Pavadinimas
Elektroninis parašas ir duomenų šifravimas

Dalykas
Informatika

Klasė
IV G

Pasiekimų sritis
Saugus elgesys (F)

Slenkstinis lygis	Patenkinamas lygis	Pagrindinis lygis	Aukštesnysis lygis
Sprendžia paprastas problemas, susijusias su asmens duomenų teisėtu naudojimu ir privatumu, siekdamas apsaugoti save virtualiojoje aplinkoje (F3.1).	Sprendžia įvairias problemas, susijusias su asmens duomenų teisėtu naudojimu ir privatumu, siekdamas apsaugoti save ir kitus virtualiojoje aplinkoje (F3.2).	Pasirenka tinkamiausius būdus spręsti problemas, susijusias su asmens duomenimis, jų privatumu ir teisėtu naudojimu, siekdamas apsaugoti save ir kitus virtualiojoje aplinkoje (F3.3).	Įsivertina gebėjimus efektyviai spręsti problemas, susijusias su asmens duomenimis, jų privatumu ir teisėtu naudojimu, siekdamas apsaugoti save ir kitus virtualiojoje aplinkoje, juos tobulinasi (F3.4).

Mokymo(si) turinio tema
Elektroninis parašas ir duomenų šifravimas

Ilgalaikio plano dalis
III gimnazijos klasė
- Higienos, ergonominių ir techninių saugaus darbo skaitmeninėmis technologijomis problemų sprendimas.
- Poveikio aplinkai prognozė taikant skaitmenines technologijas.

I-II gimnazijos klasė
- Higienos, ergonominės ir techninės saugaus darbo skaitmeninėmis technologijomis normos.
- Aplinkosaugos problemos ir jų sprendimai.
- Virtualiųjų aplinkų saugumo nuostatai.

7-8 klasė
- Saugus ir sveikatą tausojantis darbas skaitmeniniu įrenginiu.
- Rizikos žmogaus fizinei ir psichinei savijautai naudojant skaitmenines technologijas.
- Skaitmeninių technologijų svarba aplinkosaugos sprendimams.
- Saugaus darbo virtualiojoje erdvėje principai, pavojai ir problemos.

5-6 klasė
- Saugus ir sveikatą tausojantis elgesys kompiuterių klasėje.
- Veiksmai, kurie mažina skaitmeninių technologijų neigiamą poveikį aplinkai.

- Saugus bendravimas ir bendradarbiavimas virtualioje erdvėje.
- Kibernetinės grėsmės.
- Teisiniai asmens duomenų naudojimo aspektai.

3-4 klasė

- Sveikatą tausojantis darbas skaitmeniniu įrenginiu.
- Skaitmeninių technologijų poveikis visuomenei ir aplinkai.
- Saugus asmeninių duomenų pateikimas virtualiojoje erdvėje.

1-2 klasė

- Taisyklės dirbant skaitmeniniu įrenginiu.
- Skaitmeninės technologijos ir aplinka.
- Asmeninių duomenų saugumas.

Valandų skaičius nurodytas ilgalaikiame plane
1 val.

Mokymosi uždaviniai (pamatuojami) ir vertinimo kriterijai

Uždaviniai	Vertinimo kriterijai
Suprasti elektroninio parašo sąvoką ir jo tipus	Gebėjimas paaiškinti, kas yra elektroninis parašas. Gebėjimas atskirti kvalifikuotą ir nekvalifikuotą elektroninį parašą. Supratimas apie kvalifikuoto elektroninio parašo teisinę galią ir paskirtį.
Suprasti duomenų šifravimo sąvokas ir metodus	Gebėjimas paaiškinti, kas yra duomenų ir pranešimų šifravimas.
Praktiškai išbandyti elektroninį parašą ir šifravimo įrankius	Gebėjimas naudoti pranešimų šifravimo įrankį pranešimų šifravimui bei dešifravimui, 2 faktorių autentifikaciją.

Galimi mokymo(si) metodai, siūloma veikla

Metodas	Veikla
Aiškinimas, filmuota medžiaga ir diskusija	Pamoka apie elektroninio parašo sąvokas ir tipus, diskusija apie elektroninio parašo ir šifravimo svarbą bei jų teisinę galią.
Darbo grupėje metodas, minčių lietus	Grupinis darbas analizuojant elektroninio parašo ir šifravimo privalumus ir trūkumus, minčių lietus apie galimas jų naudojimo situacijas kasdieniame gyvenime.
Demonstracija ir praktinė veikla	Mokytojo demonstracija, kaip naudoti pasirašyti el. parašu dokumentą. Mokiniai patys atlieka šifravimo ir dešifravimo užduotis.

Mokymui(si) skirtas turinys
Elektroninio parašo sąvoka ir tipai

Elektroninis parašas yra skaitmeninė priemonė, leidžianti pasirašyti dokumentus elektroniniu būdu. Yra keli elektroninio parašo tipai, įskaitant kvalifikuotą ir nekvalifikuotą parašą.

Kvalifikuotas elektroninis parašas, sukurtas naudojant kvalifikuotą parašo kūrimo įrenginį ir patvirtintas kvalifikuotu sertifikatu, turi tokią pačią teisinę galią kaip ir ranka rašytas parašas. Nekvalifikuotas elektroninis parašas yra elektroninis parašas, kuris neturi tokių griežtų teisinių reikalavimų kaip kvalifikuotas parašas. Jis gali būti naudojamas įvairiose situacijose, tačiau jo teisinė galia ir pripažinimas gali skirtis priklausomai nuo konteksto ir vietinių teisės aktų.

Elektroninio parašo sertifikato galiojimui. Teikti kvalifikuotas elektroninių laiko žymų kūrimo paslaugas gali tik tam teisę turintys kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai. Jų sąrašas skelbiamas tinklalapyje www.elektroninisparasas.lt. Reikalavimai kvalifikuotam elektroniniam parašui yra vienodi visose ES šalyse. Reikalavimų kvalifikuotam elektroniniam parašui tenkinimą prižiūri ir garantuoja valstybė. Susipažįstama su praktinėmis saugiomis el. parašo kūrimo, tikrinimo priemonėmis. Jos išbandomos, pasirašant ir tikrinant įvairius dokumentus. Rekomenduojama naudoti priemones.

Paslauga	Nuoroda	Aprašymas	Palaikomi formatai
ADOC archyvai	ADOC.archyvai.lt	Lietuvos valstybės archyvų informacinė sistema, skirta elektroniniams dokumentams valdyti ir saugoti. Ši sistema leidžia vartotojams saugiai kurti, valdyti ir saugoti elektroninius dokumentus, taip pat pasirašyti juos elektroniniu parašu.	adoc
Eparašas	eparasas.lt	Elektroninio parašo paslauga, leidžianti pasirašyti ir valdyti dokumentus.	PDF, DOCX, TXT, XLSX, ir kiti
Dokobit	dokobit.com	Elektroninių parašų ir dokumentų valdymo platforma, skirta pasirašyti ir patikrinti elektroninius parašus.	PDF, DOCX, TXT, XLSX, ir kiti
Marksign	marksign.lt	Elektroninių dokumentų pasirašymo platforma, leidžianti lengvai ir greitai	PDF, DOCX, ir kiti

		pasirašyti PDF formatu paruoštus dokumentus.	
GoSign	gosign.lt	Dokumentų pasirašymo ir valdymo platforma, leidžianti organizuoti kolektyvinį pasirašymą bei valdyti elektroninius dokumentus.	PDF, DOCX, ir kiti

Pastabos
Visi šie paslaugų teikėjai siūlo elektroninio parašo paslaugas, kurios yra suderinamos su ES teisės aktais ir užtikrina aukštą saugumo bei patikimumo lygį. Kiekvienas tiekėjas turi savo savitas savybes ir privalumus, kurie gali būti naudingi priklausomai nuo konkrečių vartotojų poreikių. Keletas jų suteikia galimybę nemokamai pasirašyti keletą dokumentų per mėn.

Elektroninio parašo naudojimo privalumai
Elektroninis parašas leidžia pasirašyti dokumentus neišeinant iš namų. Todėl tai yra patogus būdas pasirašyti dokumentus, kuris taupo laiką ir saugo gamtą, pavyzdžiui, naudojant „Smart-ID“ ar „Mobile-ID“ programas.

- Kvalifikuotas elektroninis parašas yra teisiškai pripažintas ir laikomas lygiaverčiu ranka rašytam parašui.
- Elektroninis parašas užtikrina dokumentų vientisumą ir autentiškumą, nes bet koks duomenų pakeitimas yra aptinkamas tikrinimo metu.

Duomenų šifravimas
Duomenų šifravimas yra procesas, kai duomenys paverčiami koduotu formatu, siekiant juos apsaugoti nuo neatpažintos prieigos. Yra naudojami privatūs ir viešieji šifravimo raktai, kurie užtikrina duomenų saugumą ir konfidencialumą.

Praktinis šifravimo naudojimas:
Naudojant „Kleopatros“ pranešimų šifravimo įrankį (kuris yra „Gpg4win“ programų paketo dalis), mokiniai gali praktiškai išbandyti duomenų ir pranešimų šifravimą bei dešifravimą. Kaip naudotis „Kleopatra“ žiūrėti vaizdo įraše (laikas nuo 9:00 min.) https://www.youtube.com/watch?v=wrGzSAcJdaE

Pavyzdžiai iš realaus gyvenimo, kur šifravimas naudojamas apsaugoti finansinius duomenis, asmens duomenis bei kitą jautrią informaciją. Pvz.
Slaptažodžių tvarkyklė - yra įrankis, kuris saugiai saugo ir tvarko jūsų slaptažodžius. Ji padeda generuoti stiprius, unikalius slaptažodžius kiekvienai jūsų paskyrai, automatiškai užpildo prisijungimo duomenis ir saugo jautrią informaciją šifruotu formatu. Slaptažodžių tvarkyklės pagerina saugumą, sumažindamos silpnų ar pasikartojančių slaptažodžių naudojimo riziką įvairiose svetainėse. Jos gali sinchronizuotis per kelis įrenginius, užtikrinant, kad turėtumėte prieigą prie savo slaptažodžių bet kada ir bet kur.
pvz. Bitwarden, LastPass Free, KeePass, Dashlane Free, Zoho Vault, NordPass Free.

Dviejų faktorių autentifikacija (2FA) yra saugumo priemonė, kuri reikalauja dviejų nepriklausomų autentifikacijos būdų, kad būtų galima patvirtinti vartotojo tapatybę. Ši papildoma saugumo priemonė padeda apsaugoti paskyras nuo neteisėtos prieigos, net jei slaptažodis buvo pavogtas.

Kaip veikia 2FA:

Pirmasis faktorius: Dažniausiai tai yra vartotojo žinomas slaptažodis ar PIN kodas.

Antrasis faktorius: Tai gali būti fizinis įrenginys, kaip išmanusis telefonas, arba unikalus kodas, kuris siunčiamas į el. paštą arba mobilųjį telefoną.

pvz. Google Authenticator, Authy, Microsoft Authenticator, LastPass Authenticator

Praktinis šifravimo naudojimas:

Naudojant „Kleopatros“ pranešimų šifravimo įrankį (kuris yra „Gpg4win“ programų paketo dalis), mokiniai gali praktiškai išbandyti duomenų ir pranešimų šifravimą bei dešifravimą.

Pavyzdžiai iš realaus gyvenimo, kur šifravimas naudojamas apsaugoti finansinius duomenis, asmens duomenis bei kitą jautrią informaciją.

Duomenų šifravimo programos

Gpg4win

Programa naudojama elektroninių laiškų ir dokumentų šifravimui, paremta PGP standartu, integruojanti „Kleopatros“ įrankį, kuris leidžia šifruoti ir dešifruoti pranešimus bei dokumentus. https://www.gpg4win.org.

Įrenginių šifravimo funkcijos įjungimas. https://support.microsoft.com/lt-lt/windows/%C4%AFrengini%C5%B3-%C5%A1ifravimo-funkcijos-%C4%AFjungimas-0c453637-bc88-5f74-5105-741561aae838?fbclid=IwAR3jGnTraIsDePiCoCn1nBcFUIDPtwK6Me0nN95tPO3XCL_6yC6HWkBRxe4

Vaizdo medžiaga:

Kur naudoti elektroninį parašą? (Prisijungusi Lietuva, 2019)

- Trukmė: 2:28 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Kas yra kvalifikuotas elektroninis parašas? (Prisijungusi Lietuva, 2019)

- Trukmė:1:56 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Elektroninis parašas jūsų asmens tapatybės kortelėje – kur ir kaip jį pritaikyti? (Prisijungusi Lietuva, 2019)

- Trukmė: 3:07 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Kas yra mobilusis parašas? (Prisijungusi Lietuva, 2019)

- Trukmė:2:54 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Kaip pasirašyti elektroniniu parašu? (Prisijungusi Lietuva, 2019)

- Trukmė:2:05 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Kur naudoti elektroninį parašą? (Prisijungusi Lietuva, 2019)

- Trukmė: 2:28 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Kas yra dviejų faktorių autentifikacija? (Prisijungusi Lietuva, 2019)

- Trukmė:1:46 min.
- „YouTube” nuoroda (žr. 2024–07–31)

Užduotys skirtos vertinimui ir įsivertinimui

Atsakymo pavyzdys (užduotis)	Taškai	Pastabos
Testas apie elektroninio parašo ir duomenų šifravimo sąvokas ir metodus (2 priedas)	10 taškų	1 taškas už kiekvieną teisingai atsakytą klausimą.

Namų darbai (jei reikia, nurodykite, kokius namų darbus mokiniai turėtų atlikti)

Moderuoti diskusija šeimoje apie duomenų šifravimą ir savo šeimos apsauga ir parašyti refleksiją. (5 priedas)

Atsakymo pavyzdys (užduotis)	Taškai	Pastabos
Sukurti šifravimo sistemą šeimoje parašyti refleksiją (3 priedas)	6 taškai	Išvardyti įrankiai ir metodai, kuriuos naudojate šifravimo ir dešifravimo procesui (1 taškas). Nurodyti iššūkiai, su kuriais susidūrėte atliekant užduotį (2 taškai). Aprašyta šeimos narių reakcija ir supratimas (1 taškas). Šifravimo sistemos kūrimo naudingumas šeimos kasdienėms reikmėms (2 taškai).

Siūloma papildoma medžiaga / literatūra / skaitmeninės mokymo priemonės (SMP)

Vidurinio ugdymo informatikos bendrosios programos įgyvendinimo rekomendacijos

Įgyvendinimo rekomendacijas rengė: Antanas Balvočius, prof. dr. Valentina Dagienė, Povilas Leonavičius, dr. Bronius Skūpas, Aidas Žandaris

Šaltinis: https://www.emokykla.lt/upload/files/2023/07/27/vidurinio-ugdymo-informatikos-bp-ir-2023-07-20.pdf

Sąvokomis ir šių technologijų naudojimo privalumais bei ypatybėmis. Vadovaujantis Reglamento (ES) Nr. 910/2014 22 straipsnio 1 ir 2 dalimis sudaromas, tvarkomas ir skelbiamas Lietuvos Respublikoje įsisteigusių kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir jų teikiamų kvalifikuotų patikimumo užtikinimo paslaugų sąrašas (Nacionalinis patikimas sąrašas, https://elektroninisparasas.lt/lietuvospatikimas-sarasas/, žr. 2023–06–28).

Šis sąrašas – tai patikimas sąrašas, į kurį įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos prižiūri Lietuvos Respublika, taip pat informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas, laikantis atitinkamų nuostatų, nustatytų eIDAS reglamente. (https://eur-lex.europa.eu/legalcontent/LT/LSU/?uri=CELEX:02014R0910-20140917, žr. 2023–06– 28). Susipažistama su Europos Sąjungos elektroninių parašų direktyvą (https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/? uri=CELEX:31999L0093&from=LT, žr. 2023–06–28).

Elektroninis parašas yra suprantamas plačiąja prasme ir elektroniniu parašu laikoma, pavyzdžiui, elektroniniame laiške užrašytas vardas ar pavardė. Kvalifikuotam elektroniniam parašui keliami gerokai didesni saugumo reikalavimai. Elektroninis parašas yra saugus jei: yra vienareikšmiškai susietas su pasirašančiu asmeniu; leidžia identifikuoti pasirašantį asmenį; yra sukurtas priemonėmis, kurias pasirašantis asmuo gali tvarkyti tik savo valia; yra susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas. Elektroninis parašas yra kvalifikuotas, jei jis yra saugus ir sudarytas saugia parašo formavimo įranga bei patvirtintas galiojančiu kvalifikuotu sertifikatu. Kvalifikuoto elektroninio parašo teisinė galia yra tokia pat, kaip ir ranka pasirašyto parašo. Sudėtinė el. parašo koncepcijos dalis yra elektroninė laiko žyma.

Pagal eIDAS reglamentą, elektroninė laiko žyma – elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji tuo metu egzistavo. Elektroninės laiko žymos palengvina elektroninio parašo galiojimo patikrinimą pasibaigus kvalifikuoto.

Reikalingi materialiniai ir technologiniai ištekliai

- Kompiuteriai su interneto prieiga, praktinėms užduotims atlikti.
- Interneto naršyklėje („Chrome", „Firefox, „Safari").
- „Windows" operacines sistemos.
- Gpg4win „Kleopatros" šifravimo įrankio https://www.gpg4win.org.
- Pasirinkus naudoti „FigJam" užtenka turėti vidutinį kompiuterinį raštingumą. Medžiagos paruošimas praktiškai nesiskiria nuo kitų naudojamų įrankių pvz. „Microsoft PowerPoint". Principai išlieka tie patys kaip ir galimybės. Pasiruošimo laikas turint mokomąja medžiagą 1-2 valandos. „FigJam" yra nemokamas švietimo darbuotojams – jums reikia tik patvirtinti savo paskyrą, įsivesti mokyklos pavadinimą. Atlikus registraciją ir atidarę nuorodą, galite pasidaryti lentos kopiją ir ją papildyti.

Pateikta konkreti medžiaga, kurią galima naudoti pamokoje

Užduočių lapai
Veiklos planas (1 priedas)
Testas (2 priedas)
Projekto idėjos (3 priedas)
Namų darbai (4 priedas)

1 priedas.
Veiklos planas

Klasės pasirengimo lygis	Vidutiniškas
Pamokos tikslas	Suteikti mokiniams žinių apie elektroninio parašo, elektroninio spaudo ir elektroninės laiko žymos sąvokas, jų skirtumus bei naudojimo būdus. Aptarti kvalifikuoto ir nekvalifikuoto elektroninio parašo teisinę galią ir paskirtį, pabrėžiant jų svarbą dokumentų pasirašymui ir tapatybės patvirtinimui internetinėje erdvėje. Supažindinti mokinius su duomenų ir pranešimų šifravimu, bei šifravimo raktų rūšimis. Praktinėje dalyje mokiniai išbandys duomenų ir pranešimų šifravimą bei dešifravimą, naudodami „Kleopatros“ pranešimų šifravimo įrankį, kuris yra „Gpg4win“ programų paketo dalis. Supažindinti kaip pasirašytas dokumentas su elektroniniu parašu.
Įvadas (5 min.)	Pamoka pradedama mokytojui įjungus naršyklėje įrankį ir pasidalijus nuoroda („FigJam” lenta) su mokiniais. Mokiniai gali pasirinkti, kad mokytojo pelytė ir vaizdas būtų sekamas ir taip neatsilikti nuo mokamo turinio. Susitariama kokiomis komandomis dirbama ir užduotys vykdomos lentoje pagal mokytojos paruoštą medžiagą. Video medžiagą taip pat galima patalpinti „FigJam” lentoje. Pamokos mokymo metu mokytojas gali supažindinti su refleksijos priemonėmis jaustukais, štampais. Visi įrankiai yra interaktyvūs ir jais galima reflektuoti realiu laiku. Atliekant užduotis ar klausant mokytojo dėstomų minčių. **Priemonės:** „FigJam” lenta. „FigJam” yra nemokamas švietimo darbuotojams – jums reikia tik patvirtinti savo paskyrą, įsivesti mokyklos pavadinimą.
1 žingsnis: Vaizdo medžiagos peržiūra (17 min.)	Rekomenduojamos vaizdo medžiagos peržiūra (galima rasti „YouTube” nuorodose arba mokytojo pateiktą medžiagą). Visų pateiktų filmukų trukmė apie 17 minutes.
2 žingsnis: Demonstracija (5 min.)	Mokytojo demonstracija, kaip naudoti pasirašyti el. parašu dokumentą. Mokiniai patys atlieka šifravimo ir dešifravimo užduotis. Praktinis darbas
3 žingsnis: 10 min.	Praktinis darbas duomenų ir pranešimų šifravimą bei dešifravimą, naudodami „Kleopatros“ pranešimų šifravimo įrankį, kuris yra „Gpg4win“ programų paketo dalis.

5. žingsnis: Testas (8 min.)	Testas apie elektroninio parašo ir duomenų šifravimo sąvokas ir metodus.

2 priedas. Testas

Elektroninio parašo ir duomenų šifravimo sąvokas ir metodus

Vardas, pavardė	
Klasė	
Data	

Taškai: 10 (1 taškas už kiekvieną teisingai atsakytą klausimą).

1. Kas yra elektroninis parašas?
a) Skaitmeninis failas
b) Skaitmeninis autentifikavimo metodas
c) Duomenų apsaugos priemonė
d) Slaptažodis

2. Kuo skiriasi elektroninis parašas nuo tradicinio parašo?
a) Elektroninis parašas yra fiziškai parašytas
b) Elektroninis parašas yra naudojamas tik internete
c) Elektroninis parašas yra teisiškai lygiavertis tradiciniam parašui
d) Elektroninis parašas yra laikinas

3. Kokie yra pagrindiniai elektroninio parašo privalumai? (Pažymėkite visus tinkamus variantus)
a) Saugumas
b) Greitis
c) Popieriaus taupymas
d) Sunkumas naudoti

4. Kuo skiriasi kvalifikuotas elektroninis parašas nuo nekvalifikuoto?
a) Kvalifikuotas parašas turi teisinę galią.
b) Kvalifikuotas parašas naudojamas tik vyriausybinėse institucijose.
c) Nekvalifikuotas parašas yra saugesnis.
d) Kvalifikuotas parašas yra pigesnis, arba nemokamas.

5. Kas yra dokumentų šifravimas?
a) Dokumentų perkėlimas į debesiją
b) Dokumentų apsaugos priemonė, užtikrinanti, kad tik įgalioti asmenys galėtų juos perskaityti
c) Dokumentų ištrynimas po jų peržiūros
d) Dokumentų konvertavimas į kitą formatą.

6. Kodėl svarbu naudoti dokumentų šifravimą?
a) Kad būtų lengviau bendrinti dokumentus
b) Kad būtų išvengta duomenų nutekėjimo
c) Kad būtų galima naudoti senesnes technologijas

d) Kad būtų užtikrintas greitas duomenų perdavimas

7. Kokios yra būtinos sąlygos, kad elektroninis parašas būtų teisiškai galiojantis?
a) Elektroninis parašas turi būti susietas su patvirtintu sertifikatu, išduotu patikimo paslaugų teikėjo.
b) Elektroninis parašas turi būti atvaizduotas kaip paveikslėlis dokumento apačioje.
c) Elektroninis parašas turi būti naudojamas tik dokumentams, kuriuos siunčiate elektroniniu paštu.

8. Kas yra dviejų faktorių autentifikacija (2FA, kartais vadinama dviejų veiksnių autentifikacija arba dviguba autentifikacija)?
a) Saugumo procesas, kai vartotojo atpažinimui reikalingas daugiau nei vienas tapatybės nustatymo būdas.
b) Autentifikavimo metodas, kai vartotojas turi pateikti du skirtingus slaptažodžius.
c) Procesas, kai vartotojas turi prisijungti per dvi skirtingas interneto naršykles tuo pačiu metu.

9. Kas atsitinka, jei elektroninis parašas yra netinkamai naudojamas?
a) Dokumentas tampa negaliojantis
b) Dokumentas praranda teisinę galią
c) Dokumentas gali būti lengvai sugadintas
d) Dokumentas tampa nešifruotas

10. Kokie yra pagrindiniai kriterijai renkantis elektroninio parašo paslaugų teikėją? (Pažymėkite visus tinkamus variantus)
a) Saugumo lygis
B) Teisinis pripažinimas
d) Paslaugų teikėjo populiarumas

Šis testas padės įvertinti žinias apie elektroninį parašą ir dokumentų šifravimą bei jų praktinį naudojimą.

Šis testas padės mokiniams įtvirtinti žinias apie elektroninio parašo ir duomenų šifravimo sąvokas bei metodus. Kiekvienas teisingai atsakytas klausimas vertinamas 1 tašku, iš viso galima surinkti 10 taškų.

Atsakymai

1.			b.	6.	b
2.			c	7.	a
3.	a,	b,	c	8.	A
4.			a.	9.	b
5. b				10. a, b	

Informacija parengta pagal: www.esaugumas.lt. Svetainė, skirta teikti informaciją apie kibernetinį saugumą ir elektroninių paslaugų saugą. Ši svetainė skirta šviesti visuomenę apie saugų naudojimąsi internetu, asmens duomenų apsaugą, kibernetinių grėsmių atpažinimą ir vengimą. Joje taip pat pateikiami patarimai ir gairės tiek individualiems vartotojams, tiek organizacijoms, siekiančioms užtikrinti saugumą elektroninėje erdvėje.

Puslapyje galima rasti įvairių naudingų išteklių, naujienų apie kibernetinį saugumą, informacija apie asmens duomenų apsaugą, patarimai, kaip saugiai naudoti elektronines paslaugas, ir kitus aktualius klausimus, susijusius su e-saugumu.

3 priedas. Namų darbas.

Šifravimo sistemos sukūrimas šeimos

Šiuolaikiniame pasaulyje didėja sukčiavimo ir neteisėto asmens duomenų naudojimo rizika. Vienas iš naujausių sukčiavimo būdų yra balso klastojimas, kai sukčiai naudoja dirbtinio intelekto technologijas, kad imituotų šeimos nario balsą ir prašytų pagalbos ar pinigų. Todėl labai svarbu sukurti papildomas saugumo priemones, tokias kaip slaptažodis, kuris apsaugotų jūsų šeimą nuo tokių pavojų.

Ši užduotis skirta mokiniams, siekiant padėti jiems suprasti, kaip galima sukurti šeimos šifravimo sistemą naudojant slaptažodžius arba slaptus klausimus, kuriuos žino tik šeimos nariai.

Užduoties tikslai:

- Suprasti šiuolaikinius sukčiavimo būdus ir jų pavojus.
- Sukurti šeimos šifravimo sistemą, kuri padėtų apsaugoti nuo sukčiavimo.
- Praktiškai pritaikyti sukurtą šifravimo sistemą, naudojant slaptažodžius arba slaptus klausimus.

Pavyzdys:

Šeimos šifravimo sistema

- **Slaptieji klausimai:**
  Klausimas: Koks buvo jūsų pirmojo augintinio vardas?
  Atsakymas: Maxas
  Klausimas: Kur susipažino jūsų tėvai?
  Atsakymas: Kavinėje „Pasakėlė“
  Klausimas: Kokia buvo jūsų pirmoji šeimos kelionė?
  Atsakymas: Nida
- **Slaptažodžiai:**
  Slaptažodis 1: ŠeimosKodas2024!
  Slaptažodis 2: SaugiŠeima#1
  Slaptažodis 3: MūsųTurtas!

4 priedas.

Refleksija apie šifravimo sistemos kūrimą šeimoje

Parašykite trumpą refleksiją (150-200 žodžių), kaip sekėsi kurti šifravimo sistemą šeimoje. Atsakykite į šiuos klausimus:

1. Kokius įrankius ir metodus naudojote šifravimo ir dešifravimo procesui?
2. Kokie iššūkiai kilo atliekant užduotį?
3. Kaip šeimos nariai reagavo į šifravimo sistemą ir ar buvo lengva ją suprasti?
4. Ką sužinojote apie šifravimo ir dešifravimo procesus per šią veiklą?
5. Kaip manote, ar tokia sistema būtų naudinga jūsų šeimoje kasdienėms reikmėms? Kodėl?

Parengė Kotryna Tomkevičiūtė