę, t. y. užvedus pelės žymeklį galima pastebėti, kad URL adresas neatitinka užrašyto adreso

Darbuotojams nurodomas trumpas klausimyno užpildymo terminas

Valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, apklausa

LF

LR Finansų ministerijos vertinimų valdymo sistema <apklausos@finmin.group>

To

Reply | Reply All | Forward | ...

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Laba diena gerb. valstybės tarnautojai ir darbuotojai,

Lietuvos Respublikos Vyriausybės 2021 m. vasario 1 d. nutarimu Nr. 104, Finansų ministerija kartu su Valstybės tarnybos departamentu vykdo valstybės ir savivaldybės institucijų ir įstaigų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, anoniminį tyrimą, kurio tikslas yra įvertinti tarnautojų ir darbuotojų nuomonę apie jiems tenkantį darbo krūvį ir mokamą atlygį.

Mes pageidaujame ir tikimės, kad Jūsų požiūris į vertinimą bus pozityvus, nes pagrindinis jo tikslas – nešališkai įvertinti Jūsų požiūrį į darbo aplinką ir palyginti su ankstesnių tyrimų rezultatais. Jūsų dalyvavimas šiame vertinime labai svarbus, nes yra reikšminga kiekvieno valstybės tarnautojo ar darbuotojo nuomonė.

Klausimyno pildymas užtrunka apie 2 min. Klausimyną galite rasti Valstybės tarnybos departamento VATIS savitarnoje - https://www.vataras.lt/vtis/Account/0/0/LogOnExternal, prie kurios JAU galite prisijungti su kompiuterio prisijungimo vardu ir slaptažodžiu.

Labai prašome klausimynus užpildyti iki **ŠIOS DARBO DIENOS PABAIGOS**

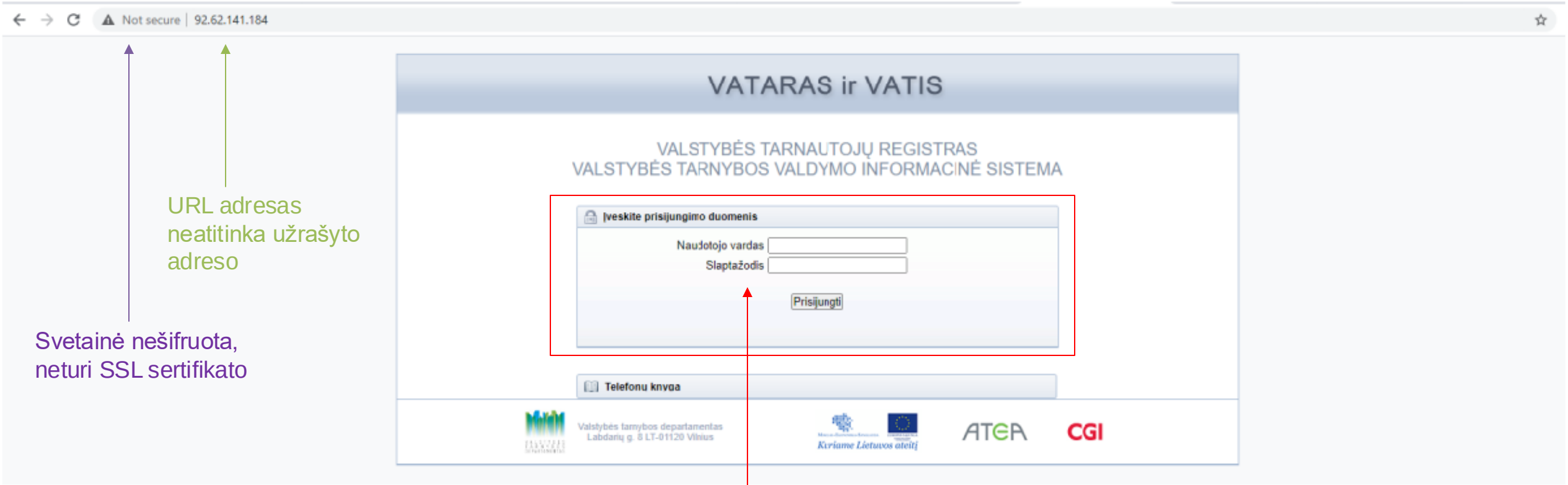
Geros dienos,

Lietuvos Respublikos FINANSŲ MINISTERIJA

VALSTYBĖS TARNYBOS DEPARTAMENTAS

El. laiško temoje atsirado prierašas „[SPAM]“ ir/arba laiškas buvo patalpintas Šlamšto kataloge.

Phishing e. laiškų pavyzdžiai (VIIb)



Prisijungti prie išorinės informacinės sistemos galima su vidiniais Institucijos prisijungimo duomenimis

Phishing e. laiškų pavyzdžiai (VIIIa)

Reply | Reply All | Forward | ...

kt 2021-02-04

VP Vatis Pastas <vatis@vatzum.lt> <vatis@it4lt.lt>

To

If there are problems with how this message is displayed, click here to view it in a web browser.

Suklastotas siuntėjo el. pašto adresas **vatis@it4lt.lt**, kuris neatitinka realaus VATIS el. pašto adreso vatis@vatzum.lt

Informuojame, kad Jums sukurta užduotis.

Atributas	Reikšmė
Užduotis	Atlikti pateiktų duomenų išsamumo vertinimą
Sukūrimo data	2021-02-04
Terminas	2021-02-05 00:00
Sukūręs darbuotojas	Raimundas Spruntulis
Vykdytojas	

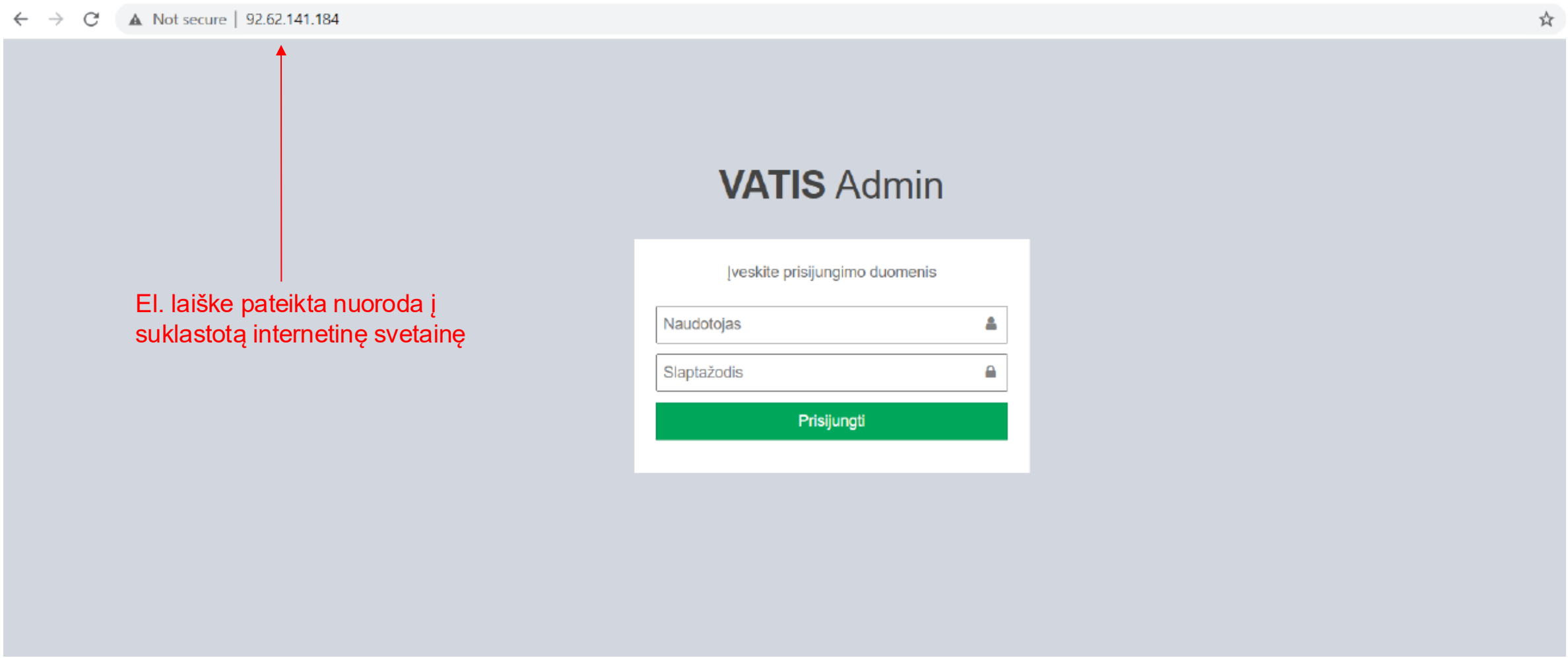
Trumpas užduoties įvykdymo terminas.

--

Dėmesio! Šis pranešimas siunčiamas automatiškai iš Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos informacinės sistemos. Prašome neatsakyti į šį elektroninį laišką.

El. laiške pateikta nuoroda į suklastotą internetinę svetainę, t. y. užvedus pelės žymeklį galima pastebėti, kad URL adresas neatitinka užrašyto adreso

Phishing e. laiškų pavyzdžiai (VIIIb)



El. laiškė pateikta nuoroda į suklastotą internetinę svetainę

ADWISERY
wise solutions

Kas galėjo suklaidinti darbuotojus, suteikti pasitikėjimo jausmą laiško tikrumu:

- Sukurtas suklastotas VATIS informacinės sistemos sisteminis pranešimas apie naują sukurtą užduotį.
- Kiekvieno darbuotojo el. laiške buvo nurodyta, kad jis yra užduoties vykdytojas.
- Užduotį sukūrė Institucijos Bendrųjų reikalų skyriaus vedėjas Raimundas Spruntulis.

ADWISERY
wise solutions

Rekomendacijos kaip apsaugoti asmens duomenis ir sumažinti kibernetinio incidento rizikas

ADWISERY
wise solutions

Rekomendacijos (I)

1. Organizuoti informacijos saugumo mokymus darbuotojams, supažindinant darbuotojus su informacijos saugumo grėsmėmis, saugiu IT įrangos, programų naudojimu, kaip reikėtų elgtis darbo ir asmeninėje aplinkoje, kad nebūtų užvaldyta ar prarasta įmonių ar asmeninė informacija.

2. Periodiškai darbuotojams priminti apie informacijos saugumo rizikas bei socialinės inžinerijos metodus. Pagrindiniai principai, kuriuos būtina priminti darbuotojams:

a) Kiekvieną gautą laišką vertinti kritiškai (ar laiškas skirtas man?; ar aš pažįstu siuntėja?; ar siunčiama informaciją reikalinga mano darbui?);

b) Patikrinti siunčiamas nuorodas (ar nuoroda yra tikra, nuorodą geriau suvesti ranka, o ne spausti ant esančios laiške);

c) Nebijoti pasitikrinti (jei darbuotojas nėra tikras ar laiškas geras, visada reikia pasitikslinti tarkim paskambinti kolegai ir paklausti ar tikrai siuntė šį laišką).

3. Informuoti darbuotojus apie veiksmus, kuriuos būtina atlikti jeigu buvo atidarytas kenkėjiškas laiškas, neaiškus failas, suvesti prisijungimo duomenys, dėl neaiškių priežasčių sulėtėjęs kompiuteris ir pan.

ADWISERY
wise solutions

10 žingsnių kibernetinio saugumo link:

1. Slaptažodžių politika
2. Kelių žingsnių autentifikavimas
3. Antivirusinės programos
4. Automatiniai atnaujinimai
5. Atsarginės duomenų kopijos
6. Prieigos kontrolė
7. Apmokyti darbuotojai
8. Darbo ir asmeninių prietaisų atskyrimas
9. Ugniasienės
10. Saugus bevielis tinklas

ADWISERY
wise solutions

Testo klausimai

1. Kokiomis priemonėmis yra valdomas kibernetinis saugumas?

A. Teisinėmis, informacijos sklaidos, organizacinėmis ir techninėmis;

B. Draudimu, informacinių sistemų priemonėmis, testavimu;

C. Techninėmis, žmogiškųjų išteklių, sankcionavimu.

1. Kokiomis priemonėmis yra valdomas kibernetinis saugumas?

A. Teisinėmis, informacijos sklaidos, organizacinėmis ir techninėmis;

B. Draudimu, informacinių sistemų priemonėmis, testavimu;

C. Techninėmis, žmogiškųjų išteklių, sankcionavimu.

2. Kuri iš žemiau išvardintų nėra rizikos valdymo strategija?

A. Sumažinimas;

B. Priėmimas;

C. Vengimas;

D. Panaikinimas.

2. Kuri iš žemiau išvardintų nėra rizikos valdymo strategija?

A. Sumažinimas;

B. Priėmimas;

C. Vengimas;

D. Panaikinimas.

3. Kas kiek laiko pagal Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą turi būti atliekamas atitikties ir rizikų vertinimas?

A. Abu turi būti atliekami ne rečiau kaip kartą per du metus;

B. Rizikos - ne rečiau kaip kartą per metus, atitikties – ne rečiau kaip kartą per du metus;

C. Abu turi būti atliekami ne rečiau kaip kartą per metus;

D. Atitikties - ne rečiau kaip kartą per metus, rizikos – ne rečiau kaip kartą per du metus.

3. Kas kiek laiko pagal Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą turi būti atliekamas atitikties ir rizikų vertinimas?

A. Abu turi būti atliekami ne rečiau kaip kartą per du metus;

B. Rizikos - ne rečiau kaip kartą per metus, atitikties – ne rečiau kaip kartą per du metus;

C. Abu turi būti atliekami ne rečiau kaip kartą per metus;

D. Atitikties - ne rečiau kaip kartą per metus, rizikos – ne rečiau kaip kartą per du metus.

4. Kas yra kibernetinis incidentas?

A. Neatsargus elgesys kibernetinėje erdvėje, kuris sukelia Informacinių sistemų ir joje saugomų duomenų trikdžius;

B. Įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui;

C. Informacinės sistemos užstrigimas asmeniniame kompiuteryje.

4. Kas yra kibernetinis incidentas?

A. Neatsargus elgesys kibernetinėje erdvėje, kuris sukelia Informacinių sistemų ir joje saugomų duomenų trikdžius;

B. Įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui;

C. Informacinės sistemos užstrigimas asmeniniame kompiuteryje.

5. Informacijos saugos pagrindas yra CIA triada. Kokios saugumo dalys ją sudaro?

A. Konfidencialumas, šifravimas, įrodomumas;

B. Konfidencialumas, vientisumas, prieinamumas;

C. Įrodomumas, sankcionavimas, matavimas.

5. Informacijos saugos pagrindas yra CIA triada. Kokios saugumo dalys ją sudaro?

A. Konfidencialumas, šifravimas, įrodomumas;

B. Konfidencialumas, vientisumas, prieinamumas;

C. Įrodomumas, sankcionavimas, matavimas.

6. Kibernetinius incidentus tiriančios / valdančios institucijos?

A. Valstybės kontrolė, Seimas ir Vyriausybė;

B. Nacionalinis kibernetinio saugumo centras (NKSC), Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija;

C. Krašto apsaugos ministerija, Specialiųjų tyrimų tarnyba, Nacionalinis kibernetinio saugumo centras (NKSC).

6. Kibernetinius incidentus tiriančios / valdančios institucijos?

A. Valstybės kontrolė, Seimas ir Vyriausybė;

B. Nacionalinis kibernetinio saugumo centras (NKSC), Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija;

C. Krašto apsaugos ministerija, Specialiųjų tyrimų tarnyba, Nacionalinis kibernetinio saugumo centras (NKSC).

7. Socialinės inžinerijos incidentas, priklausomai nuo pogrupio ir poveikio kategorijos, gali būti priskiriamas?

A. Tik nereikšmingo svarbumo kategorijos incidentui;

B. Tik didelio svarbumo kategorijos incidentui;

C. Nereikšmingo, vidutinio, didelio arba pavojingo svarbumo kategorijos incidentui.

7. Socialinės inžinerijos incidentas, priklausomai nuo pogrupio ir poveikio kategorijos, gali būti priskiriamas?

A. Tik nereikšmingo svarbumo kategorijos incidentui;

B. Tik didelio svarbumo kategorijos incidentui;

C. Nereikšmingo, vidutinio, didelio arba pavojingo svarbumo kategorijos incidentui.

8. Organizacija vykdydama veiklą naudoja IT priemones t.y. serverius, tinklo įrenginius, kompiuterius ir t.t. Kada atsiranda rizika?

A. Kai IT priemonės turi pažeidžiamumų;

B. Kai IT priemonių pažeidžiamumus išnaudoja grėsmės;

C. Kai IT priemonės neturi pažeidžiamumų ir grėsmių.

8. Organizacija vykdydama veiklą naudoja IT priemones t.y. serverius, tinklo įrenginius, kompiuterius ir t.t. Kada atsiranda rizika?

A. Kai IT priemonės turi pažeidžiamumų;

B. Kai IT priemonių pažeidžiamumus išnaudoja grėsmės;

C. Kai IT priemonės neturi pažeidžiamumų ir grėsmių.

9. Kas yra švaraus stalo politika?

A. Darbuotojas visus dokumentus ir kitas informacijos laikmenas tvarkingai laiko pasidėjęs ant stalo;

B. Darbuotojas naudoja atitinkamus dokumentus tik darbo funkcijoms atlikti, konfidencialių dokumentų nepalieka atvirai pasidėjęs ant stalo;

C. Darbuotojas visus konfidencialius dokumentus sunaikina.

9. Kas yra švaraus stalo politika?

A. Darbuotojas visus dokumentus ir kitas informacijos laikmenas tvarkingai laiko pasidėjęs ant stalo;

B. Darbuotojas naudoja atitinkamus dokumentus tik darbo funkcijoms atlikti, konfidencialių dokumentų nepalieka atvirai pasidėjęs ant stalo;

C. Darbuotojas visus konfidencialius dokumentus sunaikina.

10. Kokios rizikos kyla nesilaikant švaraus stalo ir ekrano politikos?

A. Kibernetinio incidento rizika, asmens duomenų pažeidimo rizika, konfidencialios informacijos atskleidimo rizika;

B. Asmens duomenų atskleidimo rizika;

C. Konfidencialios informacijos atskleidimo rizika.

10. Kokios rizikos kyla nesilaikant švaraus stalo ir ekrano politikos?

A. Kibernetinio incidento rizika, asmens duomenų pažeidimo rizika, konfidencialios informacijos atskleidimo rizika;

B. Asmens duomenų atskleidimo rizika;

C. Konfidencialios informacijos atskleidimo rizika.

11. Dviejų faktorių autentifikavimui paprastai reikia pateikti?

A. Vartotojo vardą, slaptažodį ir papildomą informaciją;

B. Vartotojo vardą ir slaptažodį;

C. Slaptažodį ir identifikavimo kodą.

11. Dviejų faktorių autentifikavimui paprastai reikia pateikti?

A. Vartotojo vardą, slaptažodį ir papildomą informaciją;

B. Vartotojo vardą ir slaptažodį;

C. Slaptažodį ir identifikavimo kodą.

12. Ryšys su kuria interneto svetaine yra šifruotas?

A. https://www.nksc.lt;

B. http://www.nksc.lt

12. Kuri interneto svetainė yra šifruota?

A. https://www.nksc.lt;

B. http://www.nksc.lt

13. Organizacija renka ir tvarko darbuotojų asmens duomenis?

A. Remdamasi teisėtų interesų pagrindu;

B. Remdamasi sutikimų pagrindu;

C. Remdamasi „būtina žinoti“ principu;

D. Remdamasi asmens duomenų tvarkymo principais.

13. Organizacija renka ir tvarko darbuotojų asmens duomenis?

A. Remdamasi teisėtų interesų pagrindu;

B. Remdamasi sutikimų pagrindu;

C. Remdamasi „būtina žinoti“ principu;

D. Remdamasi asmens duomenų tvarkymo principais.

14. Kuris iš žemiau išvardintų nėra sutikimo pagrindo elementas?

A. Laisva valia duotas;

B. Konkretus;

C. Viešas;

D. Nedviprasmiškas.

14. Kuri iš žemiau išvardintų nėra sutikimo pagrindo elementas?

A. Laisva valia duotas;

B. Konkretus;

C. Viešas;

D. Nedviprasmiškas.

15. Ar valstybės įmonė privalo informuoti Nacionalinį kibernetinio saugumo centrą apie kibernetinius incidentus?

A. Taip, visada teisės aktų numatyta tvarka;

B. Taip, bet tik apie pavojingus kibernetinius incidentus;

C. Ne, jeigu valstybės įmonė pati gali suvaldyti kibernetinį incidentą.

15. Ar valstybės įmonė privalo informuoti Nacionalinį kibernetinio saugumo centrą apie kibernetinius incidentus?

A. Taip, visada teisės aktų numatyta tvarka;

B. Taip, bet tik apie pavojingus kibernetinius incidentus;

C. Ne, jeigu valstybės įmonė pati gali suvaldyti kibernetinį incidentą.

16. Įvykus didelį poveikį asmens duomenų subjektams turinčiam asmens duomenų pažeidimui, organizacija privalo?

A. Imtis priemonių suvaldyti incidentą, informuoti duomenų subjektus ir Valstybinę duomenų apsaugos inspekciją;

B. Informuoti Valstybinę duomenų apsaugos inspekciją;

C. Informuoti duomenų subjektus ir visuomenę.

16. Įvykus didelį poveikį asmens duomenų subjektams turinčiam asmens duomenų pažeidimui, organizacija privalo?

A. Imtis priemonių suvaldyti incidentą, informuoti duomenų subjektus ir Valstybinę duomenų apsaugos inspekciją;

B. Informuoti Valstybinę duomenų apsaugos inspekciją;

C. Informuoti duomenų subjektus ir visuomenę.

17. Kas yra socialinė inžinerija?

A. IT įrangos pažeidžiamumų vertinimas;

B. Neteisėta prieiga prie organizacijos informacinių išteklių pasinaudojant aparatinės IT įrangos silpnybėmis;

C. Manipuliavimas žmonėmis, jų silpnybėmis, siekiant apeiti informacijos apsaugos sistemas bei pavogti ir užvaldyti konfidencialią informaciją.

17. Kas yra socialinė inžinerija?

A. IT įrangos pažeidžiamumų vertinimas;

B. Neteisėta prieiga prie organizacijos informacinių išteklių pasinaudojant aparatinės IT įrangos silpnybėmis;

C. Manipuliavimas žmonėmis, jų silpnybėmis, siekiant apeiti informacijos apsaugos sistemas bei pavogti ir užvaldyti konfidencialią informaciją.

18. Socialinės inžinerijos psichologiniai įtakos veiksniai?

A. Smalsumas, baimė, pripažinimas, empatija, skubėjimas, pasitikėjimas, pranašumo iliuzija, socialinio programavimo pinklės;

B. Pyktis, neapykanta, nusivylimas, džiaugsmas, ilgesys, ramybė;

C. Pinigai, bendradarbiavimas, ryšiai, statusas.

18. Socialinės inžinerijos psichologiniai įtakos veiksniai?

A. Smalsumas, baimė, pripažinimas, empatija, skubėjimas, pasitikėjimas, pranašumo iliuzija, socialinio programavimo pinklės;

B. Pyktis, neapykanta, nusivylimas, džiaugsmas, ilgesys, ramybė;

C. Pinigai, bendradarbiavimas, ryšiai, statusas.

19. Socialinės inžinerijos metodas – Pretekstas?

A. Sukuriamas melagingas pasitikėjimo jausmas, gali būti apsimetama – bendradarbiu, privačios arba valstybės įmonės darbuotoju;

B. Darbuotojas bauginamas, neatlikus atitinkamų veiksmų, įvyks neigiamos pasekmės;

C. Pasinaudojama darbuotojo smalsumu ir godumu, įviliojant jį į spąstus.

19. Socialinės inžinerijos metodas – Pretekstas?

A. Sukuriamas melagingas pasitikėjimo jausmas, gali būti apsimetama – bendradarbiu, privačios arba valstybės įmonės darbuotoju;

B. Darbuotojas bauginamas, neatlikus atitinkamų veiksmų, įvyks neigiamos pasekmės;

C. Pasinaudojama darbuotojo smalsumu ir godumu, įviliojant jį į spąstus.

20. Socialinės inžinerijos sukčiavimo forma „*Phishing*“?

A. Sukčiavimo forma prieš organizacijas ar privačius asmenis, kai paskambinama telefonu, siekiant išgauti konfidencialią informaciją;

B. Sukčiavimo forma, kai ateinama į organizaciją apsimetant kitu asmeniu, siekiant išgauti konfidencialią informaciją;

C. Sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis.

20. Socialinės inžinerijos sukčiavimo forma „*Phishing*“?

A. Sukčiavimo forma prieš organizacijas ar privačius asmenis, kai paskambinama telefonu, siekiant išgauti konfidencialią informaciją;

B. Sukčiavimo forma, kai ateinama į organizaciją apsimetant kitu asmeniu, siekiant išgauti konfidencialią informaciją;

C. Sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis.

21. „*Phishing*“ atakos indikatoriai?

A. Beasmenė žinutė, įtartinos nuorodos be https protokolo, įtartini prisegti failai, rašybos klaidos;

B. Išsamus e. laiško turinys skirtas konkrečiam asmeniui, gautas iš pažįstamo adresato;

C. Paslaugų teikėjo sutartis, atsiųsta el.paštu.

21. „*Phishing*“ atakos indikatoriai?

A. Beasmenė žinutė, įtartinos nuorodos be https protokolo, įtartini prisegti failai, rašybos klaidos;

B. Išsamus e. laiško turinys skirtas konkrečiam asmeniui, gautas iš pažįstamo adresato;

C. Paslaugų teikėjo sutartis, atsiųsta el.paštu.

22. Gaunate elektroninį laišką iš įmonės vadovo, kuriame prašoma skubiai atsakyti į laišką pateikiant informaciją apie pagrindinius įmonės klientus (įskaitant jų pavadinimus, adresus, mokėjimams reikalingą informaciją t.y. sąskaitų numerius). Kuris teiginys teisingas?

A. Skubiai atsakote į įmonės vadovo laišką ir pateikiate visą reikalingą informaciją;

B. Patikrinate paklausimo autentiškumą kitais kanalais t.y. telefonu, žodžiu prieš pateikiant prašomą informaciją.

22. Gaunate elektroninį laišką iš įmonės vadovo, kuriame prašoma skubiai atsakyti į laišką pateikiant informaciją apie pagrindinius įmonės klientus (įskaitant jų pavadinimus, adresus, mokėjimams reikalingą informaciją t.y. sąskaitų numerius). Kuris teiginys teisingas?

A. Skubiai atsakote į įmonės vadovo laišką ir pateikiate visą reikalingą informaciją;

B. Patikrinate paklausimo autentiškumą kitais kanalais t.y. telefonu, žodžiu prieš pateikiant prašomą informaciją.

23. Gaunate SMS žinutę iš paslaugų teikėjo, kurioje rašoma kad paslaugų teikėjas atnaujino savo internetinę svetainę ir nuo šiol ji bus pasiekiama nauju adresu http://naujasvetaine.lt. Žinutėje jūsų taip pat prašoma prisijungti prie naujos svetainės ir atnaujinti paskyros slaptažodį kuria anksčiau jungiatės į paslaugų teikėjo internetinę savitarnos svetainę, paspaudžiant SMS žinutėje esančią nuorodą. Ką turėtumėte daryti?

A. Atsakyti į SMS žinutę perklausiant ar jums tikrai reikia atnaujinti paskyros slaptažodį;

B. Patikrinti informaciją kitais kanalais, t.y. peržiūrėti ankstesnį įmonės pulapį siekiant rasti informacijos kad įmonė planuoja internetinės svetainės atnaujinimo darbus, arba paskambinti paslaugų teikėjo atstovui, kontaktiniu numeriu esančiu oficialiame įmonės puslapyje ir gauti patvirtinimą, kad paklausimas yra realus;

C. Paspausti ant nuorodos ir jei ji nukreips jus į paslaugų teikėjo internetinę savitarnos svetainę, pasikeisti slaptažodį.

23. Gaunate SMS žinutę iš paslaugų teikėjo, kurioje rašoma kad paslaugų teikėjas atnaujino savo internetinę svetainę ir nuo šiol ji bus pasiekiama nauju adresu http://naujasvetaine.lt. Žinutėje jūsų taip pat prašoma prisijungti prie naujos svetainės ir atnaujinti paskyros slaptažodį kuria anksčiau jungiatės į paslaugų teikėjo internetinę savitarnos svetainę, paspaudžiant SMS žinutėje esančią nuorodą. Ką turėtumėte daryti?

A. Atsakyti į SMS žinutę perklausiant ar jums tikrai reikia atnaujinti paskyros slaptažodį;

B. Patikrinti informaciją kitais kanalais, t.y. peržiūrėti ankstesnį įmonės pulapį siekiant rasti informacijos kad įmonė planuoja internetinės svetainės atnaujinimo darbus, arba paskambinti paslaugų teikėjo atstovui, kontaktiniu numeriu esančiu oficialiame įmonės puslapyje ir gauti patvirtinimą, kad paklausimas yra realus;

C. Paspausti ant nuorodos ir jei ji nukreips jus į paslaugų teikėjo internetinę savitarnos svetainę, pasikeisti slaptažodį.

24. Ką turėtumėte daryti, kad sumažintumėte žalą jei staiga supratote, kad darbo vietoje atidarėte suklastotą laišką, paspaudėte jame esančią nuorodą bei įvedėte prašomus duomenis (t.y. nusikaltėliui atskleidėte darbinės paskyros naudotojo vardą ir slaptažodį)?

A. Ištrinti gautą laišką;

B. Perkrauti kompiuterį, siekiant sustabdyti kenkėjiškos programinės įrangos plitimą;

C. Skubiai pasikeisti paskyros slaptažodį ir informuoti apie incidentą savo tiesioginį vadovą, saugos įgaliotinį ir (ar) IT administratorių.

24. Ką turėtumėte daryti, kad sumažintumėte žalą jei staiga supratote, kad darbo vietoje atidarėte suklastotą laišką, paspaudėte jame esančią nuorodą bei įvedėte prašomus duomenis (t.y. nusikaltėliui atskleidėte darbinės paskyros naudotojo vardą ir slaptažodį)?

A. Ištrinti gautą laišką;

B. Perkrauti kompiuterį, siekiant sustabdyti kenkėjiškos programinės įrangos plitimą;

C. Skubiai pasikeisti paskyros slaptažodį ir informuoti apie incidentą savo tiesioginį vadovą, saugos įgaliotinį ir (ar) IT administratorių.

25. Kuris iš šių teiginių geriausiai nusako, kaip reikėtų užtikrinti informacijos saugą dirbant nuotoliniu būdu?

A. Būti susipažinus su įmonės informacijos saugą reglamentuojančiomis tvarkomis bei nuotolinio darbo taisyklėmis;

B. Naudoti VPN technologiją jungiantis nuotoliniu būdu;

C. Naudoti unikalius, kompleksiškus slaptažodžius ir nepalikti darbo reikmėms naudojamų įrenginių (telefonų, kompiuterių ir kt.) be priežiūros;

D. Visi išvardinti variantai.

25. Kuris iš šių teiginių geriausiai nusako, kaip reikėtų užtikrinti informacijos saugą dirbant nuotoliniu būdu?

A. Būti susipažinus su įmonės informacijos saugą reglamentuojančiomis tvarkomis bei nuotolinio darbo taisyklėmis;

B. Naudoti VPN technologiją jungiantis nuotoliniu būdu;

C. Naudoti unikalius, kompleksiškus slaptažodžius ir nepalikti darbo reikmėms naudojamų įrenginių (telefonų, kompiuterių ir kt.) be priežiūros;

D. Visi išvardinti variantai.

26. Kuris iš šių žemiau išvardintų slaptažodžių yra saugiausias (sunkiausiai nulaužiamas)?

A. Vasara_2017

B. 123456789

C. Slaptazodis1234

D. Tw0+Pa1ang3sG313s

26. Kuris iš šių žemiau išvardintų slaptažodžių yra saugiausias (sunkiausiai nulaužiamas)?

A. Vasara_2017

B. 123456789

C. Slaptazodis1234

D. Tw0+Pa1ang3sG313s

Two+PalangesGeles

L = 1

E = 3

ADWISERY
wise solutions

ADWISERY, UAB
Konstitucijos pr. 7,
LT-09308, Vilnius, Lietuva
www.adwisery.eu