

**ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿՐԹՈՒԹՅԱՆ ԳԻՏՈՒԹՅԱՆ, ՄՇԱԿՈՒՅԹԻ ԵՎ
ՍՊՈՐՏԻ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ**

«ԱՇՏԱՐԱԿԻ Ն. ՍԻՍԱԿՅԱՆԻ ԱՆՎԱՆ ԹԻՎ 5 ԱՎԱԳ ԴՊՐՈՑ» ՊՈԱԿ

**ՀԵՐԹԱԿԱՆ ԱՏԵՍԱՎՈՐՄԱՆ ԵՆԹԱԿԱ ՈՒՍՈՒՑԻՉՆԵՐԻ
ՎԵՐԱՊԱՏՐԱՍՏՄԱՆ ԴԱՍԸՆԹԱՑԻ**

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ

Առարկա՝	Ինֆորմատիկա
Ուսուցիչ՝	Անագիտ Գրիգորյան
Թեմա՝	Տեղեկատվական գլոբալ ցանցերը, տեղեկատվության անվտանգությունը և սովորողի հոգեկան առողջության պահպանումը
Ղեկավար՝	Վարդանուշ Հովհաննիսյան

ԱՇՏԱՐԱԿ 2023

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՆԵՐԱԾՈՒԹՅՈՒՆ.....	3
ՆՊԱՏԱԿԸ.....	5
ԵՐԵԽԱՆԵՐԸ ԵՎ ՀԱՄԱՑԱՆՑԸ.....	6
ԵՐԵԽԱՆԵՐԻ ԽՈՑԵԼԻՈՒԹՅՈՒՆՆԵՐԸ.....	9
ՀԱՄԱՑԱՆՑԻ ՕԳՏԱԳՈՐԾՈՒՄԻՑ ԲԻՈՂ ՎՏԱՆԳՆԵՐԸ.....	11
ՀԱՄԱՑԱՆՑԻՑ ՕԳՏՎԵԼՈՒ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԿԱՆՈՆՆԵՐԸ.....	14
ԳՈՐԾՆԱԿԱՆ ԱՇԽԱՏԱՆՔ.....	17
ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ.....	20
ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ.....	21

ՆԵՐԱԾՈՒԹՅՈՒՆ

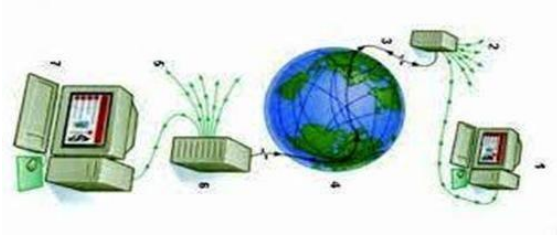
Համացանցից օգտվում են աշխարհի բնակչության ավելի քան մեկ քառորդը, շուրջ 1,5 միլիարդ մարդ՝ տարբեր սեռի և տարիքի և այդ թիվը շարունակում է աճել:

Մեզնից շատերն իրենց կյանքն այսօր ուղղակի չեն պատկերացնում առանց համացանցի: Ոչ հեռավոր անցյալում համացանցը էկզոտիկա էր, ոչ բոլորին հասանելի: Ավելի ճիշտ կլինի ասել, որ այն պարզապես քչերին էր հասանելի: Ավելին, այն ոչ միայն քչերին էր հասանելի, այլև բավական սահմանափակ էր ու շատ հնարավորություններ չէր տալիս: Իսկ այսօր համացանցը իր ցանցն է գցել ու տարածվել ողջ երկրագնդով՝ աստիճանաբար առաջարկելով նորանոր հնարավորություններ ու նորանոր գործիքներ: Այսօր դժվար է պատկերացնել, որ համացանցի նախատիպը, որը գործարկվել է 1969 թ.-ին, իր առջև դրել էր ընդամենը մեկ խնդիր՝ կազմակերպել տեքստային տվյալների փոխանցում երկրի մի կետից մյուսը: Համացանցում գործում են բազում ծառայություններ, որոնք ճիշտ կիրառելիս այն դարձնում են անփոխարինելի գործիք:

Արագագործ համացանցը հասանելի է դարձնում հեռուստատեսային ծառայություններ, ֆիլմերի, տեսահոլովակների, այլ տեսանյութերի դիտումներ: Համացանցը օգտագործողներին իրական ժամանակում հաղորդակցվելու հնարավորություն է տալիս, ինչպես գրավոր տեսքով, այնպես էլ ձայնային ու տեսաձայնային տարբերակով՝ նույն պահին լսելով և տեսնելով զրուցակցին: Էլեկտրոնային փոստն արդեն գրեթե ամբողջովին փոխարինել է սովորական փոստային ծառայությանը: Համացանցային ծառայությունները հնարավորություն են տալիս աշխարհի տարբեր ծայրերում գտնվող համակարգիչների միջև ֆայլերի փոխանակություն իրականացնել: Համացանցը նաև ժամանցի մի հսկայական տարածք է, որտեղ կարելի է գտնել առցանց (online) խաղեր, մրցույթներ, վիկտորինաներ: Սոցիալական ցանցերը, ֆորումները, բլոգները հնարավորություն են տալիս վերագտնել հին ծանոթներին, ձեռք բերել նույն հետաքրքրություններն ունեցող նոր ծանոթներ, ստանալ հուզող հարցերի պատասխանները և այլն:

Սրանք միայն մի փոքր մասն են այն ոլորտների, որտեղ համացանցի շնորհիվ արմատապես փոխվել են մարդկանց ապրելու, շփվելու, սովորելու, աշխատանքի և

հանգստանալու ձևն ու հնարավորությունները: Համացանցային ծառայությունները և տեխնոլոգիաները ներառվել են մարդկային կյանքի գրեթե բոլոր ոլորտներում:



Մտահոգիչ է նաև այն, որ շատ ծնողներ ավելի քիչ են տեղեկացված նման խնդիրներից, քան՝ երեխաները: Վտանգների հանդիպելու ռիսկն ավելանում է, երբ երեխաները համացանց մուտք են գործում սմարթֆոնի, պլանշետի կամ այլ սարքերի միջոցով: Այսպես ավելի քիչ է հավանականությունը, որ վերահսկվում են ծնողների կամ դպրոցի, մանկավարժների կողմից:

ՆՊԱՏԱԿԸ

Սովորողներին իրազեկել, թե ինչպես ապահով և արդյունավետ օգտագործել համացանցի հնարավորությունները, ինչպես ճիշտ կողմնորոշվել համացանցում՝ չդառնալով խաբեության զոհ, ինչպես պաշտպանել համակարգիչը վիրուսներից, ինչպես դրսևորել օրինակելի վարք առցանց շփման ժամանակ: Պարզել, թե որոնք են համացանցից ներթափանցող հիմնական վտանգները:



Խնդիրները

- Ուսումնասիրել համացանցում մեդիագրագիտության վերաբերյալ հայալեզու պաշարները:
- Մշակել դասի պլան, կանոններ, քարտեր, տեսական նյութ:
- Իրականացնել դաս, ծնողական ժողով, անդրադառնալ համացանցի անվտանգության թեմային, անցկացնել գործնական աշխատանքներ, դասախոսություններ:
- Կատարել անրադարձ:

Մեթոդ

- գիտական և մեթոդական գրականության տեսական վերլուծություն
- տեղեկատվության ընտրություն
- ընդհանրացում:
- նկարագրություն.

ԵՐԵՒԱՆԵՐԸ ԵՎ ՀԱՄԱՑԱՆՑԸ

Համացանցը զարգանում է օրեցօր: Օրեցօր ավելանում են թե՛ նրա հնարավորությունները, թե՛, այդ թվում, նրա բերած վտանգները: Սա նոր զարգացող աշխարհ է, նոր ստեղծվող միջավայր, նոր ստեղծվող մշակույթ: Եվ եթե մեզնից որևէ մեկն ուզում է իրեն լիարժեք մարդ զգալ այս նոր միջավայրում, պետք է մատն ամբողջ ժամանակ պահի զարկերակին, զգա փոփոխություններն ու հարմարվի: Իսկ էլ ավելի կարևոր է, որ այդ ընթացքում լրիվ չտարվի համացանցով՝ վերանալով իրական աշխարհից, իրական շփումներից:

Երեխաների համար համացանցը և այն սարքերը, որոնցով նրանք միանում են համացանցին, իրականում նրանց իրական կյանքի մասն են: Երբ երեխաների հետ խոսում ենք համացանցի և նոր տեխնոլոգիաների մասին, անհրաժեշտ է պահպանել լավատեսական և դրական տրամադրություն: Մենք պետք է նպատակ դնենք երեխաներին տեղեկացնելու համացանցի վտանգների մասին և, թե ինչպես հաղթահարել դրանք:

Ամենահաս համացանցի և սոցցանցերի ազդեցության տակ երեխաները դառնում են ուրիշ, ոչ այնպիսին, ինչպիսին կուգենային նրանց տեսնել ծնողները: Ոչ ինտերնետային անցյալ ունեցող ծնողներին թվում է, որ համացանցը կլանում է իրենց երեխաներին ճահճի պես: Չնայած այդ վիրտուալ ճահճում թաքնված են լավ և վատ կողմեր:

Նաև պետք է հիշել, որ համացանցը լոկ սոցցանցերը չեն, իսկ «մեծահասակների կայքերից» երեխաներին հեռու պահելու համար դրանք փակելու տեխնիկական հնարավորություններ գոյություն ունեն: Համակարգիչը պետք է երեխայի օրվա ռեժիմի մի մասը լինի, բայց երբեք չպետք է հասցնել պատժի սահմանին՝ հակառակ հոգեբանական ռեակցիա չառաջացնելու համար: Սխալ է երեխային համացանցից ընդհանրապես զրկելը, քանի որ այն լայն ճանաչողական, ուսուցողական, գեղեցիկի հետ շփվելու հնարավորություն է տալիս, դրանով աշխարհը ավելի փոքր և ընկալելի է դառնում երեխայի համար: Ըստ հոգեբանի, ոչինչ արգելել չի կարելի, երեխայի հետ պետք է անընդհատ երկխոսության մեջ լինել, և փորձել բացատրել համակարգչի և համացանցի օգուտներն ու վնասները: Երբ երեխայի և ծնողի միջև կա դիալոգ, ապա այդ դեպքում շատ հեշտ է երեխային հասցնել նրան, որ ինքը գիտակցի, որ դա վնասակար է:

Համացանցի լավ կողմերն են՝

Դեպի հաջողության տանող ճանապարհ է

Վաղ տարիքից, ուզած թե չուզած, յուրացնում են այդ տեխնոլոգիաները ու հաղորդակցության մյուս միջոցները: Հասունության վկայական դեռ չստացած նրանք տեխնոլոգիաների պատրաստի մասնագետներ են:

Շփման հնարավորությունների շրջանակը մեծ է

Հին կապերն ամրապնդվում են, առաջանում են նորերը, երբեմն աշխարհի մյուս ծայրից: «Կյանքը» հետաքրքիր է դառնում: Հանդիպման վայրը հետայսու նույնն է՝ ՀԱՄԱՑԱՆՑ:

Ինքնարտահայտման միջոց է՝

Հատկապես աճող սերնդի համար ի հայտ է եկել սեփական կարծիքը հայտնելու, դրանով ուրիշների հետ կիսվելու հնարավորություն:

Գիտելիքների հզոր աղբյուր է

Այսօր ավելի հեշտ է գիտելիքներ ձեռք բերել համացանցի միջոցով:

Որոշակի ճաշակ կարող է ձևավորել

Երեխան համացանցի միջոցով կարող է այցելել թանգարաններ ու պատկերասրահներ:

Համացանցի վատ կողմերն են՝

Սպառնալիք է

Սոցցանցերի միջոցով իրար սպառնալ, վախեցնել, հաճախ սպառնալիք ստացածները կարող են թողնել դպրոցը, կամ դիմել որևէ այլ վատ քայլի:

Լեզվական սահմանափակումներ

Սոցցանցերում շատ են գրում հաղորդագրություններ, որոնք գրում են կրճատ կամ սմայլիկներով: Լեզվական, այդ թվում նաև երեխայի զարգացման մշակութային հիմքերն այսպիսով վտանգված են:

1. Անընդհատ սոցիալական կայքերի, անձնական և էլփոստը ստուգելու ցանկությունը:
2. Համակարգչի մոտ լավ ինքնազգացողությունը, իսկ համակարգչից հեռու գտնվելու ժամանակ դատարկության, դեպրեսիայի, լարվածության զգացողությունը:
3. Համակարգչից կտրվելու անընդունակությունը:

4. Աշխատանքի կամ ուսման հետ խնդիրների առաջացումը:
5. Ձերքի մկանների գերլարվածության հետևանքով ցավի զգացողությունը:
6. Չորություն աչքերում:
7. Միգրենանման գլխացավեր:
8. Մեջքացավեր:
9. Անկանոն սնվելը:
10. Քնի խանգարումները:

Հիմա փորձեմ պատասխանել հետևյալ հարցին. «Ի՞նչպես պայքարել բացասական հետևանքների դեմ»:

Ներկայումս հանրակրթական բոլոր դպրոցները ապահովված են անվճար համացանցով: Հատուկ «գտիչները» թույլ չեն տալիս մտնելու ցանկացած ուսումնական կայք: Սա այն ճանապարհներից մեկն է, երբ պետությունը կարող է պայքարել համացանցի բացասական հետևանքների դեմ: Կարելի է նաև տարիքային սահմանափակում կիրառել: Օգտագործիր համացանցը կարիքներիդ համար, բայց այն մի սարքի քո բնակավայր: Համացանցը միայն օժանդակ գործիք է: Համացանցը միայն օգտագործելու համար է: Մի՛ թույլատրիր, որ համացանցը քեզ օգտագործի:

Համացանցում ձեզ կարող են սպառնալ, վիրավորել, հրավիրել հանդիպման: Հաճախ դրանք դատարկ խոսքեր, բայց ի՞նչ գիտեք, թե ով է թաքնված այդ համացանցի այն կողմում: Իսկ համացանցի այն կողմում կարող է լինել հանցագործ, կարող է լինել մոլագար: Մշտապես խուսափեք համացանցային հարաբերությունները, վեճերը իրական կյանք բերելուց: Խուսափեք կոնֆլիկտներից: Եթե ինչ-որ մեկը ձեզ սպառնացել է, մի՛ պատասխանեք: Ձեր արժանապատվությունը դրանից չի տուժելու: Արգելափակեք այդ մարդուն, որ չստանաք նրա նամակները, հաղորդագրությունները ու անմիջապես ասեք մեծահասակներին, ապա ահազանգեք, շուրջօրյա թեժ գիծ ծառայությանը՝ 08 006 1111 (անվճար) հեռախոսահամարով: Հնարավոր է, որ դուք կօգնեք ոչ միայն ձեզ, այլև ուրիշներին: Բայց մինչև զանգելը մի ջնջեք Ձեր ստացած նամակներն ու հաղորդագրությունները: Դրանք կարող են պետք գալ մեղավորին գտնելիս:

ԵՐԵՒԱՆԵՐԻ ԽՈՑԵԼԻՈՒԹՅՈՒՆՆԵՐԸ

Բազմաթիվ փորձագետների և սովորական օգտագործողների նպատակն է համացանցը դարձնել անվտանգ, սակայն, ավաղ, այդ երազանքն առայժմ անկատար է:

Գաղտնք չի, որ երեխաները ավելի խոցելի են: Սա առանցքային սկզբունք էնաև երեխաների պաշտպանության, երեխաների սոցիալական ապահովության մի շարք քաղաքականութայինների և օրենսդրության տեսանկյունից աշխարհի տարբեր մասերում գտնվող շատ տարբեր պետություններում: Ինչ վերաբերում է համացանցին, կան մի շարք խնդիրներ երեխաների խոցելիությունների հարցում, որոնք շարունակում են մտահոգիչ լինել: Դրանք ամփոփված են ստորև:

Համացանցը երեխաներին հասանելի է դարձնում տարաբնույթ ապօրինի նյութերը, մասնավորապես՝ երեխաների նկատմամբ ոտնձգություններ պարունակող պատկերները: Համացանցի միջոցով երեխաները կարող են ենթարկվել հետապնդումների չափահաս ներիկամ անչափահասների կողմից:

Համացանցն ունակ է միջնորդելու և խթանելու դիսկային սեռական փոխազդեցություններ երեխաների միջև, այդ թվում՝ խրախուսելով նրանց լուսանկարել իրենց կամ այլոց և տեղադրել դրանք ցանցում («sexting»), ինչը վնասակար լինելուց բացի կարող է լինել ապօրինի:

Համացանցն ունակ է երեխաների համար մատչելի դարձնել այնպիսի կայքեր, որտեղ նրանք կարող են գնել օրենքով արգելված ապրանքներ և ծառայություններ: Համացանցը երեխաներին հասանելի է դառնում իրենց տարիքին անհամապատասխան գովազդներ, համացանցի միջոցով երեխաները կարող են ենթարկվել խարդախության, խաբեբայության և նմանատիպ վտանգների, որոնք տնտեսական բնույթի են:¹

Հաքերները հաճախ իրականացնում են զանգվածային ավտոմատացված հարձակումներ՝ հնարավորինս մեծ քանակի անձնական տվյալների տիրանալու համար, և յուրաքանչյուրը կարող է դառնալ դրա զոհը:

Ահա կիբեր անվտանգության մի քանի կանոններ, որոնք կօգնեն առցանց հարթակում լինել առավել ապահով.

- ❖ սոցիալական ցանցերում օգտագործեք բարդ գաղտնաբառեր՝

¹ https://tert.nla.am/archive/HAY%20GIRO/Ardy/2001-2011/nordzernark_2011.pdf

համադրելով մեծատառերը, փոքրատառերը,

թվանշաններն, սիմվոլները

- ❖ անվտանգության նկատառումներից ելնելով հաճախ փոխեք գաղտնաբառը և նույնգաղտնաբառը մի' օգտագործեք տարբեր ծրագրերի համար
- ❖ սոցիալական ցանցերից կամ տարբեր վեբ-կայքերից օգտվելիս ակտիվացրեք «Two-step verification» ֆունկցիան
- ❖ գաղտնաբառը մի' վստահեք ոչ ոքի
- ❖ հրաժարվե՛ք անձանոթ մարդկանց ընկերության հայտերն ընդունել
- ❖ անհայտ ծագմամբ և կասկած առաջացնող գովազդներ ու հղումներ մի' բացեք
- ❖ համացանցում մի' տարածեք անձնական տեղեկատվություն (անուն, հասցե տարիք, հեռախոսի համար, ծննդյան ամսաթիվ ու օր, էլեկտրոնային հասցե դպրոցի/տան հասցե և այլ փաստեր ձեր մասին)
- ❖ մի' հավատացեք էլեկտրոնային հասցեին, ֆեյսբուքյան կամ այլ սոցիալական կայքերի անձնական էջերին ստացված նամակներին, որտեղ ձեզ շնորհավորում են համերգի/թատրոնի/արտասահման մեկնելու անվճար տոմսեր շահելու, հիանալի կարիերա սկսելու, ժառանգություն ստանալու մասին, և մի' շտապեք անցնել հղումով, քանի որ այն հնուտ մտածված տարբերակ է ձեզանից անձնական տվյալներ կամ գումարներ կորզելու և ձեզ հավաքագրելու համար
- ❖ յուրաքանչյուր քայլի, զգացողության, հաջողության կամ անհաջողության մասին պետք է կիսվել առցանց հարթակներում:
- ❖ Այս խորհուրդները ևս կարիք ունեն անընդհատ թարմացման, քանի որ օրական ստեղծվող նորանոր տեղեկատվական պաշարների հետ ավելանում են նաև վտանգները:
- ❖ Անվտանգության նկատառումներով միշտ պետք լինել իրազեկ ու զգոն:

ՀԱՄԱՑԱՆՑԻ ՕԳՏԱԳՈՐԾՈՒՄԻՑ ԲԽՈՂ ՎՏԱՆԳՆԵՐԸ

Ֆայլերի փոխանակման վտանգներ



- ❖ Երաժշտության, տեսանյութերի և այլ ֆայլերի ինտերնետի միջոցով փոխանակումն անձանոթներին կարող են լինել անօրինական, և հնարավորություն տան մուտք գործելու ձեր համակարգիչ և փոխանցել վիրուսներ:

Կիբերհարձակումներ



- ❖ Թե՛ երեխաները, թե՛ մեծահասակները կարող են օգտագործել ինտերնետը այլ մարդկանց անհանգստացնելու կամ վախեցնելու համար:

Ինտերնետային խաբեբայություններ



- ❖ Էլ. նամակներ, որոնք ուղարկվում են ինտերնետային հանցագործների կողմից, ովքեր փորձում են կորզել անձնական տեղեկատվություն:

Ներխուժում անձնական կյանք



- ❖ Երբ երեխան լրացնում է ինտերնետային հարցաթերթիկներ, կարող է փոխանցել տեղեկատվություն իր կամ իր ընտանիքի մասին, որն անցանկալի է փոխանցել անձանոթներին կամ ինտերնետային ծանոթներին:

Խորամանկություններ



- ❖ Էլեկտրոնային նամակներ, որոնք ուղարկվում են ինտերնետային հանցագործների կողմից, ովքեր փորձում են գումար կորզել:

Երեխաներին առցանց անվտանգ պահելը թիվ մեկ առաջնահերթությունն է

Ոչինչ չի փոխարինում ծնողների ներգրավվածությանը, երբ խոսքը վերաբերում է երեխաների առցանց անվտանգությանը: Պարզապես խոսեք ձեր երեխաների հետ, սովորեցրեք նրանց ինքնաբերաբար չսեղմել «այո» կոճակը և չհրահրվել կիբերկռվարարների կամ պոտենցիալ կիբերհանցագործների կողմից: Անվտանգության լուծումները լրացնում են այս աշխատանքը՝ վերահսկելով երեխայի վարքագիծը համացանցում, որն ապահովում է առցանց խաղահրապարակի անվտանգությունը: Տարիքին

ոչ համապատասխան կամ վնասակար օնլայն նյութերից խուսափելու համար կարելի է երեխաների իմացությամբ կիրառել վերահսկման, ֆիլտրման գործիքներ, որոնք հնարավորություն կտան տեսնել նրանց այցելած կայքերը, ինչպես նաև սահմանափակել թե որտեղի՞ց և ի՞նչ սարքերով կարելի է օգտվել համացանցից: Երեխաներին պետք է սովորեցնել, որ համացանցում հանդիպող անձանոթ/տարօրինակ երևույթները և նյութերը (նկար, վիդեո, տեքստ և այլն) անհրաժեշտ է քննարկել ծնողների հետ:

Անպատշաճ բովանդակությամբ կայքերի արգելափակում

Գաղտնիք չէ, որ ոչ բոլոր կայքերն են նախատեսված երեխաների դիտման համար: Երեխան կարող է պատահաբար հայտնվել անպատշաճ բովանդակությամբ կայքում՝ պարզապես փնտրելով որևէ բան որոնման համակարգում կամ սեղմելով ընկերոջ կողմից ուղարկված հղումը:

Ինչպե՞ս կարող եք երեխաներին անվտանգ պահել առցանց և միևնույն ժամանակ անտեղի ճնշում չգործադրել նրանց վրա: Պատասխանը կարող է լինել ծնողական վերահսկողության գործառույթը: Այն հասանելի է և՛ որպես ինքնուրույն լուծում, և՛ որպես անվտանգության համալիրլուծումների մաս: Ծնողական վերահսկողության «անվտանգ որոնում» գործառույթն արգելափակում է անպատշաճ բովանդակությունը, և լուծումների մեծամասնությունը նաև ծնողներին մանրամասն հաշվետվություններ է տրամադրում այն մասին, թե ի՞նչ է անում իրենց երեխան առցանց:

Մի մտեր անձանոթների հետ խոսակցության մեջ

Երեխան ցանկանում է վերջին առցանց խաղը խաղալ ընկերների հետ՝ զրուցելով նրանց հետ: Բայց այս չատերը պարունակում են նաև կիբերհանցագործներ, ովքեր թաքնվում են ավատարների հետևում՝ փորձելով խաբել երեխաներին անձնական տեղեկությունները բացահայտելու համար: Այս տեղեկատվությունը կարող է օգտագործել ձեր ինքնությունը՝ գումար գողանալու համար:

Վստահելի կայքերում խաղեր խաղալը կարող է պաշտպանել երեխային: Բայց նույնիսկ այդ դեպքում ձեզ համար դժվար կլինի պաշտպանել երեխային առցանց՝ պարզապես հետևելով, թե ո՞ւմ հետ են նրանք խոսում առցանց: Կայքերը, որոնք առաջին հայացքից անվնաս են թվում, կարող են պարունակել վնասակար հղումներ, որոնք կվտանգեն ձեր ողջ ցանցի անվտանգությունը:

Մի ներբեռներ վիրուս

Կիրբերհանցագործները գիտեն, որ երեխաները հաճախ համացանցում փնտրում են անվճար ծրագրեր, երաժշտություն և խաղեր: Նրանք նաև գիտեն, որ երեխաները հաճախ վստահում են էլ. փոստի հղումներին և հավելվածներին: Եթե երեխան սեղմի այս հղումներից մեկը, նա կարող է ներբեռնել վիրուս, որը կվտանգի ոչ միայն համակարգչի, այլև ամբողջ ցանցի անվտանգությունը:

Երեխան կարող է դա անել ոչ միտումնավոր և արդեն լուռ ներբեռնվում են նրա համակարգիչ և սպառնում են նրա անվտանգությանը:

Վերահսկեք ձեր երեխայի այցելած կայքերը և ծախսած ժամանակը համացանցում

Երեխաները օգտվում են տարբեր առցանց ծառայություններից, որոնք կարող են ունենալ տարբեր անվտանգության խնդիրներ: Քննարկեք Ձեր երեխաների հետ, թե ի՞նչ է նրանց հետաքրքրում համացանցում և ո՞ր կայքերից են օգտվում:

Եթե նույնիսկ չգիտեք ինչպե՞ս օգտվել՝ հարցրեք նրանց: Երեխաների համար ամենալավ օրինակը հենց դուք եք, օրինակ եթե արգելում եք նրանց օգտվել հեռախոսից ճաշի ժամին, ապա դուք նույնպես խուսափեք վերջինիս կիրառումից: Հեռախոսները և ծրագրային հավելվածները հրաշալի միջավայր են ուսման և ժամանցի համար, սակայն, ինչպես և մեզ շրջապատող աշխարհը, այն կարող է վտանգավոր լինել, եթե համապատասխան կանխարգելիչ քայլեր ձեռնարկված չեն: Իմացե՛ք թե ի՞նչ հավելվածներից և օնլայն ծառայություններից է օգտվում ձեր երեխան: Տեղեկություն ստանալու լավագույն միջոցը նրանց հարցնելն է: Երեխաների հետ պարբերաբար քննարկեք խնդիրները և կիրառեք սահմանափակումներ:

Պաշտպանեք ձեր կարևոր տվյալները

Մի պահեք կարևոր տվյալներ (բանկային քարտի տվյալներ, ծածկագրեր, առողջության վերաբերյալ փաստաթղթեր և այլն) ձեր համակարգիչներում, հեռախոսներում և այլ սարքերում, որոնք միացած են համացանցին: Ջնջեք կարևոր տվյալները, եթե դրանք այլևս անհրաժեշտ չեն: Միշտ օգտագործեք կոդավորում՝ կարևոր տվյալները պահպանելիս և ուղարկելիս: Սակայն կարևոր է հիշել, որ տունը միակ վայրը չէ, որտեղ երեխաները կարող են օգտվել օնլայն ծառայություններից:

ՀԱՄԱՑԱՆՑԻՑ ՕԳՏՎԵԼՈՒ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԿԱՆՈՆՆԵՐԸ

Մի տեղադրեք անձնական տեղեկություններև լուսանկարներ համացանցում

Ավելի ու ավելի հաճախ հարձակվողներն օգտագործում են համացանցը որպես ալիք՝ երեխաներին խաբելու, անձնական տեղեկությունները բացահայտելու համար: Տեղեկացրեք երեխաներին, որ իր կամ նրա ընտանիքի անդամների մասին լուսանկարները կամ տեղեկությունները, որոնք նրանք տեղադրել են համացանցում, չարագործները կարող են օգտագործել և տարածել անձնական շահերի համար:

Մի ներբեռներ կամ տեղադրեք համացանցից որևէ բան առանց ծնողի թույլտվության

Ասացեք երեխաներին, որ վնասակար ֆայլը կարող է թաքնվել խաղի կամ ֆիլմի քողի տակ, որը կարող է վնասել տնային համակարգչին: Ստուգեք այն էջը, որտեղից երեխան պատրաստվում է ինչ-որ բան ներբեռնել վիրուսների համար:

Մի շփվեք եւ Մի ՀԱՆԴԻՊԵՔ ՆՐԱՆՑ ՀԵՏ, ՈՒՄ ԵՐԲԵՔ ՉԵՔ ՏԵՍԵԼ

Հարձակվողները կապեր են հաստատում սոցիալական ցանցերում, ֆորումներում, զրուցարաններում կամ էլ.հասցեներում, և դա ուղղակի սպառնալիք է երեխաների անվտանգության համար: Հանցագործները հաճախ ներկայանում են որպես զոհի հասակակից, ինչը նրանց համար հեշտացնում է անձամբ հանդիպելը: Շատ կարևոր է երեխաներին բացատրել, որ նրանք չպետք է շփվեն անձանոթ մարդկանց հետ համացանցում և ոչ մի դեպքում չպետք է հանդիպեն նրանց հետ:

ԵՂԵՔ ԱՊԱՀՈՎ ՄՈՒՏՔԻ ԵՎ ԳԱՂՏՆԱԲԱՌԵՐԻ ՄԻՋՈՑՈՎ, ԳԱՂՏՆԻ ՊԱՀԵՔ

ԴՐԱՆՔ ՆՈՒՅՆԻՍԿ ՁԵՐ ԼԱՎԱԳՈՒՅՆ ԸՆԿԵՐՆԵՐԻՑ

Ասացեք երեխաներին գաղտնի պահել տեղեկատվությունը ոչ միայն օտարներից, այլև ընկերներից: Գաղտնաբառերը և մուտքերը կարող են օգտագործվել ցանկացած անձի անձնական շահերի համար: Տեղեկացրեք երեխաներին խաբեության ամենատարածված տեսակների մասին: Օրինակ՝ գովազդ ուղարկելու համար ուրիշի էջը կամ փոստարկղը օգտագործելու մասին:

ԵՂԵՔ ՔԱՂԱՔԱՎԱՐԻ, ՄԻ ՎԻՐԱՎՈՐԵՔ ՀԱՄԱՑԱՆՑԻԱՅԼ ՕԳՏՎՈՂՆԵՐԻՆ

Բացատրեք երեխաներին, որ համացանցը ահաբեկման, վիրավորանքի, սպառնալիքների կամ բամբասանքների տեղ չէ: Հարցրեք երեխաներին այն մասին, ինչ են

տեսել համացանցում, հետևեք, թե ինչ են նրանք անում այնտեղ, ու շաղկապություն դարձրեք նրանց տրամադրությանը: Փորձեք ստիպել երեխաներին խոսել համացանցում նրանց հետ պատահած բոլոր անսովոր փորձերի մասին:

ԵԹԵ ՑԱՆԿԱՆՈՒՄ ԵՔ ՎՃԱՐԵԼ ՀԱՄԱՑԱՆՑՈՒՄ ԻՆՉ–ՈՐ ԲԱՆԻ ՀԱՄԱՐ, ՆԱԽ ԹՈՒՅԼՏՎՈՒԹՅՈՒՆ ԽՆԴՐԵՔ ՁԵՐ ԾՆՈՂՆԵՐԻՑ

Բանկային քարտերի տվյալները շատ կարևոր բան են, և երեխաները պետք է տեղյակ լինեն դրա մասին: Քարտի տվյալները օգտագործելուց առաջ երեխաները պետք է տեղեկացնեն իրենց ծնողներին: Ասացեք երեխաներին, որ եթե ուշադիր չլինեն, խաբեբաները կարող են անօրինական կերպով վերցնել գումարը: Ստուգեք այն կայքը, որն առաջարկում է գնումներ կատարել: Այսօր որոշ էջերում հատուկ վճարային մուտքեր են կատարվել բանկի տվյալները մուտքագրելու համար:

ՕԳՏԱԳՈՐԾԵՔ ՁԵՐ ՏԵՍԱԽՅԻԿԸ ՄԻԱՅՆ ԸՆԿԵՐՆԵՐԻ ՀԵՏ ԶՐՈՒՑԵԼԻՍ

Համացանցային հանցագործները փորձում են կապ հաստատել պոտենցիալ զոհերի հետ առկա բոլոր միջոցներով, այդ թվում՝ տեսախցիկի միջոցով: Փորձեք տեղյակ լինել համացանցում երեխաների որևէ մեկի հետ շփվելու մանրամասներին:

Եթե երեխան ագրեսիայի զոհ է դարձել, օգնեք նրան ելք գտնել այս իրավիճակից: Բացատրեք, որ երբեք չպետք է բարի արձագանքել վիրավորական խոսքերին: Եթե չեք կարող խնդիրը լուծել խաղաղ ճանապարհով, ապա պետք է հեռանաք ռեսուրսից և այնտեղից ջնջեք ձեր տվյալները: Բացի այդ, այսօր գրեթե բոլոր կայքերն ունեն մոդերատորներ՝ մարդիկ, ովքեր հետևում են այն ամենին, ինչ գրում են օգտվողները: Նման անձը կարող է բողոքել օրինախախտից, որի պրոֆիլն այնուհետև կարգելափակվի: Եթե մոդերատորն ինչ-ինչ պատճառներով չի կարող դա անել, դիմեք կայքի ադմինիստրացիային և պահանջեք, որ ագրեսորի էջը հեռացվի: Օգտագործեք ժամանակակից ծրագրեր, որոնք զտում են վեբկայքի բովանդակությունը և օգնում վերահսկել, թե որտեղ եք այցելում համացանցում:

Եվ ամենակարևորը՝ սա քննարկեք երեխաների հետ: Նրանք պետք է հասկանան նման արգելքների անհրաժեշտությունը:

ՈՒՂԵՑՈՅԳ, ՈՐը կօգնի երեխաներին համացանցում պաշտպանված լինել

Երեխաները համացանցում բախվում են բազմաթիվ ռիսկերի ու մարտահրավերների: Անձնական տվյալների գաղտնիություն, կեղծ լուրեր, բռնության և ոչ պատշաճ բովանդակություն պարունակող նյութեր, սեռական ոտնձգության փորձեր և բազմաթիվ

նմանատիպ խնդիրներ ամեն օր սպառնում են օգտատերերին:

Հայաստանի օպերատորների միությունն այս խնդիրները պահում է իր ուշադրության կենտրոնում և հեռահաղորդակցության միջազգային միության հետ համատեղ իրականացնում երեխաների առցանց անվտանգությանն ուղղված մի շարք ծրագրեր: Աշխարհում համացանցի յուրաքանչյուր երրորդ օգտատերը երեխա է և այն անսահմանորեն հարուստ ռեսուրս է երեխաների համար: Հնարավորությունները շատ են ինչպես սովորելու, այնպես էլ ընկերների, ընտանիքի և արտաքին աշխարհի հետ կապ հաստատելու համար: Այս ամենի հետ մեկտեղ այն դարձել է շատ վտանգավոր: Երեխաները բախվում են առցանց բազմաթիվ ռիսկերի և մարտահրավերների, ինչպիսիք են՝ անձնական տվյալների գաղտնիությունը, կեղծ լուրերը, բռնության և ոչ պատշաճ բովանդակություն պարունակող նյութերը, սեռական ոտնձգության փորձերը և բազմաթիվ այլ նմանատիպ խնդիրներ: Բացի այդ, Քովիդ-19 գլոբալ համաճարակի պատճառով երեխաները ստիպված եղան շատ ժամանակ անցկացնել առցանց, մինչդեռ ծնողներից շատերը չեն կարողանում վերահսկել երեխաների գործունեությունը համացանցում՝ ծանոթացնել վտանգներին, ինչպես նաև սովորեցնել նրանց այդ վտանգներից խուսափելու և պաշտպանվելու մեթոդներ:

ԱՊԱՀՈՎ ՀԱՄԱՑԱՆՑ Ծնողական ժողով



Թեման՝ Ապահով համացանց

Նպատակը՝ ● Համացանցի անվտանգության կանոնների ուսուցանում:

- Ծնողների իրազեկության մակարդակի բարձրացում:
- Վիրտուալ աշխարհում ճիշտ կողմնորոշվելու ընդունակությունների ձևավորում:

Օգտագործվող մեթոդներ և հնարներ՝

Մտազրոհ, բանավեճ, զրույց, համառոտ դասախոսություն, ցուցադրություն:

Անհրաժեշտ նյութեր և սարքավորումներ՝

Քարտեր, համակարգիչ /ինտերնետ կապով/, պրոյեկտոր և էկրան կամ հեռուստացույց:

Մասնակիցներ՝

Ծնողներ, ուսուցիչներ, ինֆորմատիկայի ուսուցիչ

Դասը սկսել քարտային աշխատանքով, որի նպատակը համացանցի վերաբերյալ ծնողների իրազեկվածությունը ստուգելն է:

Քարտային աշխատանք

Ի՞նչ գիտեմ ես համացանցի մասին

Ծնողի ԱԱՀ.....

1. Հաճա՞խ եք օգտվում համացանցից:

2. Համացանցը օգնու՞մ է Ձեզ, թե՛ խանգարում է, իսկելով ձեր ժամանակը:

3. Ինչպիսի տնային կանոններ կարող եք սահմանել համացանցի օգտագործման համար:

4. Ունե՞ք համացանցային կախվածություն:

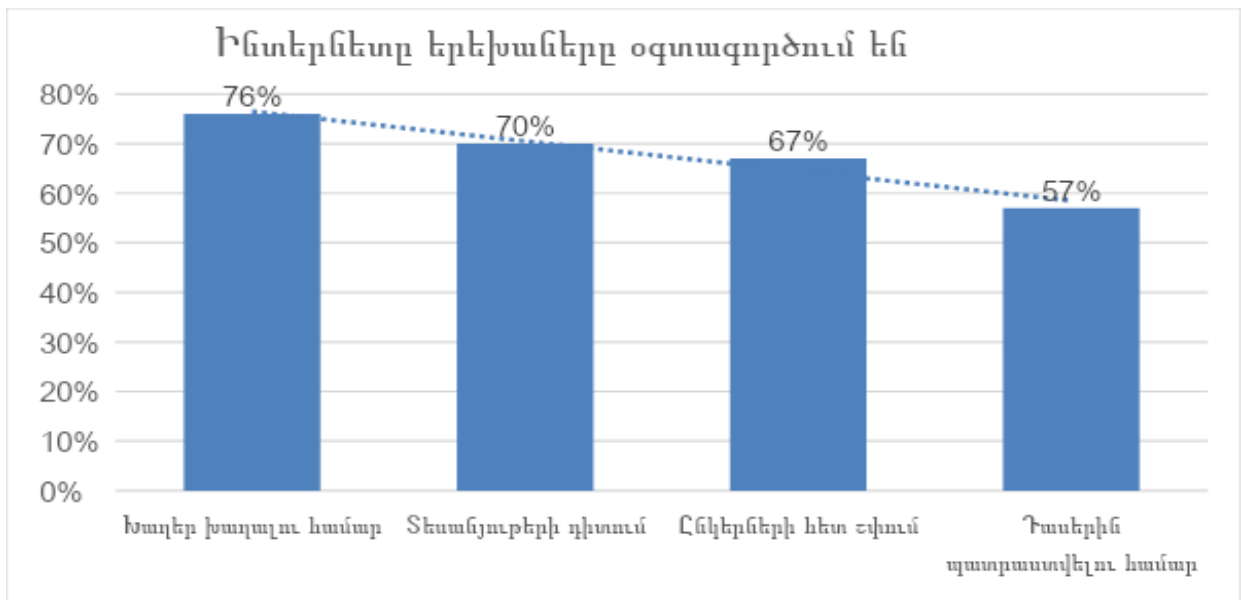
5. Արդյո՞ք անհանգստացել եք, երբ Ձեր երեխան երկար է նստել համակարգչի առաջ:

6. Որքա՞ն հաճախ է Ձեր երեխան ունենում գլխացավ, քնի խանգարում, մեկուսացում և այլառողջական խնդրներ:

Ինչպե՞ս կվարվեք, եթե Ձեր երեխան օգտվի համացանցից և հայտնվի որևէ խնդրահարույց իրավիճակում:

Այսպիսով

1. Ժամանակ գտեք պարզելու, թե ինչպես են ձեր երեխաները անցկացնում իրենց ժամանակը ցանցում և խնդրեք նրանց ցույց տալ, թե ինչպես են հաղորդակցվում իրենց ընկերների հետ: Սովորեցրեք նրանց ապահովել իրենց առցանց մասնավորությունը (մասնավոր կյանքի գաղտնիությունը)`ստեղծելով ապահով անձնական էջեր:
2. Իրենց, ընտանիքի, տան, դպրոցի և այլ նկարներ տեղադրելուց առաջ միշտ հարցնել ծնողների թույլտվությունը,- անձնական տեղեկությունները, ինչպես նաև հեռախոսի համարը, հասցեն, դպրոցի համարը, սպորտային թիմը և այլն, փոխանակել միայն այն մարդկանց հետ, ում ճանաչում են իրական կյանքում:
3. Տեղադրեք ընտանեկան համակարգիչը այնպիսի տեղում, որ կարողանաք վերահսկել նրանց առցանցային զբաղմունքները:
4. Միասին համոզվեք, որ գիտեք, ընկերության առաջարկները մերժելու և արգելափակելու գործառույթները
5. Միասին համոզվեք, որ գիտեք, անվտանգության և ահազանգելու գործառույթները, որ առկան օգտագործվող կայքերում :
6. Ձեռք բերեք երեխաների վստահությունը, քաջալերեք նրանց խոսել ձեզ հետ իրենց սխալների մասին և միասին փնտրեք լուծումները: Մխալները սովորելու անբաժան մաս են կազմում :
7. Համացանցում անցանկալի բովանդակության հանդիպելիս, զեկուցեք ազգային համացանցային թեժ գծին / <http://www.safe.am> INSAFE/
8. Հնարավորության դեպքում նստեք երեխաների կողքին, երբ նրանք նավարկում են համացանցում: Դա լավագույն ձևն է քննարկելու և վստահություն նվաճելու համար: Միասին սովորելը դարձրեք ձեր նպատակը :
9. Հիշեք, որ անվտանգության կանոնները ձեր ու ձեր երեխաների համար են: Քաջալերեք նրանց ասել այն ամենի մասին, ինչն իրենց տարօրինակ է թվում :



Աղբյուրը՝ Ծնողական ուղեցույց / <http://safe.am/esafetykit/downloads/parentsFull.pdf/>
 Ծնողներին ծանոթացնել Ծնողական ուղեցույցի հետևաբար, որպեսզի մանրամասն կարդան ծանոթանան: Էլեկտրոնային տարբերակ՝
<http://safe.am/esafetykit/downloads/parentsFull.pdf/> Ինչպես նաև օգտվել հետևյալ օգտակար հղումներից <http://safe.am/ar/faq.html> <http://safe.am/ar/parents.html>
<http://safe.am/ar/children.html>

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

«Ապահով համացանց» թեմայի ուսումնասիրությունը վերջին տարիների ընթացքում ոչ միայն անհրաժեշտ, այլ պարտադիր է ուսումնասիրել դպրոցում՝ աշակերների և ծնողների մասնակցությամբ: Այն իրականացնել խաղերի միջոցով, վերլուծությունների և փաստերի համադրմամբ: Քանի որ մենք շրջապատված ենք նաև կեղծ ինֆորմացիայով և կեղծ կայքերով, որոնք գումար աշխատելու նպատակով պատրաստ են ցանկացած քայլի, ապա մենք էլ պեք է կրթենք մեդիագրագետ սերունդ, որը վերլուծում է քննադատաբար, կարողանում է ստուգել փաստերը և օգնել ընկերներին կոմնորոշվելու ինֆորմացիոն տեղատարափի մեջ:

Հետազոտությունը նպաստեց աշակերտների մոտ ձևավորել՝

- գիտելիք ապահով համացանցի մասին
- գիտելիք համացանցից օգտվելու անվտանգության հիմնական կանոնների մասին:
- գիտելիք, որի միջոցով կորող են խուսափել մեդիայի բացասական ազդեցությունից:

Հետազոտությունը նպաստեց աշակերտների մոտ զարգացնել՝

- քննադատական մտածողություն
- լեզվական կարողունակություններ
- մեդիա և թվային կարողունակություններ
- ինքնաճանաչողական և սոցիալական կարողունակություն

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. Արտակ Հարությունյան, Վահե Երիցյան «Անվտանգ համացանց», ©Ասողիկ, 2011-64 էջ
2. Լուսինե Գրիգորյան «Կասկածիր, համեմատիր, ճշտիր. ինչպե՞ս բացահայտել և ստուգել կեղծ տեղեկությունները» © Մեդիա նախաձեռնությունների կենտրոն, 2019թ
3. <http://safe.am/ar/about.htm>
4. https://hy.wikipedia.org/wiki/%D4%B1%D5%BA%D5%A1%D5%B0%D5%B8%D5%BE_%D5%80%D5%A1%D5%B4%D5%A1%D6%81%D5%A1%D5%B6%D6%81
5. <http://teenslive.am/communication/hamacanci-apahov-ogtagortcman-10-kanonnereh>
6. https://www.youtube.com/watch?v=_EJ7u4g26VE
7. [https://www.youtube.com/watch?v=rr6H1UwRcN0&list=PLYMtfnOzqv24Vjn2G7DkyYeVijVG99gGV &index=6](https://www.youtube.com/watch?v=rr6H1UwRcN0&list=PLYMtfnOzqv24Vjn2G7DkyYeVijVG99gGV&index=6)