

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ ԻՄ ԻՐԱՎՈՒՆՔՆԵՐԸ ԵՒ ԹՎԱՅԻՆ ԱՇԽԱՐՀԸ

Նպատակը

*Ծանոթացնել համացանցում մեր
իրավունքներին, բացահայտել
դրանց պաշտպանման ձևերն ու
կանոնները:*



Բովանդակություն

1. Ներածություն
2. Իմ իրավունքները համացանցում
3. Թվային աշխարհում մեր իրավունքների ոտնահարումը
4. Համացանցից անվտանգ օգտվելու մշակույթը
5. Ինչպես ապահովել երեխաների անվտանգությունն առցանց տիրույթում
6. Օգտակար խորհուրդներ մեր անվտանգությունն ու իրավունքները պաշտպանելու համար
7. Եզրակացություն





Ներածություն



• Համացանցն առաջարկում է գաղափարների փոխանակման և տեղեկատվության ազատ հոսքի աննախադեպ հնարավորություն ամբողջ աշխարհում: Ժամանակակից տեղեկատվական հասարակությունում ազատ համացանցը նպաստում է ազատ արտահայտվելու հիմնարար իրավունքի և դրանից բխող ՉԼՄ-ների ազատության իրավունքի իրացմանը: Համացանցն աստիճանաբար դառնում է տեղեկատվություն ստանալու, փնտրելու և հաղորդելու ավելի անհրաժեշտ գործիք բոլորի համար:



• Կառավարությունները պարտավորություն ունեն իրենց քաղաքացիներին թույլ տալու անարգել մուտք գործել համացանց: Ժողովրդավարական կառավարությունների պարտավորությունն է՝ մշակել օրենսդրություն և կանոնակարգեր, որոնք հնարավորություն կտան ունենալու անկախ և բազմակարծիք ՉԼՄ-ներ, տեղեկատվության ազատ հոսք առանց սահմանների, անարգել մուտք համացանց և ցանցային գրագիտության զարգացում:

• «Իմ իրավունքները և թվային աշխարհը» հետազոտական նախագիծը կազմելուց մենք մտածեցինք. «Իսկապես, որքանո՞վ է ապահով համացանցը»: Հարցը վերաբերում էր ոչ այնքան բոլոր տեսակի վիրուսային ծրագրերին, որքան մեր անձնական տեղեկատվության անվտանգությանը:

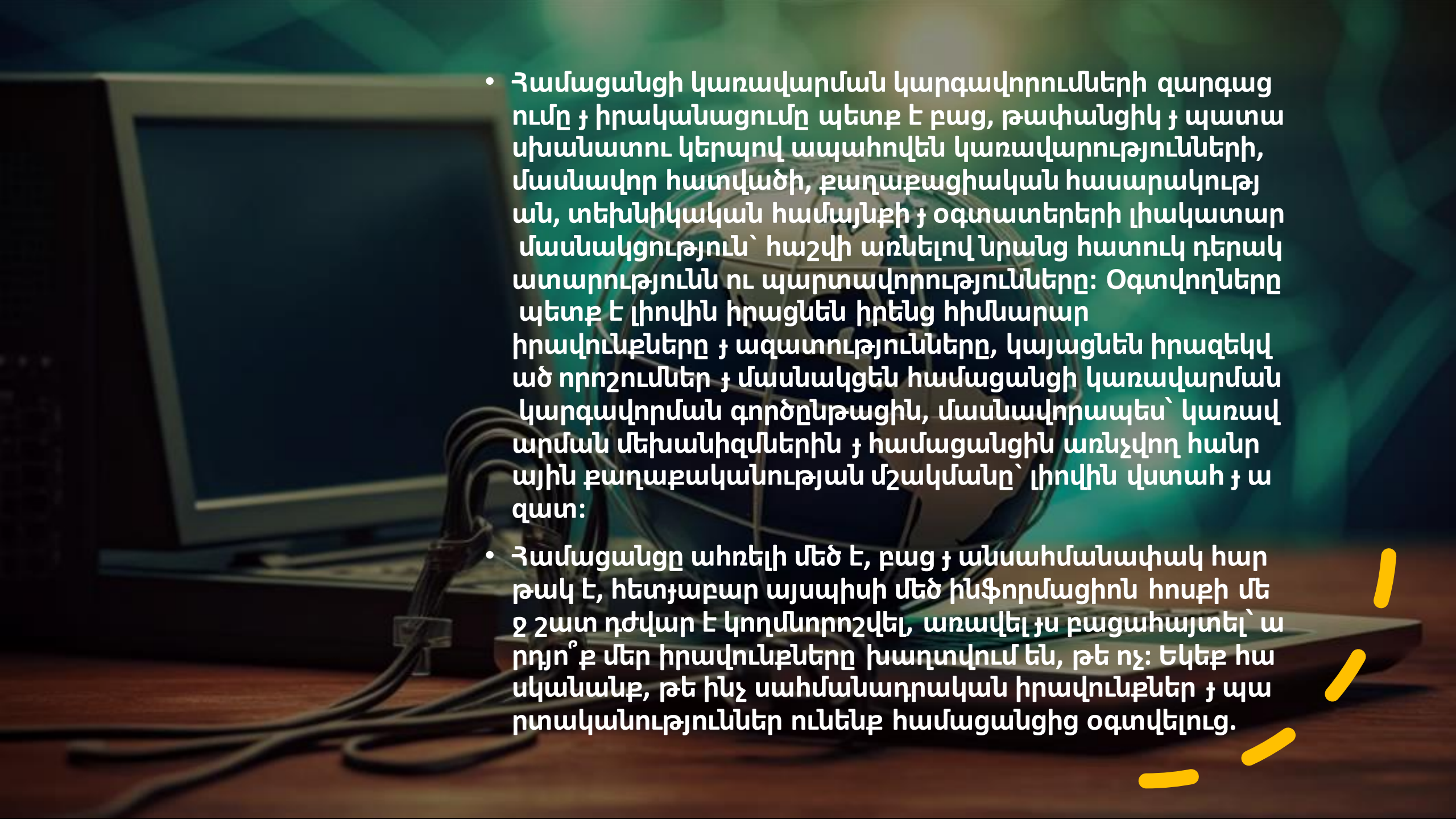
• Այսպիսով՝ որոշեցինք ուսումնասիրել թեման, բացահայտել մեր իրավունքների հնարավոր խաղտումները, բացահայտել, թե ինչպես կարող ենք պաշտպանվել:

Իմ հրավումքները համացանցում

- Կառավարությունները պետք է մեծ դերակատարում ունենան, երբ խոսքը ցանցային բովանդակության և երեխաների պաշտպանության, ռասիզմի դեմ պայքարի, ատելության և կիբեռհանցագործության հրահրման մասին է: Հարցն այն չէ՝ արդյոք կառավարությունները պե՞տք է կարգավորեն համացանցը, թե՞ ոչ, այլ թե ինչպե՞ս, ի՞նչ և ի՞նչ ծավալով բովանդակություն պետք է կարգավորվի: Արդյոք պետական կարգավորումն արդյունավե՞տ է, եթե ոչ, ապա կա՞ն այնպիսի մեթոդներ, որոնք կարող են ավելի արդյունավետ լինել:
- Համացանցի օգտագործման ցանկացած սահմանափակում օրինական է, եթե համապատասխանում է միջազգային նորմերին և չափանիշներին, որոնք անհրաժեշտ են ժողովրդավարական հասարակությանը և սահմանված են օրենքով: Պարտադիր գտումը և արգելափակումը համարվում են գերսահմանափակում



- Համացանցից գրագետ օգտվելու համար կիրառելի է ցանցային գրագիտություն տերմինը: Ցանցային գրագիտությունը մեդիա կրթության արդյունք է, որն օգտատերերին հնարավորություն է տալիս ողջամիտ որոշումներ կայացնելու համացանցի օգտագործման վերաբերյալ, գնահատելու առցանց տեղեկատվության ճշգրտությունն ու հնարավոր շեղումը և պաշտպանելու անչափահասներին հնարավոր վնասակար բովանդակությունից:
- Մասնագետներն էական դեր ունեն ավանդական մեդիակրթությունը ցանցային գրագիտությանը կամրջելու գործում, հատկապես որ հասարակությունը գնում է դեպի մեդիա հարթակների միավորում: Ոչ պաշտպանական մոտեցումը կարյոր նշանակություն ունի ուսանողներին մեդիա գրագիտության ապահովման աշխատանքումներգրավելու համար:
 - Երիտասարդությունը պետք է հզորացնի ցանցում սեփական գործողությունների մասին խելամիտ դատողություններ անելու կարողությունները: Կրթված ուղեղը լավագույն գտիչն է:
- Համաձայն մարդու միջազգային իրավունքների՝ համացանցի կառավարման կարգավորումները պետք է երաշխավորեն բոլոր հիմնարար իրավունքների և ազատությունների պաշտպանություն և հաստատեն իրենց համընդհանրությունը, անբակտեիությունը, փոխկախվածությունը և փոխշաղկապվածությունը: Դրանք պետք է խոր հարգանք երաշխավորեն նաև ժողովրդավարության և օրենքի գերակայության հանդեպ և խթանեն կայուն զարգացումը: Հանրային և մասնավոր բոլոր դերակատարները պետք է ընդունեն և պաշտպանեն մարդու հիմնարար իրավունքներն ու ազատություններն իրենց գործողություններում և գործունեության շրջանակներում, ինչպես նաև նոր տեխնոլոգիաների, ծառայությունների և դրանց կիրառության համատեքստում: Նրանք պետք է իրազեկ լինեն այն զարգացումներին, որոնք հանգեցնում են հիմնարար իրավունքների և ազատությունների ընդլայնմանը, ինչպես նաև դրանց վտանգներին և իրենց լիարժեք մասնակցությունն ունենան այն գործին, որի նպատակը նոր ձյավորվող իրավունքների ընդունումն է:



- Համացանցի կառավարման կարգավորումների զարգացումը ֆիրականացումը պետք է բաց, թափանցիկ ֆատասխանատու կերպով ապահովեն կառավարությունների, մասնավոր հատվածի, քաղաքացիական հասարակության, տեխնիկական համայնքի ֆօտատերերի լիակատար մասնակցություն՝ հաշվի առնելով նրանց հատուկ դերակատարությունն ու պարտավորությունները: Օգտվողները պետք է լիովին իրացնեն իրենց հիմնարար իրավունքները ֆազատությունները, կայացնեն իրազեկված որոշումներ ֆմասնակցեն համացանցի կառավարման կարգավորման գործընթացին, մասնավորապես՝ կառավարման մեխանիզմներին ֆհամացանցին առնչվող հանրային քաղաքականության մշակմանը՝ լիովին վստահ ֆազատ:

- Համացանցը ահռելի մեծ է, բաց ֆանսահմանափակ հարթակ է, հետոյաբար այսպիսի մեծ ինֆորմացիոն հոսքի մեջ շատ դժվար է կողմնորոշվել, առավել ֆաբացահայտել՝ արդյո՞ք մեր իրավունքները խաղտվում են, թե ոչ: Եկեք հասկանանք, թե ինչ սահմանադրական իրավունքներ ֆպարտականություններ ունենք համացանցից օգտվելուց.

Իրավունքներ

- Արժանապատվության նկատմամբ հարգանքի իրավունք
 - Վիրավորանք
 - Չրպարտություն
- Յեղինակային և հարակից իրավունքներ
 - Քաղվածքներ
 - Գրագողություն
- Անձնական տվյալների հրապարակում
 - Անուն, ազգանուն
- Աուտենտիկական տվյալների հրապարակում
- Անձնական և ընտանեկան կյանքի վերաբերյալ տեղեկությունների հրապարակում
 - Ինտիմ կյանքի վերաբերյալ տվյալներ
 - Բժշկական տվյալներ
 - Պատկերը պաշտպանելու իրավունք
 - Անոնիմ մնալու իրավունքը
 - Մոռացված լինելու իրավունք

Պարտականություններ

- Ապահովություն
 - Ապահովել երկխոսության գաղտնիությունը
 - Կարողանալ տարբերել համացանցային վիրուսներն ու չտարածել դրանք
- Գաղտնիություն
 - Կարգավորել անձնական տվյալների տրամադրման գործընթացը համացանցում
 - Էթիկա
 - Չվիրավորել համացանցից այլ օգտվողներին
 - Գրառումներ անելիս օգտագործեք ձեր անձնական էջը
 - Ակտիվություն
 - Ապահովեք ակտիվություն սոցցանցերում

Թվային աշխարհում մեր իրավունքների ոտնահարումը

- **Անօրինական մուտք գործելը:** Այս խմբի հանցագործությունները ներառում են համակարգչային համակարգ առանց թույլտվության մուտք գործելը տվյալների ձեռքբերման կամ որչիցե այլ անազնիվ նպատակով:
- **Անօրինական եղանակով հաղորդակցությունը գաղտնի որսալը:** Այս խմբի հանցագործությունները ներառում են համակարգչային կապի միջոցների օգտագործմամբ համակարգչային համակարգ մտնող, դուրս եկող եւ համակարգ(չ)ի մեջ գտնվող տվյալների ոչ հրապարակավ կատարվող փոխանցումները որսալը տեխնիկական միջոցների կիրառմամբ:
- **Միջամտություն տվյալների մեջ:** Այս խմբի հանցագործությունները ներառում են այնպիսի գործողություններ, ինչպիսիք են համակարգչային տվյալները վնասելը, ոչնչացնելը, փչացնելը, փոփոխելը կամ արգելելը:
- **Սարքերի չարաշահում:** Ներառում է վերը շարադրված հանցագործությունների կատարման նպատակով սարքը, համակարգչային ծրագիր վաճառելը, օգտագործելը, ներմուծելը կամ այլ կերպ հայթայթելը:



Համացանցից անվտանգ օգտվելու մշակույթը

- Ե՛վ լրատվամիջոցների, չ՛ քաղաքացիական հասարակության ներկայացուցիչներն ակտիվորեն օգտվում են ինչպես համակարգչային սարքերից, այնպես էլ համացանցից: Մշտապես առցանց հասանելիություն ապահովելու համար լրագրողներն ու քաղաքացիական հասարակության ներկայացուցիչները ձգտում են ունենալ շարժական այնպիսի համակարգչային սարքեր, ինչպիսիք են նոութբուքը, պլանշետը և սմարթֆոնը: Անձնական սարքերին զուգընթաց, օգտագործում են նաև աշխատանքային համակարգիչները:
- Աշխարհում օգտատերերի կեսից ավելին աշխատում է Windows օպերացիոն համակարգով (ՕՅ): Մեծ տոկոս են կազմում նաև Android ՕՅ-ով աշխատող սարքերը: Քիչ չեն iOS և Mac օպերացիոն համակարգերից օգտվողների թիվը: Չնչին է բաց կոդով գրված ՕՅ-ից օգտվողների թիվը: Իսկ նման ծրագրերը լիցենզիա չեն պահանջում, հետևաբար անվճար են:
- Համացանցից օգտվելու ժամաքանակի աճման միտումն ակնհայտ է: Օրվա առնվազն 1/3 մասն անցնում է Էկրանի առջև: Օգտատերերն օնլայն են սնվելիս, երթեկելիս, աշխատանքային քննարկումների ժամանակ, իսկ քնելուց առաջ սիրելի սմարթֆոնները պարտադիր «տեղավորում են բարձի տակ»: Արդյոք սա չի՞ նշանակում, որ կյանքն այս սիմբիոզ է՝ բաղկացած իրական և վիրտուալ պահերից, չ լինում են պահեր, երբ դժվար է տարանջատել իրականը վիրտուալից:
- Լրագրողների եւ քաղհասարակության ներկայացուցիչների համար վիրտուալ աշխարհում հաղորդակցվելու կամ տեղեկատվություն հաղորդելու, սպառելու և պահպանելու հիմնական միջոցները համարվում են սոցիալական ցանցերը, լրատվական կայքերն ու էլփոստերը: Արդյունքում՝ յուրաքանչյուրն այսօր ունի մի քանի էջ սոցիալական տարբեր կայքերում, մի քանի էլիասցե՝ էլեկտրոնային փոստային ծառայություններում և դրանք օգտագործում է տարբեր նպատակներով:
- Թվային դարաշրջանում շատ կարեւոր են նոր մեդիա տեխնոլոգիաներից օգտվելու հմտությունները, սակայն կրկնակի կարյոր անվտանգ օգտվելու կարողությունը հաշվի առնելով օրեցօր ավելացող կիբերհանցագործության ցուցանիշները: Համակարգչային սարքերում հակավիրուսային ծրագրերի առկայությունը դեռ բավարար չէ համոզված լինելու համար, որ համակարգչային սարքը և դրանում առկա տեղեկատվությունը պաշտպանված են:

- Համակարգչային սարքի անվտանգությունն ապահովելու համար անհրաժեշտ է հետոյել մի շարք կանոններ: Իսկ ոչ բոլորն են, որ հետեւում են դրանց: Օրինակ`
- համակարգչային սարքեր մուտք գործելը պաշտպանված չէ գաղտնաբառով,
- համակարգչային սարքերից ազատ օգտվում են հարազատները, այդ թվում` երեխաները, ովքեր կարող են համացանցից ներբեռնել ցանկացած ծրագիր զուգահեռաբար տարատեսակ վիրուսներ,
- ոչ միշտ են կայքերում աշխատանքն ավարտելիս` վերջում սեղմում «Դուրս գալ» (Log out) հրահանգը:
- Քանի որ նշվել էր, որ ՉԼՄ (Չանգվածային լրատվության միջոցներ) կամ ՀԿ (Հասարակական կազմակերպություն) ոլորտների ներկայացուցիչների անձնական համակարգչային սարքերն օգտագործվում են նախ գործնական նպատակներով, դա նշանակում է, որ տվյալ սարքում պահվող այլ անձանց կամ կազմակերպություններին վերաբերող տվյալների գաղտնիությունը վտանգված է, եթե անվտանգության տեսանկյունից անփույթ են օգտվում
- Թերյս չկա մեկը, ով բացառեր երբէ է իր սարքերում օտար, անցանկալի ծրագրի կամ վիրուսի հայտնաբերումը: Սա նշանակում է, որ աշխարհում բոլոր օգտատերերն առնվազն մեկ անգամ եղել են կիբերհանցագործության զոհ: Այսպիսով կիբերհարձակումներն իրականացվում են յուրաքանչյուրի նկատմամբ` անկախ պաշտոնական դիրքից, զբաղվածությունից և սոցիալական կարգավիճակից: Հաշվի առնելով կիբերհանցագործությունների ավելացումն ու կատարելագործումը` թիրախավորված հարձակումներն ավելի հաճախակի կդառնան:
- Ցանկացած տեղեկություն, որը կարող է հավելյալ միջոց դառնալ կիբերհանցագործների համար անձի եւ նրան շրջապատող հարազատների անվտանգությունը խախտելու նպատակով` գտնվելու վայրը, ընտանեկան կարգավիճակը, երեխաների անունները, ուսման եւ հանգստի վայրերը, կոնտակտային տվյալները և այլն, պետք է գերծ պահել համացանցից:
- Կիբերհանցագործության օրինակները, որոնք տեղի են ունեցել բջջային հեռախոսների միջոցով, թե՛ զանգվածային բնույթ չեն կրում, սակայն մտահոգության տեղիք են տալիս: Անկախ այն բանից նման գործողությունների հետոյում կանգնած են ներքին թե արտաքին ուժեր, մեկ մարդ թե կազմակերպված խումբ մի բան հստակ է. Հայաստանի քաղաքացին ևս այս մեծ սարդոստայնում գտնվում է կիբերհանցագործների թիրախում, որին զոհ չդառնալու համար անհրաժեշտ են բարձր զգոնություն և մշտապես լրացվող գիտելիքներ տեղեկատվական անվտանգության ոլորտի վերաբերյալ:

Ինչպես ապահովել երեխաների անվտանգությունն առցանց տիրույթում

- Ապահովեք նրա անվտանգությունը՝ անկեղծ գրույցի միջոցով: Անկեղծ խոսեք երեխայի հետ այն մասին, թե ում հետ և ինչպես կարող է շփվել: Համոզվեք, որ նա հասկանում է բարյացակամ և աջակցող շփումների կարգորությունը, և որ չարամիտ, խտրական և անպատշաճ շփումները երբեք ընդունելի չեն:
- Պաշտպանեք նրան տեխնոլոգիաների միջոցով: Ստուգեք, թե որքանով է երեխայի համապատասխան սարքը համալրված ամենավերջին ծրագրային ապահովմամբ և հակավիրուսային ծրագրերով: Հավաստիացեք նաև, որ գաղտնիության պաշտպանիչ կարգավորումները միացված են: Ծածկեք վեբ-տեսախցիկները, երբ դրանցից չեք օգտվում: Ավելի փոքր տարիքի երեխաների դեպքում, այնպիսի գործիքները, ինչպիսիք են՝ ծնողական հսկողության ծրագրերը, այդ թվում՝ ապահով որոնումները, կարող են օգնել համացանցային գործունեությունը դրական դարձնելու գործում:
- Նրա հետ ժամանակ անցկացրեք թվային աշխարհում: Ձեր երեխայի համար ստեղծեք ընկերների, ընտանիքի և անձամբ ձեզ հետ առցանց շփվելու ապահով և դրական հնարավորություններ: Ուրիշների հետ կապը պահպանելը առավել, քան երբեք, կարգավորվում է այս ժամանակներում, և դա կարող է ձեզ համար հիանալի հնարավորություն լինել՝ «վիրտուալ շփումներում» բարություն և սրտացավություն դրսևորելու լավ օրինակ ծառայել:



- Խրախուսեք առցանց տիրույթում դրսևորվող առողջ սովորությունները: Խթանեք յ հսկեք առցանց յ տեսազանգերի ժամանակ երեխաների պատշաճ վարքը: Քաջալերեք, որ երեխան բարի յ հարգալից լինի դասընկերների հետ, հաշվի առնի, թե ինչ հագուստ պետք է կրի, յ տեսազանգերին չմիանա, օրինակ՝ իր ննջարանից: Քանի որ երեխաները առցանց տիրույթում ավելի շատ ժամանակ են անցկացնում, նրանք կարող են ավելի շատ տեսնել այնպիսի գովազդներ, որոնցում գովազդվում են անառողջ սնունդ, գենդերային կարծրատիպեր կամ տարիքին ոչ հարիր նյութեր:

- Թույլ տվեք գվարճանալ յ ինթնադրսխորվել: Տանը ժամանակ անցկացնելը կարող է հիանալի հնարավորություն լինել երեխայի համար՝ սեփական տեսակետն արտահայտելու յ ճգնաժամի ընթացքում աջակցության կարիք ունեցողներին օգնելու առումով: Չմոռանաք առցանց գործունեությունը հնարավորինս հավասարակշռել իրական գործունեությամբ, այդ թվում՝ դրսում զբոսանքներով:





Օգտակար խորհուրդներ մեր անվտանգությունն ու իրավունքները պաշտպանելու համար



- Մի սեղմեք կասկածելի հղումների վրա: Մի բացեք հղումներ էլեկտրոնային փոստից, SMS-ից կամ հաղորդագրություններից սոցիալական ցանցերում, եթե վստահ չեք անվտանգության հարցում:
 - Անձնական տեղեկատվության պաշտպանություն: Խուսափեք անձնական տեղեկությունների փոխանակումից անվստահելի առցանց աղբյուրների հետ: Նախքան տվյալներ մուտքագրելը ստուգեք կայքերի անվտանգությունը:
- Օգտագործեք ուժեղ գաղտնաբառ: Օգտագործեք բարդ գաղտնաբառեր՝ բաղկացած տառերից, թվերից փոխառյալներից: Որպես գաղտնաբառ մի օգտագործեք անձնական տվյալները, ինչպիսիք են անունները, ծննդյան ամսաթիվը կամ հեռախոսահամարը:



- **Չգույշ եղեք հանրային Wi-Fi-ից օգտվելիս: Ստուգեք կապի անունը ֆ հաստատեք IP հասցեն հանրային ցանցի գտնվելու վայրի աշխատակցի հետ:**

- **Օգտագործեք հակավիրուս ֆ թարմացրեք ձեր օպերացիոն համակարգը: Տեղադրեք հակավիրուս՝ ձեր սարքը չարամիտ ծրագրերից պաշտպանելու համար, պարբերաբար թարմացրեք այն ֆ բուն սարքի օպերացիոն համակարգը**

- **Չգուշացում սոցիալական ցանցերում: Չգույշ եղեք սոցիալական ցանցերում ձեր հրապարակած տեղեկատվության նկատմամբ: Չափազանց շատ անձնական տեղեկություններ մի բացահայտեք:**

- **Սոցիալական մեդիայի հարթակներում կարող ես գեկուցել (report it): Եթե սոցիալական մեդիայի հարթակներում որիե բան ես կարդացել կամ տեսել, որից վրդովվել ես կամ վիրավորվել, ապա կարող ես գեկուցել (report it) դրա մասին:**

- **Տեղադրեք հավելվածներ պաշտոնական խանութներից: Ներբեռնեք հավելվածները միայն պաշտոնական հավելվածների խանութներից, ինչպիսիք են Google Play-ը Android-ի համար կամ App Store-ը iOS-ի համար:**

