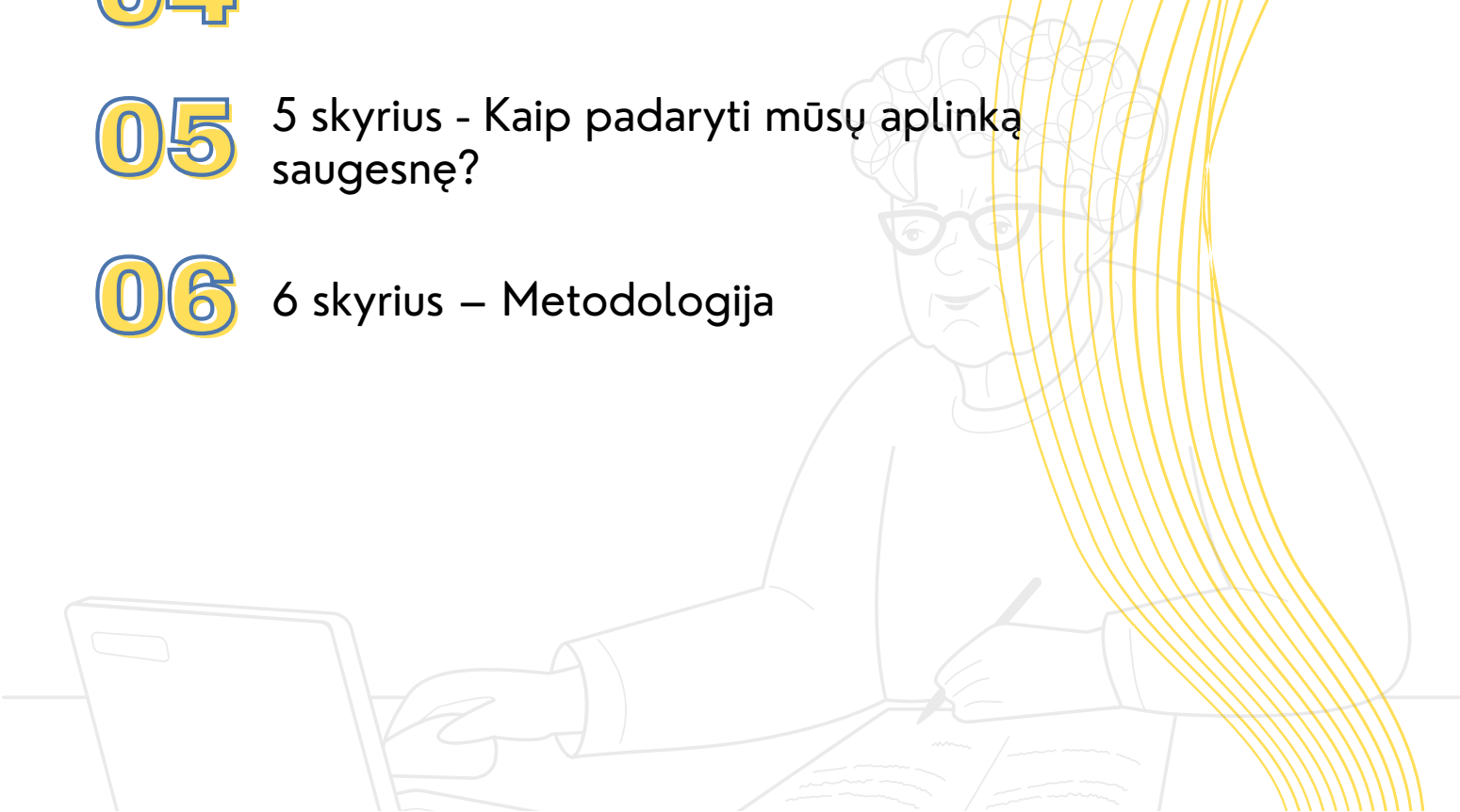
Senjorai senjorams
KURSAI
SAUGŪS INTERNETE

Saugūs internete

Turinys



Apie projektą

Projektas „Senjorai senjorams" neapsiriboja klasikine akcija ar švietimo kampanija. Šis projektas vyresnio amžiaus žmonėms suteikia konkrečius apsisprendimo ir savigynos įrankius, pagal jų gebėjimus, suteikia jiems galimybę realizuoti save, tobulėti ir rūpintis vieni kitais.

Kurso autoriai siekia ugdyti senjorų pasirengimą ir atsparumą skaitmeniniame pasaulyje, palaikydami jų kompetenciją, duodami signalą tobulėti ir tyrinėti, o ne auklėdami iš jaunosios skaitmeninės kartos autoriteto pozicijos.
Senjorai, kaip rodo jų dalyvavimas Trečiojo amžiaus universitetuose, nevyriausybinėse ir vietos organizacijose, nori būti kuo ilgiau nepriklausomi, užsiimti veikla, kuri jiems yra patogi, pritaikyta jų galimybėms, be kliūčių dėl amžiaus apribojimų.

Pripažįstame senjorų iniciatyvų galią, matome, kaip senjorai ne tik savo amžiaus grupei svarbiais klausimais, bet ir visai visuomenei, gali susivienyti ir veikti kartu. Tuo pačiu matome teigiamus rezultatus projektų, kuriuose bendraamžiai moko bendraamžius. Būtent todėl šių dviejų veiksnių sinergija prisidės prie šio projekto sėkmės ir taps svarbiu senjorų veiklos tinklų elementu.

Finansuoja Europos Sąjunga

Projekto partneriai

OSTROWIEC ŚWIĘTOKRZYSKI

CIRSA

UNIWERSYTET TRZECIEGO WIEKU WSBIP OSTROWIEC ŚWIĘTOKRZYSKI

GOŁUCHOWSKI

INICIATYVA TEZAURAS

SENASIS KĖDAINIŲ TREČIOJO AMŽIAUS UNIVERSITETAS

Kodėl vyksta kibernetiniai nusikaltimai?

Užsiėmimo forma: paskaita, pavyzdžių pristatymas ir aptarimas, diskusija
TTrukmė - 60 min.

Kas negirdėjo, kad jei tavęs nėra internete, tu neegzistuoji. Kibernetinė erdvė tapo tokia pat reali kaip mūsų kūnas ir kaulai, ji išplito ir peržengė ribas, apie kurias prieš 15 metų nebūtume nė pagalvoję. Norime to ar nenorime, kibernetinė erdvė formuoja mūsų tikrovę. Daugelis iš mūsų sutiktų, kad internetas suteikia nuostabių dalykų, pavyzdžiui, galimybę nepaisant geografinio atstumo palaikyti ryšį su šeima ir draugais, įgyti naujų gebėjimų, lengviau keliauti, susipažinti su naujais žmonėmis, dalytis žiniomis, skelbti svarbų turinį, atrasti pasaulį ir naujas galimybes ar net padėti kitiems žmonėms.

Daugelis taip pat sutiks, kad internete tenka peržvelgti begalę puslapių su šiukšlinu turiniu, kuris veiksmingai atitraukia mūsų dėmesį, dėl to jaučiamės blogai, kad gaištame tiek daug laiko. Yra ir trečioji interneto pusė, tamsioji, su kuria dauguma iš mūsų tikisi niekada nesusidurti, - kibernetiniai nusikaltimai.

Augant kibernetinių nusikaltimų mastui, tyrėjai vis labiau domisi nusikaltėlio motyvacija ir psichologiniu profiliu. Nusikaltėliai ieško tinkamų saugumo priemonių trūkumo, programinės įrangos pažeidžiamumo arba nepakankamų naudotojo žinių, prieigos prie kieno nors išteklių. Viena vertus, anonimiškumas, potencialiai maža rizika būti sugautam ir proporcingas pelnas, kita vertus, didelio masto kibernetiniai nusikaltimai suteikia nusikaltėliui galimybę būti pastebėtam ir išgarsėti, o pinigai yra tik priedas.

Mes, privatūs naudotojai, galime tapti įsilaužėlių aukomis įvairiais lygmenimis. Labiausiai tikėtina, kad susidursime su pelno siekiančiu įsilaužėliu, kuris savo tikslui pasiekti naudos įvairią nusikalstamą veiklą.
Lisa O'Reilly pateikė 9 argumentus[1], kodėl kibernetinės atakos yra tokios sėkmingos. Tarp jų yra šie:

- „Nusikaltėliai yra protingi ir įgudę. Nusikaltėlių tinklas yra organizuotas, bendradarbiaujantis ir gerai finansuojamas. Ir dabar labiau nei bet kada anksčiau jie turi techninių išteklių, kad galėtų kurti ir įgyvendinti naujus ir sudėtingus atakų metodus". Tai nereiškia, kad mes nesame protingi, bet nepamirškite, kad jie gyvena tam, kad apgaudinėtų kitus, o tai reiškia, kad jie nuolat kuria naujus būdus, kaip apgauti žmones, galvoja apie tai kaip apie „standartinį" darbą, jų pajamos priklauso, nuo jų kūrybiškumo ir darbo valandų.
- Nusikaltėliai iš savo pastangų uždirba daug pinigų.
- Organizacijos daro klaidų. Tyrimai rodo, kad organizacijos neturi tinkamų duomenų apsaugos ir atsarginių kopijų planų, kurie padėtų užtikrinti veiklos tęstinumą. Sistemų ir darbuotojų mokymo trūkumas sukuria palankią terpę kibernetinėms atakoms.
- Vartotojai daro klaidas. „Dažnai mes, naudotojai, darome klaidas, kuriomis nusikaltėliai gali pasinaudoti, kad gautų prieigą prie mūsų duomenų ir paskyrų. Pavyzdžiui, dalijamės savo prisijungimo ar tapatybės nustatymo duomenimis, naudojame tą patį slaptažodį kiekvienai paskyrai, spaudžiame įtartinas nuorodas, naudojame neautorizuotus įrenginius ar programas, atmetame programinės įrangos atnaujinimus ir pan.

[1] O'Reilly L., "9 Reasons Cyberattacks are So Successful" January 15, 2019, online: https://securityboulevard.com/2019/01/9-reasons-cyberattacks-are-so-successful/, access

- ·„Pardavėjai daro klaidas". Net tokios didelės bendrovės kaip Microsoft ar Firefox gali padaryti ką nors, dėl ko jų naudotojai susidurs su kibernetinėmis atakomis.
- „Dauguma kibernetinio saugumo sprendimų veikia NE realiuoju laiku". Žmonės, atsakingi už kibernetinį saugumą, visada per žingsnį atsilieka nuo nusikaltėlių.

Kibernetiniai nusikaltėliai taip pat naudoja vadinamąją socialinės inžinerijos taktiką, kuria manipuliuojant apgaudinėjami žmonės, pasitelkiant labai įtikinamas istorijas tam, kad įgytų mūsų pasitikėjimą, apgautų mus, o tada gautų svarbią informaciją ir pavogtų mūsų pinigus, asmeninius duomenis ar net tapatybę.

Baimė gali kilti, kai pagalvojame apie beribę ir sienų neturinčią kibernetinę erdvę, kuri rodo tas pačias kibernetinių nusikaltimų savybes, ir galime pasijusti bejėgiai, maži ir nereikšmingi. Vienas blogiausių dalykų, kuriuos galime padaryti kaip naudotojai, yra neprašyti pagalbos. Kova su kibernetiniais nusikaltimais yra mūsų visų atsakomybė. Turime padėti vieni kitiems įveikti baimę būti atstumtiems vien dėl to, kad tapome kibernetinių nusikaltimų aukomis.

Labai klystumėte, jei manytumėte, kad kibernetinių nusikaltimų aukomis tampa tik vyresnio amžiaus žmonės. FTB 2021 m. paskelbtoje ataskaitoje apie elektroninius nusikaltimus pateikia tikslų užregistruotų nusikaltimų Jungtinėse Amerikos Valstijose (JAV) skaičių kartu su aukos amžiumi ir bendru nuostoliu tam tikrose amžiaus grupėse. Senjorai yra reikšmingiausia, bet ne vienintelė grupė. Ne naujiena, kad net ir skaitmeninėje eroje užaugęs jaunimas tampa vis išradingesnių sukčiavimo būdų aukomis. Fully-verified.com duomenimis, vienas populiariausių žmonių apgaudinėjimo būdų yra interneto svetainės ir mobiliosios programėlės, kuriomis kasdien naudojasi jaunimas.

Apgavystės pavyksta, nes jos atrodo kaip tikri dalykai. Norint pastebėti skirtumą, reikalingas mūsų įžvalgumas, sąmoningumas ir žinios apie tai, ko gali ir ko negali prašyti įstaigų atstovai. Sukčiavimai paremti skubėjimu ir baime kiekviename žingsnyje, vagys nori įvesti skubėjimo elementą, baimę, kad netrukus prarasime kažką brangaus. Tokiose situacijose tik nedaugelis gali išlikti ramūs ir elgtis racionaliai, mūsų pasąmonė perima mūsų minčių ir veiksmų kontrolę. Eddy Willemsas aprašė šešis įtakos principus, kurie paaiškina psichologinius kibernetinių nusikaltimų aspektus, ir tai galima pavadinti esme, kodėl kibernetiniai nusikaltimai veikia.

Eddy Willemsas aprašė šešis įtakos principus, kurie paaiškina psichologinius kibernetinių nusikaltimų aspektus, ir tai galima pavadinti esme, kodėl kibernetiniai nusikaltimai veikia.

1 **Abipusiškumo principas** reiškia, kad žmonės jaučiasi tam tikru būdu skolingi asmeniui, kuris arba ką nors dėl jų padarė, arba ką nors pasiūlė ar davė, aiškiai nesitikėdamas grąžos"[2]. Įsivaizduokite tokią situaciją: klientė buvo informuota, kad banko konsultantas išgelbėjo jos pinigus, dabar jie paprašys ko nors nedidelio, pavyzdžiui, prisijungti prie savo banko sąskaitos, pateikti jiems pagrindinius asmens duomenis, juk jie išgelbėjo jūsų santaupas, abejoti jų gerais ketinimais atrodo absurdiška, todėl duosime jiems tai, ko jie nori.

„Konsensusas/sutarimas" - kai žmonės nėra tikri, jie stengiasi rasti kitų, kurie padėtų jiems suformuluoti nuomonę. Net jei jie yra tikri dėl savo įsitikinimų, konsensuso nuomonė gali būti labai įtikinama"[2]. Prisimenate didelio masto savanorišką pagalbą Ukrainai po Rusijos agresijos 2022 m. vasarį? Daugelis žmonių įkūrė labdaros fondus, rinko aukas, kurios pasiekė realius žmones ir pakeitė padėtį ukrainiečių labui. Kibernetiniai vagys tuo naudojasi kaip dar viena galimybe apgauti tuos, kurie norėjo padėti.

2

3

Nuoseklumo principas grindžiamas tuo, kad mums patinka veikti nuosekliai pagal savo anksčiau turėtas pažiūras. Dėl įsipareigojimo jaučiame tam tikrą spaudimą elgtis tam tikru būdu"[2]. Galbūt dvejojome arba jautėmės nesaugiai, kai kas nors mums paskambino ir paprašė paaukoti, bet kadangi laikome save gerais žmonėmis, norinčiais padėti kitiems, ypač, kai vagis pavartos tokius sakinius: kiekvienas įneša savo indėlį, geros širdies žmonės sumokės net ir nedidelę sumą, galėjome jaustis priversti sumokėti/padėti.

Simpatija: Kibernetinis nusikaltėlis dažnai naudojasi savo žavesiu. Telefonu atrodydami simpatiški, jie stengiasi priversti aukas paklusti prašymui pateikti slaptą informaciją.

4

5

Kartais jie taip pat žaidžia autoriteto principu, siųsdami suklastotą generalinio direktoriaus el. laišką. Žmonės linkę paklusti, nes prašymas tariamai ateina iš aukšto rango asmens"[2]. Mūsų smegenys iš tiesų linkusios sekti autoritetais, pavyzdžiui, įžymybe, mokslininku, politiku, kuriam simpatizuojame.

Laiko stoka - kai įsivaizduojama, kad laikas, per kurį reikia atsakyti į tam tikrą prašymą, yra labai trumpas, žmonės labiau linkę šį prašymą vykdyti. Pavyzdys - apgaulingi laiškai neva iš mokesčių inspekcijos, kuriuose prašoma skubiai reaguoti paspaudžiant nuorodą, nes kitaip gresia bauda. Labiausiai tikėtina, kad paspausime, nepagalvoję apie galimas pasekmes.

6

Niekas nėra nuolat pasiruošęs, kiekviename žingsnyje laukiantis atakos, kaskart tikrinantis žalią pakabinamą spyną, nuorodos adresą ar prašantis skambinančio kliento tarnybos patvirtinti jų autentiškumą. Sukčiai tampa vis gudresni ir naudojasi naujomis technologijomis, naujais produktais ar paslaugomis ir svarbiais įvykiais, kad sukurtų įtikinamas istorijas, kurios įtikintų jus atiduoti jiems savo pinigus ar asmeninius duomenis. Jie naudojasi žmonių naivumu, žinių stoka ar net noru padėti kitiems. „Po kibernetinės atakos daugelis nukentėjusiųjų teigia, kad jaučiasi traumuoti, apiplėšti, pažeidžiami arba bijo, kad ataka gali pasikartoti. Kaltės ir gėdos jausmas dažnai dar labiau sustiprėja, kai dėl to, kad jie tapo atakos ir (arba) sukčiavimo auka, juos kaltina jų organizacija, šeimos nariai ar apskritai visuomenė".

Dėl nuolatinio aukų smerkimo sukuriama aplinka, kurioje žmonės apie nusikaltimą nenori pranešti ir kenčia vieni. Šiuo atveju tai turėtų tik neigiamų pasekmių ne tik asmeniui, bet ir visai sistemai. Saugumo institucija, negalės veiksmingai mokytis ir kovoti su kibernetiniais nusikaltimais, jei negaus informacijos apie juos. Tuo pat metu mūsų fizinis kūnas ir psichika dėl neišsakytų, nepraneštų tragiškų įvykių, negaunant reikiamos pagalbos ir paramos, gali sutrikti.

[2] Willems E., The psychology of cybercrimes, online: https://www.gdatasoftware.com/blog/2022/07/cybercrime-psychology

Tendencija investuoti į kibernetinį saugumą pastebima labiau nei bet kada anksčiau. Bankai, policija, valstybinės institucijos ir net medicinos įstaigos stengiasi atlikti savo vaidmenį apsaugant piliečius ir klientus nuo neigiamo kibernetinių atakų poveikio. Jei ši tema tokia opi ir visuotinė, kodėl skundų ir nuostolių mastas vis dar auga? Ar tie veiksmai neefektyvūs, praleidžiami, nepasiekia adresato, ar yra pernelyg sunkiai suprantami?

Dažniausiai, adresuojant juos bendram gavėjui, neišskiriami konkrečių grupių poreikiai ir reikalavimai. Daroma prielaida, kad trumpa informacija „nedaryk taip", „daryk taip", „būk atsargesnis" išugdys saugų elgesį. Kibernetiniai nusikaltimai metams bėgant tampa tiesiogine, įprasta grėsme ir, kaip rodo statistika, kiekviena grupė yra pažeidžiama. Vis dėlto viena iš labiausiai pažeidžiamų grupių yra senjorai.

Yra dar vienas dalykas, kurį reikia aptarti. Kalbėjome apie psichologinius nusikaltimų ir aukos aspektus, apie tai, kokia gali būti situacija ir kokios emocijos mus gali apimti naršant internetą. Išsiaiškinsime, kaip netapti auka, tačiau labai svarbu žinoti, kaip gali jaustis žmonės, padėti jiems suprasti, kad jų jausmai yra normalūs, įprasti. Ką galime daryti, kai tampame auka:

- „Nustatykite, kaip jaučiatės ir kokios yra jūsų mintys. Supraskite, kad esate ne vienas.
- Priminkite sau savo teigiamas puses, savybes ir, nepaisant su kibernetiniais nusikaltimais susijusių praradimų, pasiekimus.
- Venkite kaltinti save. Skirkite laiko ir energijos tam, ką galite kontroliuoti; ir konstruktyviai panaudokite tai, ką sužinojote, kad geriau apsaugotumėte save ir kitus.
- Surinkite tinkamą paramą, išteklius ir paslaugas, kad užtikrintumėte savo saugumą ir sumažintumėte riziką vėl tapti auka.
- Praktikuokite užuojautą sau: būkite sau geri, nesmerkite savęs, įsidėmėkite savo mintis ir jausmus ir pažvelkite į juos iš perspektyvos; pripažinkite ir supraskite, kad esate žmogus, ir priimkite netobulumus, kurie būdingi žmogui.
- Ieškokite socialinės paramos. Jums gali būti naudinga prisijungti prie paramos grupių, skirtų elektroninių nusikaltimų aukoms, arba prie bet kokių paramos aukoms grupių.
- Nedvejodami kreipkitės profesionalios pagalbos, jei vis jaučiate didėjančią psichologinę įtampą; sunkumus vykdant užduotis ar rūpinantis pareigomis; chronišką prislėgtą nuotaiką ar pernelyg didelį nerimą, kurį vis sunkiau suvaldyti; nejaučiate malonumo užsiimant veiklomis; miego ir (arba) dėmesio koncentracijos sunkumus; ar kitus psichologinius simptomus, kurie gali kelti jums nerimą"[3]

Jūsų, kaip švietėjo, mokytojo, sąmoningo piliečio ir vietos bendruomenės nario, vaidmuo - ne tik šviesti žmones, parodyti jiems, kaip išvengti nusikaltėlių internete, supažindinti juos su naujausiais pavojais, bet ir padėti, jei jie buvo tapę aukomis.

Peržiūrėkite papildomą šio skyriaus medžiagą

[3] Willems E., The psychology of cybercrimes, online: https://www.gdatasoftware.com/blog/2022/07/cybercrime-psychology

Sukčiavimo būdai - mechanizmai

Informacija lektoriui:
Trukmė - 3 val.
1.Išdalykite korteles su pavyzdžiais ir užduotimis.
2. Pristatykite toliau pateiktą medžiagą.
3. Pasinaudokite pavyzdžiais ir pratimais, kai žemiau esančiame tekste matysite informaciją, nurodančią juos atlikti ar pasižiūrėti pavyzdį. Aptarkite pratimus su dalyviais.
4. Stebėkite laiką - turite 3 valandas pagal sistemą 45 min. mokymasis, 15 min. pertrauka.

Yra daug įvairių sukčiavimo būdų. Sukčiai išradinėja vis naujus būdus, kaip pavogti pinigus, duomenis ir persekioti jus tol, kol negaus to, ko nori. Įgyvendinant kurso tikslus suskirstėme žinomus sukčiavimo atvejus į keletą kategorijų:

- Asmens duomenų vagystės.
- Sukčiavimai, kada daugiausia siekiama apgauti perkant ir parduodant.
- Sukčiavimai, susiję su romantiniais santykiais ir pasimatymais.
- Sukčiavimai, susiję su labdara.
- Sukčiavimai, susiję su investavimu ir pinigų uždirbimu.
- Sukčiavimai, susiję su darbo pasiūlymais.
- Sukčiavimai, susiję su loterijomis ir prizais.
- Pavojingos SMS žinutės

01 ASMENS DUOMENŲ VAGYSTĖS

Kodėl kas nors norėtų pavogti mano duomenis? Kam reikia mano asmens tapatybės kortelės ar paso numerio? Esu eilinis pilietis. Nusikaltėliams labai vertingi yra ir paprastų piliečių asmens duomenys. Kaip minėjome anksčiau, pagrindinis daugelio kibernetinių nusikaltėlių motyvas yra pinigai, jūsų asmens tapatybės dokumento numeris dažnai būna susietas su banko sąskaita, kurioje laikote savo santaupas. Kai nusikaltėliai gauna prieigą prie jūsų asmens tapatybės dokumento numerio, kredito kortelės numerio, banko sąskaitos prisijungimo duomenų arba prisijungimo prie jūsų banko sąskaitos ar el. pašto duomenis, jie gali atlikti pervedimus, pirkimus, atidaryti naujas sąskaitas, imti paskolas. Vienu ar kitu būdu jie gali priversti jus prarasti pinigų arba priversti grąžinti ne jums priklausančias paskolas.
skolas.

Kodėl vagišiams reikia mano duomenų:

1. apsimesti jumis, imti kreditus, apgaudinėti kitus žmones ir siųsti jūsų melagingas nuorodas kitiems žmonėms jūsų vardu;
2. jūsų duomenys gali būti naudojami siekiant gauti prieigą prie kitų jūsų virtualaus gyvenimo sričių, įskaitant prieigą prie bankininkystės, socialinės žiniasklaidos, kredito kortelių duomenų;
3. pavogti kitų su jumis susijusių asmenų, pavyzdžiui, šeimos narių, draugų, kolegų, asmeninius duomenis;
4. pakenkti jūsų reputacijai, sukelti viešą pažeminimą, patyčias virtualiame pasaulyje;
5. gauti prieigą prie kitos informacijos, pavyzdžiui, profesinės informacijos, ypač jei užimame aukštas pareigas;
6. prieiti prie mūsų finansinės istorijos ir panaudoti ją prieš mus;
7. pavogti mūsų socialinės žiniasklaidos paskyrą, ypač jei turime daug sekėjų, parduoti tokią paskyrą arba naudoti mūsų paskyrą bandant apgauti kitus naudotojus.

Ar prisimenate kokių nors pranešimų apie didelio masto naudotojų duomenų vagystes ar nutekėjimą? Su tokiomis problemomis susidūrė Sony PlayStation Network, Uber, Yahoo, viešbutis „Mariott" ir net populiarusis Facebook. Galbūt manote, kad šios problemos jūsų niekaip nepaveikė. Galbūt esate teisūs, tačiau pagalvokite apie mastą, apie milijonus duomenų, kurie pateko į erdvę, prie kurių gali prieiti visi, ypač tie, kuriems rūpi kieno nors kito patiriama žala. Ne visi buvo paveikti tokiu pat mastu. Daugelis žmonių dėl šių veiksmų prarado savo paskyras, pradėjo gauti el. laiškus ir pranešimus su keistomis nuorodomis ir turiniu, nuorodas į kitas svetaines, prašymus sumokėti, šantažą. Kai kurie taip pat gavo žinutę iš savo draugų, kad gavo keistą nuorodą iš mūsų paskyros. Vien dėl to, kad iš savo banko sąskaitos nepraradome nė cento, nereiškia, kad nepatyrėme nuostolių dėl kibernetinių nusikaltėlių.

Kalbant apie asmens duomenų vagystes, svarbu paminėti šias atakas phishing, t. y. pinigų išviliojimas naudojant socialinės inžinerijos metodus, psichologinių mechanizmų naudojimas siekiant apgauti žmones ir pavogti jų duomenis, pavyzdžiui, prisijungimo vardus, slaptažodžius ir kredito kortelių duomenis. Nusikaltėliai apgaule įtikina žmones atidaryti nesaugias nuorodas, tokių situacijų dažnai pasitaiko parduodant ir perkant internetu.

ATLIKITE 1 PRATIMĄ

02 SUKČIAVIMAI PERKANT IR PARDUODANT

Pagal visas prognozes, susijusias su pardavimu internetu, tai - dinamiškai ir nenutrūkstamai besivystanti šaka. Tai reiškia, kad sukčiavimų šioje srityje taip pat daugės. Vis daugiau žmonių perka daiktus internetu, tarp jų ir senjorai. Šiandien senjorai nebesijaučia pasimetę ir neužtikrinti internete, priešingai, jie naudojasi kompiuteriais, išmaniaisiais telefonais, žaidžia konsolėmis, jie moka pirkti internetu. Senjorai tampa svarbia grupe, kurios buvimas vis labiau pastebimas. Kartu tampa kibernetinių vagių taikiniu.

Gana įprasta prie savo asmeninės banko sąskaitos prisijungti kredito kortele, kartais dėl netinkamų saugumo metodų, pavyzdžiui, antivirusinės programos nebuvimo, mūsų duomenys gali patekti į vagišių rankas. Ką daryti, kad išvengtumėte tokių situacijų? Galbūt sakysite, kad nesinaudokite kreditine kortele internete, ir tai būtų tiesa, tačiau ar turėtume leisti vagišiams turėti įtakos jūsų apsisprendimams? Ar dėl kažkieno neteisėtų veiksmų turėtume save apriboti?

Apie tai, kaip užkirsti kelią mūsų duomenų praradimui, daugiau sužinosite 3 skyriuje.

Prekių pardavimas

Labai populiarūs sukčiavimai, susiję su pardavimo platformomis, pavyzdžiui, Vinted arba Olx, kuriose galime parduoti įvairius daiktus. Didžiąja dalimi tai yra portalai, nors ir ne išimtinai, skirti privatiems naudotojams. Kai bandome ką nors parduoti, pvz.: drabužius, žaislus ar kitus daiktus, galime gauti žinutę, dažniausiai per žinučių tarnybą „What's up" arba SMS žinutę, kurioje prašoma šio konkretaus daikto su nuoroda į mūsų aukcioną.

Kaip tai paprastai daroma:

1. Pradedame kalbėtis su pirkėju ir sužinome, kad jis ar ji nenori derėtis dėl kainos ar sutinka su daikto trūkumais, jie siekia kuo greičiau užbaigti sandorį.
2. Mums sutikus su sąlygomis, jie atsiunčia mums keistą nuorodą su informacija, kad ją paspaustume, ir pinigai bus automatiškai išsiųsti į mūsų sąskaitą.
3. Taip pat dažnai pasitaiko, kad potencialaus pirkėjo žinutėse yra daug rašybos klaidų, keistų sakinių, tarsi kažkas ne visai mokėtų mūsų kalbą.
4. Kai kurie vagišiai taip pat naudojasi riboto pasitikėjimo mūsų atžvilgiu taisykle, aukcionuose išsirenka didelės vertės daiktus ir praneša, kad daiktą pirks, bet tik grynaisiais pinigais. Jie atsiunčia mums nuorodą į, jų teigimu, kurjerio puslapį su jau sugeneruota transportavimo etikete. Informacija apie apmokėjimą gudriai paslėpta, iš tikrųjų pirkėjai generuoja etiketę be grynųjų pinigų pristatymo būdo, tačiau iš pirmo žvilgsnio tai sunku pastebėti.
5. Spustelėję nuorodą, galime būti nukreipti į puslapį, per kurį mūsų kompiuteryje įdiegiama kenkėjiška programinė įranga arba kuriame, įvedus mūsų duomenis, jie kopijuojami.

Pigios prekės ir netikros parduotuvės

Kaip žinoti, kad greičiausiai turime reikalų su netikra parduotuve?

- Atrodo kaip tikra parduotuvė, graži grafika, su pavadinimu, kuris nekelia abejonių, arba pavadinimas, artimas kitoms panašioms parduotuvėms.
- Labai palankios kainos, daug mažesnės nei kitose žinomesnėse svetainėse.
- Standartinė pirkimo procedūra, tokia pati mokėjimo galimybė kaip ir kitose svetainėse.

Baigę mokėjimo procedūrą galime gauti el. laišką su užsakymo patvirtinimu, kuris iš tikrųjų tik atbukins mūsų budrumą. Tikėsimės, kad kažką nusipirkome legalioje parduotuvėje. Praeis kelios dienos, o prekės taip ir nebus pristatytos. Ryšys su pardavėju staiga nutrūks arba jis net gali paprašyti mūsų papildomai sumokėti dėl nenuspėjamų mūsų šalies muitinės įstatymų. Siuntinys iš tiesų niekada nebuvo išsiųstas, arba vietoj naujo „iPhone", už kurį sumokėjome, galime gauti siuntinį su kojinių pora.

Atlikite 2 pratimą

03 PASIMATYMAI IR ROMANTINĖS PAŽINTYS

Per pastaruosius kelerius metus buvome liudininkais nesuskaičiuojamų sukčiavimų, pagrįstų netikromis meilės istorijomis, internetinės romantikos sukčiavimais, kurie statista.com duomenimis, užima trečiąją vietą kibernetinių nusikaltėlių naudojamų metodų sąraše. Pirmą kartą šis metodas buvo aprašytas 2008 m. ir nuo to laiko buvo apgauta daugybė žmonių, o didžioji dauguma jų - moterys, nors ir ne tik jos. Internetas yra didžiulė mūsų gyvenimo dalis, romantinės pažintys ir pasimatymai taip pat persikėlė į šią sritį.

Daugeliu atžvilgių tai prasideda panašiai:

1. Gavote el. laišką laišką arba žinutę socialinėje žiniasklaidoje ar pasimatymų portale.
2. Asmuo yra iš kitos šalies arba turi įdomią, neįprastą profesiją, paprastai reikalaujančią pasiaukojimo, izoliacijos, dažnų kelionių, kartais pavojingų ir, be abejo, jaudinančių.
3. Su šiuo asmeniu bendraujate kelias dienas, savaites, net mėnesius. Sukčius įgyja jūsų pasitikėjimą; jūs neturite visiškai jokių priežasčių ką nors įtarti.

4.Pradedate emociškai įsitraukti į šiuos santykius, būtent šito sukčiai ir nori pasiekti nuo pat pradžių. Jie žino, kad labai sunku pasakyti ne žmogui, kuriuo pasitikime ar net mylime.

5.Gali būti vaizdo skambučių, nuotraukų, mūsų „partneris“ atrodo labai įsitraukęs, yra žavus, jaučiame, kad sutikome tinkamą žmogų. Jis žada susitikti, patikina mus savo jausmais, įsipareigojimu, žada bendrą ateitį, tačiau visus planus sužlugdo jo reiklus darbas.

6. Įgiję mūsų pasitikėjimą ar meilę, sulaukiame dažnai dramatiško prašymo, dažniausiai tada, kai jie pagaliau atvyksta su mumis susitikti. Sužinome, kad mūsų draugas ar mylimas žmogus iš interneto turi problemų, jis (ji) buvo apiplėštas (-a), jam (jai) reikia pinigų lėktuvui ar kitai transporto priemonei, jis (ji) buvo suimtas (-a) oro uoste ir už jį (ją) reikia sumokėti užstatą, jis (ji) buvo pagrobtas (-a), jam (jai) reikia kyšio oro uosto pareigūnams, policijos valdybos apsaugai.

Kartais šis asmuo prašo ne tik pinigų, bet ir prieigos prie jūsų banko sąskaitos, pervesti pinigus jų vardu, paimti už juos paskolą, asmens dokumentų, pavyzdžiui, pasų ar vairuotojo pažymėjimų kopijų, nupirkti ir atsiųsti „Amazon" ar „iTunes" dovanų kortelių kodus. Prašymas dažnai būna derinamas su skubotumo ir pavojaus jausmu, todėl negalime išanalizuoti situacijos ir racionaliai pažvelgti į reikalą. Sukčius nori, kad mes būtume emocionalūs, dažnai neapgalvotai ir neracionaliai elgtumės. Romantinio sukčiavimo mastai vis didėja. ir toks sukčiavimo būdas buvo įprastas siekiant apgauti žmones Kovid-19 pandemijos metu. Tuo metu informacija, kad kažkas negali susitikti dėl apribojimų, sveikatos problemų ar karantino, buvo labai tikėtina ir nekėlė įtarimų. Tuo pat metu namuose užsidarę žmonės jautėsi kaip niekada vieniši, daugelis jų internete ieškojo draugų ar mylimų žmonių.

Atlikite 3 pratimą

04 NETIKRA LABDARA

Sukčiai, ieškant naujų žmonių apgaudinėjimo būdų, nežino ribų. Melaginga labdara yra itin veiksminga, ypač, kai ji derinama su manipuliavimo metodais, nes apeliuojama į žmonių gerumą ir grindžiama mažais, nieko neįtariančiais prašymais, pavyzdžiui, galimai mažomis aukų sumomis. Pasitikėdami labdaros organizacijomis net negalime įsivaizduoti, kad kas nors pasinaudotų kieno nors liga ar kančia, kad iš to uždirbtų pinigų.

Sukčiai taip pat supranta, kad yra tam tikrų situacijų, kurios tiesiogine prasme atveria žmonių širdis ir pinigines, pavyzdžiui, smurtas prieš vaikus, stichinės nelaimės kitose šalyse arba ginkluoti konfliktai. Kai kurie sukčiai puikiai kopijuoja arba apsimeta tikromis institucijomis, dažnai naudodami ir jų metodus, pavyzdžiui, tiesioginiais prašymais siunčiamais, pavyzdžiui, elektroniniu paštu, arba labdaros aukcionus. Kartais sukčiai veikia prisidengdami registruota organizacija, kuri galbūt net ir nedideliu mastu vykdo labdaringą veiklą, iš tikrųjų procentinė šios organizacijos realios paramos dalis yra nežymi.

Labdaros sukčiai veikia panašiais būdais:

- ·Spaudimais, kaip ir kitų rūšių kibernetiniuose nusikaltimuose. Tai yra pirmasis ženklas, kad kažkas gali būti negerai. Labdaros dažnai reikia kuo greičiau, tačiau tikros NVO nereikalauja, kad mokėtumėte dabar, šiandien, šią minutę. Jos mielai duos jums lankstinuką, daugiau informacijos ir paprašys paaukoti, kai būsite pasiruošę, naudodamos jums tinkamiausius būdus, pavyzdžiui, mokėjimą internetu.
- Nusikaltėliai dažnai norės priversti mus taikyti mokėjimo būdus, kurie yra greiti, paprasti ir sunkiai atsekami bei atšaukiami.
- Sukčiai gerai pasiruošia savo vaidmeniui ir turi atsakymus į daugelį klausimų, kuriuos gali užduoti kitoje pusėje esantis asmuo.
- Atsisakymas pateikti daugiau informacijos: sukčiai dažnai atsisako pateikti daugiau informacijos, motyvuodami: laiko stoka, aplinkos tausojimu (todėl jie neturi lankstinukų), tuo, kad organizacijoje yra naujokai savanoriai, todėl negali prisiminti viso organizacijos pavadinimo ir asmens kodo.
- Dokumentai, kurie atrodo teisingi, bet dažnai yra parašyti kita kalba arba yra labai bendro pobūdžio, migloti.
- Sukčiai žino, kad racionaliąją mūsų smegenų dalį reikia užmigdyti, įvedant sumaištį, skubėjimą, baimę, emocionalumą, kad negalvotume apie tai, ką darome, kad veiktų pasąmonė, vedama paprastų žinučių, darytų tai, ko prašo nusikaltėlis.

https://www.aarp.org/money/scams-fraud/info-2019/charity.html

Atlikite 4 pratimą

05 INVESTAVIMAI

Kasdieniame gyvenime dažnai daug dėmesio skiriame pinigams, galvojame, kaip praturtėti, kur gauti pinigų remontui, kelionėms. Mums, žmonėms, taip pat patinka paprasti sprendimai, dažnai nereikalaujantys daug pastangų. Kai išgirstame ir pamatome straipsnio antraštę apie "didelį pelną, unikalią galimybę padidinti savo uždarbį, neįtikėtiną galimybę, apie kurią žino nedaug žmonių", mūsų pasąmonė reaguoja susidomėjimu ir noru ištirti šią neįtikėtiną galimybę praturtėti.
Apgaulingos investicijos, grindžiamos veiksmais, kuriais siekiama įgyti mūsų pinigų, viliojami didelės grąžos, investuojame visas savo santaupas ir net imame paskolas, manydami, kad investicijų grąža leis mums jas iš karto grąžinti.

Kaip paprastai atrodo investiciniai sukčiavimai?

- Jie dažnai atrodo labai realistiški, juose daug techninių, finansinių detalių, kurių iki galo nesuprantame. Kibernetiniai nusikaltėliai yra gerai pasirengę, patyrę kurti melagingas istorijas, kurios skamba labai tikroviškai, paremtos suklastotais dokumentais, duomenimis.

- Jie susiję su mūsų tuštybe, mūsų sunkia padėtimi. Teigiama, kad mums pasisekė, kad mes buvome tokie pakankamai išmintingi, kad nusprendėme investuoti. Pasiūlymai dažnai atrodo pernelyg geri, grąža itin didelė, nedaug apribojimų, puikios galimybės, dažnai nereikia jokių papildomų dokumentų, patvirtinimų, ir galiausiai jaučiame, kad sėkmė mums nusišypsojo - radome unikalią galimybę.

- Laiko spaudimas, verčiantis mus priimti greitus sprendimus. Kas negirdėjo ar neskaitė: „Šis pasiūlymas skirtas tik jums, privalote apsispręsti tuojau pat, pasiūlymas yra ribotas, eilėje laukia daug žmonių, todėl turėtumėte būti dėkingi". Nenuostabu, kad visa tai girdėdami žmonės nusprendžia dalyvauti abejotinose akcijose.
- Naudojasi tikrais įvykiais, naujomis technologijomis ir net gandais apie finansines situacijas, pavyzdžiui, kriptovaliutų rinka. Kibernetiniai nusikaltimai grindžiami visiems gerai žinomomis istorijomis, apie kurias visi yra girdėję, pateikiami pavyzdžiai žmonių, kurie iš kriptovaliutų ar kitų spekuliacijų uždirbo daug pinigų. Internete gausu vadovėlių, kuriuose girdime, kad tik greiti, dažnai rizikingi veiksmai atneša pelną, juk sunkiu darbu niekas nepraturtėjo. Mes nusprendžiame imtis veiksmų, kuriais iki galo nepasitikime, bet tikime, kad jie mums taip pat atneš turtus. Kibernetiniai nusikaltėliai verčia mus jaustis patenkintais savo investicijomis, įtikinėja mus eiti toliau, įvairiais metodais priveda mus prie situacijos, kai nebegalime atsiimti pinigų, bijome tai padaryti, nežinome kaip, kol galiausiai prarandame visas savo santaupas, įsitikinę, kad kažkur padarėme klaidą.

https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams/virtual-money-investments.html

06 DARBO PASIŪLYMAI IR ĮDARBINIMAS

Kaip galima užsidirbti pinigų iš melagingų darbo skelbimų? Atsakant į šį klausimą, reikia priminti, kad mūsų asmeniniai duomenys yra labai vertingi, vagišiai gali uždirbti daug pinigų arba panaudoti juos kitais tikslais. Antra, sukčiai daugina savo pelną, prašydami mažų pinigų sumų iš daugybės žmonių, prašydami nedidelių sumų, pavyzdžiui, registracijos mokesčio, užstato, atlikti nedidelį banko pervedimą, patvirtinantį banko duomenis, kuris vėliau grąžinamas. Jie nesukelia daug abejonių, net jei įsidarbinantys asmenys su tokia veikla susiduria pirmą kartą. Dažnai, būdami pensininkai arba gaudami pensiją, norėtume užsidirbti papildomų pinigų, kad būtų lengviau gyventi. Tuomet ieškome darbo, kuriame nereikėtų atlikti per daug varginančių fizinių darbų. Sakome sau, kad galėtume rasti papildomų pinigų, paprasčiausiai internetiniuose darbuose, spausdami ant skelbimų, pildydami apklausas ir pan. Iš pradžių ieškome ko nors greito, lengvo ir vidutiniškai apmokamo darbo ir randame, kuris, atrodo, atitinka visus mūsų lūkesčius, kaip ir pirmiau minėtais atvejais, beveik per daug tobulas, kad būtų tiesa.

Yra trys pagrindiniai darbo pasiūlymų sukčiavimo būdai.

Pirma. Sukčiai siūlo darbą, kuris nereikalauja daug pastangų, kurį galima atlikti namuose, su viena sąlyga: sumokėti už pradinį rinkinį arba medžiagas. Galiausiai nieko negausite arba gausite visai ką kita, nei tikėjotės. Net jei sukčiams darbą atlikote, jie jums visai nesumokės arba sumokės mažai, nes darbas bus atliktas ne pagal jų standartus. Teikti ieškinį taip pat nepadės, nes dažnai įmonė neegzistuoja arba mes nesame pasirašę jokios sutarties.

Antra. Padarykite mažai, o gaukite daug daugiau. Vagys prašys atlikti smulkmenas: pateikti daugiau asmens duomenų, užsiregistruoti specialioje nemokamoje platformoje, atsiųsti gyvenimo aprašymą. Tai atlikę jie gaus asmens duomenis, kuriuos parduos kitoms bendrovėms arba panaudos apsimesdami jumis, pavogs jūsų tapatybę ar įdiegs virusą į jūsų kompiuterį.

Trečia. Prašom, susimokėkite už kelionę.Sukčiai jums pasakys, kad esate pačioje įdarbinimo proceso pabaigoje, tačiau turite sumokėti nedidelį mokestį už kelionės ir (arba) apgyvendinimo išlaidas - vien tam, kad būtų užtikrintas jūsų dalyvavimas.

Žinoma, įmonė pinigus grąžins kartu su pirmuoju atlyginimu. Akivaizdu, kad po to, kai asmuo sumokės, sukčiai ryšį nutrauks.

Kodėl tai veikia?

Sukčiai puikiai žino, kaip apsimesti tikromis įmonėmis, apeliuoti į mūsų sąmonę, emocijas ir poreikius.
Žino, kaip ir ko prašyti, kad prašymą įvykdytume nė akimirkos nesuabejoję, nes nesukelia jokio įtarimo ir, mūsų požiūriu, tai yra smulkmena, atsižvelgiant į tai, ką galime gauti. Naudodami manipuliacines priemones jie mus užliūliuoja, todėl galiausiai nesijaučiame apgauti arba neigiame savo nuojautas.
https://www.scamwatch.gov.au/types-of-scams/jobs-employment/jobs-employment-scams
https://www.windrosenetwork.com/Employment-Scams

Žiūrėkite 1 pavyzdį

07 NETIKĖTI LAIMĖJIMAI, PAVELDĖJIMAI, PRIZAI, MOKESČIAI, NEBAIGTI MOKĖJIMAI

„Sveikiname! Tapote pagrindinio prizo laimėtoju, tereikia tik spustelėti, kad taptumėte 1 milijono eurų savininku" - skamba viliojančiai, tiesa? Pinigai - ne vienintelė sukčių naudojama vilionė. Tai gali būti prizai natūra, telefonai, ausinės, batai, automobilis, kelionės „viskas įskaičiuota". Nusikaltėliai naudoja įvairius metodus, kad priverstų mus spustelėti įtartiną nuorodą, panaudos daugybę metodų savo tikslui pasiekti. Deja, deja, mūsų smegenys ne visada tokiais atvejais bus mūsų sąjungininkas. Žmonės, norėdami praturtėti maža kaina, linkę tikėti netikėta likimo dovana.

Dažniausiai pasitaikantys sukčiavimo būdai: paveldėjimas, nuolaidos, mokesčiai, laimėjimai.

Paveldėjimo apgavystės. Su jumis susisiekė nepažįstamas asmuo ir teigia, kad paveldėjote didelę sumą, nes esate vienintelis likęs gyvas mirusio asmens įpėdinis. Beveik be jokių nereikalingų dokumentų tvarkymo procedūrų, pinigai jau beveik jūsų, tereikia sumokėti nedidelį mokestį už kai kuriuos sudėtingus oficialius reikalus arba atsiųsti asmens tapatybės dokumento skenuotą kopiją, priešingu atveju paveldėtas turtas atiteks valstybės iždui. Galbūt kai kurie iš mūsų yra kada nors gavę tokią žinutę. Sėdėdami čia galime sakyti, kad tai juokinga, juk negalima patikėti kažkuo panašiu. Tačiau turėtume prisiminti, kad sukčiai gali būti labai įtikinantys, be to, naudodamiesi internetu jie gali atlikti net ir nedidelį tyrimą apie asmenį, kad rastų dalykų, kuriais galima pasinaudoti, pasirenkant tinkamą sukčiavimo būdą. Jie taip pat gali nusitaikyti į asmenį, kuris, pavyzdžiui, yra atsidūręs labai sunkioje finansinėje padėtyje, jam reikia pinigų, yra neviltyje. Daugelis tikriausiai pagalvos, na, tada tai jau statistikos klausimas, niekas nesiruošia gaišti laiko ieškodamas kieno nors socialinių profilių dėl kelių dešimčių eurų arba tikėtis sėkmės, kad suras žmogų, atsidūrusį sunkioje padėtyje.

Tačiau nepamirškite, kad žmonės, kurie pragyvena iš internetinių sukčiavimų, dažnai yra labai motyvuoti vykdyti įvairias, skirtingo masto, skirtingo pobūdžio apgavystes. Ne visi įsilaužėliai tyko tik didelių bendrovių ir bankų, daugelis specializuojasi vogti iš paprastų žmonių, tokių kaip aš ar jūs.

Nepakankamas sąskaitų apmokėjimas. Itin paplitęs žmonių apgaudinėjimo būdas - dažniausiai yra SMS žinutės apie nesumokėtus mokesčius už energijos šaltinius, pavyzdžiui, dujas, elektrą ar kitus mokesčius: už vandenį, šildymą, kredito įmokų sistemos pakeitimus, nuomos mokesčio pakeitimus. Tačiau kiekvieną kartą tai bus informacija apie nepriemoką ir būtinybę ją skubiai sumokėti, nes priešingu atveju arba bus atjungtas atitinkamas energijos šaltinis, arba reikalas bus perduotas skolų išieškojimui, o mes būsime įtraukti į kreditorių sąrašą. Kaip ir daugeliu kitų atvejų, atsiradusi skuba, nerimas ir galima bauda už pavėluotą mokėjimą verčia mus pradėti elgtis neracionaliai. Telefono numerio ar el. pašto adreso, iš kurio gavome nerimą keliantį pranešimą, netikriname. Mūsų nenustebins pridėtoje nuorodoje esančios rašybos klaidos, mūsų nesuglumins keistas sąskaitos faktūros pavadinimas arba tai, kad sąskaitas apmokame reguliariai. Ypač jei nepriemokos suma nedidelė, norėsime kuo greičiau sumokėti įsiskolinimą, išvengdami palyginus su "nusižengimu“ neproporcingai didelės baudos.

Laimėjimai loterijoje. Vagys atsiunčia pranešimą, kad konkurse ar loterijoje laimėjote daug pinigų arba fantastišką prizą. Norėdami atsiimti prizą, turite sumokėti nedidelį mokestį. Vėlgi - sukčiai prašys tai padaryti greitai, antraip neteksite prizo, jie nesuteiks laiko juos patikrinti. Sukurs netikrą konfidencialumo atmosferą, kad užtikrintų jums saugumą. Dažnai jie naudos tikrų loterijų ir organizacijų pavadinimus. Net jei sukčiai nenori pinigų, vis tiek gali paprašyti asmens duomenų - ir pavogti juos tolesniems nusikaltimams vykdyti. Taip pat yra naujas sukčiavimo būdas, kai, naudodamiesi jūsų socialine žiniasklaida, susisiekia su kitais žmonėmis ir, pasinaudodami jūsų tapatybe, naudodamiesi suklastotu pranešimu apie laimėtą prizą, atiduoda juos į sukčių rankas.

Žiūrėkite 2 pavyzdį

08 Pavojingos SMS žinutės

Asmeninio kibernetinio saugumo srityje Lietuvos gyventojai nesijaučia stiprūs – tik 29% apklaustųjų savo žinias šioje srityje vertina gerai. Apie pusė (47%) gyventojų savo šios srities žinias vertina vidutiniškai, o 20% mano turintys labai mažai kibernetinio saugumo įgūdžių. Tokie yra duomenys apklausos, kurią užsakė tarptautinė informacinių technologijų bendrovė „Accenture“. Į paieškos sistemą įvedę žodžius sukčiavimas trumposiomis žinutėmis, gauname daug informacijos apie didėjantį sukčiavimo atvejų skaičių, naujus žmonių apgaudinėjimo būdus, augantį pavogtų lėšų ir prarastų duomenų skaičių. Jei vagys tampa vis išradingesni, jiems padeda net ir dirbtinis intelektas. Kiek šansų turime mes?

Galbūt būsite nustebinti, bet daug. Sąmoningumas, atsargumas ir abejonės bus jūsų skydas internete. Sukčiai naudoja vis naujus ir naujus žmonių apgaudinėjimo būdus, tačiau jie vis dar pasikliauja labiausiai pasiteisinusiais. Peržiūrėkite į toliau pateiktus pavyzdžius. Ar esate gavę:

- SMS žinutė su įspėjimu apie tam tikros laikmenos atjungimą dėl neapmokėtų sąskaitų;
- SMS žinutė, informuojanti, kad jūsų siuntinys ar laiškas buvo sulaikytas muitinėje ar pašte dėl per mažos sumos, per didelio svorio ar neteisingų adreso duomenų;
- SMS žinutė apie praleistą skambutį, ypač kai žinote, kad tokio nebuvo;
- SMS žinutė su pranešimu apie nesėkmingą bandymą prisijungti prie interneto portalo;
- SMS žinutės iš populiarių socialinės žiniasklaidos platformų apie tai, kad kažkas bandė įsilaužti į jūsų paskyrą, kad kažkas jus pažymėjo nuotraukoje ar vaizdo įraše arba kad jūsų paskyra pažeidė saugumo standartus;
- SMS žinutė su įspėjimu, kad buvo nutekintas jūsų asmens kodas;
- SMS žinutės iš biurų ir valstybės institucijų, reikalaujančios jūsų skubaus įsikišimo;
- SMS su informacija, kad internete plinta jūsų įrašai, nuotraukos ar kitaip naudojamas jūsų atvaizdas;
- SMS su pranešimu apie aktualius įvykius, pavyzdžiui, karą Ukrainoje arba pandemiją, nacionalinį gyventojų surašymą, mokesčių grąžinimą ir t. t., kai esate raginami atlikti tam tikrus veiksmus, pavyzdžiui, pervesti pinigų.

Sukčių SMS žinutės gali būti įvairaus turinio, tačiau paprastai jos būna trumpos, glaustos ir be papildomos informacijos. Dažniausiai jose taip pat būna keli pagrindiniai elementai:

1. pranešimas apie įvykį, incidentą, pvz., kažkuo nepasirūpinome, kažkas bando mus apiplėšti, turėtume kažką padaryti arba sustabdyti, pvz., vagį, bandantį pavogti mūsų duomenis;
2. pasekmių grėsmė, pvz., sulaikytas siuntinys, nutrauktas elektros energijos tiekimas, vagišiaus pasinaudojimas mūsų duomenimis;
3. raginimas kovoti su pasekmėmis - paprastai trumpas imperatyvas: „Spustelėkite toliau pateiktą nuorodą" arba tiesiog duota pati nuoroda, nurodant ją spustelėti.

Kibernetiniai vagišiai sukuria pranešimo turinį taip, kad sukeltų baimę, netikrumą ir baimę dėl pasekmių. Sukčiai nori, kad veiktume greitai, negalvodami ir instinktyviai spustelėtume nuorodą tam, kad atitolintume neigiamas pasekmes. Dažnai tokios SMS žinutės neleidžia tiksliau nustatyti siuntėjo, jų bendras turinys verčia mus be dvejonių manyti, kad tai atėjo iš mūsų žiniasklaidos paslaugų teikėjo, iš mūsų siuntinio kurjerio ir panašiai

Šaltiniai:

https://www.acma.gov.au/articles/2021-09/scam-alert-malware-scam-now-targeting-parcel-delivery-sms
https://www.stuff.co.nz/technology/132293264/text-scams-what-these-look-like-and-what-to-do-about-it https://malwaretips.com/blogs/fake-bank-of-america-email-text-message-scam-explained/

Nepriklausomai nuo to, ar susiduriame su suklastota SMS žinute, ar el. laišku, veiksmai, kurių turėtume imtis, bus panašūs:

- Atkreipkite dėmesį į rašybą, gramatiką, skyrybą, lietuviškų simbolių trūkumą ir sakinių sudarymo būdą. Ar jums tai atrodo įtartina? Atminkite, kad daugelis sukčių nemoka lietuvių kalbos ir žinutes generuoja remdamiesi internetiniu vertimu.
- Gerai pagalvokite apie žinutės turinį, ar neseniai užsisakėte kokį nors siuntinį, ar kada nors praleidote sąskaitų apmokėjimo terminą? Nepatikėkite iš karto savo kalte.
- Įsitikinkite, kad SMS žinutės turinys susijęs su jumis, ar ji yra pakankamai bendro pobūdžio, kad būtų skirta visiems? Ar SMS žinutėje nurodytas jūsų kliento sąskaitos numeris, siuntos numeris ar kiti duomenys, leidžiantys jums patvirtinti, kad SMS žinutė tikrai yra iš įstaigos, organizacijos ar įmonės, su kuria dirbate?
- Neapsigaukite dėl beveik nemokamo laimėjimo ar siuntinio gavimo per kieno nors kito klaidą. Laimėjimai paprastai neatsiranda, kaip ir praturtėjimas dėl kieno nors klaidos. Atminkite, kad kibernetiniai sukčiai veikia stambiu mastu, jei tūkstantis žmonių sumokės net 1 eurą, vagys gaus didelį pelną.
- Atminkite ir niekada nespauskite nuorodų, kurios jus pasiekia bet kokiose žinutėse. Jei, pavyzdžiui, tikitės tokios žinutės, tada: atidžiai perskaitykite, kas yra nuorodos pavadinime, ar yra duomenys/įstaigos pavadinimas; rašybos klaidos ir keistoki pavadinimai turėtų iš karto sukelti jūsų įtarimą.
- Atminkite, kad visada galite paskambinti oficialiu konkrečios institucijos pagalbos telefono numeriu arba susisiekti su įmone, kuri tariamai atsiuntė jums SMS žinutę. Niekada neskambinkite numeriu, iš kurio gavote žinutę ar skambutį - net jei jūsų telefone rodomas kontaktinio asmens vardas.
- Jei SMS žinutė jums atrodo įtartina arba esate įsitikinę, kad tai bandymas sukčiauti - galite pranešti apie tokią žinutę ir tada užblokuoti nurodytą numerį.

Kaip pranešti apie bandymus sukčiauti?

- Pirmasis impulsas bus pranešti policijai, tačiau nepamirškite, kad negalima blokuoti 112 numerio. Skambinkite tiesiogiai arba nuvykite į artimiausią policijos nuovadą.
- Apie įtartiną SMS žinutę taip pat galite pranešti NACIONALINIAM KIBERNETINIO SAUGUMO CENTRUI https://www.nksc.lt/ Čia rasite specialią formą. Jūsų gautas pranešimas bus užregistruotas incidentų valdymo sistemoje ir tada pradėtas tyrimas. Apie tyrimo rezultatus jus informuos el. paštu.

- Pranešti apie incidentą galite elektroniniu paštu cert@nksc.lt arba skambinant tel. 1843
- Jei nukentėjote nuo sukčių, taip pat galite pranešti policijai naudojantis elektroninių paslaugų portalu https://www.epolicija.lt/?fbclid=IwAR0pbcK-vuTIht86rBKUi3sb-mUrul5ZsSJkT-WOOCHzIFUfMW1q16NlO08
- Svarbu siųsti tik pranešimus, turinčius sukčiavimo požymių arba bandymus sukčiauti, o ne, pavyzdžiui, mūsų operatoriaus SPAM pranešimus. Taip pat reikėtų nepamiršti, kad tik siunčiant žinutę su visa jos formuluote, bus galima teisingai ją patikrinti.

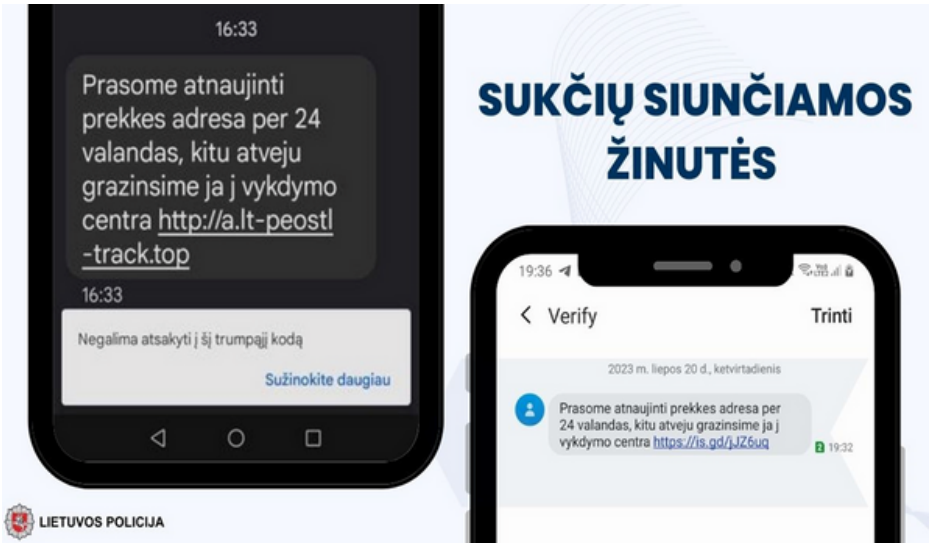
Sąmoningumas, atsargumas ir abejonės padės analizuoti situaciją, kurioje kas nors gali norėti apgaule išvilioti mūsų duomenis arba pavogti mūsų pinigus.

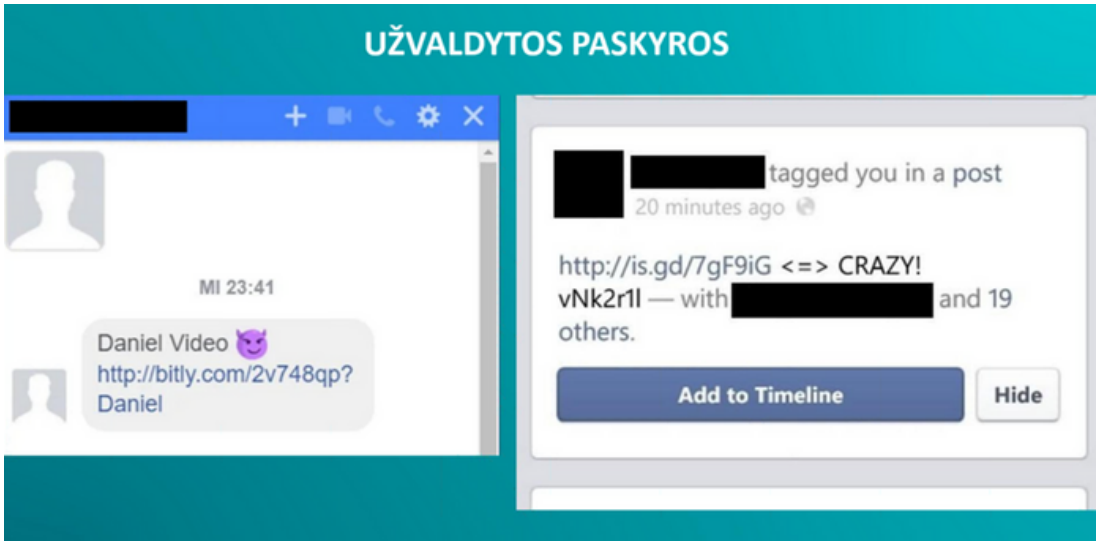
Sąmoningumas - jei žinosime, kad tokio pobūdžio sukčiavimo atvejų pasitaiko ir jie yra labai dažni, gavę tokią žinutę būsime budresni.

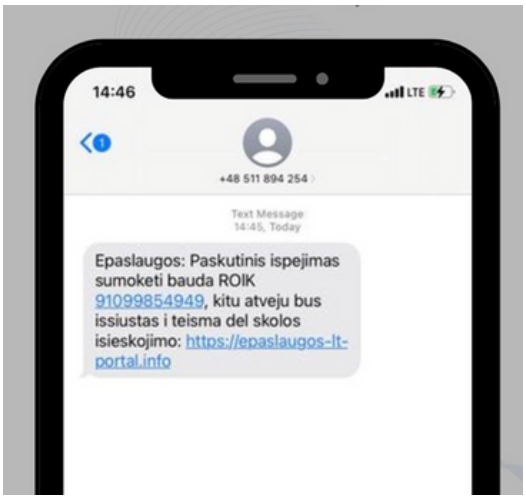
Atsargumas - nedelsdami ir nedvejodami iš karto nespausime prisegtos nuorodos.

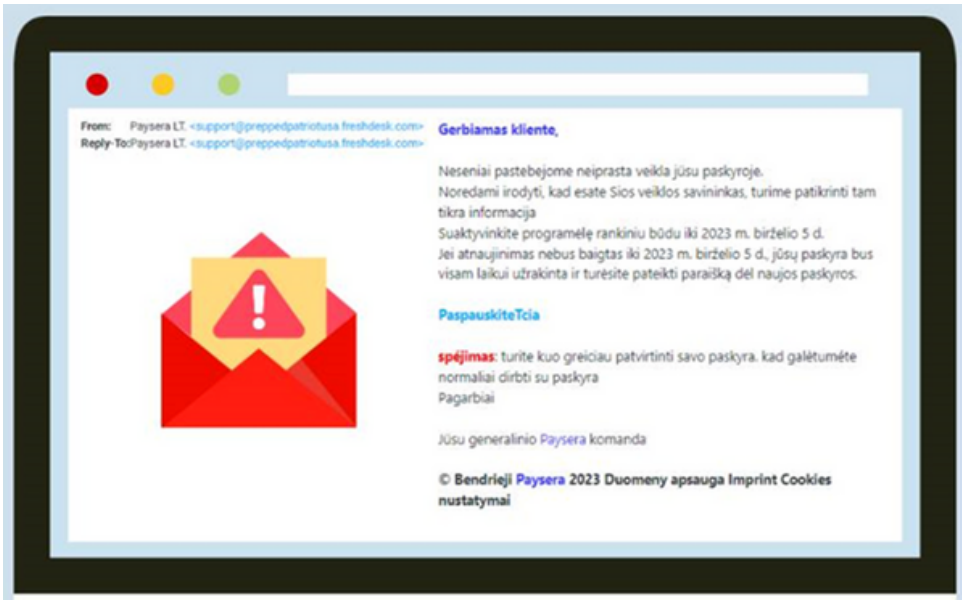
Abejojantys - pagalvosime, ar tikrai esame tikri, kad tai, kas pateikta teksto žinutėje, mums tinka. Paskambinsime oficialiu pagalbos telefonu, pasiteirausime apie situaciją, įsitikinsime, kad tikrai nesame apmokėję sąskaitų arba kad siuntinys iš tikrųjų mums buvo išsiųstas.

Atminkite, kad nė viena institucija niekada neskiria savo klientams 5 minučių atsakymams. Pagal įstatymus visada turime būti informuoti gerokai iš anksto, kad galėtume imtis tinkamų, nediskutuotinų veiksmų.









Šaltiniai:

https://www.metrobank.com.ph/articles/fight-fraud/spotting-fake-sms
https://www.nksc.lt/pranesti.html
https://byt.lt/XvHFC

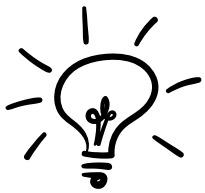
Kaip apsisaugoti nuo kibernetinių grėsmių

Informacija lektoriui:
Trukmė - 3 val.
1. Išdalykite lapą su pavyzdžiais ir užduotimis.
2. Dalyviams išdalykite atspausdintus kontrolinius sąrašus;
3. Supažindinkite su toliau pateikta medžiaga;
4. Remkitės pavyzdžiais ir pratimais, kaip nurodyta žemiau tekste. Aptarkite pratimus su dalyviais;
5. Stebėkite laiką - turite 3 valandas pagal sistemą 45 min. mokymasis, 15 min. pertrauka.

Kibernetiniai nusikaltimai kelia itin didelę grėsmę. Kiekvienas turėtų žinoti, kaip juos atpažinti. Žinojimas - pirmas žingsnis siekiant apsaugoti save ir savo duomenis internete. Šiame skyriuje kontrolinio sąrašo forma pateikėme 8 patarimus, kurie padės jums apsunkinti kibernetinių nusikaltėlių darbą. Yra daug dalykų, kuriuos galime padaryti, kad apsaugotume save ir savo duomenis. Nereikia bijoti naudotis internetu, daugumą pavojų, išklausę šį kursą, pastebėsite be vargo. Atminkite, kad kibernetinių nusikaltimų aukomis tampa net jauni žmonės, „gimę su telefonu rankoje".

Kontrolinis sąrašas

01 NAUDOKITE ANTIVIRUSINĘ IR (ARBA) KITĄ SAUGUMO PROGRAMĄ



Programa, kuri užtikrina apsaugą nuo esamų ir naujų kenkėjiškų programų, įskaitant išpirkos reikalaujančias programas ir virusus, taip pat padeda apsaugoti jūsų asmeninę ir finansinę informaciją, kai lankotės internete.

Tinkama antivirusinė programa yra pirmoji ir būtinas, kartu ir lengviausias, žingsnis siekiant apsisaugoti internete. Antivirusinė programa gali būti būti laikoma pirmąja gynybos linija, jūsų skydu apsaugančiu nuo virusų ir kenkėjiškų programų.

Daugelis nemokamų programų turi biudžetui palankių variantų, tokios programos įdiegimas yra geresnė išeitis, negu jos neturėti iš viso.

Nesvarbu, ar norite naudoti kompiuterį, ar telefoną, galite ir turėtumėte apsaugoti bet kurį iš jų. Šiandien antivirusinės programos vienoje licencijoje siūlo kelių įrenginių apsaugą.

1.Tokia programa yra gera pradžia blokuoti virusus ir suklastotas programas. Tačiau šiais laikais antivirusinės programos suteikia mums daug daugiau galimybių, kuriomis turėtume pasinaudoti veiksmingai apsaugai. Dauguma jų turi automatinių priemonių, kurias įdiegus, jos apsaugo mūsų įrenginį, dokumentus, slaptažodžius, informaciją, duomenis ir net mūsų tapatybę.

1.Atminkite, kad nemokama programinė įranga ne visiškai apsaugo nuo įvairių grėsmių. Nemokamos programinės įrangos atnaujinimai paprastai pridedami vėliau nei mokamos. Pirkdami vieną licenciją galite pasidalyti išlaidas su šeima ir draugais, nes daugelyje programinės įrangos programų siūlomos kelios licencijos skirtingiems įrenginiams.

Neįrenginėkite daugiau nei vienos antivirusinės programinės įrangos tame pačiame įrenginyje - šios programos gali atpažinti viena kitą kaip grėsmę ir kovoti viena su kita, dėl to jūsų prietaisas sulėtės.

Štai keletas pagrindinių funkcijų, į kurias turėtumėte atkreipti dėmesį, jei norite išsirinkti gerą antivirusinę programą:

Mažiausiai 95 % kenkėjiškų programų aptikimo efektyvumas.

El. pašto paskyros apsauga - gera antivirusinė programa patikrins ir prireikus užblokuos kenksmingus priedus prieš juos atidarant.

Lengvas naudojimas ir intuityvus naudotojo skydelis - tai galite patikrinti, pavyzdžiui, norimos įsigyti antivirusinės programos nemokamose versijose.

Apsaugos daugiau įrenginių

02 NAUDOKITE GERĄ, STIPRŲ SLAPTAŽODĮ

Stiprus slaptažodis yra dar vienas svarbus žingsnis siekiant apsisaugoti nuo kibernetinių nusikaltimų.
Keletas bendrų taisyklių, kurių turėtumėte laikytis

Įsitikinkite, kad kiekvienos paskyros slaptažodis yra skirtingas.

Slaptažodžių įsiminimas per naršyklę tikrai palengvins jūsų gyvenimą, tačiau kartu tai yra lengvas kibernetinių vagių grobis.

Slaptažodis turėtų būti pakankamai stiprus ir reguliariai keičiamas.

Jei jums sunku įsiminti slaptažodžius, visada:

- naudokite slaptažodžių valdymo programą;
- sukurkite slaptažodžių failą (pvz., word arba excel), bet nelaikykite visų slaptažodžių viename faile kompiuteryje arba telefone;
- užsirašykite slaptažodžius į užrašų knygelę arba bloknotą. Venkite užrašinėti telefono PIN kodų ant popieriaus lapų, kuriuos laikote piniginėje, arba užsirašyti elektroninės bankininkystės slaptažodžio į elektroninės bankininkystės aplanką kompiuteryje;
- susikurkite savo slaptažodžių kūrimo sistemą, kurią bus lengva įsiminti ir atkurti slaptažodžius.

Naudokite ne mažiau kaip 8 raidžių, skaičių, simbolių.

Slaptažodis turėtų būti pakankamai stiprus ir reguliariai keičiamas.

Niekada nesiųskite savo slaptažodžio el. paštu

Neįvedinėkite slaptažodžio, kai kas nors žiūri per jūsų petį.

Neįveskite slaptažodžio kompiuteryje, kuris nepriklauso jums.

Atlikite 1 pratimą

03 REGULIARIAI ATNAUJINKITE PROGRAMINĘ ĮRANGĄ

Kibernetiniai nusikaltėliai naudojasi žinomomis programinės įrangos spragomis, kad galėtų lengviau pasiekti jūsų telefoną ar kompiuterį. Jei reguliariai atnaujinsite programas, ir (arba) žaidimus, turėsite naujausias saugumo pataisas, jūsų duomenys bus veiksmingiau apsaugoti. Taip pat žinokite, kad kibernetinės grėsmės nuolat keičiasi, bet kuriuo metu siūlomi atnaujinimai skirti apsaugoti jus nuo šiuo metu kylančių grėsmių ir apsaugoti jūsų įrenginius nuo jų žalingo poveikio.

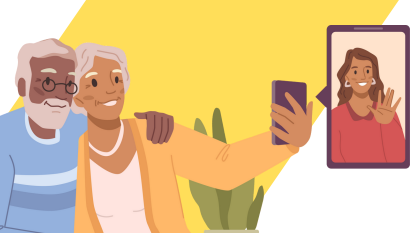
- Pasistenkite nenaudoti mygtuko „ignoruoti" arba „priminti man vėliau", kai pasirodo pranešimas įdiegti atnaujinimus.
- Jei nesate tikri, ar atnaujinimas yra teisėtas, galite patikrinti jį programinės įrangos leidėjo arba programėlės kūrėjo svetainėje.
- Naudokite naujausias interneto naršykles.

Atlikite 2 pratimą **Rodykite 1 pavyzdį** **Rodykite 2 pavyzdį**

04 TVARKYKITE SAVO SOCIALINĖS ŽINIASKLAIDOS NUSTATYMUS

Svarbu prisiminti, kad jei ką nors paskelbiame Internete, tai lieka ten visam laikui. Visiškai turinio neištrinsime, jo pėdsakas visada išliks. Kibernetiniai nusikaltėliai gali gauti jūsų duomenis, jiems užtenka tik kelių svarbių informacijos detalių. Jie stengsis jus pažinti, kartais net įgyti jūsų pasitikėjimą, o tada apgaudinės naudodami priedus ar nuorodas.
Atminkite, kad kuo mažiau informacijos patenka į internatą, tuo geriau.

- Būtinai atminkite, kad negalima internete skelbti savo adreso, augintinio vardo, motinos mergautinės pavardės, nes tai dažnai būna atsakymai į klausimus, kuriais apsaugomos jūsų paskyros tinkle.
- Minėta informacija taip pat dažnai būna mūsų slaptažodžių dalis, todėl svarbu daugiau dėmesio skirti savo slaptažodžiams, o kartu ir tam, ką skelbiame internete.
- Iš pirmo žvilgsnio nekaltas atostogų nuotraukų skelbimas būnant toli nuo namų, vagims gali suteikti vertingos informacijos, kad mūsų namai buvo palikti be priežiūros - socialiniai tinklai yra svarbus įrankis ne tik kibernetiniams nusikaltėliams, bet ir tiems, kurie veikia realiame gyvenime.
- Svarbu nepamiršti tinkamai tvarkyti visų naudojamų socialinės žiniasklaidos priemonių privatumo nustatymus, kad tik jūsų draugai matytų tai, ką rašote.
- Kibernetiniai nusikaltėliai dažnai sukuria netikras paskyras. Jei gaunate pranešimą, kad bendraujate su paskyra, kurios savininko nepažįstate, nesvarbu, ar tai būtų žinutė, ar kvietimas į draugus, būkite atsargūs ir patikrinkite pagrindinę informaciją apie tą asmenį, pavyzdžiui, profilio nuotrauką, draugų skaičių, bendrus draugus. Jei manote, kad tai gali būti bandymas išvilioti pinigus, neatsakykite į žinutę / kvietimą ir neįtraukite asmens į draugų sąrašą.



05 APSAUGOKITE SAVO EL. PAŠTO PASKYRĄ

Kai kalbama apie elektroninius nusikaltimus, paprastai pirmiausia minimi el. paštai. Šlamštas, įtartini el. laiškai ir nesaugūs priedai - vieną dieną galite gauti bet kurį iš jų. Tačiau yra keletas bendrų taisyklių, kurių reikia laikytis, kad būtumėte saugūs:

Niekada neatidarinėkite nepažįstamų asmenų priedų. Jei vis dėlto nusprendėte juos atidaryti, pirmiausia atidžiai patikrinkite el. pašto adresą, iš kurio gavote failą, rašybos ir spausdinimo klaidos parodys, kad tas, kas siuntė el. laišką, neturi draugiškų ketinimų:

- kontakt@oraneg.pl;
- info_faktury@tuaron.pl;
- ...@ocjk.pl;
- ...@rlcysystem.com

Jei netyčia atidarėte pridėtą dokumentą/nuorodą, kuri tikriausiai yra apgaulinga, vis tiek galite ką nors padaryti. Nepanikuokite. Pirmiausia nuskaitykite priedėlį antivirusine programa. Pakeiskite savo prieigos į el. pašto dėžutę slaptažodį, taip pat galite paskambinti
savo bankui ir informuoti, kad tapote internetinio nusikaltimo auka, kad jie galėtų stebėti bet kokią įtartiną veiklą jūsų paskyroje ir ją užblokuoti.

Atverti priedai iš nuorodos taip pat gali būti apgaulė. Atminkite, kad visada geriau dukart patikrinti siuntėją arba el. laiško turinį, o ne automatiškai spustelėdami įtartiną nuorodą.

Dauguma populiariausių el. pašto paskyrų teikėjų patys informuos, kad priedas yra įtartinas, todėl jei pamatysite tokį pranešimą, neatidarykite to el. laiško ir jo priedų. Jei nesate tikri, ar priedas yra saugus, patikrinkite tai paskambinę telefonu arba parašę žinutę el. laiško siuntėjui, patikrinkite tikslų adresą, iš kurio siunčiamas el. laiškas buvo išsiųstas. Jei nusprendėte atidaryti priedą/nuorodą, atminkite, kad pdf formatas laikomas saugesniu. Neatidarinėkite priedų su keistais, nesuprantamais pavadinimais.

PARODYKITE 3 PAVYZDĮ **PARODYKITE 4 PAVYZDĮ** **ATLIKITE 3 PRATIMĄ**

06 VENKITE ĮTARTINŲ PRAŠYMŲ, INFORMACIJOS

Bet kokius prašymus, informaciją, kurioje yra grasinimų, bandymų įbauginti ar kito prieštaringo turinio, pavyzdžiui, laimėjimus loterijoje, prašymus padėti surasti nusikaltėlį, reikėtų labai atidžiai patikrinti, nes jie pagrįsti socialine inžinerija. Kibernetiniai nusikaltėliai nori, kad manytumėte, jog privalote veikti, nes kitaip prarasite pinigus ar privačius duomenis arba kas nors nukentės.

Jei kas nors jūsų paprašo informacijos, gąsdina jus, naudoja grasinimus prieš jus ar jūsų šeimą, jūsų sąskaitas ir pan., neatsakykite, padėkite ragelį, blokuokite siuntėją. Jei prašymo siuntėjas buvo asmuo, atstovaujantis valstybei, valstybinei institucijai ar įmonei, skambinkite arba rašykite el. paštu įmonei, paskambinkite arba parašykite el. laišką el. pašto adresu, nurodytu oficialioje institucijos/bendrovės interneto svetainėje. Visada galite nutraukti pokalbį ir dar kartą paskambinti oficialiu numeriu arba parašyti el. paštu klientų aptarnavimo tarnybai - geriau būti atsargesniems, nei duoti kam nors netinkamą informaciją.

Prisiminkite patikrinti informaciją, kuria dalijatės. Pandemijos metu buvo labai daug melagingos informacijos, kurią vėliau dažnai panaudojo nusikaltėliai, siųsdami netikras nuorodas, kurios buvo skirtos įdiegti kenkėjišką programinę įrangą telefone ir (arba) mobiliajame telefone.

Atminkite, kad prieš pateikiant kam nors savo asmeninius duomenis, visada geriau pasitikrinti, net jei paaiškėtų, kad iš tikrųjų reikia padaryti pakeitimus savo paskyroje, kad galėtumėte apmokėti tam tikrą sąskaitą. Vis dėlto bet kurios institucijos, valstybinės ar privačios, darbuotojai privalo teikti visuotinai priimtino standarto paslaugas, o tai reiškia, kad jie negali jūsų gąsdinti, skubinti - reikalaudami, kad privalote tai padaryti dabar, antraip bus rimtų pasekmių.

Pakartotinis numerio rinkimas, perskambinimas į numerį, iš kurio buvo gautas skambutis gali pasirodyti neveiksmingas, nes kibernetiniai nusikaltėliai geba apsimesti institucijų ir įmonių atstovais, kad mes manytume, jog kalbame būtent su jais.Geriau nutraukti pokalbį ir skambinti numeriu, nurodytu oficialioje įmonės/ institucijos interneto svetainėje

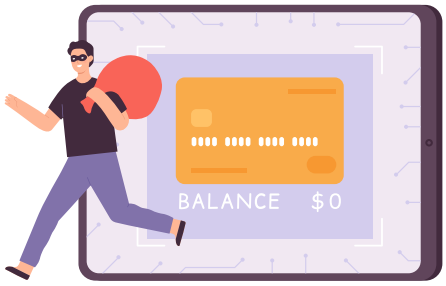
PARODYKITE 5 PAVYZDĮ

ATLIKITE 4 PRATIMĄ

07 APSAUGOKITE SAVO INTERNETINES OPERACIJAS

- Turėtumėte būti atsargūs atlikdami operacijas internetu, nesvarbu, ar tai būtų apsipirkimas, ar dokumentų siuntimas internetu.
- Kiekviena svetainė turėtų turėti SSL sertifikatą, kuris garantuoja saugų bendravimą internetu. Kai naršyklė kreipiasi į saugią svetainę, SSL sertifikatas užtikrina šifruotą ryšį. Jo simbolis - tai adreso juostoje esanti pakabinama spyna naršyklėje prieš www. Kartais net ir sukčiavimo svetainėse yra pakabinamos spynos simbolis, tačiau paskubomis sukurtose svetainėse jo gali ir nebūti.
- Visada patikrinkite svetainės, kuria naudojatės, pavadinimą, atkreipkite dėmesį į rašybos ir kitas gramatines klaidas.
- Visada patikrinkite, ar svetainė atrodo kaip įprasta. Nauji mygtukai, kitoks išdėstymas, nuorodos gali rodyti, kad svetainė yra netikra.
- Apsvarstykite galimybę atlikti dviejų etapų patikrą - pavyzdžiui, gauti papildomą slaptažodį/PIN kodą el. paštu, SMS žinute. Jei turite galimybę - apsvarstykite galimybę naudoti apsaugos nuo internetinių sandorių programinę įrangą, kadangi daugelis antivirusinių programų savo naudotojams šią galimybę siūlo .
- Jei įmanoma, atsisiųskite savo veiklą patvirtinančius dokumentus, pavyzdžiui, sąskaitas faktūras, sandorių kvitus.
- Svarbu tai, kad net jei šie veiksmai bus nesėkmingi ir tapsite nusikaltimo auka, nesvarbu, ar inicijuojate pinigų grąžinimo procedūrą, ar pateikiate pretenziją bankui, ar net pranešate apie nusikaltimą, banko darbuotojai ar policijos pareigūnai paklaus, kaip jūs apsisaugojote internete, kokią turite antivirusinę programinę įrangą, apie jūsų programinės įrangos atnaujinimų istoriją, jūsų interneto svetainės saugumo patikrinimą ir t. t.

PARODYKITE 6 PAVYZDĮ



08 NEBIJOKITE PRAŠYTI PAGALBOS

Nusikaltimų elektroninėje erdvėje aukomis tampa įvairaus amžiaus žmonės iš įvairių socialinių grupių.

1. Jei nesijaučiate patogiai klausdami šeimos narių, draugų ar klientų aptarnavimo tarnybos apie jums rūpimus dalykus, atminkite, kad net ir tie, kurie užaugo interneto amžiuje ir turi laisvą prieigą prie interneto, taip pat tampa kibernetinių nusikaltėlių aukomis.
2. Jei manote, kad tapote kibernetinio nusikaltimo auka, nedvejodami praneškite apie tai savo šeimos nariams, policijai ir atitinkamoms institucijoms (pavyzdžiui, jei jus apgavo banko darbuotoju prisistatęs asmuo - informuokite banko darbuotojus).
3. Jei paspaudėte įtartiną nuorodą arba atsisiuntėte kenkėjišką priedą - sustokite ir vėl informuokite šeimos narį, draugus, policiją arba banko darbuotoją.
4. Žmonės, tapę elektroninių nusikaltimų aukomis, dažnai kaltina save dėl to, kad nepastebėjo pavojaus, kad neprašė pagalbos, kad pasitikėjo nepažįstamuoju. Tačiau daug blogiauslėpti šiuos jausmus ir nepadėti kitiems išvengti galimybės tapti auka. Gauti emocinę paramą tokiu metu yra labai svarbu, ypač kai auka jaučia kaltę dėl visos situacijos.

ATLIKITE 5 PRATIMĄ

Vartotojų duomenų apsauga

Informacija lektoriui:
Trukmė - 60 minučių.
1. Supažindinkite su šia medžiaga;
2. Stebėkite laiką - turite 45 min. paskaitos ir 15 min. pertraukos.

Lietuvos teisės aktuose yra vartotojų apsaugos mechanizmų, kurie gali padėti kovoti su nesąžiningais pardavėjais ir kibernetiniais nusikaltimais. Nepamirškite atidžiai patikrinti parduotuvės, kai ką nors perkate internetu, patikrinkite atsiliepimus apie ją, nustatykite, ar parduotuvė apsaugo jūsų duomenis (žalia pakabinama spyna). Naudokitės gerai patikrintomis parduotuvėmis, įtartinai mažos kainos arba specialūs pasiūlymai tik keliems išrinktiesiems gali būti bandymas išvilioti iš jūsų pinigus arba duomenis. Taip pat verta pasinaudoti kai kurių e. parduotuvių siūloma pirkėjo apsauga, t. y. pardavėjas negaus jūsų pinigų, kol jūs nepatvirtinsite, kad pirktos prekės buvo pristatytos ir atitinka sutarties sąlygas. Taip pat verta pasinaudoti mūsų, kaip vartotojų, teisėmis, kurios gali padėti mums atgauti prarastus pinigus arba apsaugoti savo asmens duomenis.

1. SUTARTIES ATSISAKYMAS

Prekių ir (arba) paslaugų pirkimas yra tam tikra sutartis tarp pirkėjo ir pardavėjo. Abi šalys susitaria, kad viena iš jų už pinigus teiks atitinkamas prekes ar paslaugas. Todėl, jei ką nors perkame ne prekybai skirtose patalpose, t. y., pavyzdžiui, internete, interneto svetainėje, „Allegro" aukcione arba per pristatymą, mugę ar telefonu, galime atsisakyti tokio pirkimo - galime atsisakyti sutarties. Tokiam atsisakymui turime 14 dienų ir, kas svarbu, neprivalome nurodyti priežasties ir dėl to patirti išlaidų išskyrus prekių grąžinimo išlaidų, t. y. kurjerio ar pašto paslaugų išlaidų. Atsisakymas turėtų būti pateiktas raštu.
Atminkite - prekės negali būti naudotos. Parduotuvė neturėtų reikalauti, kad grąžinimas priklausytų nuo to, ar turite originalią dėžutę, kuri skirta tik apsaugoti prekes. Tačiau jei galite, siųskite prekes pardavėjui toje pačioje dėžutėje ir (arba) pakuotėje, kurioje jas gavote. Tam tikros prekės negali būti grąžinamos, pvz., pagamintos pagal specialų mūsų užsakymą, higienos prekės, medicinos prekės, tam tikros paslaugos, pvz., transporto.

PATIKRINKITE 1 PAVYZDĮ

2.NEPRAŠYTOS PASLAUGOS

Kai kurie nesąžiningi pardavėjai ar nusikaltėliai siunčia mums neprašytas prekes ar teikia paslaugas, kurių neprašėme. Išsiuntę tokią siuntą, sukčiai teigia, kad mes sutikome už ją sumokėti. Jie mums grasina antstoliais arba teismais, siunčia reikalavimus sumokėti. Dažnai manome, kad siuntinio gavimas reiškia sutikimą priimti prekes, tačiau tai yra netiesa. Jei gavote prekę ar paslaugą, kurios neprašėte ar neužsakėte, prekes teikiantis ar siunčiantis asmuo tai daro savo rizika. Jis negali reikalauti apmokėjimo. O tai, kad mes gavome siuntą, nėra tolygu bet kokių išlaidų prisiėmimui. Jei jus persekioja telefono skambučiai ar raginimai sumokėti, verta apie tai pranešti policijai.

3. KLAIDINGAS PERVEDIMAS

Kartais tik atlikę pervedimą suprantame, kad galėjome būti apgauti. Tada dažnai manome, kad mūsų pinigai dingo, tačiau yra būdų, kaip sukčiams nušluostyti nosį. Kuo greičiau kreipkitės į savo banką. Praneškite apie savo įtarimus ir paprašykite atšaukti pervedimą. Kai kuriuos pervedimus galima atšaukti lengvai ir greitai, kitiems taikoma skundų nagrinėjimo procedūra, tačiau svarbiausia, kad galite atgauti savo pinigus. Labai svarbu prašymą pateikti iki "ELIKSIR sesijos". ELIKSIR sesija yra tada, kai jūsų bankas užregistruoja jūsų pervedimą. Tačiau jei tai pastebėsite vėliau, nepasiduokite.

Taip pat nepamirškite, kad galite pasinaudoti teisine konsultacija. Bankai turi daugiau galimybių iš sukčiaus sąskaitos susigrąžinti pinigus, nei jums atrodo. Greičiausias būdas susigrąžinti pinigus, jei mokėjote kortele; tokiu atveju galite pasinaudoti mokesčio grąžinimo procedūra bei greitai atsiimti pinigus be didelių rūpesčių.

Nepamirškite turėti kuo daugiau informacijos apie galimą sukčių - sąskaitos numerį, pervedimo laiką, pervedimo pavadinimą, sąskaitos savininko vardą ir pavardę.

PATIKRINKITE 2 PAVYZDĮ

4. ASMENS DUOMENŲ APSAUGA - BDAR

Naudodami BDAR galime veiksmingiau apsaugoti savo asmens duomenis. Kas tiksliai yra BDAR? Tai ES teisės aktas, reglamentuojantis asmens duomenų apsaugą, taikomas nuo 2018 m. gegužės 25 d. Pilnas BDAR pavadinimas: 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

Pagal BDAR - duomenų valdytojas, t. y. asmuo, kuris turi jūsų duomenis, turi turėti konkretų tikslą juos gauti ir tvarkyti. Pagal BDAR 15 straipsnį taip pat turite tam tikras teises, tarp jų: susipažinti su savo duomenimis, prašyti juos ištrinti arba vieną iš naudingesnių - sužinoti, kur atitinkama bendrovė turi jūsų duomenis.

<u>Kaip praktiškai naudotis BDAR?</u>

- Jei prie jūsų priekabiauja el. laiškais, SMS žinutėmis ar skambučiais su pasiūlymais, įtikinėjančiais pirkti, pasinaudokite BDAR 15 straipsniu (teisė į ištrynimą). Reikalaukite, kad jūsų duomenys būtų ištrinti iš skambinančiojo įmonės duomenų bazės. Jei tai nepadeda, praneškite apie tai BDAR (Duomenų apsaugos tarnybos pirmininkui), nes už jūsų teisių nepaisymą gali būti skirta administracinė bauda, o kai kuriais atvejais net iškelta baudžiamoji byla.
- Taip pat galite gauti informacijos apie tai, iš kur atitinkamas subjektas gavo jūsų duomenis. Taip galėsite išsiaiškinti, ar kokia nors kita įmonė jūsų duomenis gavo neteisėtai, apgaulės būdu, ar jūsų sutikimas buvo suklastotas. Paprašykite, kad su jumis susisiekusi įmonė pateiktų informaciją, kodėl ji tai daro ir iš kur gavo jūsų duomenis. Atminkite, kad apie neaiškius atsakymus arba jūsų nuvertinimą galima pranešti BDAR.
- Taip pat galite pasinaudoti BDAR, kad sužinotumėte, kokius duomenis turi konkreti įmonė, pvz. telekomunikacijų. Pasirodo, kad prieš BDAR įmonės rinko daugybę duomenų apie mus. Galite prašyti atitinkamos bendrovės nurodyti, kokius duomenis ji turi, kada juos rinko ir kam juos naudoja, jei manote, kad jų turimų duomenų kiekis yra per didelis, galite prašyti juos ištrinti.

Nebijokite, kad nesuprasite įmonės atsakymo arba kad ji vartos teisininkų kalbą. BDAR aiškiai nurodė naudoti draugiškus, lengvai suprantamus pranešimus. Be to, pagal BDAR, jums nereikia savo prašymo pagrįsti konkrečiais punktais - administratorius įpareigotas atsakyti į paprasčiausią jūsų klausimą, pvz., kokių duomenų apie mane turite. Jei įmonė vengia atsakyti, atstumia jus, nenori pateikti informacijos, argumentuodama jums neišsiuntus konkretaus laiško, praneškite apie tai BDAR.

Jūsų asmens duomenys:

- vardas, pavardė, asmens kodas, pilietybė, kultūriniai ypatumai;
- socialinio draudimo numeris;
- gyvenamosios vietos adresas;
- banko sąskaitos ir/ar banko kortelės numeris;
- išsilavinimo duomenys;
- pajamos, darbo užmokestis;
- duomenys apie turimą turtą;
- veido atvaizdas, pirštų antspaudai, balso tembras ir kiti jūsų unikalūs biometriniai duomenys;
- jūsų šeimos narių, jei jie siejami su jumis, duomenys.

5. ASMENS TAPATYBĖS KORTELĖS BLOKAVIMAS

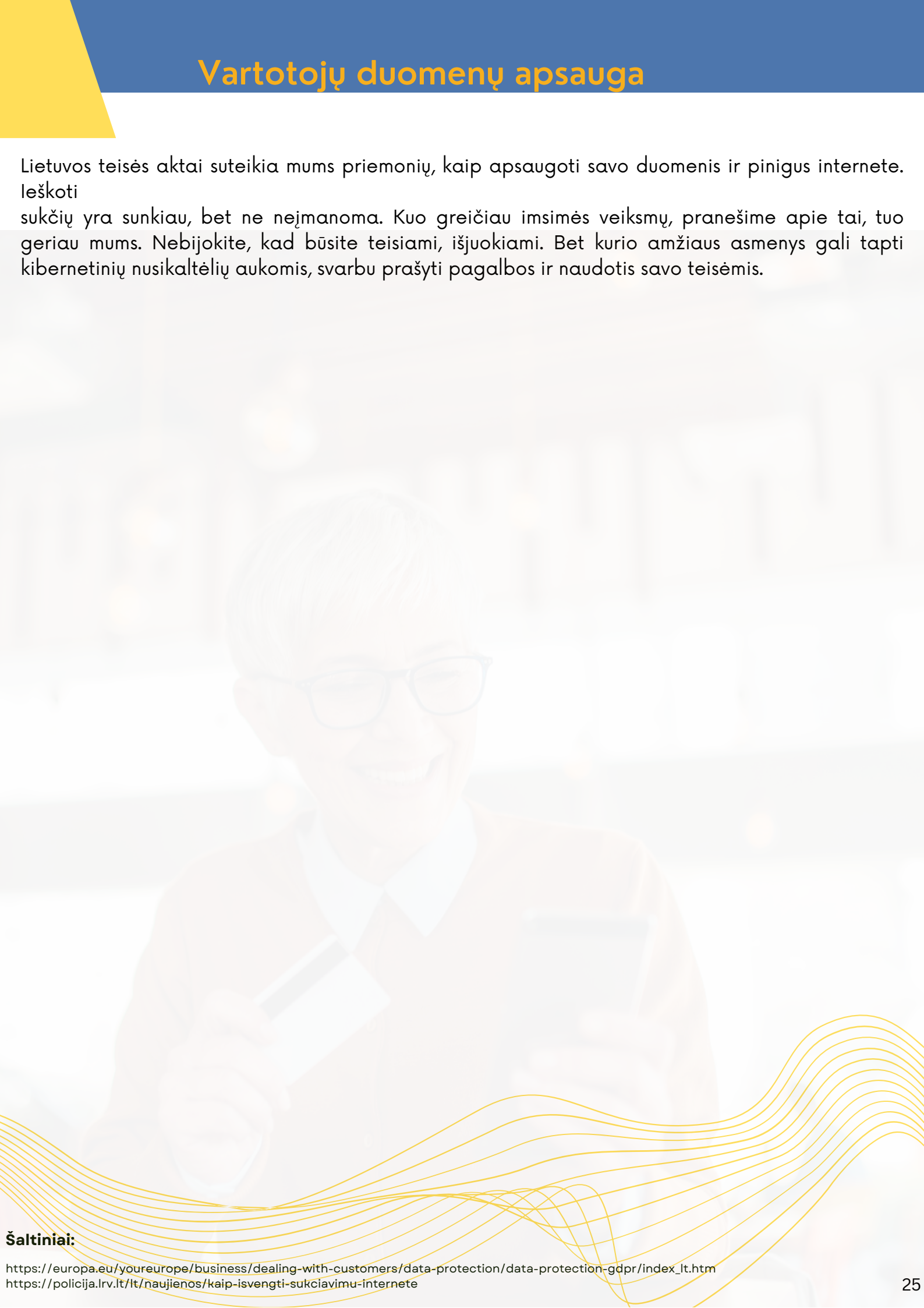
Sukčiai vagia ne tik pinigus, bet ir asmeninę informaciją.
Jei nerimaujate, kad kas nors galėjo gauti informacijos apie jus iš jūsų asmens tapatybės kortelės arba jei tapote sukčiavimo auka - turėtumėte užregistruoti savo asmens tapatybės kortelę savivaldybėje (merijoje) arba internetu. Gavęs jūsų prašymą, pareigūnas panaikins jūsų kortelę. Jei jūsų asmens tapatybės kortelė buvo pavogta - tereikia apie tai pranešti policijai. Tuomet apie dokumento praradimą valdžios institucijoms pranešti nereikia. Jūsų asmens tapatybės kortelė bus anuliuota nuo tos dienos, kai apie tai pranešite policijai.

AR PRANEŠTI APIE SUKČIAVIMĄ DĖL NEDIDELĖS SUMOS?

Dažnai svarstome, ar pranešti apie sukčiavimą dėl nedidelės sumos. Tikimės, kad policija nepriims pranešimo arba kad mums bus sunku jį įrodyti. Kartais pardavėjas dingsta, uždaro sąskaitą, o mums lieka tik suklastoti duomenys ir telefono numeris, kuriuo jis neatsiliepia. Svarbu suprasti, kad sukčiavimas internetu niekuo nesiskiria nuo įprasto sukčiavimo. Sukčius, norėdamas gauti finansinės naudos, jus suklaidins, pasinaudos jūsų klaida arba pasinaudos situacija, o auka dėl įvairių priežasčių negalės tinkamai suprasti jo veiksmų. Už tokį sukčiavimą baudžiama laisvės atėmimu nuo 6 iki 8 metų, o tais atvejais, kada sukčiaujama mažomis sumomis, baudžiama viešaisiais darbais, bauda, laisvės apribojimu arba areštu. Išviliojimas, nepriklausomai nuo sumos, yra baudžiamasis nusikaltimas, o ne nusižengimas. Tikriausiai bus sudėtinga nustatyti internetinio keliolikos eurų sukčiavimo kaltininką, tačiau galite būti ne vienintelis apgautas asmuo, galbūt policija jau atlieka tyrimą, o prokuratūra ieško nukentėjusiųjų. Mes galime patys savarankiškai internete pabandyti surasti kitų žmonių, nukentėjusių nuo konkrečios elektroninės parduotuvės ar sukčiaus. Mūsų veiksmai - pranešimas arba kitų informavimas - taip pat atlieka prevencinę funkciją.

Vartotojų duomenų apsauga

Lietuvos teisės aktai suteikia mums priemonių, kaip apsaugoti savo duomenis ir pinigus internete. Ieškoti
sukčių yra sunkiau, bet ne neįmanoma. Kuo greičiau imsimės veiksmų, pranešime apie tai, tuo geriau mums. Nebijokite, kad būsite teisiami, išjuokiami. Bet kurio amžiaus asmenys gali tapti kibernetinių nusikaltėlių aukomis, svarbu prašyti pagalbos ir naudotis savo teisėmis.



Šaltiniai:

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm
https://policija.lrv.lt/lt/naujienos/kaip-isvengti-sukciavimu-internete

Kaip padaryti mūsų aplinką saugesnę?

Informacija lektoriui:
Trukmė - 2 val.
Lektorius:
1. Išdalinkite korteles su pavyzdžiais.
2. Supažindinkite su toliau pateikta medžiaga;
3. Remkitės pavyzdžiais, vaizdo įrašais, kai toliau esančiame tekste matote informaciją, kad reikia žiūrėti pavyzdį ir nuorodą į YouTube vaizdo įrašą. Aptarkite pavyzdį su dalyviais;
4. Stebėkite laiką - turite 2 valandas pagal sistemą 45 min. mokymasis, 15 min. pertrauka.

Jau žinome, kas yra BDAR, kaip ES teisė saugo mūsų privatumą ir duomenis, taip pat sužinojome, kokie mechanizmai lemia psichologinius aspektus tapus auka. Iš šio kurso sužinojome, kaip kibernetiniai nusikaltėliai bando mus apgauti ir pavogti mūsų duomenis bei pinigus ir kaip tam pasipriešinti. Šiame skyriuje sužinosime, kaip rūpintis savo aplinka, kad ji taptų vis saugesnė ne tik mums patiems, bet ir mūsų šeimai bei draugams. Mahatma Gandis kartą pasakė: „Būkite pokyčiu, kurį norėtumėte matyti pasaulyje". Jei norime, kad pasaulis, mūsų aplinka, mūsų artimieji būtų saugūs taip pat ir kibernetiniame pasaulyje, kiekvienas iš mūsų turi prisidėti. Tai galime padaryti paremdami žmogų, kuris tapo nusikaltimo auka, papasakodami kam nors apie šį kursą, rekomenduodami vadovėlį, nurodydami, kur ieškoti pagalbos, pranešdami apie žalingą/apgaulingą pranešimą, nuorodą, svetainę, kuri apgaudinėja žmones, pranešdami policijai apie bandymą sukčiauti.

Šiame skyriuje sužinosite daugiau apie:

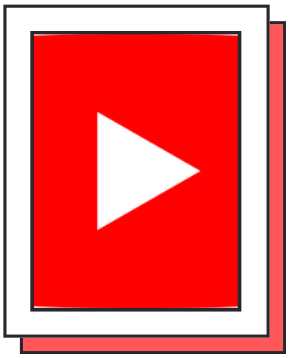
1. socialinę žiniasklaidą ir platformas;
2. kaip išlikti saugiems socialinėje žiniasklaidoje;
3. socialinės žiniasklaidos privalumus ir trūkumus;
4. kaip pranešti apie žalingą turinį;
5. patarimus socialinės žiniasklaidos naudotojams.

01 SOCIALINĖ ŽINIASKLAIDA IR PLATFORMOS

- Socialiniai tinklai leidžia mums susisiekti su artimaisiais ir draugais per daugybę internetinių platformų;
- Kibernetinė erdvė ir toliau suteikia mums daugybę galimybių, kurios neapsiriboja tik jaunimu.
- Daugelis socialinių platformų pagrįstos dalijimusi aistromis, interesais, nuomonėmis, patirtimi ar tiesiog sekant naujienas, kas vyksta su pažįstamais žmonėmis.
- Socialinių tinklų yra šimtai, šiame skyriuje paliesime kai kuriuos iš jų, populiariausius Lietuvoje: Facebook, YouTube, MS Teams, Skype, Instagram, WhatsApp, Pinterest, LinkedIn.

Facebook

- Draugų paieška;
- Dalijimasis nuotraukomis, nuomonėmis, vertinimais, patarimais;
- Gerbėjų puslapių, informacijos apie renginius, interesų grupių kūrimas;
- Įmonių, menininkų, politikų ir kt. paieška

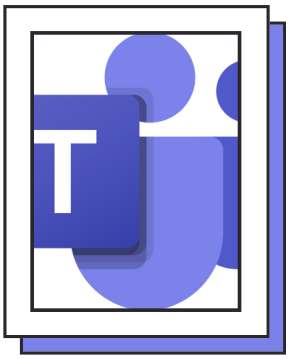


YouTube

- Dalijimasis vaizdo įrašais, muzika ir trumpais klipais
- Komentarai apie kitų naudotojų turinį ir jo vertinimas
- Labai platus pramogų, muzikos, žaidimų ir mokomojo turinio, pavyzdžiui, mokomųjų ir motyvacinių vaizdo įrašų ir pan. temų spektras

Skype

- Platforma, leidžianti atlikti balso ir vaizdo skambučius su kitu asmeniu ar žmonių grupe, kad ir kur jie būtų;
- Galime naudoti ir telefonu;
- Taip pat galime skambinti iš jos telefono numeriu, ne tik skype-skype



MS Teams

- Galimybė skambinti balsu ir vaizdo skambučiais
- Susitikimų, renginių kūrimas
- Darbų planavimas kalendoriuje

Instagram

- Nuotraukų ir ataskaitų, vaizdo įrašų įkėlimas
- Peržiūra, vertinimas ir rekomendacijų kūrimas
- Tiesioginė transliacija - įrašai realiuoju laiku
- Kontaktų, draugų ir sekėjų tinklo kūrimas

Pinterest

- Dalijimasis nuotraukomis, patarimais, įkvėpimu;
- Grupavimas pagal pomėgius, aistras;
- Patinkančio turinio duomenų bazės kūrimas;
- Įdomių nuotraukų, grafinio turinio paieškos palengvinimas.

02 Kaip išlikti saugiems socialinėse svetainėse

Yra daug saugaus naudojimosi internetu taisyklių, tačiau šiame kurse nuolat raginame jus atsargiai ir atidžiai naudotis žiniatinkliu. Taip pat žinome, kad yra daugybė vertingos informacijos, kurios turinys turėtų pasiekti kuo platesnę auditoriją. Tai yra vienas iš didžiausių interneto privalumų - vertingas, mokomasis turinys, didinantis informuotumą, žinių lygį ir leidžiantis apsaugoti save ir kitus nuo žalos ir nuostolių.
Atrodo, kad dabar viskas sukasi apie internetą ar internete. Čia žiūrime vaizdo įrašus, klausomės muzikos, žaidžiame, bendraujame, apsiperkame, net dirbame ar mokomės.
Internetas gali būti jungiantis ir šaunus, bet kartu pavojingas, nes jame taip pat egzistuoja melagienos, netikri vaizdai ar žmonės.
„Swedbank" informacinės saugos vadovė Žygeda Augonė padės atpažinti grėsmes ir patars, kaip jų išvengti.

https://www.youtube.com/watch?v=XMcr2-Ke3I4

03 SOCIALINIŲ TINKLŲ PRIVALUMAI IR TRŪKUMAI

PRIVALUMAI

1. Suteikia galimybę užmegzti naujus ryšius ir palaikyti santykius su šeima ir draugais, droviems žmonėms ir tiems, kurie turi fobijų, palengvina kontaktus su išoriniu pasauliu;
2. Vertinimas ir nuomonių apie kelionių vietas, restoranus, įmones, paslaugas ir pan. teikimas;
3. Dalijimasis pomėgiais, jų ugdymas, žmonių ir grupių, turinčių tokias pačias aistras, paieška;
4. Naujausios informacijos apie pasaulio ir vietos įvykius, įžymybių, politikų, menininkų sekimas.
5. Įkvėpimo, motyvacijos ieškojimas;
6. Galimybė įsigyti daiktų, paslaugų;
7. Savo verslo plėtojimas, prekės ženklo kūrimas;
8. Skatinimas gyventi sveikai, būti fiziškai ir protiškai pajėgiam;
9. Kova už gerus tikslus, labdaros, savanorių grupių kūrimas;
10. Kartais pagalba ieškant dingusių žmonių, pvz., greitai dalijantis informacija.

TRŪKUMAI

1. Nuotraukų klastojimas, kitų naudotojų turinio naudojimas;
2. Profilių vagystė, jų pasitelkimas siekiant apgauti kitus naudotojus;
3. Kitų naudotojų šmeižimas ir šantažas, patyčios internete;
4. Sunkumai suprasti pasidalintą turinį dėl šou, "sėkmės iliuzijos" ir "instagramo gyvenimo" ir su tuo susiję nerviniai sutrikimai, depresija, bet kokia kaina nerealaus tikslo siekimas ;
5. Melagingos ir net žalingos informacijos, dažnai keliančios pavojų sveikatai, skleidimas;
6. Sveikatai ir net gyvybei žalingų įpročių kūrimas ir skleidimas;
7. Realių santykių, susitikimų akis į akį palaikymo ribojimas;
8. Visuotinai įprastų komunikacijos būdų keitimas;
9. Neigiamas poveikis poilsiui, miegui, sveikatai;
10. Priklausomybės, prisirišimo prie telefonų ir kompiuterių sukėlimas;

Žalingas ir teigiamas socialinės žiniasklaidos poveikis priklauso nuo mūsų ir nuo to, kaip mes ja naudosimės.

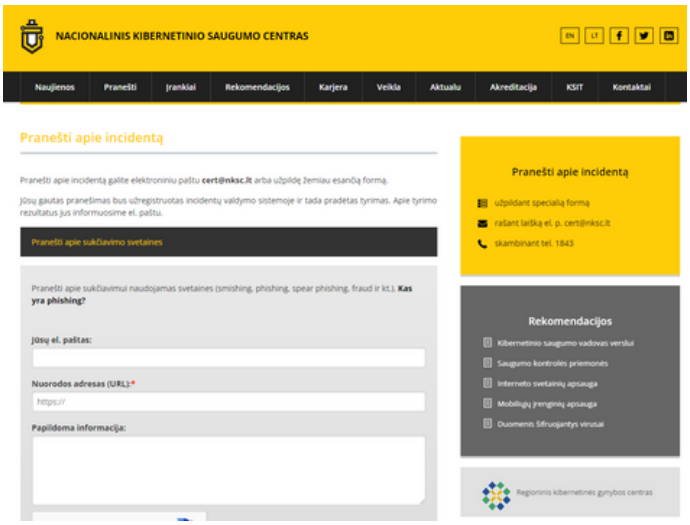
04 KAIP PRANEŠTI APIE ŽALINGĄ TURINĮ

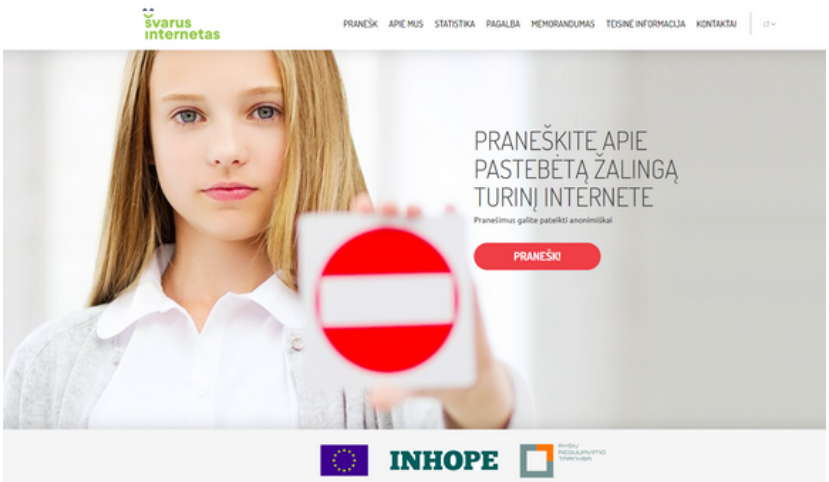
Lenkijoje 54 proc., Lietuvoje 47 proc, (https://byt.lt/tPazU) vyresnio amžiaus žmonių teigė, kad internete yra susidūrę su žalingu, pažeidžiančiu įstatymus, turiniu ir apie tai niekur nepraneša . Apie 30% apklaustųjų nežino, kur ir kaip apie tai pranešti.

Lietuvoje padėti žmonėms pranešti apie kibernetinius nusikaltimus sukurtos svetainės:

- pranešti apie žalingą turinį internete - www.svarusinternetas.lt
- pranešti apie aptiktas saugumo spragas - https://www.nksc.lt/pranesti.html

Yra daugiau vietų, kuriose galime pranešti apie pavojingą ar žalingą turinį. Kiekvienas socialinis tinklas turi savo tvarką ir galimybes pranešti apie tokias situacijas. Nebijokite reaguoti, visada galite pranešti policijai.





PATIKRINKITE 1 PAVYZDĮ

05 PATARIMAI SOCIALINĖS ŽINIASKLAIDOS NAUDOTOJAMS

Būkite atidūs

- Prieš ką nors publikuodami pagalvokite, ar kas nors galėtų tai panaudoti prieš jus;
- Nespauskite nežinomų nuorodų, reklamų ir pan;
- Atidžiai patikrinkite, su kuo bendradarbiaujate, su kuo susipažįstate;
- Išjunkite buvimo vietos stebėjimą per socialinę žiniasklaidą;
- Apribokite savo paskyros matomumą;
- Skelbkite kuo mažiau informacijos apie save ir savo gyvenimą.

Nebūkite patiklūs

- Venkite netikrų paskyrų; tikrinkite draugų sąrašus, paskyros informaciją, profilio nuotraukas ir kitą bendrai naudojamą turinį;
- Informacija, kuria dalijasi jūsų draugai, nebūtinai turi būti teisinga, daugelis žmonių netikrina informacijos tikrumo;
- Nedarykite nieko neapgalvoto, viliojami greito atlygio pažadu;
- Nesidalykite savo ar kieno nors kito privačia informacija, pvz. finansine, sveikatos, asmenine.

Būkite atsargūs

- Nesidalykite neskelbtinomis nuotraukomis, pvz., nuogomis arba rodančiomis jūsų dokumentus;
- Nekreipkite dėmesio į žinutes ir pranešimus, parašytus svetima kalba, su klaidomis, nesuprantamas;
- Atminkite, kad jei ką nors pridedate kaip draugą, suteikiate jam didesnę prieigą prie savo duomenų.

Būkite atsargūs, ką publikuojate

- Atminkite, kad tuo, kas patenka į internetą, gali pasinaudoti pašaliniai asmenys neteisėtai veiklai;
- Kai kurie asmenys gali pasinaudoti pasidalinta privačia informacija tam, kad jus įskaudintų ar pažemintų;
- Jūsų duomenys gali palengvinti kam nors apsimesti jumis ir apgauti jūsų šeimą ar draugus.

Valdykite leidimus

- Kiekviena svetainė ir portalas suteikia galimybę valdyti savo privatumo teises. Labai svarbu jomis naudotis, ypač kai kalbama apie socialinę žiniasklaidą. Tai leis jums išvengti situacijos, kai visiškai nepažįstami asmenys gaus jūsų duomenis arba stebės jūsų profilį.

Ar žinojote, kad...

- 2019 m. I ketvirtį Facebook pašalino daugiau nei 2 mlrd. netikrų paskyrų;
- Apskaičiuota, kad apie 5 % socialinių tinklų paskyrų yra netikros;
- Kai kuriose šalyse netikras paskyras kuria kibernetinių nusikaltėlių tinklai ir specialūs kibernetiniai bei propagandiniai "būriai", kad paveiktų žmonių nuomonę opiomis temomis, poliarizuotų ir suskaldytų žmones bei skleistų melagingą informaciją ir propagandą.

Metodologija

Informacija lektoriui:
Trukmė - 2 val.
Lektorius:
1. Išdalykite lapus su užduotimis.
2. Supažindinkite su toliau pateikta medžiaga;
3. Remkitės pavyzdžiais ir pratimais.
4. Stebėkite laiką - turite 2 val. pagal sistemą 45 min. mokymas, 15 min. pertrauka.

Šiuolaikinė civilizacija siūlo daugybę sprendimų, kurie palengvina gyvenimą. Deja, ji taip pat gali mus išblaškyti, atitraukti dėmesį, išsunkti mūsų energiją, priversti prarasti budrumą ir tapti aukomis žmonių, kurie blogais tikslais naudojasi technologijų pasiekimais.
Šiame skyriuje rasite keletą pratimų, patarimų ir pavyzdžių, kaip lavinti mūsų dėmesingumą, analitinius ir pastabumo įgūdžius. Nepriklausomai nuo amžiaus, mokymasis praktikuojant duoda gerų rezultatų. Todėl, kaip besikuriančio Socialinio edukatorių tinklo ir šio kurso dalyviai, rasite pratimų, parodančių įvairias situacijas, kurios gali nutikti jums, jūsų šeimai ir draugams. Kuo daugiau realių pavyzdžių matysite, tuo lengviau bus atpažinti bandymus sukčiauti ir apsisaugoti nuo jų.

01 Sujunkite frazes, kad sudarytumėte teisingus teiginius:

Kibernetiniai sukčiai piktiems kėslams dažnai pasitelkia...	...įtartinus elektroninius laiškus turiu iškart pašalinti.
Tam, kad išvengčiau kenkėjiškų programų...	...legali ir patikima.
Mano pasirinkta antivirusinė programa privalo būti...	...apgaulingus laimėjimus.
Išsaugoti savo prisijungimo duomenis naršyklės sistemoje...	...yra nepatartina.
Išvengti netinkamo internetinio turinio padeda...	...kritiško informacijos vertinimo įgūdžiai

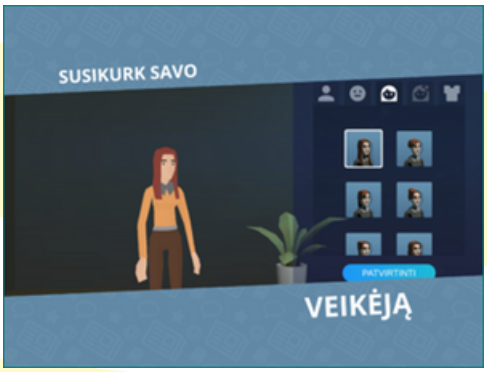
02 Kritiškas informacijos vertinimas

Kasdien mūsų smegenys greitai priima sprendimus, o mūsų patirtis, išankstiniai nusistatymai ir stereotipai atlieka savo vaidmenį. Nors kai kuriuos iš jų suvokiame neigiamai, jie padeda mums pasąmoningai, greičiau ir dažniausiai tiksliau priimti sprendimus. Dėl to negalvojame, ar puodą su verdančiu vandeniu kelsime plikomis rankomis ar, pavyzdžiui, naudosime virtuvinį rankšluostį. Mūsų smegenys veikia automatiškai, kad apsaugotų mus nuo galimos žalos. Kibernetiniai nusikaltėliai puikiai žino, kokie mechanizmai ir mąstymo procesai vyksta žmogaus smegenyse, ir bando juos panaudoti prieš mus. Pavyzdžiui, anksčiau minėti laimėjimai loterijoje. Mums patinka greiti ir lengvi prizai, ir to nereikėtų gėdytis. Mūsų smegenys pasąmoningai siūlo mums sprendimus, kurie, trumpai tariant, jų manymu, yra geresni, veiksmingesni, tokie, kurie leis mums pajusti dopamino - laimės hormono – antplūdį.
Nesijaudinkite, mes visi jį turime. Mūsų smegenys yra tiesiog pritaikytos efektyviems, greitiems ir teigiamiems rezultatams, o ne ilgoms analizėms, galimam laiko švaistymui ir mažam efektyvumui. Galų gale, kam nepatinka gerai jaustis dėl minties, kad jiems pavyko ką nors sumedžioti dėl skatinimo, kad jie sutaupė pinigų, gavo kažką gražaus be didelių pastangų.

Kibernetiniai nusikaltėliai remiasi schemomis, jos mums suteikia viziją gauti kažką malonaus, dovanojimą, paaukštinimą, laimėjimą, nors tikrovė yra visai kitokia.
Jei prie to pridėsime: skubėjimą, nervingumą, baimę, manipuliavimą, netikrumą ar nežinojimą, nenuostabu, kad nustojame mąstyti racionaliai ir griebiamės pirmųjų sprendimų, kurie pasirenkami emociškai ir neretai tampa mūsų pražūtimi. Štai kodėl taip svarbu kritiškai įvertinti informaciją ir situacijas

Žaidimas „REDAKCIJA 2030“

Žaidimas „Redakcija 2030“ – tai ateities pasaulio istorija apie vienintelį Lietuvoje likusį naujienų portalą. Šioje vizijoje žaidėjai turės padirbėti naujienų redaktoriumi, galinčiu paveikti visus ateities Lietuvos gyventojus.



Praktinės žaidimo užduotys padės ugdyti kritinį mąstymą ir žaidėjų gebėjimą atskirti tiesą nuo melo, tikras naujienas nuo melagienų.

NEMOKAMĄ žaidimą „Redakcija 2030“ parsisiųskite iš Google Play arba Apple Store parduotuvių.

Žaidimas sukurtas naudoti išmaniuosiuose telefonuose ir planšetėse.

03 Žaidimas „GALIMA – NEGALIMA“

GALIMA		NEGALIMA
☐	1.Kurdami slaptažodį būtinai įtraukite simbolius ir skaičius, kad būtų sunkiau „nulaužti“.	☐
☐	2. Siųsdami programas iš interneto,visada pirmiausia nuskaitykite antivirusinę programą, kad patikrintų, ar yra virusų.	☐
☐	3. Leisti žiniatinklio naršyklėms prisiminti jūsų naudotojo vardą ir slaptažodį.	☐
☐	4. Pateikti asmeninę informaciją internete.	☐
☐	5. Duoti savo slaptažodį visiems ir nuolat visur naudoti tą patį slaptažodį.	☐
☐	6. Atidaryti ir atsisiųsti priedų iš nežinomo šaltinio, nes juose gali būti virusų.	☐
☐	7. Užpildyti visas interneto apklausas, kuriose prašoma jūsų asmeninės informacijos ar banko informacijos.	☐
☐	8. Jei naudojate pokalbių kambario svetaines, naudoti slapyvardį kaip savo vartotojo vardą.	☐
☐	9. Naudokite antivirusinę programinę įrangą ir reguliariai atnaujinkite.	☐
☐	10. Įrašyti visas atliktas operacijas internetu ir reguliariai tikrinti savo banko sąskaitą.	☐

04 10 būdų, kaip patikrinti informacijos publikacijų internete patikimumą

1 Ar straipsnyje pateikiamos citatos, šaltiniai ir nuorodos?

Ar rūksta autoriaus vardo ir pavardės? 2

3 Jei autoriaus vardas ir pavardė nurodyti, ar jis yra patikimas, gerai žinomas asmuo?

Ką galima rasti interneto svetainės, kurią peržiūrime, skiltyse "apie mus", "taisyklės ir sąlygos", "susisiekite su mumis"? 4

5 Ar tekste yra rašybos, gramatikos, kalbos klaidų? Ar išlaikyta taisyklinga sakinių struktūra?

Ar straipsnyje yra citatų, kurios panaudotos netinkamai arba ištrauktos iš konteksto? 6

7 Ar galite rasti panašų straipsnį internete?

Ar straipsnyje pateikiama tik viena ginčo pusė? 8

9 Ar antraštė neatitinka straipsnio turinio?

Ar straipsnis yra absoliučiai skandalingas? 10

Atminkite: vien dėl to, kad pranešimas turi daug komentarų ir "patinka" arba juo pasidalijo vienas iš jūsų draugų, dar nereiškia, kad jis yra patikimas.

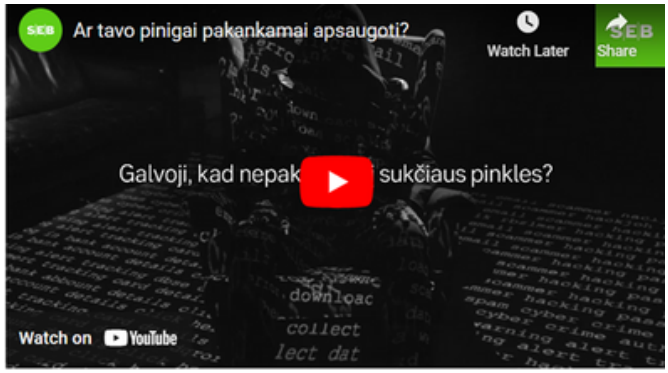
Tikriausiai ne kartą internete matėte antraštę su labai neįprastu pavadinimu, kuris privertė jus pagalvoti: "Neįmanoma, turiu tai patikrinti/perskaityti". Tačiau, kai perskaitėte straipsnį, pamatėte, kad jis arba visai nesusijęs su pavadinimu, arba buvo ištrauktas iš konteksto vien tam, kad atkreiptų jūsų dėmesį. Tačiau yra straipsnių, kurių autoriai nori imituoti realias publikacijas, kad skaitydami patikėtumėte, jog tai tiesa. Aukščiau išdėstyti punktai leis jums kritiškai pažvelgti į jo autentiškumą ir patikrinti, ar galite pasitikėti tuo, kas jame rašoma, ar ne.

05 Žaidimas „Pinklės“

Finansinių sukčių pinklės: kaip į jas neįkliūti?

Norite pamatyti, kaip atrodo sukčių auka? Tiesiog apsidairykite. Nukentėti kibernetinėje erdvėje gali bet kas – nuo studento ir bedarbio iki senjoro, verslininko ar universiteto dėstytojo. Sukčiavimo būdai darosi vis sudėtingesni ir sunkiau atpažįstami, todėl kiekvienas turime būti budrus, domėtis ir, kiek galime, apsisaugoti.

Sukčiavimas yra nusikaltimas. Juo siekiama jus apgauti ir pavogti jūsų pinigus. Sukčiavimo metu – bet kokiu kanalu bendraujant su sukčiumi – jums sudaromas klaidingas įspūdis apie tai, ko iš tiesų nėra.
Pirmiausia pasitikrinkite savo kibernetinio saugumo žinias, kad nepakliūtumėte į sukčių pinkles.
Interaktyvus testas, kuriame pateikiama dešimt realaus sukčiavimo internete situacijų, kurių paskirtis šviesti gyventojus, didinti jų finansinį raštingumą ir taip padėti apsisaugojanti nuo vis dažnėjančių finansinių apgavysčių.
Testą galima rasti www.seb.lt/pinkles



06 Mobilioji programėlė „Saugesnis internetas“

Programėlėje kiekvienas gali linksmai ir interaktyviai pasitikrinti savo žinias apie saugų elgesį internete. NEMOKAMĄ programėlę galima parsiųsti Google Play arba Apple Store parduotuvėse.
Ieškokite „Saugesnis internetas“ programėlės.
Programėlė sukurta naudoti išmaniuosiuose telefonuose ir planšetėse.

Norite sužinoti daugiau:

https://www.prisijungusi.lt/medziaga/norm/11/#/lessons/VH3j1MSunDKnFHp-u-1Y-rfqXDsPFBjI

Projektas "Senjorai senjorams“

Finansuoja
Europos Sąjunga

Kontaktai:

Asociacija Tezauras https://www.facebook.com/profile.php?id=100092026013697

tezaurask@gmail.com

Projektas „Senjorai senjorams", Respublikos g. 32-40, LT-57405 Kėdainiai, Lietuva