Saugokis apgaulės internete

arba

atsargiai, – socialinė inžinerija!

Pamokos planas ir rekomendacijos 9-12 klasėms

Kritinį mąstymą ugdykime kartu!

LANGAS | ATEITI

VIPT @asociacija

European MEDIA AND INFORMATION Fund
Managed by Calouste Gulbenkian Foundation

Projektas „Medijų raštingumo stiprinimas bendruomenėse: kritinį mąstymą ugdykime kartu!“

Šio projekto tikslas – stiprinti medijų raštingumą, ypač kritinį mąstymą, suteikiant aktyviems vietos bendruomenių atstovams žinių ir priemonių, kaip to mokyti kitus savo bendruomenės narius.

Projekte ypač daug dėmesio bus skiriama mokyklų bibliotekininkams, kurie, organizuodami informacijos bei medijų raštingumo švietimo renginius ir pasiekdami platesnę mokyklos bendruomenę, galės naudotis projekto metu sukurtais ištekliais ir perduoti kritinio mąstymo žinias bei įgūdžius mokytojams, mokiniams ir jų tėvams. Dalyvaudami projekto veikloje jie ne tik sustiprins savo įgūdžius, bet ir taps stipriu žinių daugikliu savo bendruomenėse.

Projektą įgyvendina dvi asociacijos iš Lietuvos, dalyvaujančios kuriant žinių visuomenę šalyje: asociacija „Langas į ateitį“ bei asociacija „Viešieji interneto prieigos taškai“.

Projekto socialinis partneris - Lietuvos mokyklų bibliotekų darbuotojų asociacija.

Projektą finansuoja Europos žiniasklaidos ir informacijos fondas (EMIF).

Pamokos tikslas

Ugdyti mokinių kritinį mąstymą ir atsparumą socialinei inžinerijai: priminti mokiniams apie asmeninės informacijos saugos ir atsargumo internete svarbą, supažindinti su įvairiais socialinės inžinerijos pavyzdžiais, požymiais, paaiškinti galimą žalą ir pasekmes. Svarbu įtvirtinti tinkamą mokinių elgesio modelį, kai gaunama informacija kritiškai vertinama, atsižvelgiama į jos patikimumą, kontekstą, išraiškos formą, o įtarimus keliančiais atvejais, ar patyrus žalą – kreipiamasi į tėvus ar patikimus suaugusiuosius.

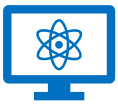
Pamokos trukmė

Orientacinė pamokos trukmė – 45 min., tačiau mokytojas gali ją sutrumpinti atsirinkdamas temas ir priemones savo nuožiūra.

Priemonės

Kompiuteris su projektoriumi ir ekranas arba interaktyvioji lenta, interneto ryšys, lenta arba didelis bloknotas užrašams.

Pamokos skaidrių rinkinys, kuris gali būti mokytojo pritaikomas konkrečiai pamokai: pateiktis, viktorinos klausimai.



– toks ženklas nurodo, kad aiškinant tam tikrą medžiagos temą ar rengiant veiklą (įvadinį pokalbį, viktoriną, užduotį), galima pasinaudoti interaktyviuoju mokymo objektu, kuris gali būti demonstruojamas vietoje skaidrės. Tai pagyvintų pamoką, labiau atkreiptų mokinių dėmesį, tuo pačiu galėtų padėti mokytojui labiau struktūriškai ar grafiškai pateikti reikiamą informaciją. Reikalingus interaktyviuosius mokymo objektus rasite svetainėje ties kiekvienos temos medžiaga.

Prieš pamoką pasitikrinkite, ar klasėje tinkamai veikia internetas, ar mokykla neblokuoja prieigos prie reikalingų pamokai interneto išteklių.

Šaltiniai

Papildoma medžiaga:

- NKSC informacinis biuletenis: klastotės ir duomenų vagystės, https://www.nksc.lt/doc/biuleteniai/2018-05-15%20phishing%20klastotes%20ir%20duomenu%20vagystes.pdf
- Medijų ir informacinio raštingumo programa – https://mirkt.bibliotekavisiems.lt/
- Seminaro „IT saugumo rekomendacijos" medžiaga https://lm.lt/images/pdf/LITNET_elpasto_saugumas20201209n.pdf
- Kaip atpažinti virusu užkrėstą laišką? https://virusai.lt/kaip-atpazinti-virusu-uzkresta-elektronini-laiska/
- Medijų raštingumo medžiaga mokykloms (anglų k.) – https://www.commonsense.org/education/articles/news-media-literacy-101
- Apie duomenų išviliojimą per 6 minutes (anglų k., įvairių metodų apžvalga, geras iliustracijų šaltinis) - https://www.youtube.com/watch?v=XBkzBrXlle0
- http://www.draugiskasinternetas.lt/lt/adult/news?id=8713 – lietuviškas tėvų ir vaikų sutarties variantas (*Word* dokumentas)

- Socialiniai tinklai: kas tavo draugai? http://pamoka.draugiskasinternetas.lt/socialiniai-tinklai-kas-tavo-draugai/
- Apsisaugok nuo apgaulės internete http://pamoka.draugiskasinternetas.lt/apsisaugok-nuo-apgaules-internete/
- Sukčiai internete: kaip apsisaugoti? Diskusijos įrašas. http://pamoka.draugiskasinternetas.lt/sukciai-internete-kaip-apsisaugoti/
- Saugesnis internetas vaikams (priemonė viktorinai rengti). https://www.epilietis.eu/kursai/saugesnio-interneto-viktorina-2/
- Testas. Ar esate atsparus sukčių pasiūlymams? (13+) https://www.lb.lt/lt/investavimas-kaip-atpazinti-sukcius

Pamokos planas

1. Temos pristatymas – 5 min.

Prisistatykite, paaiškinkite pamokos tikslą, kas vyks jos metu. Jei turite pasiruošę prizų, galite mokinius sudominti būsima viktorina.

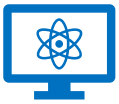
2. Pateikties demonstravimas – 15-20 min.

Skaidrė	Turinys ir rekomendacijos
1.	Pavadinimo skaidrė.
2.	Su kuo bendraujame internete? • Susirašinėjimo programėlėse: ... ? • Socialiniuose tinkluose: ... ? • Žaisdami internetinius žaidimus: ... ? • Lankydamiesi interneto svetainėse: ...? Įvadinė diskusija (2, 3 ir 4 skaidrės, apie 10 min.), skirta prisiminti ar pagilinti žinias apie tai, kas yra asmens duomenys ir kodėl reikia juos saugoti. Mokinių klausiama, su kuo jie bendrauja internete. Jų atsakymus galima surašyti lentoje (bloknote) trimis stulpeliais – artimieji, draugai ir nepažįstamieji. Kokia informacija galima dalytis su kitais? Kaip ir realiame pasaulyje, asmeninę informaciją sakyti galima tik artimiesiems, o su nepažįstamaisiais reikia bendrauti atsargiai. Asmeninė informacija yra tokia, kuri leidžia atpažinti ir surasti vieną asmenį iš daugelio. Jei vienas požymis atskirai nėra labai svarbus (pavyzdžiui, amžius, vardas), tai keli tokie požymiai kartu leistų, pavyzdžiui, surasti vieną mokinį tarp visos mokyklos mokinių. Galimi asmeninės informacijos pavyzdžiai (galima dalytis ar ne). • Vardas – Greta (ne) • Pavardė – Gretaitė (ne) • Amžius – 16 metų (dažniausiai ne) • Mėgstamiausia spalva – žalia (taip) • Namų adresas – Zuikių 196-3, laiptinės kodas 1234 (ne) • Mokyklos ir klasės pavadinimas – Rytinė progimnazija, 9B klasė (ne) • Mamos ir tėčio vardai – Audronė ir Aurimas (ne) • Šuniuko vardas – Rikis (taip) • Pomėgiai – muzika, knygos (taip). Galite pasiūlyti užduotį, kad mokiniai nuspręstų, ką iš minėtos informacijos galima sakyti nepažįstamiesiems, kurią draugams, o kurią tik artimiesiems.  (Asmeninės informacijos pavyzdžiai)
3.	Kas gali nutikti atskleidus per daug informacijos apie save? • Į mūsų namus gali įsilaužti vagys; • piktavaliai mus gali surasti mokykloje; • pavogti žaidimo ar socialinio tinklo paskyrą; • iš mūsų tyčiotis; • apsimesti mumis ir kurti netikras paskyras. Iš kur sukčiai sužino aukos vardą, duomenis, kitą informaciją, kurios reikia apgaulingai žinutei ar skambučiui?

	Paaiškinkite mokiniams, kokios grėsmės kyla atskleidus asmeninę informaciją nepažįstamiesiems. Galite pateikti šį pavyzdį: https://www.15min.lt/naujiena/aktualu/nusikaltimaiirnelaimes/vagys-klaipedieciu-namuose-pasidarbavo-pamate-keturiolikmecio-irasa-socialiniame-tinkle-59-918356. Mokinių tarpe aktuali patyčių problema, kai gali būti panaudojamos aukos paskelbtos netinkamos nuotraukos, taip pat aukos vardu sukuriamos netikros paskyros. Kitas pavojus, kuris kyla ypač nepilnamečiams socialinių tinklų vartotojams, tai agresyvūs, bendraamžiais apsimetantys, neteisėtą prekybą vykdantys, bandantys įtraukti į nusikaltimus ir pan. asmenys. Savaime tokių piktavalių asmenų internete nėra daugiau nei realiame gyvenime, tiesiog socialiniuose tinkluose lengviau susisiekti su nepažįstamais vartotojais ir išlikti anonimu. Vaikai socialiniuose tinkluose susipažįsta su įvairiais žmonėmis ir gali būti įvairiai jų paveikti, kviečiami susitikti ir pan., labai dažnai susiduria su netinkamu nepilnamečiams turiniu. Čia nepadės jokie tėvų priekaištai, nei draudimai naudotis internetu, nei griežta tėvų kontrolė. Vienintelis būdas – abipusis vaikų ir tėvų pasitikėjimas, kai vaikai dalijasi su tėvais savo atradimais internete, o tėvai pataria sudėtingose situacijose. Apibendrinimas – „pagalvok prieš spausdamas“.  (Kas gali nutikti atskleidus per daug informacijos apie save?)
4.	Socialinė inžinerija – kas ir kodėl? Asmeninės ir privačios informacijos išviliojimas norint: • pasipelnyti; • pakenkti; • apsimesti Vertimas priimti nenaudingus sprendimus: • įsigyti nereikalingų ar netinkamų prekių; • sumokėti per didelę kainą. Tai manipuliavimas žmonėmis pasitelkiant psichologijos žinias ir apgaulę, kad jie elgtųsi tam tikru jiems nenaudingu būdu. Socialinė inžinerija yra būdas, kurį naudoja žmonės norėdami valdyti kitų žmonių poelgius ir veiksmus. Tai gali būti daroma žodinėmis manipuliacijomis, įtikinėjimu, klaidinančia informacija ir pan. Tai daugiausia interneto amžiaus reiškinys, kai nusikaltėliai tokiu būdu stengiasi sukčiauti, pavogti privačią informaciją, įbrukti kenksmingą programinę įrangą ir kt. Socialinė inžinerija: • tai manipuliacijos forma, kuria naudojasi žmonės norėdami pasiekti savo tikslus ar gauti naudos; • plačiai pasireiškia internete, žinutėmis, e. paštu, socialiniuose tinkluose ar kitomis internetinėmis priemonėmis; • gali padaryti rimtos žalos, – nuo privačios informacijos vagysčių iki paskyrų pagrobimo ir finansinių nuostolių.  (Socialinė inžinerija – kas ir kodėl?)
5.	Kaip išviliojama asmeninė informacija? • Apgaulingi laiškai: • apsimetus pažįstamais, įstaigų atstovais;

	• siūlant lengvai praturtėti; • raginantys skubiai veikti; • sukeliantys smalsumą. • Apgaulingos svetainės • Suklastotos svetainės, kuriose prašoma įvesti slaptažodžius ir pan., • Svetainės, kuriose reikalaujama registruotis ir nurodyti išsamią asmeninę informaciją. • Netikros loterijos. • Apgaulingos parduotuvės ir pan. Dažniausiai pasitaikantis socialinės inžinerijos metodas yra duomenų išviliojimas (angl. phishing) – nusikaltėliai, apsimesdami pažįstamais ir patikimais asmenimis, siunčia melagingas žinutes, siekdami apgauti žmones ir gauti jų asmeninę informaciją. Šie laiškai gali atrodyti, jog juos siuntė jūsų mokykla, bankas, socialinis tinklas arba kita patikima organizacija. Pasidalykite savo turima patirtimi, kokių suklastotų laiškų esate gavę (prašymai žiūrėti pridėtas „nuotraukas“, raginimai pakeisti slaptažodžius, prisijungti prie banko, „Nigerijos princų“ laiškai ir pan.). Paklauskite mokinių, kokia jų patirtis susidūrus su socialine inžinerija, – kokių žinučių yra gavę paštu ar socialiniuose tinkluose, kokių pranešimų apie laimėjimus ar gąsdinimus virusais yra matę interneto svetainėse. Mokiniams turbūt geriausiai bus suprantama socialinio tinklo paskyros vagystė, kai pasinaudojus išviliotais duomenimis piktavaliai pagrobia paskyrą ir kurį laiką naudojasi svetima tapatybe, keldami žalą buvusiam jos savininkui. Vyresniems mokiniams galima paaiškinti, kokio masto atakos vykdomos Lietuvoje ir pasaulyje. LBA duomenimis, 2020 m. Lietuvos gyventojai dėl socialinės inžinerijos patyrė per 4,5 mln € žalos. JAV gyventojų per metus patiriama žala siekia kelis milijardus dolerių. 2022 m. Lietuvos gyventojai kas mėnesį prarasdavo po 20 tūkst. paskyrų, – jų prisijungimus išviliodavo ar atspėdavo piktavaliai. Vienas iš plačiau žinomų socialinės inžinerijos atvejų Lietuvoje įvyko 2017 metais, kai nežinomi asmenys siuntė fiktyvius elektroninius laiškus, apsimetę SEB banko darbuotojais, ir prašė klientų patikrinti savo banko sąskaitas. Laiškų turinys buvo labai įtikinamas, todėl daugelis žmonių atsiuntė savo asmeninius duomenis, tokius kaip prisijungimo vardai ir slaptažodžiai, o kartais net ir jų asmens kodai. Tais pačiais 2017 m. kibernetinių nusikaltėlių grupė pavogė Lietuvos ryšių reguliavimo tarnybos darbuotojų prisijungimo duomenis. Duomenų išviliojimo atakos metu buvo siunčiamos melagingos žinutės su nuoroda į sukurtą melagingą prisijungimo svetainę, kurioje prašoma įvesti savo prisijungimo vardą ir slaptažodį. Kai darbuotojai tai padarė, kenkėjai įgijo prieigą prie jų e. pašto paskyrų ir galėjo pavogti jų asmeninius duomenis. 2019 m. Lietuvoje „Luminor“ banko klientams buvo siunčiami e. pašto laiškai, apsimetant banko darbuotojais. Šiuose laiškuose buvo siunčiamos nuorodos, vedančios į melagingas banko prisijungimo svetaines, kuriose buvo prašoma įvesti savo prisijungimo vardą ir slaptažodį. Kai klientai tai padarė, nusikaltėliai gavo jų prisijungimo duomenis ir prieigą prie jų banko sąskaitų. 2021 m. prasidėjus Seimo rinkimams Lietuvoje, kenkėjai apgaulingais laiškais siekė gauti prieigą prie politinių partijų duomenų ir pakenkti rinkimų procesui. Iš įdomesnių atvejų galima paminėti 2019 m. rudenį vykusį plataus masto socialinės inžinerijos atvejį, kai nežinomi asmenys, naudodamiesi melagingais e. laiškais, Lietuvoje privertė atleisti iš darbo keliolika darbuotojų. Laiškuose buvo kviečiama dalyvauti JAV aukšto lygio mokymuose ir pateikti savo asmens duomenis kelionės dokumentams parengti.

	Naudojantis išviliotais duomenimis buvo pateikti atleidimo prašymai įmonėms, kuriose tie darbuotojai dirbo.
6.	Nenaudingi sprendimai • Raginimas skubiai ką nors daryti (trumpalaikės akcijos ir pan.) • Siūlomos „prekės“ su nerealiomis kainomis ar nuolaidomis • Gąsdinama netikrais pavojais ir pan. Tam, kad žmonės nespėtų pagalvoti, piktavaliai juos ragina skubiai priimti sprendimus („akcija baigsis po valandos“) ar pribloškia fantastiškais laimėjimais ir pusvelčiui siūlomomis žinomų ženklų prekėmis. Kaina įvairiose parduotuvėse gali skirtis daugiausia trečdaliu, bet tikrai ne tris ar dešimt kartų! Žmonės paprastai gąsdinami užblokuotomis paskyromis, netikrais virusais (siunčiant įspėjimus ir siūlant netikras „antivirusines programas“) ar raginant optimizuoti kompiuterį arba išmanųjį telefoną, kad jis esą geriau veiktų (9 iš 10 siūlomų „optimizavimo“ programėlių yra vienaip ar kitaip kenkėjiškos). Yra paplitę išpirkos reikalaujantys laiškai, grasinantys atskleisti privatų aukos kompiuterio ar išmaniojo telefono turinį, nors kenkėjas iš tiesų neturi prie jo jokios prieigos ir pasikliauja tik aukos išgąsčiu.
7.	Įtartini požymiai • Žadami lengvi ir dideli prizai. • Gąsdinama, kad kas nors nutiks. • Netaisyklinga, keista kalba. • Prašoma slaptažodžių ir asmens duomenų. • Reikalaujama skubiai veikti. Netgi svetainių išvaizdą reikia vertinti kritiškai, – ar jos parašytos taisyklinga kalba, ar tinkamai veikia navigacija, ar jose nesiūloma keistų dalykų. Svarbu pajusti įtartiną įtikinėjimą, raginimą skubiai ką nors daryti nespėjus net gerai pagalvoti, taip pat suprasti, kad nebūna laimėjimų dykai ar pusvelčiui parduodamų šaunių dalykų. Jei prašoma asmens duomenų, reikia elgtis itin atsargiai, geriausia iškart nutraukti tokį bendravimą ar naršymą svetainėje. Slaptažodžių negalima atskleisti net artimiausiems draugams!  (Įtartini požymiai)
8.	Ką daryti? • Elgtis atsargiai • Neatskleisti savo asmeninės informacijos • Apie nepažįstamųjų žinutes pasikalbėti su tėvais ar patikimais žmonėmis • Visada papasakoti tėvams, mokytojams, kitiems patikimiems suaugusiems, jeigu internete nutinka kas nors nemalonaus! Patariama nespausti atsiųstų nuorodų, o reikiamų svetainių adresus visada surinkti patiems. Netgi naudoti paieškos sistemas rizikinga, nes paieškos rezultatuose pasitaiko ir kenkėjiškų ar suklastotų svetainių. Atsakingų svetainių adresas visada prasideda https://. Savo asmeninę informaciją reikia saugoti, jos neįvesti jokiose interneto svetainėse, nesidalinti socialiniuose tinkluose su mažai pažįstamais žmonėmis.

	Į jokias raginančias ar grasinančias žinutes atsakyti negalima, jokių susitarimų tylėti, išpirkų, jokių derybų negalima net pradėti. Visada apie nemalonius nutikimus internete reikia pasikalbėti su tėvais, mokytojais ar kitais patikimais suaugusiais.  (Ką daryti?)

3. Situacijų viktorina. Trukmė - apie 10 min.

Padalykite mokinius į 3-4 komandas. Kiekviena komanda pasiskiria savo atstovą, kuris kelia ranką ir su draugų pagalba aiškina situacijas.

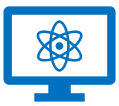
Paprašykite mokinių, kad įdėmiai išnagrinėtų parodytus pavyzdžius ir pasakytų bei paaiškintų po keletą įtarimus keliančių požymių.

Kiekvieną situaciją aiškina po dvi greičiausiai ranką pakėlusios komandas, o geriausiai atsakiusią komandą nustato arba mokytojas, arba aiškinime nedalyvavusios komandos.

Mokytojas gali pakomentuoti ir detaliai paaiškinti situaciją, jei komandų aiškinimai nėra pakankamai išsamūs.

Galite šiam žaidimui pateikti ir daugiau situacijų.

Laimi komanda, kuri geriausiai išaiškina daugiausiai situacijų.

 (Situacijų viktorina)

9.	Viktorina Ar atpažinsi socialinę inžineriją? Įdėmiai pažiūrėk į 5 situacijas ir pasakyk, kas tau jose sukelia įtarimą
10.	1. E. pašto žinutė *Pranešame, kad baigiasi jūsų slaptažodžio galiojimas.* *Slaptažodį turite pasikeisti per 2 dienas paspaudę šią nuorodą:* *password.facebook.xyz* *Klientų centras* *(00) 465-123-5555* Mokiniams turėtų sukelti įtarimą keista nuoroda, skubinimas, o ir pats raginimas pasikeisti slaptažodį, kokių paslaugų teikėjai paprastai nesiunčia. Patarimai: nespausti nuorodų žinutėse, – nuorodos gali vesti į kenksmingus tinklalapius, taip pat jos gali būti suklastotos (matome vienokį adresą, o faktinis yra kitas), todėl reikiamus adresus naršyklėje reikia surinkti patiems. Kilus įtarimui, slaptažodžius pasikeisti reikia, bet tik paslaugos teikėjo svetainėje.
11.	2. Žinutė feisbuke *Čia aš, tavo draugas Laurynas,* *mano paskyrą užblokavo, todėl rašau iš naujos.* *Primink, kada jūs su tėvais išvažiuojate atostogauti?*

	Tai bandymas apsimesti kitu asmeniu ir išgauti neviešą informaciją. Siuntėjo negalima patikrinti, be to jis klausia informacijos, kuri labai rūpi nusikaltėliams. Jei kyla įtarimų, geriausia žinutės siuntėjui paskambinti telefonu ar susisiekti kitu būdu.
12.	3. SMS žinutė *+372956232233* *Sveiki,* *Turime jums siuntinį.* *Parašykite savo adresą.* *Paštininkė* Tai bandymas išgauti adresą. Piktavalis rašo žinutes atsitiktiniais arba interneto skelbimuose rastais telefono numeriais, siekdamas patekti į namus arba surinkti duomenų sudėtingesnei apgavystei. Į nežinomų asmenų žinutes išvis nereikia atsakyti, o jas parodyti tėvams ir patikimiems suaugusiems. Visais atvejais, asmeninės informacijos atskleisti nepažįstamiems negalima.
13.	4. Interneto svetainė Čia parodyta suklastota Lietuvos banko svetainė. Įtarimų turėtų sukelti tai, kad prašoma pernelyg detalių asmens duomenų, slaptažodžio ir netgi banko kortelės duomenų. Be to, svetainės adresas atrodo irgi įtartinai. Vyresniems mokiniams galima būtų pasakyti, kad LB ir kitos valstybės institucijos jokių atskirų vartotojų paskyrų netvarko, banko kortelių duomenų nerenka ir prisijungti prie jų vartotojai gali tik su jų turimu elektroniniu parašu arba komercinių bankų suteiktomis priemonėmis. Apklausų duomenimis, tik ketvirtadalis gyventojų galėtų atskirti tikrą svetainę nuo suklastotos. Pirmiausia, reikia įsitikinti, kad tinkamai veikia svetainės meniu mygtukai, kad galima pakeisti jos kalbą, o dar geriau – visų svetainių adresus naršyklėje surinkti patiems, nespausti žinutėse gautų nuorodų.
14.	5. Nuomonių formuotoja „12 kg per 2 savaites!“ Greičiausiai, kad neįmanoma numesti tiek svorio rimtai nepakenkiant savo sveikatai. Įtarimą turėtų sukelti ir tai, kad pati nuomonės formuotoja neatrodo pati turėjusi svorio problemų, o perdėtai demonstruojami žinomų TV kanalų ženklai tarsi turėtų pridengti reputacijos dėmes ir įtikinti netikinčius. Nuomonės formuotojai, kurie naudojasi socialinės inžinerijos metodais, gali turėti didelį poveikį asmenims, organizacijoms ar net visai visuomenei. Jie gali skleisti neteisingą ar klaidinančią informaciją apie sveikatą arba skatinti žalingus įpročius, reklamuoti kenksmingas dietas. Tai gali sukelti ilgalaikę žalą sveikatai. Vyresniems mokiniams būtų galima pasiūlyti patiems internete pasitikrinti, kokius mokslus baigę šias dietas ir papildus rekomenduojantys žinovai ir sveikatos specialistai, jei jie išvis egzistuoja, o jaunesniems tiesiog patarti apie tai pasikalbėti su savo tėvais.

4. Pademonstruokite vieną savo pasirinktą vaizdo įrašą (ištrauką iki 5 min. trukmės). Rekomenduojama vaizdo medžiaga:

- „Justas“. Trukmė 3:39 min. https://www.youtube.com/watch?v=TFkXqoa0PS4
- „Phishing. Kaip apsaugoti savo duomenis?“ Trukmė 2 min. https://www.youtube.com/watch?v=Z46VMJvQwC8

5. Atvejų studija – diskusija – 10 min.

1 variantas. Aptarkite matytą siužetą. Galimi klausimai mokiniams: ar jie susidūrė su matytomis situacijomis, kaip jie jas sprendė, galbūt turi savo naudingos patirties, kuria norėtų pasidalyti su kitais. Galima paskatinti diskutuoti ir kitomis, skaidrėse paliestomis temomis. Mokytojui nereikia vertinti diskusijos turinio, tik ją paskatinti.

2 variantas. Padalykite mokinius į kelias grupes. Kiekviena grupė turi sukurti ir aprašyti vieną socialinės inžinerijos scenarijų, kaip galima internetu (žinutėmis, socialiniuose tinkluose, e. paštu ir pan.) įtikinti žmogų (pavyzdžiui, Marių, Birutę, Dovilę) atskleisti asmeninę informaciją (adresą, mokyklą ir klasę, laiptinės kodą, telefono Nr. ir pan.).

Po to kiekviena grupė pristato savo scenarijų ir paaiškina, kaip jų manymu reikia elgtis, kad būtų galima apsisaugoti nuo tokios atakos.

6. Apibendrinimas – 5 min.

15.	Klauskite! Sužinokite daugiau: www.draugiskasinternetas.lt Pabaigai apibendrinkite šios pamokos patirtį, pagirkite viktorinos laimėtojus ir aktyviausius mokinius.