«ԵՐԵՎԱՆԻ ԼԵՈՅԻ ԱՆՎԱՆ Հ.65 ԱՎԱԳ ԴՊՐՈՑ» ՊՈԱԿ

ՀԵՐԹԱԿԱՆ ԱՏԵՍՏԱՎՈՐՄԱՆ ԵՆԹԱԿԱ ՈՒՍՈՒՑԻՉՆԵՐԻ

ՎԵՐԱՊԱՏՐԱՍՏՄԱՆ ԴԱՍԸՆԹԱՑԻ

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ

ԱՌԱՐԿԱ՝ ԻՆՖՈՐՄԱՏԻԿԱ

ՄԱՍՆԱԿԻՑ՝ Վ.ՍԱՐԳՍՅԱՆԻ ԱՆՎԱՆ N1 ՄԻՋՆ. ԴՊՐՈՑԻ ՈՒՍՈՒՑԻՉ ԱՐԹՈՒՐ ՄԱՐԳԱՐՅԱՆ

ՂԵԿԱՎԱՐ՝ ՎԱՐԴԱՆՈՒՇ ՀՈՎՀԱՆՆԻՍՅԱՆ

ԹԵՄԱ՝ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՆՈՆՆԵՐԻ ԿԻՐԱՌՈՒԹՅՈՒՆՆ ՈՒ ՊԱՀՊԱՆՈՒՄԸ ԴՊՐՈՑԱՀԱՍԱԿ ԵՐԵԽԱՆԵՐԻ ԿՈՂՄԻՑ

ԵՐԵՎԱՆ 2022Թ.

Բովանդակություն

Նախաբան

Ներկայիս հասարակությունների կյանքում մեծ դեր են զբաղեցնում տեղեկատվական տեխնոլոգիաները, համացանցը: Դժվար է պատկերացնել ժամանակակից կյանքը առանց ինտերնետի և համակրագիչների, իսկ հասարակական գործունեության ոլորտների մեծ մասը այժմ անքակտելիորեն կապված են կիբեռտարածքի, տեղեկատվական տեխնոլոգիաների հետ: Սակայն միևնույն ժամանակ տեղեկատվական տեխնոլոգիաների և համացանացի արագ և ակտիվ զարգացումը իր հետ բերում է որոշակի ռիսկեր, որոնք առնչվում են ընդհուպ հասարակության և պետության անվտանգությանը: Տեղեկատվական անվտանգությունը դարձել է պետության անվտանգային համակարգի ամենակարևոր բաղկացուցիչներից մեկը և ժամանակակից հասարակությունների անվտանգային խնդիրներից մեկը: 2020թ. արցախյան պատերազմը առավել արտահայտիչ դարձրեց Հայաստանում կիբեռանվտանգության մակարդակի բարձրացման անհրաժեշտությունը:

Հիմնվելով վերոնշյալի վրա կարող ենք նշել, որ առավել արդիական է դառնում դպրոցահասակ երեխաների մեդիագրագիտության բարձրացումը, կիբեռանվտանգության կանոների իմացությունն ու տիրապետումը, տեղեկատվական տեխնոլոգիաների առավելությունների և թերությունների, հնարավորությունների և սպառնալիքների մասին տեղեկացվածության և գիտելիքների մակարդակի բարձրացումը:

Նպատակը: Հետազոտական աշխատանքի նպատակն է ուսումնասիրել կիբեռանվտանգության դերը պետության և հասարակության անվտանգային համակարգում, ինչպես նաև կիբեռանվտանգության կանոնների կիրառությունն ու պահպանումը դպրոցահասակ երեխաների կողմից:

Խնդիրները: Հետազոտական աշխատանքի նպատակին հասնելու համար դրվել են հետևյալ խնդիրները.

- Ուսումնասիրել կիբեռանվտանգության էությունը:
- Ներկայացնել դեռահասների կողմից կիբեռանվտանգության պահպանման կանոնները:
- Ուսումնասիրել դպրոցահասակների իրավունքները առցանց տիրույթում:

Գլուխ 1.Կիբեռանվտանգություն

21-րդ դարում համացանցը ժամանակակից մարդու համար հոսանքի և ջրի պես կարևոր է: Նույնը կարելի է ասել պետությունների մասին: Հայաստանում այժմ մշակվում է կիբեռանվտանգության ռազմավարություն, որը համակցել է տեղեկատվական անվտանգությունը կիբեռանվտանգության հետ: Սակայն կարծում

եմ, որ սրանք պետք է միմյանցից տարանջատել: Եթե կիբեռանվտանգություն ասելով ընկալում ենք այդ համացանցերը՝ տեղեկատվական տեխնոլոգիաները, ապա տեղեկատվական անվտանգության մասին խոսելիս պետք է կարևորենք ինֆորմացիան: Մարդիկ կարծում են, որ իրենք չունեն էական տեղեկատվություն, որպեսզի հարձակման ենթարկվեն, սակայն դա այդպես չէ: Բոլորս կարիք ունենք պաշտպանվելու ***կիբեռհարձակումներից:***

Եթե հարձակումները պետությունների կողմից ֆինանսավորվող հարձակումներ են, ապա սա վերածվում է միջազգային դիտարկման և անվտանգության խնդրի: Եթե հարձակումը խմբային է, այն դիտարկվում է կիբեռհարձակումների տիրույթում: Մենք շատ անելիքներ ունենք այս ոլորտում ինքնակրթության և կրթության հետ կապված: Եթե մենք ճիշտ տեղեկացված լինենք, մենք կարող ենք շահել, սակայն հակառակ պարագայում կարող ենք լուրջ խնդիրների առաջ կանգնել: Քանի որ այս ոլորտը նոր է, յուրաքանչյուր պետություն յուրովի է մոտենում այս հարցին: Որոշ պետություններ այս հարցին շատ լուրջ են մոտենում, սակայն որոշ պետություններ չեն կարծում, որ սա այնքան լուրջ ոլորտ է, որտեղ պետք է ազգային անվտանգության մեխանիզմներ կիրառվեն:

Հայաստանում կիբերանվտանգության ապահովման համակարգը բավարար զարգացած չէ: Ոլորտում բացակայում են դրա համար արդյունավետ իրավական կարգավորումները: Երկրի օրենսդրությամբ կիբերանվտանգությունը չի դիտարկվում որպես կարգավորման առանձին համակարգ: Այն ավելի շատ համարվում է տեղեկատվական անվտանգության բաղկացուցիչ մաս: Ոլորտի չհամակարգված

լինելու պատճառով է նաև, որ կիբերհարձակումների ենթարկված երկրների շարքում Հայաստանը 14-րդ տեղում է:

Հայաստանում կիբերանվտանգության կարևորությունը թե՛ պետության, և թե՛ հասարակության կողմից, կարծես, գիտակցված չէ այնպես, ինչպես զարգացած երկրներում: Կիբերանվտանգության ապահովման պետական քաղաքականությունը չի ենթադրում կիբերանվտանգության ապահովում երկրի այնպիսի ենթակառուցվածքների համար, ինչպիսիք էներգետիկայի, խմելու ջրի, օդանավակայանի կամ ատոմային արդյունաբերության համակարգերն են: Այդ ենթակառուցվածքներում ընդհանուր աուդիտի բացակայության պատճառով հնարավոր չէ պարզել, թե ինչպիսի համակարգերով են աշխատում այդ ծառայությունները, և ինչպիսին է պաշտպանվածության աստիճանը կիբերսպառնալիքների նկատմամբ:

Հայաստանում կիբերանվտանգության ապահովման պատասխանատվությունը դրված է Ոստիկանության, Ազգային անվտանգության ծառայության (ԱԱԾ) և Պաշտպանության նախարարության վրա: Սակայն այս գերատեսչությունները հիմնականում կենտրոնացած են պետական համակարգի պաշտպանության վրա: Մինչդեռ կիբերհարձակումների ժամանակագրությունը ցույց է տալիս, որ միշտ չէ, որ ամենավտանգվածը պետական կայքերն են:

Հասարակության գիտակցության մակարդակն այս հարցում պատկերացնելու համար բավարար է նշել միայն այն, որ Հայաստանում քաղաքացիների կողմից օգտագործվող համակարգիչների ծրագրային ապահովման 86%-ն արտոնագրված չէ: Թեև համակարգչային տեխնոլոգիաներն ակտիվ տարածում են գտնում Հայաստանում:

Շուրջ տասը տարի առաջ Հայաստանում միջին ընտանիքում առկա էր մեկ համակարգիչ, որից օգտվում էին ընտանիքի բոլոր անդամները, որոշ դեպքերում նույնիսկ հարևանները: Այդ համակարգիչներից շատ քիչ տոկոսն էր, որ ուներ ինտերնետ հասանելիություն: Մինչդեռ վերջին տարիներին Հայաստանում մեկ անձին բաժին է ընկնում մի քանի թվային հաղորդակցության սարք՝ համակարգիչ, պլանշետ կամ բջջային հեռախոս: Թե՛ քաղաքային, թե՛ գյուղական համայնքներում համակարգիչները հավասարապես ներթափանցել են առօրյա կյանք: Համաշխարհային բանկի տվյալների համաձայն, 2015թ. Հայաստանում համացանց

օգտագործողների թիվը կազմել է բնակչության շուրջ 58%-ը: Մեկ այլ աղբյուրի համաձայն, 2016թ. այդ ցուցանիշը հասել է 70%-ի: «Ֆեյսբուք» մուտք գործած հայաստանցի օգտատերերի թիվն ամսական կտրվածքով կազմում է 1 մլն, գրեթե նույնքան է նաև ռուսական «Օդնոկլասնիկի» կայքից օգտվողների թիվը: Սրանք այն երկու հիմնական սոցիալական կայքերն են, որոնցից օգտվում են Հայաստանի օգտատերերը: Երիտասարդ սերնդի մոտ նոր թափ է առնում նաև «Ինստագրամը», որտեղ օգտատերերի թիվն արդեն 300 հազարի է հասնում՝ ամսական 15-20% աճի միտումով: Մեսինջերներից ամենակիրառելին դարձել է «Վայբերը»:

Հայաստանյան օգտատերերի թվի աճին համընթաց աճում է նաև կիբերհանցագործությունների քանակը: Ըստ «Կասպերսկու լաբորատորիայի» տվյալների, 2016թ. Հայաստանի յուրաքանչյուր 3-րդ օգտատեր բախվել է կիբերսպառնալիքի, այն էլ տարեկան միջինը 82 անգամ:

Այս առումով Հայաստանը փաստացի գտնվում է խոցելի պետությունների ցանկում: Խոցելիությունը պայմանավորված է նաև նրանով, որ կապի մալուխները երկու ելք ունեն, որոնք ճանապարհին անցնում են նաև Հայաստանի համար ոչ բարեկամ պետությունների՝ Ադրբեջանի և Թուրքիայի տարածքներով: Իսկ կիբերանվտանգության ապահովման համընդհանուր քաղաքականության բացակայությունը կարող է ավելի խոցելի դարձնել երկրի ցանցային և տեղեկատվական համակարգերը:

Գլուխ 2. Կիբեռանվտանգության կանոններ դեռահասների համար

Ներկա ինտերնետային սերնդի դաստիարակությունը մեզ նոր մարտահրավերներ է

նետել: Երեխաները նոր տեխնոլոգիաների մասին ավելին գիտեն, քան իրենց ծնողները, ուստի զարմանալի չէ, որ ծնողները հաճախ ոչ շահեկան վիճակում են երեխաների համեմատ:

Որքան որ պահանջված է համակարգչի դերը մեր առօրյայում, այնքան վտանգները շատ են, ուստի շատ կարևոր է ծնողների ներգրավումը երեխաների համացանցային կյանքին:

Երեխաները կարող են շատ հմտորեն տիրապետել համակարգչին, սակայն նրանք մեծահասակների կարիքն ունեն՝ ճիշտ կողմնորոշվելու, ինֆորմացիայի խառնաշփոթում հնարավորինս չսխալվելու և ցանցային բարեհաջող շփումներ ունենալու համար:

Այս հսկայական սարդոստայնում չխճճվելու, անձնական տվյալները անվտանգ պահպանելու համար՝ հարկավոր է հետևել որոշակի կանոնների.

1. Թարմացրու՛ համակարգչի կամ հեռախոսի ծրագրերդ՝ ներբեռնելով համապատասխան ծրագրեր կամ ակտիվացնելով ավտոմատ թարմացման գործառույթը. սա արվում է քո անվտանգության համար:

2. Վիրուսներից մաքրի՛ր հեռախոսդ կամ համակարգիչդ, եթե չգիտես ինչպես, քեզ կօգնեն համակարգչային դասընթացի ուսուցիչներդ կամ մասնագետները:

3. Խաղեր խաղալիս կամ որևէ կայքում գրանցվելիս՝ փորձի՛ր չհրապարակել անունդ, ազգանունդ, տան, դպրոցի հասցեդ, հեռախոսի համարդ: Համացանցը լի է չար ու նենգ մարդկանցով, հաքերներով, որոնք, քո տվյալները օգտագործելով, կարող են վնասել քեզ:

4. Համացանցում ընկերացի՛ր միայն այն մարդկանց հետ, ում ճանաչում ես իրական կյանքում, գուցե կեղծ էջերով փորձում են գողանալ քո անձնական տվյալները:

5.Անձնական տվյալներ մի՛ հրապարակիր համացանցում և մի՛ կիսվիր անծանոթների հետ, անգամ եթե ներկայանան որպես բարեկամ կամ ծանոթ։

6. Քեզ համար սահմանի՛ր գաղտնաբառեր, որոնք դու հեշտ կհիշես, բայց միևնույն ժամանակ դրանք անհասկանալի կլինեն անծանոթներին։ Ոչ մեկին մի՛ ասա գաղտնաբառերդ, դրանք քո ապահովության բանալիներն են։ Քո անձնական տվյալներն ու տեղեկատվությունը կարևոր ու արժեքավոր են։

7.Անհայտ հասցեներից, եթե հողումներ ես ստանում մի՛ տարածիր, անգամ եթե այն քեզ փող, հաջողություն կամ երջանկություն է խոստանում, գուցե դա նպատակ ունի գողանալու քո անձնական էջի տվյալները և քեզ վնասելու։

8. Զգույշ եղի՛ր անհայտ թեստեր կատարելուց, որքան էլ, որ դրանք գրավիչ ու հետաքրքիր լինեն, այդ էջեր մտնելով՝ դու կարող ես վտանգել քո անձնական տվյալները, որոնք կհայտնվեն անծանոթ մարդկանց մոտ և նրանք էլ կեղծ էջեր կբացեն քո նկարներով և քո տվյալներով։

9. Օգտվի՛ր անվտանգ կայքերից. երբ մուտք ես գործում որևէ էջ, ուշադիր եղի՛ր հասցեի առաջին հատվածին, այն պետք է սկսի այսպես՝ https:// կամ shtpp://, ահա այս դեպքում էջն անվտանգ է։

10. Համացանցից որևէ բան ներբեռնելուց կամ նյութերով կիսվելուց առաջ մտածի՛ր դրանց անհրաժեշտության և անվտանգության մասին։ Համացանցում ամեն ինչ մնում է հավերժ, դու կարող ես ինչ-որ բան ջնջել, բայց այլոց էջերում դրանք կպահպանվեն։

ԿԻԲԵՌՀԵՏԱՊՆԴՈՒՄՆԵՐ

Համացանցում մեկը մյուսին ծաղրելը, վիրավորելը, նեղացնելը կոչվում են կիբեռհետապնդումներ։

Ինչպես կյանքում, այնպես էլ համացանցում անհրաժեշտ է հարգել միմյանց, հետևել քաղաքավարության կանոններին.

• Լինել քաղաքավարի

• Լինել անկեղծ

• Չնեղացնել, չծաղրել, չվիրավորել ոչ մեկի

• Մարդկանց հետ վարվել այնպես, ինչպես, որ կուզենայիր քեզ հետ վարվեին

Եթե քեզ կամ քո ընկերներին չար, սպառնացող կամ անհարմար բովանդակության նամակներ են ուղարկում,վախեցնում, ապա կատարի՛ր հետևյալը.

• Պատմի՛ր ծնողներիդ կամ ուսուցիչներիդ

• Պահապանի՛ր սպառնալիքները, հետագայում ապացույցներ ունենալու համար

• Ապաակտիվացրո՛ւ կամ փակի՛ր տվյալ սպառնացողի հետ հաղորդակցման աղբյուրը

• Հիշի՛ր, որ անհրաժեշտության դեպքում կարող ես դիմել ոստիկանություն։

Չնայած բոլոր մարտահրավերներին՝ համացանցը անսպառ, օգտակար և անհրաժեշտ գիտելիքի հսկայական աղբյուր է, սակայն ճիշտ օգտվելու համար անհրաժեշտ է պահպանել կանոնները.

• Սովորի՛ր ճիշտ ու անվտանգ օգտվել համացանցից. ծնողներիդ ու ուսուցիչներիդ հետ համատեղ սահմանի՛ր անվտանգության կանոնները։

• Ընկերներիդ, ուսուցիչներիդ, ծնողներիդ հետ կարելի է մտածել և հետաքրքիր նախագծեր իրականացնել։

• Պետք է բարի և հանրության համար պիտանի նյութերով լցնել համացանցը։

Գլուխ 3. Ձեր իրավունքները առցանց

- Դուք ունեք իրավունքներ, և այլ մարդիկ պետք է հարգեն դրանք:
- Դուք երբեք չպետք է հանդուրժեք այլ մարդկանց կողմից հետապնդումները կամ ահաբեկումները: Իրական կյանքի օրենքները գործում են նաև առցանց միջավայրում:
- Դուք իրավունք ունեք օգտագործելու ***<u>ժամանակակից տեխնոլոգիաներ</u>*** զարգացնել ձեր անհատականությունը և ընդլայնել ձեր հնարավորությունները:
- Դուք իրավունք ունեք պաշտպանելու ձեր ***<u>անձնական տվյալները</u>...***
- Դուք իրավունք ունեք օգտվելու տեղեկատվությունից և ծառայություններից, որոնք համապատասխանում են ձեր տարիքին և անձնական ցանկություններին:
- Դուք իրավունք ունեք ազատ արտահայտվելու և ինքներդ ձեզ հարգելու իրավունք, և միևնույն ժամանակ միշտ պետք է հարգեք ուրիշներին:
- Դուք կարող եք ազատորեն քննարկել և քննադատել այն ամենը, ինչ հրապարակված կամ հասանելի է համացանցում:
- Դուք իրավունք ունեք ***ՈՉ*** ասել մեկին, ով առցանց միջավայրում ձեզանից մի բան է խնդրում, որը ձեզ անհարմար է: Սոցիալական ցանցերից և առցանց խաղերից օգտվելու խորհուրդներ Սահմանեք ձեր սեփական սահմանները Օգտվելով սոցիալական ցանցերից կամ ցանկացած այլ առցանց ծառայություններից՝ հոգ տանեք ձեր և ձեր ընտանիքի և ընկերների գաղտնիության մասին: Եթե դուք գրանցվել եք սոցիալական ցանցում, օգտագործեք ձեր գաղտնիության կարգավորումները ձեր առցանց պրոֆիլը պաշտպանելու համար, որպեսզի միայն ձեր ընկերները կարողանան դիտել այն: Խնդրեք ձեր ծնողներին օգնել կարգավորումների հարցում, եթե դժվարանում եք: Այս կանոնը շատ կարևոր է. Ձեր անձնական տվյալները գաղտնի պահեք, հատկապես մեծահասակների սոցիալական ցանցերում շփվելիս: Օգտագործեք ձեր մականունը ձեր իսկական անվան փոխարեն:

Հիշե՛լ. Դա կարևոր է: Անտեսեք այլ օգտատերերի վատ պահվածքը, հեռացեք տհաճ խոսակցություններից կամ ոչ պատշաճ բովանդակությամբ կայքերից: Ինչպես իրական կյանքում, կան մարդիկ, ովքեր տարբեր պատճառներով իրենց ագրեսիվ, վիրավորական կամ սադրիչ են պահում ուրիշների նկատմամբ, կամ ովքեր ցանկանում են չարամիտ բովանդակություն տարածել: Սովորաբար լավագույնն է

անտեսել, ապա արգելափակել այդպիսի օգտվողներին: Մի հրապարակեք այն, ինչը չէիք ցանկանա, որ ուրիշներն իմանային, որը երբեք նրանց անձամբ չեք ասի: Հարգեք այլ մարդկանց բովանդակությունը, որը դուք հրապարակում եք կամ կիսում:

Այս հսկայական սարդոստայնում չխճճվելու, անձնական տվյալները անվտանգ պահպանելու համար՝ հարկավոր է հետևել որոշակի կանոնների.

- Թարմացրու՛ համակարգչի կամ հեռախոսի ծրագրերդ՝ ներբեռնելով համապատասխան ծրագրեր կամ ակտիվացնելով ավտոմատ թարմացման գործառույթը. սա արվում է քո անվտանգության համար:
- Վիրուսներից մաքրի՛ր հեռախոսդ կամ համակարգիչդ, եթե չգիտես ինչպես, քեզ կօգնեն համակարգչային դասընթացի ուսուցիչներդ կամ մասնագետները:
- Խաղեր խաղալիս կամ որևէ կայքում գրանցվելիս՝ փորձի՛ր չհրապարակել անունդ, ազգանունդ, տան, դպրոցի հասցեդ, հեռախոսի համարդ: Համացանցը լի է չար ու նենգ մարդկանցով, հաքերներով, որոնք, քո տվյալները օգտագործելով, կարող են վնասել քեզ:
- Համացանցում ընկերացի՛ր միայն այն մարդկանց հետ, ում ճանաչում ես իրական կյանքում, գուցե կեղծ էջերով փորձում են գողանալ քո անձնական տվյալները:
- Անձնական տվյալներ մի՛ հրապարակիր համացանցում և մի՛ կիսվիր անծանոթների հետ, անգամ եթե ներկայանան որպես բարեկամ կամ ծանոթ:
- Քեզ համար սահմանի՛ր գաղտնաբառեր, որոնք դու հեշտ կհիշես, բայց միևնույն ժամանակ դրանք անհասկանալի կլինեն անծանոթներին: Ոչ մեկին մի՛ ասա գաղտնաբառերդ, դրանք քո ապահովության բանալիներն են: Քո անձնական տվյալներն ու տեղեկատվությունը կարևոր ու արժեքավոր են:
- Անհայտ հասցեներից, եթե հղումներ ես ստանում մի՛ տարածիր, անգամ եթե այն քեզ փող, հաջողություն կամ երջանկություն է խոստանում, գուցե դա նպատակ ունի գողանալու քո անձնական էջի տվյալները և քեզ վնասելու:
- Զգույշ եղի՛ր անհայտ թեստեր կատարելուց, որքան էլ , որ դրանք գրավիչ ու հետաքրքիր լինեն, այդ էջեր մտնելով՝ դու կարող ես վտանգել քո անձնական տվյալները, որոնք կհայտնվեն անծանոթ մարդկանց մոտ և նրանք էլ կեղծ էջեր կբացեն քո նկարներով և քո տվյալներով:

- Օգտվի՛ր անվտանգ կայքերից. երբ մուտք ես գործում որևէ էջ, ուշադիր եղի՛ր հասցեի առաջին հատվածին, այն պետք է սկսի այսպես՝ ***https:// կամ shtpp://,*** ահա այս դեպքում էջն անվտանգ է։
- Համացանցից որևէ բան ներբեռնելուց կամ նյութերով կիսվելուց առաջ մտածի՛ր դրանց անհրաժեշտության և անվտանգության մասին։ Համացանցում ամեն ինչ մնում է հավերժ, դու կարող ես ինչ-որ բան ջնջել, բայց այլոց էջերում դրանք կպահպանվեն։

Գլուխ 4. Կիբեռհետապնդումներ

Համացանցում մեկը մյուսին ծաղրելը, վիրավորելը, նեղացնելը կոչվում են կիբեռհետապնդումներ: **Ինտերնետ-հալածանք** կամ **կիբերհալածանք**, դիտավորյալ վիրավորանքներ, սպառնալիքներ, զրպարտություն և այլ վարկաբեկող տվյալների հաղորդագրություն ժամանակակից կապի միջոցներով, սովորաբար երկար ժամանակով: Հալածանքն իրականացվում է տեղեկատվական տարածության միջոցով, տեղեկական և հաղորդակցական ուղիներով և միջոցներով: Այդ թվում համացանցում՝ առցանց էլեկտրոնային փոստի միջոցով, ակնթարթային հաղորդագրությունների ծրագրեր (օրինակ, ICQ) սոցիալական ցանցերում, ֆորումներում:

Ինչպես կյանքում, այնպես էլ համացանցում անհրաժեշտ է հարգել միմյանց, հետևել քաղաքավարության կանոններին.

• Լինել քաղաքավարի
• Լինել անկեղծ
• Չնեղացնել, չծաղրել, չվիրավորել ոչ մեկի
• Մարդկանց հետ վարվել այնպես, ինչպես, որ կուզենայիր քեզ հետ վարվեին
Եթե քեզ կամ քո ընկերներին չար, սպառնացող կամ անհարմար բովանդակության նամակներ են ուղարկում,վախեցնում, ապա կատարի՛ր հետևյալը.
• Պատմի՛ր ծնողներիդ կամ ուսուցիչներիդ
• Պահապանի՛ր սպառնալիքները, հետագայում ապացույցներ ունենալու համար
• Ապաակտիվացրո՛ւ կամ փակի՛ր տվյալ սպառնացողի հետ հաղորդակցման աղբյուրը
• Հիշի՛ր, որ անհրաժեշտության դեպքում կարող ես դիմել ոստիկանություն:

Ինչից պետք է զգուշանալ

Գաղտնալսում (անգլ.՝ Eavesdropping), մարդկանց հաղորդակցության, հեռախոսային, մասնավոր համակարգչի «խոսակցություն» (հաղորդակցություն) լողալիս լսելն է, որը սովորաբար գտնվում է ցանցում գտնվող հաղորդավարների միջև: Ինչպիսիք են Carnivore- ը և NarusInSight- ը, որոնք օգտագործվում են FBI-ի և NSA- ի

կողմից, ինտերնետ-ծառայություններ մատուցողների համակարգերի գաղտնալսման համար: Նույնիսկ մեքենաներ, որոնք գործում են որպես փակ համակարգ (այսինքն՝ առանց արտաքին աշխարհի հետ կապ չունենալու) կարող են գաղտնալսվել ապարատային սարքավորումներով առաջացած թույլ էլեկտրամագնիսական փոխանցումները դիտարկելու միջոցով. TEMPEST- ը ԱԱԾ-ի կողմից ներկայացվող ճշգրտում է, որը վերաբերում է այս հարձակումներին:

Ֆիշինգ(անգլ.՝ phishing), որի նպատակն է ստանալ որևէ սոցիալական կայքի օգտատիրոջ[6] գաղտնի տվյալները, ծածկագիրը և ծածկանունը: Սա կատարվում է զանգվածային էլեկտրոնային սպամ նամակների միջոցով, որոնք հասցեատիրոջը հասնում են հայտնի բրենդների անունից, ինչպես նաև տարբեր ծառայությունների վերաբերյալ անձնական նամակներ, օրինակ բանկի կամ սոցիալական ցանցերի կողմից: Նամակը հաճախ պարունակում է ուղղակի կայքի հղումը, որը արտաքնապես չի տարբերվում իրական նույն կայքից: Այն բանից հետո, երբ հաղորդագրության օգտատերը ստանում է կեղծ էջը, հաքերները տարբեր հոգեբանական հնարքներով փորձում են դրդել օգտատիրոջը մուտք գործել կեղծ էջ՝ իրենց իրական մուտքանունը և գաղտնաբառը լրացնելով, որը հաքերներին թույլ է տալիս մուտք գործել դեպի օգտատիրոջ բանկային հաշիվ կամ ակաունտ:

Ստեղնաշարային լրտեսը վնասատու ծրագիր է, որը արձանագրում է յուրաքանչյուր ստեղնի սեղմումը: Այսպիսի ծրագրերը օգտագործում են գաղտնի տվյալներ՝ գաղտնաբառերի, բանկային հաշվեհամարների և դրանց կոդերի, կրեդիտ քարտերի ծածկագրերը կորզելու համար:

Տրոյական կորզող ծրագրերը նախատեսված են գումար կորզելու համար: Սովորաբար այդպիսի տրոյական ծրագիրը կամ ծածկագրում է զոհի տվյալները նրա համակարգչի կոշտ սկավառակի վրա, կամ համակարգիչը դարձնում է անհասանելի: Դրանից հետո կորզիչ ծրագիրը այդ փոփոխությունները վերացնելու համար գումար է պահանջում:

Գլուխ 5. Կիբեռսպառնալիքներից պաշտպանվելու համար պետք է պահպանել հետևյալ կանոնները.

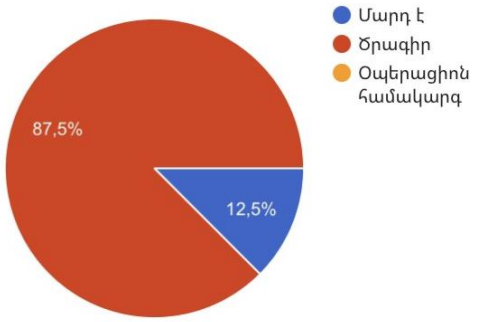
- Չանցնել նամակների, մեսենջերների և SMS-հաղորդագրությունների կասկածելի հղումներով;
- Կանոնավոր կերպով տեղադրել օպերացիոն համակարգի և հավելվածների թարմացումները;
- Հավելվածներ տեղադրել միայն պաշտոնական հարթակներից;
- Օգտահաշիվներում կիրառել բարդ և տարբեր գաղտնաբառեր;
- Կարևոր տվյալները կանոնավոր կերպով պատճենել ամպում, ֆլեշ քարտում կամ կոշտ սկավառակում;
- Հավելվածներին չտալ հասանելիություն այն գործառույթներին, որոնք դրանց անհրաժեշտ չեն:

Երեխաների կողմից լրացված թեստը՝ կիբեռանվտանգության կանոնների կիրառության ու պահպանման վերաբերյալ

Ստեղնաշարային լրտեսը դա՝

Պատճենել

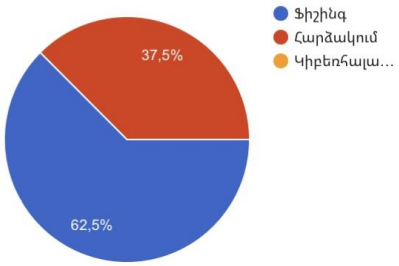
8 պատասխան



Սոցիալական ցանցերում ծածկագիր և ծածկանուն ստանալը կոչվում է

Պատճենել

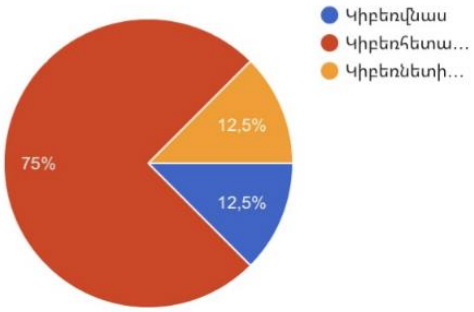
8 պատասխան



Համացանցում մեկը մյուսին ծաղրելը, վիրավորելը, նեղացնելը կոչվում է

Պատճենել

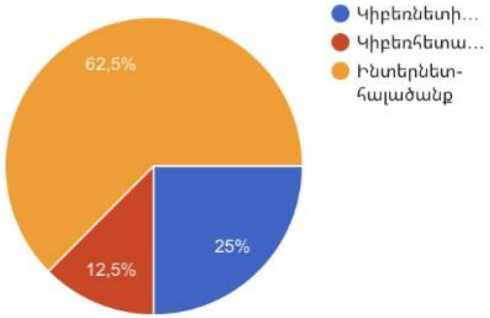
8 պատասխան



Ինչ է կոչվում դիտավորյալ վիրավորանքները, սպառնալիքներ, զրպարտությունը

Պատճենել

8 պատասխան



Եզրակացություն

Չնայած բոլոր մարտահրավերներին՝ համացանցը անսպառ, օգտակար և անհրաժեշտ գիտելիքի հսկայական աղբյուր է, սակայն ճիշտ օգտվելու համար անհրաժեշտ է պահպանել կանոնները.

- Սովորե՛լ ճիշտ ու անվտանգ օգտվել համացանցից. ծնողների ու ուսուցիչների հետ համատեղ սահմանել անվտանգության կանոնները։
- Ընկերների, ուսուցիչների, ծնողների հետ կարելի է մտածել և հետաքրքիր նախագծեր իրականացնել։
- Պետք է բարի և հանրության համար պիտանի նյութերով լցնել համացանցը։

Սակայն այս ամենի հետ մեկտեղ այն ունի թերություններ, քանի որ համացանցում առկա է կեղծ և ոչ հավաստի ինֆորմացիա, որը կարող է սխալ կարծիք ձևավորել տվյալ տեղեկատվության վերաբերյալ: Եվ ինչքան մարդը խճճվում է իրեն հուզող հարցերի շուրջ համացանցում, այնքան հանդիպում է շատ վտանգների, որոնց նա պետք է կարողանա ճիշտ լուծում տալ: Եվ սա է հիմնական պատճառը, որ մեր անչափահասները միշտ ունենում են խնդիրներ: Եվ մենք կարծում ենք, որ մեր անչափահասները չպետք է գրանցվեն սոցցանցերում: Իսկ գրանցվելու դեպքում պետք է միշտ լինեն իրենց ծնողների հսկողության ներքո: Ծնողը պետք է ինքը ուղղություն ցույց տա երեխային ,ինչու չէ նաև սահմանափակումներ դնի , ինչու չէ նաև այլընտրանքային զբաղմունք ցույց տա անչափահասին: Համացանցից դուրս կարելի է իրական կյանքում ուսումնասիրել մշակույթը՝ հաճախակի գնալ թատրոն, համերգների, այցելել տարբեր ցուցահանդեսներ ու պատկերասրահներ և ծանոթանալ ներկայիս մշակույթի ներկայացուցիչների հետ: Ի վերջո աշխարհն առանց համացանցի անհնար է պատկերացնել, բայց չպետք է մոռանալ ինտերնետից դուրս գտնվող մեկ այլ կյանքի մասին։

Գրականություն

1) https://libArmEdu.am
2) https://wisemotors.ru
3) https://dprocashakert.wordpress.com/
4) https://www.poqrikishkhan.am/կիբեռանվտանգության-կանոններ-դեռահաս/
5) https://hy.wikipedia.org/wiki
6) https://hy.wikipedia.org/wiki/ինտերնետ-հալածանք