RestartVET

RESTART VET:

An innovative approach to support VET teachers/trainers through the digital transformation of VET education

Digital Safety Security (Lithuanian)

Co-funded by the Erasmus+ Programme of the European Union

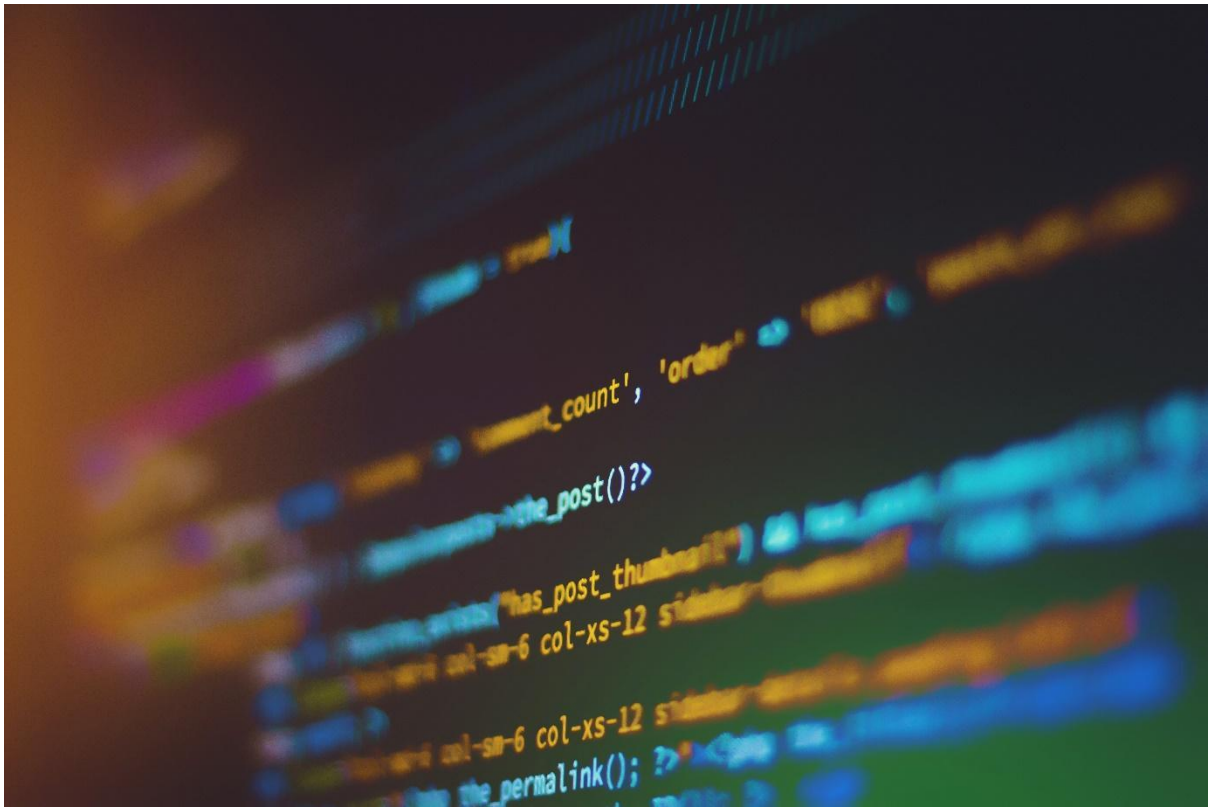
Skaitmeninė sauga ir saugumas

Įvadas:

Kai kurie iš labiausiai paplitusių mūsų kasdienio gyvenimo aspektų dar prieš porą dešimtmečių būtų atrodę kaip mokslinė fantastika! Mobiliųjų įrenginių naudojimas beveik visiems mūsų technologiniams poreikiams tenkinti, interneto greitis ir pasiekiamumas, gausybė taikomųjų programų ir IT sprendimų pakeitė mūsų kasdienę patirtį, prekybą, švietimą, pramogas, mokslinius tyrimus ir net mūsų tarpusavio gyvenimą.

Apskaičiuota, kad šiuo metu pasaulyje yra 4,66 mlrd. aktyvių interneto naudotojų iš 7,83 mlrd. pasaulio gyventojų, o tai reiškia, kad 92,6 proc. planetos žmonių turi prieigą prie pasaulinio interneto per įvairius įrenginius. Be to, 56,8 proc. pasaulio gyventojų asmeniniame ir profesiniame gyvenime nuolat naudojasi socialinės žiniasklaidos programomis.

Kadangi technologijos pasiekia tokį didžiulį mastą, nenuostabu, kad kyla keletas pavojų, galinčių neigiamai paveikti patirtį, ir grėsmių, galinčių pakenkti naudotojų saugai ir saugumui skaitmeniniame pasaulyje. Šiame modulyje nagrinėsime ir pristatysime pagrindinius skaitmeninės saugos ir saugumo aspektus, susijusius tiek su bendru internetinių priemonių naudojimu, tiek su mokymosi / mokymo aspektu profesinio rengimo ir mokymo sektoriuje.



Mokymosi tikslai:

Šio modulio pabaigoje:

- suprasti su skaitmeninių ir internetinių priemonių naudojimu susijusią riziką.
- geriau informuoti apie skaitmeninę saugą ir saugumą.
- įgijote pagrindinių įgūdžių, kad galėtumėte patenkinti savo skaitmeninės saugos ir saugumo poreikius.
- įgijote įgūdžių, kurie padės užtikrinti saugų ir patikimą besimokančiųjų mokymąsi internetu.
- būtų įgalioti ir motyvuoti užtikrinti skaitmeninę saugą ir saugumą bei taikyti naujausią geriausią praktiką ir sprendimus.

Bendrieji patarimai treneriui:

Įsitikinkite, kad šiame modulyje vartojami terminai suprantami vienodai, kad būtų užtikrintas sklandus turinio perteikimas; gali būti naudinga skirti šiek tiek laiko skirtingiems žodžiams ir skirtingoms priemonėms atskirti.

Paprašykite besimokančiųjų pagalvoti, kaip jie patys naudojasi skaitmeninėmis ir internetinėmis priemonėmis ir kiek plačiai jomis naudojasi; galbūt paklauskite, kaip jų gyvenimas pasikeistų, pasunkėtų ar net pagerėtų, jei artimiausias 24 valandas nebūtų interneto.

Paraginkite besimokančiuosius pasidalyti savo patirtimi ar rūpesčiais, susijusiais su skaitmeniniu saugumu ir sauga, atkreipkite dėmesį į šiuos klausimus ir, jei įmanoma, susiekite juos su modulio turiniu. Jei yra klausimų, kurie neaptarti, pasistenkite pasiūlyti papildomų išorinių šaltinių.

1. Kokios pagrindinės grėsmės ir (arba) pavojai kyla internete?

Adware

Reklaminė programinė įranga - tai nepageidaujama programinė įranga, skirta ekrane rodyti reklamą, dar vadinamą iššokančiaisiais langais.

Štai keletas tipinių požymių, rodančių, kad jūsų sistemoje yra reklaminių programų:

- Skelbimai rodomi tose vietose, kur jų neturėtų būti.
- Jūsų interneto naršyklės pagrindinis puslapis paslaptingai pasikeitė be jūsų leidimo.
- Tinklalapiai, kuriuose paprastai lankotės, rodomi netinkamai.
- Svetainės nuorodos nukreipia į kitas svetaines, nei tikėjotės.
- Jūsų interneto naršyklė sulėtėja.
- Naršyklėje staiga atsiranda naujų įrankių juostų, plėtinių ar įskiepių.
- Kompiuteryje pradedamos automatiškai diegti nepageidaujamos programinės įrangos programos.

Kenkėjiška reklama

Kenkėjiška reklama - tai kibernetinių atakų metodas, kai į skaitmeninius skelbimus įterpiamas kenkėjiškas kodas. Šiuos užkrėstus skelbimus sunku aptikti ir interneto naudotojams, ir leidėjams, todėl jie paprastai vartotojams pateikiami per teisėtus reklamos tinklus. Kadangi skelbimai rodomi visiems svetainės lankytojams, praktiškai kiekvienam puslapio žiūrovui kyla rizika užsikrėsti.

Phishing

"Phishing" - tai dažniausiai el. paštu siunčiama ataka, kuria galutiniai naudotojai viliojami spustelėti kenkėjišką nuorodą arba priedą. Užpuolikai gali naudoti phishing, kad įsitvirtintų organizacijoje, dažnai platindami kenkėjišką programinę[1] įrangą.

1

Spear phishing

"Spear phishing" - tai sukčiavimo būdas, kuriuo siekiama apgauti konkrečius asmenis ar grupes organizacijoje. Tai galingas sukčiavimo variantas - kenkėjiška taktika, kai elektroniniais laiškais, socialine žiniasklaida, trumposiomis žinutėmis ir kitomis platformomis siekiama, kad naudotojai atskleistų asmeninę informaciją arba atliktų veiksmus, dėl kurių pažeidžiamas tinklas, prarandami duomenys arba patiriami finansiniai nuostoliai. Įprastą "spear phishing" ataką sudaro el. laiškas ir priedas. Elektroniniame laiške pateikiama konkreti informacija apie taikinį, įskaitant jo vardą, pavardę ir rangą įmonėje. Ši socialinės inžinerijos taktika padidina tikimybę, kad auka atliks visus užkrėtimui būtinus veiksmus, įskaitant el. laiško ir pridėto priedo atidarymą.

Cybersquatting (domenų skvotinimas)

Kibernetinė skvotininkystė - tai neteisėtas interneto domenų vardų, kurie yra identiški arba panašūs į prekių ženklus, paslaugų ženklus, įmonių pavadinimus ar asmenvardžius, registravimas ir naudojimas siekiant suklaidinti, piktavališkai pritraukti naudotojus arba sukčiauti.

Šnipinėjimo programos

Šnipinėjimo programinė įranga - tai kenkėjiška programinė įranga, kuria siekiama rinkti informaciją apie asmenį ar organizaciją ir siųsti ją kitam subjektui taip, kad būtų padaryta žala naudotojui.

Smishing

Smishing atakose naudojamos trumpųjų žinučių paslaugos arba SMS, dažniau žinomos kaip tekstinės žinutės.

"Smishing" - tai asmeninių duomenų vagystė apsimetant banko atstovu, priverčiant spustelėti teksto žinutėje esančią nuorodą, kad prisijungtumėte prie banko tinklalapio ir patikrintumėte neseniai atliktą įtartiną mokestį, prašant paskambinti klientų aptarnavimo numeriu, kuris patogiai pateikiamas teksto žinutėje, ir pasikalbėti apie neseniai atliktą įtartiną mokestį arba pažeistą sąskaitą.

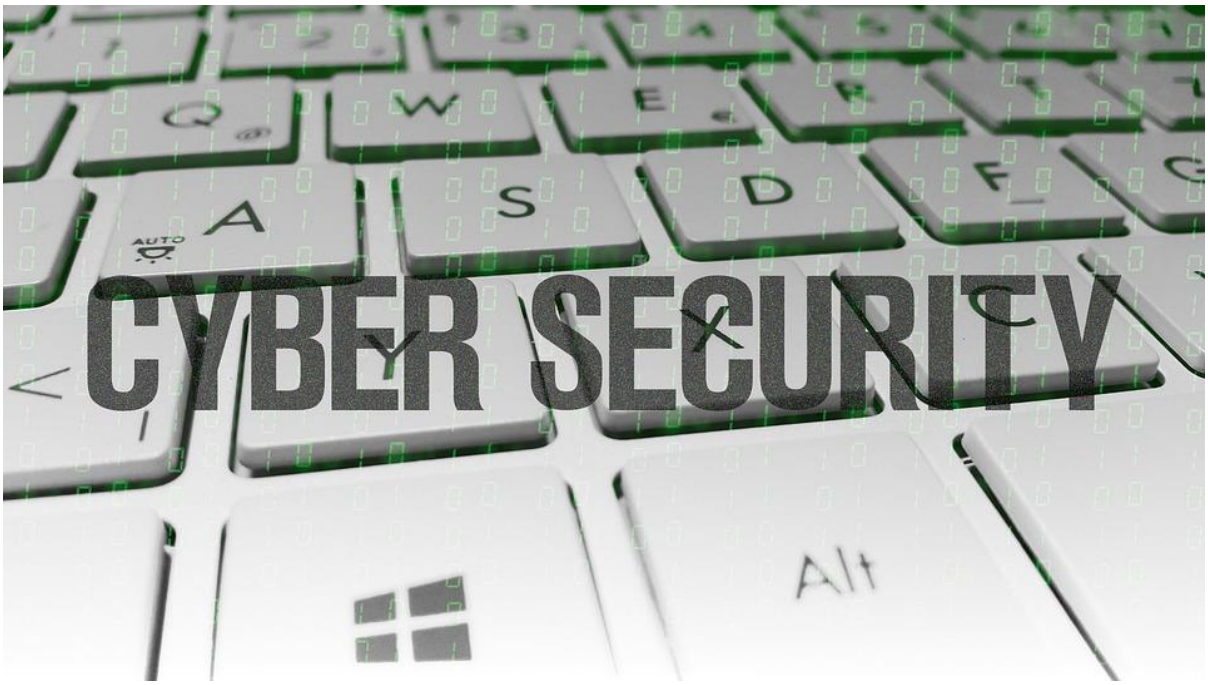
Pirmiau išvardytos tik kelios šiuo metu paplitusios internetinės grėsmės, kurios kasdien atakuoja milijonus naudotojų. Naudotojams rekomenduojama nuolat informuoti apie pokyčius ir naujas grėsmes, reguliariai stebint svetaines, pvz., tas, kurios pateiktos toliau, skiltyje "Kiti šaltiniai":

Kiti ištekliai

ENISA (europa.eu)

Kibernetinio saugumo rizika | NIST

Mokymų vadovams rekomenduojama papildyti papildomų išteklių sąrašą medžiaga savo kalba ir (arba) medžiaga, susijusia su šalimi / regionu. Geras informacijos šaltinis taip pat gali būti kibernetinio saugumo ekspertų ir tyrėjų straipsniai ir publikacijos internete.



2. Skaitmeninės saugos ir saugumo priemonės

Sukurkite slaptažodžius ir pasirūpinkite, kad jie būtų stiprūs.

Daugelis naudotojų nenaudoja slaptažodžio funkcijos bent viename iš savo įrenginių, kuriuose įjungtas internetas, ir palieka jį atvirą bet kam, kas gali jį paimti. Užrakinkite visus savo įrenginius, įskaitant kompiuterius, planšetinius kompiuterius ir išmaniuosius telefonus, saugiais slaptažodžiais. Tai neleis pašalinėms akims patekti į jūsų įrenginius ir suteiks papildomą apsaugos liniją, jei jie būtų pamesti, pamesti ar pavogti. Stiprus slaptažodis yra bent 12 simbolių ilgio. Patarimai dėl patikimų slaptažodžių apima mažųjų ir didžiųjų raidžių, skaičių ir simbolių derinį ir vengimą naudoti asmeninę informaciją, kurią galima lengvai atpažinti (sutuoktinio vardą, augintinio vardą, gimtadienius ir t. t.). Silpnas slaptažodis būtų toks, kurį bet kas galėtų lengvai sužinoti, pavyzdžiui, mylimo augintinio vardas "KittkyCat"; stiprus slaptažodis galėtų atrodyti taip: "1Kitty234Cat!!!".

Kaip dažnai reikia keisti slaptažodžius?

Jei nesužinote apie slaptažodžių pažeidimą, nereikia reguliariai keisti slaptažodžių, jei kiekvienas slaptažodis yra stiprus ir unikalus. Tai dar svarbiau, jei naudojate dviejų veiksnių autentifikavimą.
Jei įmanoma, naudokite tam tikrą dviejų veiksnių autentifikavimo būdą, kad nulaužus slaptažodį nebūtų pažeista jūsų paskyra. Suderinus dviejų veiksnių autentifikavimą su mašinomis generuojamais slaptažodžiais, daugumos naudotojų paskyrų praktiškai neįmanoma nulaužti.

Kas yra unikalus slaptažodis?

Unikalus slaptažodis yra:

1. Niekada pakartotinai nenaudotas. Vieną kartą panaudoję slaptažodį, jo niekada negalėsite naudoti kitoje paskyroje.
2. Pakankamai ilgai. Stiprus slaptažodis turi būti bent 12 simbolių ilgio. Patarimai dėl stipraus slaptažodžio - naudoti raidžių, skaičių ir simbolių derinį.
3. Nieko, kas būtų susiję su jumis. Tai reiškia, kad slaptažodyje nenaudokite vaiko ar augintinio vardo arba kitos informacijos, kurią galima lengvai susieti su jumis.

Kadangi šiais laikais naudotojai naudoja daugybę programų ir įrenginių, gali būti labai viliojanti mintis naudoti vieną slaptažodį daugumai įrenginių ir programų. Tačiau, kad ir kaip būtų patogu, tokia praktika gali sukelti didelį pažeidžiamumą, nes viena kenkėjiška ataka gali paveikti daugumą jūsų paskyrų ir net pakenkti internetinės bankininkystės ar debesų saugyklų sprendimams. Todėl primygtinai rekomenduojama naudoti skirtingus unikalius slaptažodžius skirtingiems įrenginiams ir programoms ir būti atsargiems dalijantis šiais slaptažodžiais ar juos įvedant viešuosiuose tinkluose.

Kaip veikia dviejų veiksnių autentifikavimas?

Dviejų veiksnių autentifikavimą galite įjungti savo socialinės medijos paskyros, el. pašto ar kitų profilių nustatymuose. Dviejų veiksnių autentifikavimas bus atliekamas naudojant jūsų telefono numerį arba autentifikavimo programėlę išmaniajame telefone. Aktyvavus dviejų veiksnių autentifikavimą, kiekvieną kartą prisijungus prie paskyros iš naujo įrenginio ar naršyklės, į jūsų telefoną arba autentifikavimo programėlę bus siunčiamas saugumo kodas. Turėsite įvesti šį kodą ir jums bus leista prisijungti. Jei kibernetinis nusikaltėlis bandys prisijungti prie jūsų paskyros, jis negalės to padaryti, jei neturės prieigos prie jūsų mobiliojo telefono. Jūs taip pat galėsite pastebėti bandymą prisijungti prie savo paskyros, nes gausite pranešimą su kodu. Niekada nesidalykite šiuo kodu su kitais asmenimis! Užpuolikas bandys jį

gauti. Jei gavote kodą, bet nebandėte prisijungti, ištrinkite pranešimą su kodu ir kuo greičiau pakeiskite slaptažodį.

Privatumo nustatymai socialinėje žiniasklaidoje

Kurdami pranešimus socialiniuose tinkluose galite pasirinkti privatumo nustatymus. Pavyzdžiui, galite pasirinkti, kokia auditorija matys jūsų įrašą. Tai gali būti tik jūsų draugai, kuriuos įtraukėte į socialinį tinklą, tai gali būti viešas įrašas, skirtas visiems, arba tai gali būti privatus įrašas, skirtas tik jums. Taip pat galite nurodyti arba nenurodyti savo buvimo vietą. Įsitikinkite, kad jūsų privati informacija nėra bendrinama. Pavyzdžiui, jūsų slaptažodžiai, telefono numeris, el. pašto adresas ir pan.

Saugos taisyklės socialinėje žiniasklaidoje, žinutėse ir el. paštuose

Bendraudami per socialinius tinklus, žinučių siuntimo programas ir el. paštą turite būti atsargūs, kad nenukentėtumėte nuo pretenzijų, kenkėjiškos reklamos ar įvairių rūšių sukčiavimo. Nespauskite nuorodų, kurias jums atsiuntė nežinomas asmuo. Būkite atsargūs - kibernetiniai nusikaltėliai gali apsimesti, pavyzdžiui, "Facebook" darbuotojais arba "Instagram" saugos tarnybos darbuotojais. Nepasitikėkite tais pranešimais, jei juos gaunate per įprastą pokalbį, žinutę ar iš įprasto "Facebook" puslapio. Saugumo pranešimus gausite per pranešimus arba juos galėsite rasti nustatymuose. Socialinės žiniasklaidos darbuotojai niekada neprašys jūsų slaptažodžio ar privačios informacijos.

Kažkas prašo pinigų?

Jei draugai ar šeimos nariai prašo jūsų padėti jiems nelaimės atveju, visada paskambinkite ir pasikalbėkite su jais asmeniškai, kad įsitikintumėte, jog žinutė atėjo iš jų. Priešingu atveju tos žinutės gali būti iš kibernetinių nusikaltėlių. Jie gali sukurti profilį, kuris bus identiškas jūsų šeimos nario ar draugo profiliui, ir bandyti iš jūsų gauti pinigų.

Įrenginio saugumas

Naudokite saugumo programinę įrangą. Įdiekite patikimo šaltinio saugumo programinę įrangą į savo įrenginius ir nuolat ją atnaujinkite. Geriausia reguliariai paleisti antivirusinę ir šnipinėjimo programinę įrangą. Būkite atsargūs dėl saugumo atnaujinimų iš iššokančių reklamų ar el. laiškų. Jie iš tikrųjų gali būti kenkėjiška programinė įranga, galinti užkrėsti jūsų kompiuterį.

Naudokite numatytąją kompiuterio ugniasienės apsaugą. Jūsų operacinėje sistemoje (OS) greičiausiai yra numatytieji ugniasienės nustatymai, kurie apsaugo kompiuterį ir kurių nereikia koreguoti. Jei jūsų antivirusinėje programoje yra papildoma ugniasienės apsauga, kurią galite reguliuoti atskirai, apsvarstykite galimybę kreiptis pagalbos į kompiuterių specialistą, kad užtikrintumėte saugią apsaugą, pernelyg neužblokuodami reguliariai naudojamų svetainių ir programų.

Atsijungti. Nepamirškite atsijungti nuo programų ir svetainių, kai baigsite jomis naudotis. Palikę jas atidarytas kompiuterio ekrane, galite patirti saugumo ir privatumo pavojų.

10 patarimų, kaip apsisaugoti internete

1. Sukurkite slaptažodžius ir pasirūpinkite, kad jie būtų stiprūs.

2. Saugi prieiga prie paskyrų. Kadangi slaptažodžius galima pavogti, paskyrų papildymas dviejų etapų autentifikavimu suteikia antrą apsaugos lygį. Daugelyje internetinių paslaugų, įskaitant programėles ir svetaines, siūlomos nemokamos parinktys, kurios gali padėti apsaugoti jūsų informaciją ir užtikrinti, kad prie paskyros iš tikrųjų bandote prisijungti jūs, o ne kas nors, turintis jūsų slaptažodį.

3. Pagalvokite prieš pradėdami veikti. Elektroniniai laiškai ir pranešimai, sukeliantys skubos jausmą, pvz., apie banko sąskaitos ar mokesčių problemą, greičiausiai yra sukčiai. Apsvarstykite galimybę tiesiogiai susisiekti su įmone telefonu ir nustatyti, ar el. laiškas yra teisėtas, ar ne.

4. Kai abejojate, išmeskite. Spustelėdami nuorodas el. laiškuose sukčiai dažnai gauna prieigą prie asmeninės informacijos. Jei el. laiškas atrodo neįprastai, net jei pažįstate jį siuntusį asmenį, geriausia jį ištrinti. Atminkite, kad sukčiai gali pasisavinti draugų el. pašto adresus ir siųsti jums žinutes prisistatydami jų vardu. Įjunkite savo el. pašto dėžutės nepageidaujamų laiškų filtrus, kurie padės filtruoti įtartinus pranešimus.

5. Dalytis atsargiai. Būkite atidūs tam, kuo viešai dalijatės tokiose socialinės žiniasklaidos svetainėse kaip "Facebook". Sureguliuokite privatumo nustatymus, kad apribotumėte, kas gali matyti jūsų informaciją. Venkite dalytis savo buvimo vieta.

6. Naudokite saugumo programinę įrangą. Į savo įrenginius iš patikimo šaltinio įdiekite saugumo programinę įrangą ir nuolat ją atnaujinkite. Geriausia reguliariai paleisti antivirusinę ir šnipinėjimo programinę įrangą. Būkite atsargūs dėl saugumo atnaujinimų iš iššokančių reklamų ar el. laiškų. Jie iš tikrųjų gali būti kenkėjiška programinė įranga, galinti užkrėsti jūsų kompiuterį.

7. Sureguliuokite naršyklės saugos nustatymus. Naujienų, informacijos ir produktų greičiausiai ieškote naudodami interneto naršyklę, pavyzdžiui, "Firefox", "Google Chrome", "Internet Explorer" ir "Safari". Sureguliuokite kiekvienos iš šių naršyklių nustatymus, kad nustatytumėte optimalaus saugumo parinktis. Šiuos meniu dažnai rasite viršutiniame dešiniajame naršyklės kampe. Apsvarstykite galimybę pasibaigus sesijai išvalyti naršymo istoriją, kad nepaliktumėte slaptų duomenų pėdsakų.

8. Naudokite numatytąją kompiuterio ugniasienės apsaugą. Jūsų operacinėje sistemoje (OS) greičiausiai yra numatytieji ugniasienės nustatymai, kurie apsaugo kompiuterį ir kurių nereikia koreguoti. Jei jūsų antivirusinėje programoje yra papildoma ugniasienės apsauga, kurią galite reguliuoti atskirai, apsvarstykite galimybę kreiptis pagalbos į kompiuterių

specialistą, kad užtikrintumėte saugią apsaugą, pernelyg neužblokuodami reguliariai naudojamų svetainių ir programų.

9. Atsijungti. Nepamirškite atsijungti nuo programų ir svetainių, kai baigsite jomis naudotis. Palikę jas atidarytas kompiuterio ekrane, galite būti pažeidžiami saugumo ir privatumo pavojų.

Apsvarstykite paramą. Jei nerimaujate dėl skaitmeninio saugumo ir saugos, kreipkitės į patikimą specialistą arba paprašykite paramos ir įžvalgų iš savo organizacijos IT skyriaus.

SAVĘS VERTINIMAS:

- Apmąstykite savo kasdienius įpročius ir praktiką, ar manote, kad galite būti pažeidžiami skaitmeninio saugumo / saugos požiūriu?
- Kiek iš 10 siūlomų patarimų šiuo metu įgyvendinate?
- Kokius patarimus ar idėjas planuojate panaudoti?
- Kokius tris patarimus besimokantiesiems galėtumėte duoti apie skaitmeninį saugumą ir (arba) saugą?