# Slaptažodžiai

Dalyviai išmoks geriau apsaugoti savo internete esančią informaciją naudodami ir tvarkydami sudėtingus slaptažodžius. Dalyviai sužinos apie sudėtingo slaptažodžio kūrimo principus ir galimas slaptažodžių bendrinimo problemas. Jie taip pat sužinos, kaip saugoti savo slaptažodžius ir kokių veiksmų imtis siekiant išvengti neleistinos prieigos prie jų paskyrų.

## Medžiaga

Mokymasis apie su slaptažodžiais susijusią padalomąją medžiagą

# Slaptažodžio pagrindai

## 1 dalis

**Papasakokite mokiniams**

Dažnai daug negalvojame apie interneto svetainėse, programėlėse ir paslaugose naudojamus slaptažodžius. Tačiau jūsų slaptažodžių sudėtingumas lemia jūsų duomenų saugumo lygį.

**Kurso veikla**

Įtraukite dalyvius į diskusiją naudodami toliau nurodytus klausimus. Priminkite dalyviams, kad per šią ir visas kitas užduotis svarbu nebendrinti tikrųjų savo slaptažodžių.

**Paklauskite mokinių**

Kiek slaptažodžių turite?

> Ar kiekvienai el. pašto ir socialinių tinklų paskyrai naudojate skirtingus slaptažodžius?
>
> Ar jie visiškai skirtingi, ar tai vieno slaptažodžio variantai?

Jei turite daugiau nei vieną slaptažodį, kaip prisimenate, kuris slaptažodis skirtas kuriai paskyrai?

**Paklauskite mokinių**

Kaip dažnai esate pamiršę svarbų slaptažodį?

> Ką darėte, kai pamiršote savo slaptažodį?
>
> Ką darote, kad slaptažodžiai būtų lengvai įsimenami?

Ar turite slaptažodį, kurį naudojate kasdien?

Kas nutiktų, jei kas nors be jūsų žinios sužinotų jūsų slaptažodį?

> Ar tai priklausytų nuo to, kas jį sužinotų?

Kokią informaciją apie jus galėtų sužinoti kitas žmogus prisijungęs prie jūsų paskyros

naudodamas jūsų slaptažodį?

# 2 dalis

### Kurso veikla

Suskirstykite dalyvius poromis.

### Papasakokite mokiniams

Kartu su partneriu aptarkite, kas nutiktų, jei piktų ketinimų turintis žmogus sužinotų jūsų mėgstamiausio socialinio tinklo platformos slaptažodį?

### Kurso veikla

Skirkite dalyviams 5 minutes tai aptarti. Paprašykite dalyvių pasidalinti savo mintimis.

### Papasakokite mokiniams

Dabar su savo partneriu aptarkite, kas nutiktų, jei įsilaužėlis sužinotų jūsų tėvų / globėjų internetinės bankininkystės paskyros slaptažodį.

### Kurso veikla

Skirkite dalyviams 5 minutes tai aptarti. Tada paprašykite grupių pasidalinti savo aptarimu.

# 3 dalis

### Papasakokite mokiniams

Galbūt galvojate, kaip įsilaužėlis galėtų sužinoti privatų slaptažodį. Yra keletas būdų. Vienas iš jų – socialinis projektavimas arba žmogaus apgavimas siekiant iš jo išgauti slaptažodį. Įsilaužėlis tai gali padaryti atsiųsdamas el. laišką, kuris atrodo beveik taip pat, kaip jį būtų siuntusi platforma arba interneto svetainė, kurioje naudotojas turi paskyrą. El. laiške gali būti prašoma spustelėti nuorodą ir prisijungti su savo naudotojo vardu ir slaptažodžiu. Jums prisijungus įsilaužėlis sužino šią informaciją.

Įsilaužėliai kartais bando atspėti slaptažodžius naudodami dažnas frazes, pvz., „slaptažodis123“, „testas“, jūsų vardas arba pavardė.

Kitas būdas, kaip įsilaužėliai gali sužinoti privatų slaptažodį, yra naudojant vadinamą „brutalios jėgos“ ataką. „Brutalios jėgos“ ataka vykdoma įsilaužėliui daug kartų mėginant prisijungti prie jūsų paskyros naudojant įvairius slaptažodžius. Įsilaužėlis „brutalios jėgos“ ataką gali vykdyti savo rankomis, tačiau dažniausiai ji vykdoma paleidus kompiuterio programą, kuri labai greitai ir automatiškai bando visus

įmanomus slaptažodžių derinius. Pavyzdžiui, tikėtinų slaptažodžių sąrašą arba slaptažodžių rinkinį, kurį sudaro skirtingų raidžių ir skaičių deriniai, kol surandamas tinkamas slaptažodis.

Žinoma, kai kurios „brutalios jėgos“ atakos yra sudėtingesnės. Jei jūsų slaptažodis yra tikėtinų slaptažodžių sąraše, pvz., „fido123“ arba „slaptažodis“, kai kurios programos jį gali atspėti greičiau, nes iš pradžių bandomi šie variantai, o mažiau tikėtini ir atsitiktiniai slaptažodžiai bandomi vėliau. Ataka taip pat gali būti labiau įmantri, jei įsilaužėlis turi informacijos apie jus. Jei, pvz., įsilaužėlis žino, kad jūsų augintinio vardas yra Tobis, jis gali bandyti naudoti slaptažodį „Tobis“ su skirtingais skaičių deriniais pabaigoje (pvz., „Tobis629“, „Tobis3020“).

# Dizaino principai

## 1 dalis

### Paklauskite mokinių

Kas žino, ką reiškia naudoti „sudėtingą“ arba „sudėtingesnį“ slaptažodį? Kodėl tai yra gerai?

### Papasakokite mokiniams

Sudėtingas slaptažodis padeda apsaugoti jūsų informaciją. Sudėtingo slaptažodžio naudojimas negarantuoja, kad į jūsų paskyrą nebus įsilaužta, tačiau naudojant nesudėtingą slaptažodį kitiems žmonėms pasiekti jūsų informaciją yra daug lengviau.

## Slaptažodžių užduotis

### Paklauskite mokinių

Kokie yra nesudėtingų slaptažodžių pavyzdžiai?

1. Keletas pavyzdžių: „Slaptažodis“, „12345“, „Sveiki!“, gimimo data, slapyvardis.

Kodėl manote, kad šie slaptažodžiai yra nesudėtingi?

1. Juos lengvai gali atspėti kitas žmogus ir (arba) kompiuteris, vykdantis „brutalios jėgos“ ataką.

Kokiais būdais galima slaptažodį padaryti sudėtingesniu?

1. Įtraukiant skaičių, didžiųjų ir mažųjų raidžių, simbolių, renkantis ilgesnį slaptažodį bei vengiant dažnai vartojamų frazių ar atskirų žodžių.

### Kurso veikla

Dalyviams pateikus savo atsakymus, ant lentos užrašykite šias instrukcijas:

Įtraukite bent vieną skaičių.

Įtraukite bent vieną simbolį.

Įtraukite bent vieną didžiąją ir mažąją raidę.

Slaptažodžiai turi būti sudaryti bent iš 7 ženklų.

Slaptažodžiai turi būti lengvai įsimenami (nebent naudojama slaptažodžių tvarkyklė).

Slaptažodžių tvarkyklė – tai interneto svetainė / programėlė, kuri padeda naudotojams saugoti ir tvarkyti savo slaptažodžius.

Slaptažodžiai neturi būti sudaryti iš vieno dažnai vartojamo žodžio arba asmens informacijos (gimimo datos, tėvų vardai ir pan.).

Skirtingose interneto svetainėse turi būti naudojami skirtingi slaptažodžiai.

**Papasakokite mokiniams**

Yra du būdai sukurti sudėtingus slaptažodžius. Pirmasis yra vadovautis „slaptažodžio receptu“, kurio pavyzdys pateiktas lentoje. Vadovaujantis šiuo receptu į tekstinį / skaitinį slaptažodį skatinama įtraukti sunkiau atspėjamus elementus, todėl ir pats slaptažodis tampa sunkiau atspėjamas. Šio būdo trūkumas – tokie slaptažodžiai sunkiau įsimenami.

# Sudėtingi slaptažodžiai

**Papasakokite mokiniams**

Kitas sudėtingų slaptažodžių kūrimo būdas yra susijęs su slaptažodžio ilgiu. Kadangi slaptažodžio sudėtingumas susijęs su slaptažodžio ilgiu, naudojant keturių ar daugiau nesusijusių žodžių seką slaptažodžius yra daug sunkiau atspėti žmonėms ir vykdant „brutalios jėgos“ atakas. Vadovaujantis šiuo metodu slaptažodžiai yra lengviau įsimenami, palyginus su recepto metodu.

Taip pat galima naudoti šių metodų derinį, kai sugalvojama keturių ar daugiau nesusijusių žodžių seka ir įtraukiami simboliai ir skaičiai.

Šių skirtingų metodų tikslas yra toks pat: sukurti unikalius ir kitiems žmonėms sunkiai atspėjamus slaptažodžius.

**Papasakokite mokiniams**

Suskirstykite dalyvius poromis

Dirbdami porose pamėginkite sukurti sudėtingą slaptažodį vadovaudamiesi anksčiau ant lentos užrašytomis instrukcijomis. Atminkite, kad slaptažodį, kurį kompiuteriui atsitiktinai atspėti yra sudėtinga, vis tiek gali lengvai atspėti žmogus arba kompiuteris su dažniausiai naudojamų ilgų slaptažodžių sąrašu. Popierius, kuriame užrašytas jūsų slaptažodis nebus surinktas šios veiklos pabaigoje. Rekomenduojama šio

slaptažodžio nenaudoti vienai iš savo paskyrų, nes grupėje esantys žmonės jį žinos.

Skirkite dalyviams 5 minutes šiai užduočiai atlikti. Tada prieikite prie kiekvienos grupės ir paklauskite dalyvių, kokie jų manymu slaptažodžių pavyzdžiai yra sudėtingiausi. Paklauskite dalyvių, ar jie gali prisiminti sukurtus slaptažodžius tiesiogiai į juos nežiūrėdami.

Kai kurios interneto svetainės reikalauja, kad slaptažodžiai atitiktų keletą (arba visas) iš nurodytų sąlygų, o kitos netaiko šių apribojimų. Slaptažodžius sukurti taip pat galite naudodami atsitiktinę dažnai vartojamų žodžių seką.

**Kurso veikla**

Liepkite dalyviams tomis pačiomis poromis sukurti naujų slaptažodžių iš žodžių sekų. Praneškite, kad slaptažodį turi sudaryti bent keturi žodžiai, jog jis būtų saugus ir lengvai įsimenamas. Skirkite dalyviams 5 minutes šiai užduočiai atlikti. Tada prieikite prie kiekvienos grupės ir paprašykite dalyvių pateikti sugalvotus slaptažodžių pavyzdžius. Dar kartą priminkite dalyviams, kad po užsiėmimo popieriaus lapai surenkami nebus, o slaptažodžiai nebus naudojami dalyvių paskyrose.

**Papasakokite mokiniams**

Kai kuriose interneto svetainėse jūsų tapatybei patvirtinti naudojama sistema, vadinama keleto veiksnių (arba dviejų veiksnių) autentifikavimu. Šios interneto svetainės dažnai naudoja tekstinius pranešimus, programėlę arba el. paštą vienkartiniam kodui, kurį reikia įvesti kartu su slaptažodžiu, išsiųsti.

Šis metodas gali ženkliai padidinti jūsų paskyrų saugumą pridėdamas papildomą saugumo lygmenį, kurį apeiti yra daug sudėtingiau. Pavyzdžiui, norėdami prisijungti prie savo paskyros, turite žinoti savo slaptažodį ir turėti prieigą prie su paskyra susietos programėlės, įrenginio ar el. pašto adreso.

# Slaptažodžių saugojimas

## Pirma dalis

**Papasakokite mokiniams**

Net jei ir sukursite kompiuteriui arba žmogui sunkiai atspėjamą slaptažodį, jis gali būti pažeidžiamas kitu požiūriu.

**Paklauskite mokinių**

Kokiais kitais būdais slaptažodis gali būti lengvai pažeidžiamas?

1. Kai kurie pavyzdžiai: to paties slaptažodžio naudojimas keliose paskyrose, slaptažodžio su asmens informacija naudojimas, to paties slaptažodžio naudojimas daugelį metų, slaptažodžio pamiršimas.

Kaip manote, kaip dažnai reikėtų keisti slaptažodžius?

**Papasakokite mokiniams**

Net ir geri slaptažodžiai gali būti pažeidžiami arba pavagiami, tačiau yra būdų apsisaugoti. Jei interneto svetainėje, kurioje turite paskyrą, pažeistas duomenų saugumas, būtinai pakeiskite savo slaptažodį toje interneto svetainėje ir visose kitose interneto svetainėse, kuriose naudojate panašius slaptažodžius.

Prisiminti daug ir sudėtingų slaptažodžių gali būti sudėtinga.

**Paklauskite mokinių**

Ar jums atrodo, kad užsirašyti savo slaptažodžius popieriaus lape arba dokumento faile kompiuteryje yra gera mintis? Kodėl arba kodėl ne?

**Kurso veikla**

Nurodykite galimas priežastis, pvz., kitas žmogus gali surasti popieriaus lapą arba pastebėti failą kompiuteryje. Paaiškinkite, kad vienas sprendimo būdas yra naudoti slaptažodžių tvarkyklę – programą, kuri padeda naudotojams saugoti ir tvarkyti savo slaptažodžius.

## Antra dalis

**Papasakokite mokiniams**

Kasdien naudojame daug skirtingų paskyrų įvairiose interneto svetainėse. Kiekvieną

kartą prisijungti prie kiekvienos interneto svetainės ir nuo jų atsijungti gali būti sudėtinga.

**Paklauskite mokinių**

Ar kada nors naudojote „slaptažodžio įrašymo“ funkciją savo naršyklėje norėdami įrašyti interneto svetainės slaptažodį? Kodėl arba kodėl ne?

Ar suprantate, kaip interneto svetainė prisimena, kas jūs esate?

1. Paprašykite paaiškinimų. Tada paaiškinkite, kad interneto svetainės prisimena jūsų prisijungimą saugodamos slapuką. Slapukai yra maži jūsų kompiuteryje saugomi failai, padedantys interneto svetainei žinoti, kas jūs ir jūsų kompiuteris esate jums kitą kartą ten apsilankius ir iš naujo neprisijungus. Tačiau slapukai taip pat gali būti naudojami norint sekti jūsų naršymą skirtingose interneto svetainėse. Tai vienas būdas tikslinei reklamai teikti.

Ar galima įrašyti slaptažodį, jei tai jūsų kompiuteris?

**Paklauskite mokinių**

Ar jūsų kompiuteryje yra prisijungimo slaptažodis?

Kas nutiks bendrinant kompiuterį su kitais žmonėmis?

1. Tokiu atveju, net jei slaptažodžio eilutėje esantis jūsų slaptažodis užmaskuotas juodais taškais arba žvaigždutėmis, kiti jūsų kompiuteriu besinaudojantys žmonės gali išsiaiškinti jūsų slaptažodį. Nors ir ekrane nematote paties slaptažodžio, tai dar nereiškia, kad jis niekur nėra saugomas.

**Paklauskite mokinių**

Ar išvis yra atvejų, kai galima bendrinti slaptažodį? Kada? Kodėl?

1. Kai kuriais atvejai tai gali būti tėvai, norintys žinoti savo vaikų slaptažodžius, arba tokių paslaugų kaip „Netflix“ bendra / šeimos paskyra.

Ar bendrinate savo slaptažodžius su kitais žmonėmis? Jei taip, tai su kuo / kodėl?

Jei artimas draugas jums pasakytų „jei aš tau rūpiu“, ar tai motyvuotų bendrinti savo slaptažodį su juo? Kodėl arba kodėl ne?

**Papasakokite mokiniams**

Galite nuspręsti bendrinti savo slaptažodį su sau svarbiu žmogumi, tačiau tai, kad šis žmogus jums rūpi, dar nereiškia, kad jis nusipelno turėti visišką prieigą prie jūsų interneto paskyrų.

Prieš bendrindami gerai pagalvokite apie savo santykius su konkrečiu žmogumi, įskaitant galimus šių santykių pokyčius laikui bėgant. Pavyzdžiui, bendrinimas su tėvais / globėjais yra visiškai kitoks pasirinkimas, nei bendrinimas su geriausiu draugu.

**Paklauskite mokinių**

Kas jums gali nutikti, jei bendrinsite slaptažodį?

1. Kitas žmogus gali įsilaužti į jūsų banko paskyras, apsimesti jumis internete arba sužinoti jūsų paslaptis.

Jei bendrintumėte paskyros slaptažodį, ar šią paskyrą naudotumėte kitaip?

**Paklauskite mokinių**

Ar yra dalykų, kurių nežiūrėtumėte „Netflix“ arba nerašytumėte el. laiškuose, jei kitas žmogus galėtų matyti, ką darote?

**Kurso veikla**

Dalyviai turėtų išreikšti savo pastebėjimus, susijusius su bendrintos paskyros naudojimu. Jie turėtų įvertinti, kad jų veikla internete yra matoma kitiems paskyros naudotojams.

**Paklauskite mokinių**

Jei jūsų paskyra yra virtualus jūsų atspindys, pvz., socialinio tinklo profilis, ar galima leisti kitiems žmonėms naudotis jūsų paskyra?

**Kurso veikla**

Aptarkite kito žmogaus apsimetimo jumis ir pranešimų jūsų draugams siuntimo galimybę.

**Paklauskite mokinių**

Ar leidžiate kuriam nors iš įrenginių saugoti jūsų slaptažodžius? Kodėl arba kodėl ne? Ar tai reiškia, kad saugoti slaptažodžius savo asmeniniame telefone arba kompiuteryje yra saugu? Kas nutiks, jei paskolinsite draugui savo telefoną arba kompiuterį?

Ar yra įrenginių, kuriuos bendrinate su kitais žmonėmis, pvz., šeimos nariais ar draugais? Ar bendrinate paskyrą šiame įrenginyje, ar kiekvienas žmogus turi savo paskyrą?

Ar tenka naudoti „viešus“ įrenginius, pvz., bibliotekoje, mokykloje ar kitoje vietoje? Ar su šiuo įrenginiu elgiatės taip pat, kaip ir su visais kitais?

# Trečia dalis.

### Kurso veikla

Suskirstykite dalyvius poromis.

### Papasakokite mokiniams

Porose aptarkite, ar kada nors esate prisijungę prie kompiuterio mokykloje, bibliotekoje ar kitoje visuomeninėje įstaigoje. Taip pat, ar matėte, kad kitas žmogus liktų prisijungęs prie savo socialinio tinklo arba el. pašto paskyros. Paprašykite jų apsvarstyti, ar jie naršytų paskyrą arba atliktų kitus veiksmus.

### Kurso veikla

Skirkite dalyviams 5 minutes tai aptarti, tada paprašykite pasidalinti savo mintimis. Įtraukite grupę į diskusiją apie tokį neleistiną naudojimą.

# Neleistina paskyros prieiga

## Pirma dalis

### Kurso veikla

Atkreipkite dėmesį: dalis šios veiklos turinio aptarta „1 veikloje: Slaptažodžio pagrindai“. Galite nuspręsti, ar norite vėl peržiūrėti šią medžiagą, ar ją praleisti.

### Papasakokite mokiniams

Kiti žmonės gali pasiekti jūsų paskyrą net nežinodami ir atsitiktinai neatspėdami jūsų slaptažodžio. Jei kitas žmogus žino pakankamai asmeninės informacijos apie jus, jis gali bandyti apgalvotai atspėti jūsų slaptažodį arba gali įtikinti įmonėje dirbantį asmenį perduoti jūsų informaciją. Kadangi norint įsilaužti į paskyrą nenaudojamos technologijos, šis atakos būdas vadinamas socialiniu įsilaužimu arba socialiniu projektavimu.

### Paklauskite mokinių

Pakelkite ranką, jei kada nors pamiršote prisijungimą prie interneto svetainės.

Kas atsitinka spustelėjus „Pamiršau slaptažodį“?

1. Interneto svetainėje įprastai prašoma atsakymų į saugos klausimus arba bandoma susisiekti su jumis telefono numeriu arba el. paštu.

Kokie yra interneto svetainių užduodami saugos klausimai?

1. Paaiškinkite, kaip į kai kuriuos klausimus galėtų atsakyti (arba atspėti atsakymus) draugai arba pažįstami. Klausimų pavyzdžiai: augintinio vardas, gimtinė, motinos mergautinė pavardė, mėgstamiausio mokytojo vardas, geriausio draugo vardas, mėgstamiausios sporto komandos pavadinimas.

Kas dar galėtų žinoti šią informaciją apie jus?

Kaip interneto svetainė susisiekia su jumis jums pamiršus slaptažodį?

Kas dar galėtų turėti prieigą prie jūsų susisiekimo taškų?

### Paklauskite mokinių

Kaip nepažįstamas žmogus galėtų sužinoti asmeninę informaciją, susijusią su jūsų atsakymais į saugos klausimus ?

1. Socialinių tinklų įrašai, internetinės viešos informacijos paieškos, daugybiniai spėjimai, susisiekimas su jūsų draugais ir pan.

Kokie yra socialinių tinklų įrašų su asmens informacija pavyzdžiai?

1. Pavyzdžiui, jūsų katės nuotrauka „Instagram“ ir antraštėje nurodytas jos vardas, nuotrauka su pažymėta vieta, vieši gimtadienio įrašai.

Kaip galima naudoti „Google“ norint daugiau sužinoti apie kitus žmones ir įsilaužti į jų paskyrą?

1. Jei paieškos sistemoje pateikiama žmogaus devintos klasės nuotrauka mokyklos internetiniame laikraštyje, galite sužinoti to žmogaus mokytojo vardą.

## Antra dalis

**Papasakokite mokiniams**

Informacijos skelbimas, kurioje pateikiami atsakymai į jūsų saugos klausimus, gali būti labai nesaugus. Įsitikinkite, kad pasirinkote tokius saugos klausimus, kurių atsakymus žinote tik jūs. Taip pat galite sugalvoti atsakymus į saugos klausimus, jei juos įrašysite į slaptažodžių tvarkyklę arba juos lengva atsiminti.

Interneto svetainės gali susisiekti su naudotojais naudodamos su jų paskyra susietą telefono numerį arba el. paštą. Naudotojui pamiršus slaptažodį interneto svetainės dažnai suteikia laikiną slaptažodį arba saitą, kurį naudodamas naudotojas gali atkurti savo slaptažodį.

**Paklauskite mokinių**

Ar tai yra saugus būdas užtikrinti, kad naujo slaptažodžio užklausą pateikęs asmuo yra naudotojas?

Kas nutiks bendrinant su paskyra susietą el. pašto adresą?

1. Slaptažodžio atkūrimo nuorodos metodas dažniausiai yra saugus, tačiau bendrinant paskyrą ar slaptažodį su kitu žmogumi, jūs tampate pažeidžiamas.

**Papasakokite mokiniams**

Socialinį įsilaužimą kiti žmonės gali atlikti tiesiogiai su jumis susisiekdami ir mėgindami jus apgauti, kad suteiktumėte informaciją apie save. Kartais žmonės siunčia el. laiškus apsimesdami kitais asmenimis (pvz., daugu, šeimos nariu ar

banko darbuotoju) ir prašo bendrinti svarbią informaciją (pvz., gimimo datą), taip siekiant patvirtinti jūsų tapatybę. Tai gali būti atliekama subtiliau, pvz., kitam asmeniui įsilaužus į jūsų draugo paskyrą ir pateikus jums (ir galimai daugeliui kitų žmonių) klausimų apie jūsų gimtadienį arba gimtinę. Jei iš draugų gaunate žinučių, kurios atrodo keistos, pamėginkite iš pradžių susisiekti su draugu (ne socialinio tinklo platformoje) ir išsiaiškinkite, ar draugas tikrai siunčia šį turinį.

Atakos, kai naudojami į tikrus panašūs el. laiškai arba interneto svetainės, vadinamos duomenų vagyste, ir jos gali prisidėti prie tapatybės vagystės. Pavyzdžiui, tapatybės vagis gali jūsų vardu gauti kredito korteles ir jomis naudotis. Dėl to jums ateityje gali kilti sunkumų norint gauti kredito kortelę.

Įvykdęs duomenų vagystę, vagis gali apsimesti jumis ir pasiekti daugiau informacijos – peržiūrėti jūsų el. laiškus, siųsti pranešimus jūsų draugams apsimesdamas jumis arba pavogti jūsų pinigus. Taip pat vagis gali užblokuoti jūsų prieigą prie paskyros sukurdamas naują jums nežinomą slaptažodį.

# Užduotis

## Padalomoji medžiaga

### Užduotis

Paprašykite dalyvių atsakyti į toliau pateiktus klausimus ir įtraukite jų atsakymus teksto arba iliustracijų forma į mokymosi apie slaptažodžius padalomąją medžiagą.

1. Kokias tris šio seanso įžvalgas taikysite kitą kartą kurdami slaptažodį?

2. Nurodykite vieną pavyzdį, kai jums atrodo priimtina bendrinti savo slaptažodį su kitu žmogumi.

3. Kokias tris strategijas galite naudoti norėdami saugiai bendrinti savo slaptažodį su kitu žmogumi?

4. Nurodykite tris pavyzdžius, kas gali nutikti blogo slaptažodžiui patekus į netinkamas rankas.