ԾՆՈՂԱԿԱՆ ՈՒՂԵՑՈՒՅՑ

ԵՐԵԽԱՆԵՐԻ ԱՌՑԱՆՑԱՅԻՆ ԱՊԱՀՈՎՈՒԹՅՈՒՆԸ

European Commission

MEDIA EDUCATION

ins@fe

World Vision Armenia

LIBERTYGLOBAL

Աջակցությամբ

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

Ա. Ինչպե՞ս օգտագործել այս հավաքածուն էջ 4

Բ. Ուղեցույց ծնողների և մանկավարժների համար էջ 5

1. Անվտանգությունը ապահովության գրավականն է էջ 6
2. Հաղորդակցություն էջ 10
3. Կիբերհետապնդում էջ 15
4. Զվարճանք և ներբեռնում էջ 17

Գ. Վարժությունների համար առաջարկվող լուծումներ էջ 21

1. Անվտանգությունը ապահովության գրավականն է էջ 21
2. Հաղորդակցություն էջ 24
3. Կիբերհետապնդում էջ 26
4. Զվարճանք և ներբեռնում էջ 27

Դ. Բառարան էջ 29

Ե. Օգտակար հասցեներ էջ 39

Ա. Ինչպե՞ս օգտագործել այս հավաքածուն

Եթե մեկ տարվա համար ես ծրագրում, բրինձ ցանի՛ր:
Եթե տաս տարվա համար ես ծրագրում, ծառ տնկի՛ր:
Եթե ամբողջ կյանքի համար ես ծրագրում, երեխայիդ կրթի՛ր:

Չինական առակ

Հարգելի ծնող

Համացանցային ապահովության խնդիրների լուսաբանմանը նվիրված հավաքածուն նախատեսված է 6-12 տարեկան երեխաներ ունեցող ընտանիքների համար :

Այս կրթական ռեսուրսը ստեղծվել է այն խորին համոզմամբ, որ նոր տեխնոլոգիաները պետք է միավորեն, այլ ոչ թե բաժանեն սերունդները: Այն կառուցվել է Insafe Համացանցի ապահովության իրազեկման ազգային կենտրոնների համաեվրոպական ցանցի փորձի հիման վրա: Հավաքածուի մշակմանն ու թողարկմանը օժանդակել է UPS կազմակերպությունը:

Խաղահրապարակում խաղալու և փողոց անցնելու նման, համացանց և բջջային տեխնոլոգիաներ օգտագործելը նույնպես կարող է վտանգավոր լինել: Բարեբախտաբար, կան գործիքներ, որոնք օգնում են իմանալ համացանցում նավարկելու օգուտների և ռիսկերի մասին:

Նոր հավաքածուն կօգնի սովորեցնել ձեր երեխաներին, թե ինչպես ապահով և արդյունավետ օգտագործել համացանցը: Հավաքածուն պարունակում է համացանցային ապահովությանը նվիրված ավելի քան հիսուն օգտակար խորհուրդներ և վարժություններ, որոնք կօգնեն զվարճալի և պատկերավոր եղանակով սովորեցնել ձեր երեխաներին: Այն ներառում է.

- էլ-ապահովությանը նվիրված 2 գիրք. Ընտանեկան ուրախ ձեռնարկ և Ծնողական ուղեցույց,
- ոսկե կանոններ,
- ընտանեկան վկայական,
- տիպերի (sticker) հավաքածու;
- 12 իրավիճակային քարտեր

Ընտանեկան ու ծնողական ձեռնարկները գունավորմամբ կոդավորված են էլ-ապահովության չորս հիմնական թեմաները լուսաբանելու համար. Ապահովություն, Հաղորդակցություն, Զվարճալիքներ և ներբեռնում, Կիբերհետապնդում: Ծնողական ուղեցույցը՝ Ընտանեկան ուրախ ձեռնարկը լրացնող ռեսուրս է, որը պարունակում է լրացուցիչ տեղեկություններ, ինչպես նաև վարժությունների և իրավիճակային քարտերի համար առաջարկվող լուծումներ:

Ծնողական ուղեցույցը նախատեսված է ծնողների ու երեխաների համատեղ օգտագործման համար:

Չորս թեմաները ներկայացվում են երկու երեխաների՝ Ալեքսի ու Աննայի, նրանց ծնողների ու համակարգչային գիտունիկի՝ Հեդվիգի միջոցով:

Յուրաքանչյուր գլուխ պարունակում է ուսումնական գործունեության համար նախատեսված առցանց վարժություններ, վիկտորինաներ, ոսկե կանոններ, օգտակար հղումներ և այլն:

Կարդացեք պատմությունը բարձրաձայն ձեր երեխաների հետ և միասին կատարեք առաջադրանքները: Ձեր երեխաների հետ քննարկում սկսելու և բովանդակությունը ավելի լավ հասկանալու համար, կարող եք օգտագործել յուրաքանչյուր գլխի վերջում տրված համապատասխան իրավիճակային քարտերը:

Երբ ձեր երեխաները հաջողությամբ կվերջացնեն աշխատանքը նյութերի հետ, պարգևատրեք նրանց: Այնուհետև ընտանիքի բոլոր անդամները պետք է ստորագրեն վկայականի տակ: Վերջում երեխաները կարող են ձեռնարկները զարդարել տիպերով:

Կարևոր է ձեր կապը մեզ հետ: Դիմեք Insafe հայաստանյան կենտրոնին՝ հարցերի ու մեկնաբանությունների համար:

Ձեզ և ձեր ընտանիքի անդամներին ուրախ և ապահով նավարկություն ենք մաղթում:

MEDIA EDUCATION

ins@fe

Բ. Ուղեցույց ծնողների և մանկավարժների համար

1. Անվտանգությունը ապահովության գրավականն է

ԵԹԵ ՏԱՆԸ ՈՒՆԵՔ ՀԱՄԱԿԱՐԳԻՉ

Համակարգիչը տանը կարող է հզոր կրթական ու ստեղծագործական միջոց դառնալ ընտանիքի բոլոր անդամների համար: Տեղադրելով համակարգիչը հյուրասենյակում, կամ ընտանիքի բոլոր անդամների համար հասանելի և հարմար այլ տեղում, անպայման մշակեք համընդհանուր օգտագործման կանոններ. ցուցարկիչի առջև ժամանակ անցկացնելու ու պայմանների մասին: Դրանով դուք կօգնեք ընտանիքի կրտսեր անդամներին շատ ավելի ապահով լինել համացանցում:

Երեխաները կարող են համացանցից օգտվել ընկերների մոտ, համացանցային սրճարաններում և այլն: Այդ պատճառով շատ կարևոր է, որ միասին հաստատեք ապահով ու անվտանգ այնպիսի վարվելակերպ ու կանոններ, որոնք մշտապես ու ամենուր կկիրառվեն:

ԱՊԱՀՈՎՈՒՄ ԵՆՔ ՀԱՄԱԿԱՐԳՉԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ

Անվտանգությունը ապահովվում է հնարավոր վտանգների իմացությամբ և պարզ միջոցների կիրառմամբ: Իսկ լավագույն միջոցները օգտակար տեխնոլոգիական գործիքներն ու մեր ողջամտությունն են: Սակայն նման ամեն ինչին, վերջինս զարգանում է տարիքին ու փորձին զուգընթաց:

Հիշողության կրիչների և **սկավառակների (CD-ROM)** օգտագործումը, **կից ֆայլերի** բացումը կամ **ֆայլերի ներբեռնումը** ռիսկեր են պարունակում: Դրանք կապված են վնասակար համակարգչային ծրագրերի **(malware)** հետ, որոնք ստեղծվում են համակարգիչները վնասելու, անձնական տվյալները գողանալու և հրապարակելու համար:

Ձեռնարկում ներկայացված են վնասակար ծրագրերի տեսակները՝ **վիրուսները**, **որդերը**, **Տրոյական ձիերը** և **լրտես ծրագրերը**, ինչպես նաև վարակված համակարգչի ախտանիշները:

Երեխաները կսովորեն, թե ինչպես արդիական հակավիրուսային ու հակալրտեսային ծրագրերով կանխել համակարգչի վարակումը: Նրանց նաև խորհուրդ է տրվում զգույշ լինել, անծանոթ հասցեներից ստացված էլեկտրոնային նամակները բացելու, համացանցից ծրագրեր ներբեռնելու, USB հիշողության կրիչներ կամ CD-ROM սկավառակներ օգտագործելու ժամանակ:

ՊԱՅՔԱՐՈՒՄ ԵՆՔ ՓՈՍՏԱՂԲԻ ԴԵՄ

Համացանցում շրջանառվող էլեկտրոնային նամակների 80 %-ը **փոստաղբ** է (spam, անցանկալի նամակներ): Պատահմամբ գրելով ձեր **էլեկտրոնային հասցեն նորությունների խմբերում, զրուցարանում (chat), ֆորումներում, սոցիալական ցանցերում** կամ **առցանցային ձևաթղթերում** (on-line form), կարող եք փոստաղբի թիրախ դառնալ:
Հատուկ ծրագրաշարերով համացանցից հավաքվող էլեկտրոնային հասցեների վրա ուղարկվում է ահռելի քանակությամբ փոստաղբ:
Նման գործերում ներգրավված ընկերությունները հաճախ տեղակայված են այնպիսի երկրներում, որտեղ չկա անցանկալի նամակների առաքումը կանխարգելող օրենսդրություն:

Այդպիսի նամակները մեծամասամբ անպարկեշտ ծանոթությունների, կասկածահարույց ֆինանսական գործառույթների, դեղերի գնման առաջարկներ են: Ավելին, փոստաղբը կարող է լինել նաև վնասակար ծրագրերի աղբյուր: Փոստաղբը հիմնականում առաքվում է խարդախ նպատակներով:

Ձեր ընտանիքի պաշտպանության համար առաջարկում ենք՝

- Օգտագործել փոստաղբի ֆիլտրեր (փոստաղբային զտիչներ): Էլեկտրոնային փոստ տրամադրող ընկերությունը սովորաբար առաջարկում է հակափոստաղբային միջոցներ, որոնք պետք է ակտիվացնել: Առավել մանրամասն տեղեկատվության համար կապվեք նրանց հետ: Դարբերաբար ստուգեք junk (աղբ) կամ spam (փոստաղբ) թղթապանակները տեսնելու համար արդյո՞ք նորմալ նամակները չեն հայտնվել այնտեղ: Տեխնոլոգիան այնքան էլ կատարյալ չէ և հնարավոր է spam (փոստաղբ) թղթապանակում հայտնվեն նաև ձեր բարեկամների ուղարկած նամակները:
- Սովորեցնել երեխաներին չբացել անծանոթներից ստացված նամակները: Փոստաղբը համարյա միշտ պարունակում է հրավերներ և կից ֆայլեր: Ցույց տվեք նրանց՝ ինչպես արգելափակել ուղարկողին կամ խնդրեք առանց բացելու ջնջել կասկածելի նամակները:

ՆԱՎԱՐԿԵԼՈՎ ՀԱՄԱՑԱՆՑՈՒՄ

Նույնիսկ շատ փոքր երեխաները կարող են զվարճանալ և սովորել համացանցում: Սակայն, համացանցը առաջարկում է նաև բազմապիսի և անչափահասների համար չնախատեսված բովանդակության նյութեր:

Որոնման համակարգերը հրաշալի միջոց են համացանցում որևէ բան գտնելու համար: Բայց, քանի որ որոնումը կախված է հիմնաբառերի ընտրությունից, հեշտ է նաև անցանկալի բովանդակություն հանդիպելը: Անմեղ թվացող հիմնաբառերը կարող են բերել ոչ պատշաճ բովանդակությամբ կայքեր: Ստորև կան որոշ խորհուրդներ, որ կօգնեն ձեր երեխաներին առավել ապահով նավարկել համացանցում:

- Ստեղծեք օգտվողի անհատական գրանցում ձեր երեխայի համար և օգտագործեք ծնողական հսկողությունը ակտիվացնող ծրագրեր ունեցող Windows կամ Linux, Mac OS **օպերացիոն համակարգեր**:
- Ստուգեք ծնողական հսկողության գործառույթները ձեր **համացանցային զննարկիչի** (browser) և որոնման համակարգի վրա: Համոզվեք, որ դուք գիտեք **ընտանեկան ապահովության** համար նախատեսված բոլոր **կարգավորումները**,
- Ձեր խնամքի տակ գտնվող անչափահասներին առաջարկեք օգտագործել երեխաների համար նախատեսված **որոնման համակարգեր**: Օրինակ՝ http://kids.yahoo.com, http://www.askforkids.com;
- Երեխաների ամենահաճախ այցելած կայքերի հասցեները պահպանեք **նախընտրելի** (favorite) թղթապանակներում (զնարկիչը ունի նման հնարավորություն): Այդպիսով դուք կօգնեք նրանց առանց որոնման համակարգի օգնության այցելել իրենց սիրելի կայքերը:

Ակտիվացնելով ծնողական հսկողությունը ձեր զննարկիչի և որոնման համակարգի վրա, դուք կարող եք օգտագործել լրացուցիչ **ֆիլտր** (զտիչ)՝ ծրագրային ապահովում, որի նպատակն է ցանցում վահանի պես պաշտպանել երեխաներին անցանկալի բովանդակությունից: Խորհրդակցեք մասնագետի հետ կամ փնտրեք համացանցում փորձնական ժամանակահատվածով **ծրագրաշարեր**:

Հիշեք, որ ոչինչ չի կարող փոխարինել ձեր կամ մանկավարժների կողմից երեխաների ուղղորդումը: Տեխնիկական միջոցները կատարյալ չեն և եթե չզուգակցվեն առողջ դատողությամբ, կարող են ստեղծել ապահովության կեղծ զգացողություն:

Զտող (ֆիլտրող) ծրագրաշարը կարող է այնքան սահմանափակումներ առաջացնել, որ արգելափակի նաև անմեղ բովանդակությունը: Այն կարող է, օրինակ, արգելափակել Երկրորդ համաշխարհային պատերազմի մասին տեղեկատվությունը, քանի որ փնտրտուքը տանում է բռնություն նկարագրող էջեր:

Ավելին, ցանկացած ֆիլտր, որն ակտիվացնում են մեծահասակները, կարող է նաև անջատվել խելացի պատանիների կողմից, ովքեր հաճախ իրենց հետքերը վերացնելու մեծ վարպետներ են: Դուք կարող եք իմանալ այդ մասին, եթե սովորեք օգտագործել համակարգիչն ու հմապատասխան ծրագրաշարերը:

Այցելեք SIP-Bench կայք-էջը (տես Օգտակար հղումներ), ուր հրապարակված է Եվրոպական Հանձնաժողովի օժանդակությամբ իրականացված հետազոտական ծրագիրը:

Ծրագրի շրջանակներում ուսումնասիրվել է ծնողական վերահսկողության և հակափոստաղբ 30 գործիքների արդյունավետությունը: Դրանք կիրառվել են 6-16 տարեկան երեխաներին վնասակար բովանդակությունից պաշտպանելու գործում՝ զննարկման, էլեկտրոնային նամակագրության, ֆայլերի փոխանակման և ակնթարթային հաղորդակցման ընթացքում:

Խուսափելով վնասակար բովանդակությունից՝ պետք է նաև համոզված լինեք, որ երեխաները չեն հավատում այն ամենին, ինչ տեսնում կամ կարդում են համացանցում: Ընտանեկան ուրախ ձեռնարկում մենք առաջարկում ենք նրանց այցելել առնվազն երեք կայք-էջ՝ համեմատելու համար ցանցում որոնվող տեղեկույթը: Նրանց նաև խորհուրդ է տրվում հանձնարարությունները կատարելիս նշել գտած տեղեկույթի աղբյուրը:

ՈՍԿԵ ԿԱՆՈՆՆԵՐ ՆԱՎԱՐԿՈՂ ԵՐԵԽԱՆԵՐԻ ԾՆՈՂՆԵՐԻ ՀԱՄԱՐ

- Համոզվեք, որ ձեր համակարգիչը ապահովված է հրապատով (fi rewall) , ինչպես նաև հակավիրուսային ու հակալրտեսային ծրագրաշարով: Թարմացրեք այդ ծրագրերը և հետևեք դրանցից եկող ազդանշաններին: Ստուգեք, արդյո ք ձեր ինտերնետային ծառայության մատուցողը առաջարկում է հակավիրուսային և հակալրտեսային գործիքներ, որ կարող եք օգտագործել:
- Օգտագործեք փոստաղբային զտիչ (ֆիլտր) և հնարավորինս գաղտնի պահեք ձեր էլեկտրոնային հասցեն՝ այն վերում չհրապարակելով: Խուսափեք անծանոթների կողմից ուղարկված էլեկտրոնային նամակներից և անպայման զննեք այն, եթե այնուամենայնիվ որոշել եք բացել:
- Օպերացիոն համակարգի, համացանցային զննարկիչի, որոնման համակարգի և էլեկտրոնային փոստ ծրագրերի համար առավելագույնի հասցրեք ծնողական վերահսկողության կարգավորումները: Երեխաների համար ստեղծեք օգտվողի անհատական գրանցումներ: Համոզվեք, որ գաղտնիության կարգավորումները ամենաբարձր աստիճանի վրա են (այցելեք ձեր զննարկչի ,,options/ընտրանք,, հրահանգացանկը):
- Օգտագործեք լրացուցիչ ֆիլտրող ծրագրաշար:
- Կապվեք մասնագետի հետ, երբ ձեր համակարգիչը սկսում է վատ աշխատել. այն կարող է վարակված լինել: Ինտերնետային ծառայության մատուցողը նույնպես պետք է կարողանա խորհրդատվություն տրամադրել:
- Համացանցում անցանկալի բովանդակության հանդիպելիս, զեկուցեք ազգային համացանցային թեժ գծին (տես Օգտակար հղումներ):
- Հնարավորության դեպքում նստեք երեխաների կողքին, երբ նրանք նավարկում են համացանցում: Դա լավագույն ձևն է քննարկելու և վստահություն նվաճելու համար: Միասին սովորելը դարձրեք ձեր նպատակը:
- Հիշեք, որ անվտանգության կանոնները ձեր ու ձեր երեխաների համար են: Քաջալերեք նրանց ասել այն ամենի մասին, ինչն իրենց տարօրինակ է թվում:

ՕԳՏԱԿԱՐ ՀՂՈՒՄՆԵՐ

Երեխաները կարող են էլ-ապահովության դասընթաց անցնել և հետևել Webwise կայքում Նիամի և Ֆիոնի առցանց արկածներին. *http://www.webwise.ie/index.aspx*

Գիտելիքը ապահով նավարկելու բանալին է. Իմացեք ռիսկերը, իմացեք ինչպես պաշտպանվել և ձգտեք իմանալ ավելին: Մանրամասներին կարելի է ծանոթանալ makeITsecure վեբ կայքում. *http://www.makeitsecure.ie*

Եթե համացանցում նավարկելիս հանդիպում եք ապօրինի կամ ոչ պատշաճ բովանդակության, խնդրում ենք հաղորդագրություն ուղարկել Հայաստանի թեժ գիծ ծառայությանը. *http://www.safe.am*

Եվրոպական Հանձնաժողովի օժանդակությամբ իրականացված SIP-Bench հետազոտական ծրագիրը. *http://www.sip-bench.org*

2. Հաղորդակցվում ենք

ԳԼՈՒԽԿՈՏՐՈՒԿԻ ՄԱՍԵՐԸ

Հիշու՞մ եք, թե որքան կարևոր էր ձեզ համար ընկերների հետ շփումը, երբ դուք փոքր էիք: Համացանցը ընկերներին հանդիպելու բազմաթիվ հնարավորություններ ունի և առաջարկում է ինքնարտահայտման և հասարակական կյանքին ներգրավվելու նոր եղանակներ՝ էլեկտրոնային նամակագրության, ֆայլերի փոխանակման, բլոգների և սոցիալական ցանցերի միջոցով (ինչպիսիք են՝ MySpace, Facebook, Hi5, Habbo-hotel): Նոր տեխնոլոգիաների միջոցով պատանիներն ընդգրկվում են ծնողական հսկողությունից անկախ և ազատ տարածության մեջ:

«Հաղորդակցություն» գլուխը ծնողներին ու երեխաներին ծանոթացնում է հետևյալ հասկացությունների հետ՝ **անձնական տվյալներ**, **մասնավոր կյանքի գաղտնիություն** (մասնավորություն), դրական առցանց փոխգործակցություն, ռիսկերի կառավարում, մասնավորապես, անծանոթների հետ շփումներ:

Առցանց գաղտնիությունը սերտորեն կապված է **հաշիվների** և **անձնական էջերի** հետ:

Հաշիվ գրանցելու շնորհիվ առցանց ծառայությունը հասանելի է դառնում:

Արտացանցային կյանքում ավտոբուսի անցաթուղթը կամ մարզադահլիճի անդամատոմսը պարունակում են անհատական ինֆորմացիա ձեր մասին: Առցանց հաշիվները և ծառայությունները նույնպես: Դուք դրանք չեք ստանա, մինչև որոշ անհատական տվյալներ չներկայացնեք ձեր անձնական էջի համար: Շատ կարևոր է, որ ինքներդ կարողանաք ընտրել ձեր մասին տրամադրվող տվյալները և այն անձանց, ում համար ձեր էջը հասանելի է դառնում:

Մասնավոր կյանքի գաղտնիության պահպանումը կարգավորելու, այլ ոչ թե կեղծելու նպատակ ունի:

Երիտասարդներին ոգևորում է ընկերների հետ առցանց շփվելու հնարավորությունը և նրանք ստեղծում են իրենց վիրտուալ կերպարը: Սակայն նրանք միշտ չէ, որ գիտակցում են, թե ինչի կարող է հանգեցնել անձնական տվյալների հրապարակումը:

ՍՏԵՂԾՈՒՄ ԵՆՔ ԱՆՁՆԱԿԱՆ ԷՋ

Անձնական տվյաների պաշտպանության առաջին քայլը պետք է լինի ապահով անձնական էջի (նկարագիր, profi le) ստեղծումը: Անհրաժեշտ է նախապես որոշել հրապարակվող անձնական տվյալների ծավալը և գաղտնիության կարգավորման աստիճանը:

Տարբեր համացանցային համատեքստերի համար ստեղծեք տարբեր էլեկտրոնային հասցեներ: Օրինակ, զրուցարանի, ակնթարթային հաղորդակցության կամ բլոգի համար երեխային քաջալերեք օգտագործել չեզոք էլեկտրոնային հասցե և **մականուն**: Այս ձևով զրուցող երեխան չի օգտագործի իր ամբողջ անունը բացահայտող էլեկտրոնային հասցե:

Գաղտնաբառը պետք է գաղտնի պահել: Համոզվեք, որ երեխաները իրենց անձնական էլ.հաշիվների և հասցեների գաղտնաբառերը չեն ասում իրենց ընկերներին. վերջիններս կարող են նաև չարաշահել **նրանց վստահությունը**:

Մյուս կողմից, դուք պետք է որ ցանկանաք իմանալ ձեր երեխաների գաղտնաբառերը, որպեսզի կարողանաք վերահսկել նրանց փոստարկղերը: Խոսեք այդ մասին նրանց հետ: Մի մոռացեք կարգաբերել ձեր անձնական էջի/հաշվի գաղտնիության կարգավորումները: Ընտրեք մասնավոր, այլ ոչ թե հանրային կարգավորման եղանակ: Այս եղանակով դուք հսկում եք ձեր տեսանելիությունը և փոխգործակցությունը: Կառավարեք ձեր- **հասցեացանկը**: Սովորեցրեք երեխաներին ընդունել այն մարդկանց առաջարկները, ում ճանաչում են արտացանցային կյանքում:

Եթե երեխաները օգտվում են զրուցարաններից, ստուգեք.

- զրուցարան **վարողների** (մոդերատորներ) առկայությունը: Վարող չլինելը անապահով միջավայրի մասին է խոսում,
- անցանկալի զրուցընկերներին մերժելու կամ արգելափակելու միջոցների առկայությունը,
- վեբ կայքում օգնության և **ահազանգելու** գործառույթի առկայությունը,
- ծառայության կանոնները հստակությունն ու տեսանելիությունը:

ՆԿԱՐՆԵՐ ԵՎ ՎԵԲ ԽՑԻԿՆԵՐ

Երեխաները պետք է հասկանան, որ թվանշային նկարներն իրենց մասնավոր կյանքի անբաժան մասն են և բացառիկ ուժ ունեն: Դրանք հեշտ են շրջանառվում ու մեքենայությունների ենթարկվում, բացի այդ շատ դժվար են ջնջվում:
Եթե նկարը անգամ մեկ անգամ ուղարկվել է համակարգչի կամ բջջային հեռախոսի միջոցով, ապա այն հավերժ կարող է մնալ է առցանցում:
Երեխաները առանց հսկողության չպետք է օգտագործեն վեբ խցիկները: Դրանց զրուցարանային գործիքների և տեղեկատուների օգտագործումը կարող է ռիսկային լինել:
Դուք և ձեր երեխաները պետք է անձնական նկարներ փոխանակեք նրանց հետ ում գիտեք և վստահում եք. միշտ թույլտվություն պահանջեք, երբ ուրիշի նկար եք հրապարակում: Մի թույլատրեք ձեր երեխաներին օգտագործել համակարգիչ և վեբ խցիկ, երբ միայնակ են իրենց սենյակում:

ՀԱՂՈՐԴԱԿՑՈՒԹՅՈՒՆՆ ԱՆԾԱՆՈԹՆԵՐԻ ՀԵՏ

Համացանցային նոր ծանոթները միշտ չէ, որ այնպիսին են, ինչպիսին ներկայանում են: Սովորեցրեք ձեր երեխաներին աչալրջորեն պահպանել իրենց մասնավոր կյանքի գաղտնիությունը՝ ինչպես կանեին արտացանցային կյանքում: Դուք ունեք կանոններ, թե ինչպիսի վարքագիծ ունենան օտարների նկատմամբ իրական աշխարհում, ինչու՞ չհետևել նույն կանոններին համացանցում:
Ձեր երեխաները կարող են ամուր կապեր հաստատել իրենց առցանց ընկերների հետ և դյուրահավատորեն վստահել նույնիսկ անծանոթ մարդկանց:
Հետևաբար, նրանք կարող են գայթակղվել հանդիպելու այս նոր ընկերներին արտացանցային կյանքում՝ առանց ձեզ տեղեկացնելու: Երեխաները հաճախ չգիտակցելով այդ հանդիպումների վտանգը, հեշտությամբ դառնում է առցանց **գրումինգի** զոհեր (grooming – երեխայի հանդեպ սեռական ոտնձգություն կատարելու նպատակով վստահության ձեռքբերում, հուզական կապի հաստատում):
Ուսումնասիրությունները ցույց են տալիս, որ շատ երեխաներ առցանց «ընկերներին» հանդիպում են առանց ծնողներին տեղյակ պահելու: Քաջալերեք երեխաներին, որ ձեզ անպայման տեղյակ պահեն այդ հանդիպումների առաջարկների մասին:
Հաղորդակցությունը լավագույն բանալին է:

ՀԱՄԱՑԱՆՑԱՅԻՆ ԷԹԻԿԱՆ

Համացանցային էթիկայի, կամ ցանցային քաղաքավարության կանոնների համաձայն, այլ մարդկանց պետք է վերաբերվել այնպես, ինչպես կցանկանայիք, որ վերաբերվեն ձեզ: Երեխաները հնարավոր է չհասկանան, որ համացանցում կարող են պատահաբար վիրավորել ինչ որ մեկին: Ցավոք, շատերը համացանցը կամ բջջային հեռախոսը օգտագործում են ուրիշներին նեղացնելու կամ վիրավորելու համար: Յուրաքանչյուր չորս երեխաներից մեկը **կիբերհետապնդման** (cyber-bullying՝ համացանցի, բջջային հեռախոսի կամ այլ կապի միջոցներով վիրավորական տեքստի տարածում) թիրախ է դառնում:

ԶՐՈՒՅՑԱՐԱՆԻ ԼԵԶՈՒՆ

Առցանց զրույցի ընթացքում երիտասարդներն օգտագործում են **էմոթիկոններով** և **հապավումներով** լի յուրահատուկ լեզու: 😀

Համացանցային զրույցի հիմնական հապավումներն են.

121: անհատական շփում

AFK: հեռու ստեղնաշարից

A/S/L: տ/ս/վ տարիք, սեռ, վայր (տսվ)

BBB: հաջող բալիկս

B4N: առայժմ

BBL: հետո կգամ

BF: ընկեր կամ ամենալավ ընկեր

BFF: հավերժ լավագույն ընկեր

C: կտեսնվենք

Comp: համակարգիչ

CU: կտեսնվենք

CUL: հետո կտեսնվենք

CYO: ցանցում կտեսնվենք

EGBOK: ամեն ինչ լավ կլինի

F2F: դեմ առ դեմ

JJ: կատակում եմ

K: ամեն ինչ լավ է/ լավ

KFY/K4Y: համբուրում եմ

KISS: պարզեցրու, հիմար

KPC: ծնողներից թաքուն

L8R: հետո

IRL: իրական կյանքում

LMIRL: արի հանդիպենք իրական կյանքում

LOL: շատ ծիծաղելի է, մեծ սիրով

LY4E: հավերժ սիրով

NE1: որևէ մեկը

NP: հարց չկա/ աղմկոտ ծնողներ

OIC: օ, տեսնում եմ

OLL: առցանցային սեր

PAL: ծնողներս լսում են

G2G կամ GTG: պետք է գնալ

<G>: ժպիտ

GFN: բացակա են այս պահին

GL: ամենայն հաջողություն

GM: բարի լույս

HAND: լավ ժամանակ անցկացնեք

^5: ժեստ, որը նշանակում է «լավ աշխատեցիր»

H2G: պետք է գնամ

HDOP: օգնեք ջնջել առցանց գիշատիչներին

IDK: չգիտեմ

ILU/ILY: Ես քեզ սիրում եմ

PAW: ծնողները տեսնում են, հետևում են

PIR: սենյակում ծնող/մարդ կա

POS: ծնողս թիկունքում է

RL: իրական կյանք

S^, S'UP: Ի՞նչ է պատահել

TTYL: կզրուցենք ավելի ուշ

TY: շնորհակալություն

WB: վերադարձիր, պատասխանիր

WDYT: ի՞նչ ես կարծում

WTGP: Ուզու՞մ ես առանձնանանք

WYCM: Ինձ կզանգե՞ս

Դուք կարող եք էմոթիկոններ ստեղծել համադրելով կետադրական նշանները և տառերը, տես ստորև բերված օրինակները

Ժպտացող դեմք (քթով կամ առանց քթի)	:) կամ : -) վերջակետ, (գծիկ), փակագիծ
Տխուր դեմք (քթով կամ առանց քթի)	:(կամ :-(վերջակետ, (գծիկ), փակագիծ
Թարթող աչքերով դեմք (քթով կամ առանց քթի)	;) կամ ;-) Կետ ստորակետ, (գծիկ), փակագիծ
Զարմացած դեմք (քթով կամ առանց քթի)	: o կամ :-o վերջակետ, (գծիկ), փոքրատառ կլոր o
Մեծ ժպիտ (քթով կամ առանց քթի)	:-D կամ : D վերջակետ, (գծիկ), մեծատառ D
Լեզուն հանած (քթով կամ առանց քթի)	: p կամ :-p վերջակետ, (գծիկ), փոքրատառ p

ՈՍԿԵ ԿԱՆՈՆՆԵՐ

- 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. ակտիվացրած մասնավորության կարգավորումներով,
  - պահպանելով իրենց գաղնաբառերը,
  - հաղորդակցվելով և պատասխանելով միայն այն մարդկանց, ում ճանաչում են արտացանցային կյանքում,
  - 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,
- տեղադրեք ընտանեկան համակարգիչը այնպիսի տեղում, որ կարողանաք վերահսկել նրանց առցանցային զբաղմունքները;
- միասին համոզվեք, որ գիտեք, ընկերության առաջարկները մերժելու և արգելափակելու գործառույթները
- անվտանգության և ահազանգելու գործառույթները, որ առկա են օգտագործվող կայքերում;
- ձեռք բերեք երեխաների վստահությունը, քաջալերեք նրանց խոսել ձեզ հետ իրենց սխալների մասին և միասին փնտրեք լուծումները: Սխալները սովորելու անբաժան մաս են կազմում:

ՕԳՏԱԿԱՐ ՀՂՈՒՄՆԵՐ

«Հսկիր տարածքդ» պատանիների ու երիտասարդների համար նախատեսված Webwise internet safety նախաձեռնության մի մասն է, որի նպատակը համացանցի երիտասարդ օգտվողներին աջակցելն է.
http://www.watchyourspace.ie

Կարծում եք՝գիտեք. ծնողների համար.
http://www.thinkuknow.co.uk/parents

Բացեք զրույցի ծածկագիրը այցելելով wikiHow.
http://www.wikihow.com/Understand-Chat-Acronyms

Երեխաների համար ավելի ապահով ինտերնետ Եվրոբարոմետրի 2007թ. զեկույց
http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Կիբերհետապնդում

ԿԻԲԵՐՀԵՏԱՊՆԴՄԱՆ ՄԻՋԱԴԵՊ

Հաղորդակցությունը համացանցի և բջջային հեռախոսների միջոցով ունի բազմաթիվ հետաքրքիր առավելություններ: Ցավոք, այն կարող է նաև հրաշալի չլինել. երեխաները կարող են ստանալ կամ ուղարկել այնպիսի բովանդակությամբ հաղորդագրություններ, որ վիրավորում են իրենց կամ ուրիշների արժանապատվությունը: Կարևոր է, որ երեխաները սովորեն հասարակության համար ընդունելի վարվելակերպի՝ մեր սեփական երեխաներն էլ միշտ չէ, որ հրեշտակներ են ;-)

Կիբերհետապնդումը նոր տեղեկատվական ու հաղորդակցային տեխնոլոգիաների և ծառայությունների օգտագործումն է՝ անհանգստացնելու եւ ահաբեկելու համար անհատին կամ խմբին:

Կարող են օգտագործվել էլ.փոստը, զրուցարանը, ակնթարթային հաղորդակցությունը, բջջային հեռախոսը կամ այլ թվային գործիքները: Վիրտուալ խաղային միջավայրերում, կիբեր խուլիգանները կարող են վնասել ձեր երեխայի ավատարին. կրակել նրա վրա, գողանալ կամ էլ ստիպել, որ նա անցանկալի վարվի:

Սովորաբար, երեխաների խնդիրները կապված են հասարակական վայրերում անձնական տեղեկությունների բացահայտման հետ: Դպրոցական կամ բակային խուլիգանության նման, այդպիսի վարքը ընդունելի չէ և ծնողները, ուսուցիչները և երեխաները պետք է զգոն և պատրաստ լինեն արձագանքելու: Ի տարբերություն «ավանդական» հետապնդման՝ կիբերհետապնդումը կարող է ազդել երեխայի վրա, երբ հետապնդողը արդեն ներկա չէ: Օրինակ, խուլիգանները կարող են սպառնալից հաղորդագրություններ ուղարկել ընտանեկան էլ.փոստին և բջջային հեռախոսներին օրվա ցանկացած ժամի:

Ծնողները կարող են օգնել ստեղծելու այնպիսի վիրտուալ միջավայր, ուր ագրեսիվ վարվելակերպը չի հանդուրժվում. սովորեցրեք երեխաներին, որ անանուն լինելը համացանցում չի նշանակում անպատասխանատու լինել: Նրանք պետք է իմանան իրենց իրավունքներն ու պարտականությունները և միաժամանակ հարգեն այլ մարդկանց իրավունքները:

Միշտ անկեղծորեն երեխաների հետ քննարկեք բոլոր անհանգստացնող իրավիճակները: Համացանցը և բջջային հեռախոսները կարող են հրաշալի հնարավորություն ընձեռել դրա համար:

ՈՍԿԵ ԿԱՆՈՆՆԵՐ

- Պահպանեք երեխաներին բացասական փորձից, հավաստիացեք, որ նրանք պահպանում են սեփական մասնավորությունը և հարգում են ուրիշներինը:

- Սովորեցրեք երեխաներին չարձագանքել սպառնալից հաղորդագրություններին,
- Օգնեք երեխաներին հասկանալ, թե որ հաղորդագրությունները և ինչպիսի վարքագիծը կարող են հակազդեցություն առաջացնել եւ բացասական զգացմունքներ պատճառել: Սովորեցրեք խուսափել դրանցից:
- Համոզվեք, որ նրանք գիտեն՝ ինչպես արգելափակել անցանկալի հասցեատերերին:
- Պահպանեք վիրավորական նամակները. հնարավոր է դրանց կարիքը զգաք որպես կարևոր ապացույց:
- Պարզեք ձեր երեխայի դպրոցում ընդունված ագրեսիվ վարքագծի դեմ պայքարելու ռազմավարությունը: Խուլիգանությունից և կիբեր հետապնդումներից խուսափելու համար աշխատեք այլ ծնողների և ուսուցիչների հետ:
- Մտեք ձեր երեխաների միջավայր, ճանաչեք նրանց ընկերներին, ընկերների ծնողներին, ուսուցիչներին ու դասընկերներին:
- Խրախուսեք երեխաներին պատմել ձեզ յուրաքանչյուր անհանգստացնող ցանցային և արտացանցային փորձառության մասին: Վստահեցրեք նրանց, որ եթե նրանք նույնիսկ անզգույշ են վարվել, դուք իրենց կողքին եք և միասին լուծում կգտնեք:
- Համոզվեք, որ երեխաները հասկանում են, որ երբեք չեն մեղադրվի, երբ ինչ որ մեկը անհանգստացնում է իրենց:

ՕԳՏԱԿԱՐ ՀՂՈՒՄՆԵՐ

Այս հայտնի առցանց կայքում դուք կգտնեք տեղեկություններ դպրոցներում կիբեր հետապնդումների մասին և թե ինչպես կարող է դրանց վերջ տրվել:
http://www.nehb.ie/coolschoolbullyfree/kids1.htm

Այս կայքում դուք կգտնեք կիբերհետապնդումների մասին մուլտֆիլմեր և դրանց դեմ պայքարի խաղեր: *http://www.stopbullying.org*

241580 կամ (080) 06 11 11 թեժ գիծը 24-ժամյա ծառայություն է անչափահասների համար: *https://www.safe.am/*

4. Զվարճանք եվ ներբեռնում

ԻՆՉ ՓԱՅԼՈՒՄ Է, ՈՍԿԻ ՉԷ

Համացանցը նաեւ բազմապիսի առևտրային գործունեության վիրտուալ տարածություն է: Եթե դուք թույլ չեք տալիս երեխաներին ունենալ այն ամենը, ինչ գրավում է նրանց ուշադրությունը հեռուստատեսային գովազդներում կամ խանութներում, ապա պետք է նաև սովորեցնեք չհավատալ համացանցում գովազդվող բազմապիսի պարագաների եւ առցանցային ծառայությունների առաջարկներին:

Երեխաների հետ համացանցում նավարկելիս հնարավորություն ունեք բացատրելու, որ զանգի մեղեդիները, պաստառները, mp3 ֆայլերը, ավատարները և այլն, հազվադեպ են անվճար լինում: Երբ էլ գտնեք այդպիսի գովազդներ, ցույց տվեք, որ համացանցում ամեն ինչ հալած յուղի տեղ չընդունեն:

Ցանկացած ծառայության բաժանորդագրվելու համար դուք պետք է լրացնեք առցանց ձևաթուղթ: Դրանք լրացրեք միայն այն դեպքում, երբ համոզված եք, որ ձեր անձնական տվյալները չեն օգտագործվի ձեզ ի վնաս: Երեխաներին սովորեցրեք առանց ձեր գիտության չօգտագործել այդ էլեկտրոնային փաստաթղթերը:

Դուրս լողացող (pop-up) **պատուհանները** հաճախ օգտագործվում են տարբեր իրերի վաճառքի համար: Դրանք միշտ չէ, որ վատն են, կախված է նրանից, թե ինչպիսի հուսալի թե անհուսալի վեբ կայքից են հայտնվել: Եթե վստահում եք կայք-էջին, ապա կարող եք վստահել նաև դուրս լողա ցող **(pop-up)** պատուհանին:

Այնուամենայնիվ, որոշ դուրս լողացող **(pop-up)** պատուհաններ օգտագործվում են անվստահելի ապրանքի վաճառքի համար, կամ էլ առաջնորդում են դեպի անաձնական տվյալների լրացում պահանջող առցանցային հարցաշարեր:

Սովորոցրեք երեխաներին փակել անհուսալի դուրս լողացող **(pop-up)** պատուհանները՝ սեղմելով վերին աջ անկյունի կարմիր խաչի վրա:

ԱՌՑԱՆՑ ԽԱՂԵՐ

Առցանցային խաղերը տարբերվում են ավելի հին՝ թվային խաղերից, որովհետև պահանջում են համացանցային **կապ**: Երեխաները կարող են խաղերը բացել CD/DVD սկավառակների, համացանցի համապատասխան **կայք-էջերի**, խաղային կոնսոլների կամ բջջային հեռախոսների վրա:

Առցանցային խաղերը լինում են պարզ՝ Pacman-ի կամ Tetris-ի տիպի և բարդ՝ վիրտուալ իրականության խաղեր, որտեղ մի քանի խաղացողներ միասին ստեղծում են նոր բովանդակություն և պատմություններ:
Այդպիսի **բազմաթիվ մասնակիցներով խաղերը** աջակցում են խաղացողների վիրտուալ համայնքների ձևավորմանը: Դա կարող է ռիսկային իրավիճակներ ստեղծել երեխաների արտացանցային կյանքում անծանոթ մարդկանց հետ հանդիպելու պատճառով (տես Հաղորդակցություններ գլուխը):

Խաղերը մեծ դեր ունեն երեխաների զարգացման մեջ, քանի որ սոցիալական հմտություններ և ռազմավարական մտածողություն են զարգացնում: Շատ թվային խաղեր գրավիչ են ու ինտերակտիվ և օգտագործվում են կրթական նպատակներով:

Այնուամենայնիվ, ոչ բոլոր խաղերն են լավ որակի: Դուք պետք է որոշեք, ինչպիսի խաղերն են հարմար ձեր երեխային և կանոններ մշակելով՝ երաշխավորեք, որ համացանցային խաղերին հատկացվող ժամանակը չի խանգարում ձեր երեխայի մյուս զբաղմունքներին:

Ինտերակտիվ խաղերի համար մշակվել է PEGI on-line համաեվրոպական տարիքային սանդղակ, որը դասակարգում է խաղերը ըստ տարիքի և բովանդակության: Համակարգին օժանդակում են շատ արտադրողներ, որոնց թվում են PlayStation, Xbox և Nintendo, ինչպես նաև ինտերակտիվ խաղերի մշակողներ և հրատարակիչներ ամբողջ Եվրոպայից: Անպայման ուշադրություն դարձրեք գնվող խաղի հատկանիշների վրա, միաժամանակ հիշելով որ բոլոր 12-ամյա երեխաները նման չեն միմյանց:

ՈՍԿԵ ԿԱՆՈՆՆԵՐ

- Համոզվեք, որ օրինական կայք եք օգտագործում համացանցից երաժշտություն ու ֆիլմեր ներբեռնելու համար:
- Քաջալերեք ձեր երեխաներին օգտվել այն կայքերից, որոնք առաջարկում են օրինական բովանդակություն և բացատրեք, որ ցանցում ամեն ինչ այն չէ, ինչ թվում է:
- Բացատրեք ցանցից նյութերի անփույթ ներբեռնման ռիսկերը:
- Համոզվեք, որ ձեր համակարգիչը պաշտպանված է և միշտ օգտագործեք թարմացված հակավիրուսային ծրագրեր:
- Սովորեցրեք երեխաներին պահպանել օրինական ներբեռնված ֆայլերը կոշտ սկավառակների վրա և նախքան բացելը սկանավորեք:
- Միշտ կարդացեք անձնական տվյալների պաշտպանության մասին դրույթները և օգտվողի համաձայնագիրը: Համացանցում ստուգեք ներբեռնվող ծրագրի հուսալիությունը:
- Փակեք անհուսալի դուրս լողացող (pop-up) պատուհանները սեղմելով վերին աջ անկյունի կարմիր խաչի վրա: Երբեք մի սեղմեք ներսին:

ԵՐԵԽԱՆԵՐԸ ԵՎ ԽԱՂԵՐԸ

- Կարգ սահմանեք երեխայի խաղալու ժամանակի վրա:
- Նրանք պետք է խաղան վերահսկելի սենյակում:
- Հսկեք ձեր երեխաների խաղային սովորույթները. եթե դուք վերահսկում եք նրանց խաղահրապարակում, ապա ինչու չանել նույնը, երբ նրանք խաղում են վիրտուալ միջավայրում:
- Քննարկեք խաղի բովանդակությունը, ո՞ր հատկանիշներ են իրականության նման և որը՝ ոչ, ի՞նչ են նրանք սիրում:
- Նախքան ձեր երեխայի համար խաղ գնելը, համոզվեք, որ խաղի բովանդակությունը տարիքին համապատասխան է (համաեվրոպական PEGI համակարգ կամ որևէ ազգային չափանիշային/չափման համակարգ)

Երբ ձեր երեխան խաղում է առցանցային խաղեր բազմաթիվ խաղացողների հետ

- Ընտրեք կայքեր խիստ կանոններով ու ակտիվ հսկիչներով/մոդերատորներով:
- Զգուշացրեք նրանց չտալ իրենց անձնական տվյալները ուրիշ խաղացողների:
- Զգուշացրեք նրանց չհանդիպել այլ խաղացողների արտացանցային կյանքում, եթե դուք չեք մասնակցում հանդիպմանը:
- Քաջալերեք ձեր երեխաներին տեղեկացնել հետապնդումների/ագրեսիվ դրսևորումների, սպառնալիքների, անպարկեշտ բառերի, անցանկալի բովանդակությամբ նյութերի ցուցադրության կամ խաղից դուրս հանդիպման հրավերների մասին:
- Դուրս բերեք ձեր երեխային խաղից կամ փոխեք նրա ID-ն, եթե ինչ-որ բան խաղի ընթացքում անհանգստության տեղիք է տալիս:

ՕԳՏԱԿԱՐ ՀՂՈՒՄՆԵՐ

Իմացեք ավելին առցանցային խաղերի և տարիքային PEGI համակարգի մասին
http://www.pegioline.eu

Կայք-էջեր, որտեղ կարող եք գնել օրինական երաժշտություն.
http://www.pro-music.org

Օգտակար գործիքներ զրուցարանում, փոխանակման կայքերում ու խաղերում իմաստանալու համար: Ինտերակտիվ դասեր, որ կարող եք ուսումնասիրել ձեր երեխաների հետ միասին.

http://www.webwise.ie/index.aspx

Իմաստավորիր TXT լեզուն transl8it կայքում.

http://www.transl8it.com

Կատարելագործիր ցանցային “lingo”-ն այցելելով.

http://www.netlingo.com

1. Գ. Վարժությունների համար առաջարկվող լուծումներ

ՎԱՐԺՈՒԹՅՈՒՆՆԵՐ

Յուրաքանչյուր բառի համար գտե՛ք ճիշտ անվանումը. համակարգչային իրան, մկնիկի տակդիր, բարձրախոս, ցուցարկիչ /դիսփլեյ, մոնիտոր/, վեբ խցիկ, տպիչ, USB կրիչ (կամ հիշողության կրիչ), մկնիկ, հիշողության սկավառակ (CD rom):

Նախավարժանք՝ ձեր երեխաներին համակարգչի և այլ սարքավորումների տարբեր մասերին ծանոթացնելու համար: Դուք կարող եք այն զարգացնել ձեր հայացողությամբ:

Խնդրե՛ք ձեր ծնողներին որպեսզի ձեզ ուղարկեն կից հաղորդագրությամբ էլեկտրոնային նամակ կամ դա արե՛ք ինքներդ: Կատարե՛ք հետևյալ վարժությունը. մկնիկի աջ սեղմակի օգնությամբ այն պահե՛ք (Save) ձեր համակարգչի աշխատանքային սեղանին: Այդ փաստաթղթի վրա մկնիկի աջ սեղմակը պահելով՝ ընտրե՛ք scan (դիտել, զննել) հրահանգը: Երբ պարզեք, որ փաստաթուղթն ապահով է, բացեք այն: Հիշե՛ք, աջ սեղմակի հպումով կատարել ՊԱՀՊԱՆԵԼ, ԴԻՏԵԼ և ԲԱՑԵԼ (SAVE-SCAN-OPEN) հրահանգները:

Ուղարկե՛ք կից հաղորդագրությամբ նամակ ձեր երեխայի կամ ձեր անձնական հասցեին: Թողե՛ք, որ ձեր երեխաները հետևեն վարժության մեջ նշված ցուցումներին և պահպանեն փաստաթուղթը մկնիկի աջ սեղմակի օգնությամբ՝ առանց այն բացելու: Ֆայլը համակարգչի

աշխատանքային սեղանին կամ թղթապանակում, օրինակ, «Իմ փաստաղթերում» (My Documents) պահպանելուց հետո ցույց տվե՛ք երեխային՝ ինչպես փաստաթուղթը բացելուց առաջ աջ սեղմակի ևս մեկ հպումով զննել այն: Դուք այսպիսով կխրախուսեք ապահով գործելակերպ:

Հետևե՛ք Հելենի խորհրդին և սովորե՛ք՝ ինչպես նկարագրել ձեր էլեկտրոնային հասցեն, երբ ձեզ իսկապես հարկավոր է այն հրապարակել ցանցում: Դուք այսպիսով կխուսափեք փոստաղբ տարածողների անհարկի գրոհներից:

Որպեսզի փոստաղբ տարածող համակարգչային ծրագրերը ավտոմատ կերպով չգրանցեն ձեր էլեկտրոնային հասցեն, այն ոչ թե ճշգրտությամբ գրեք, այլ պարզապես նկարագրե՛ք: Թողե՛ք, որ ձեր երեխաները փորձեն կիրառել այս տեխնիկան վերը նշված եղանակով: Սակայն հիշե՛ք, որ երեխաները պետք է խուսափեն իրենց էլեկտրոնային հասցեն համացանցում հրապարակելուց կամ եթե հրապարակում են, օգտագործեն այնպիսի հասցե, որը չի բացահայտում նրանց անունը (տես Հաղորդակցում գլուխը):

Մինչև Հելենի կշարունակի, եկե՛ք օգնենք Աննային: Նայե՛ք վանդակում նշված գործողությունները և շրջանակի մեջ առե՛ք նրանք, որոնց իրականացումը հնարավոր է միայն համացանցին միացած լինելու դեպքում:

Եթե ձեր երեխաները շատ փոքր են, ապա կարող է հստակ չիմանան, թե գործունեության որ տեսակներն են պահանջում միանալ ցանցին և որոնք չեն պահանջում: Տեքստ գրելը չի պահանջում, որպեսզի համակարգիչը միացված լինի ցանցին, սակայն զրուցարանում հաղորդակցվելը պահանջում է: Դուք կարող եք համակարգչով լսել երաժշտություն՝ օգտագործելով սկավառակ կամ համակարգչում պահպանված երաժշտական ֆայլ, սակայն երաժշտություն կարող եք ունկնդրել նաև առցանց համակարգից: Ձեր երեխաները պետք է նշեն միայն գործունեության այն տեսակները, որոնց դեպքում ցանցին միանալը էական է:

Ծնողների հետ միասին համացանցային զննարկիչում հավաքե՛ք http://kids.yahoo.com հասցեն: Գտե՛ք տիրանոզավրի մասին տեղեկությունները և պարզե՛ք՝ երբ է այն բնակվել երկրագնդի վրա: Փորձե՛ք նաև գտնել տիրանոզավրի մի լավ նկար: Չմոռանաք համեմատել երեք տարբեր կայքերից ստացած տեղեկությունները:

Ձեր երեխաներին սովորեցրե՛ք որոնումներ կատարելու ճիշտ եղանակներ՝ հիշեցնելով նրանց, որ չպետք է վստահել համացանցում տեսած ամեն ինչի: Երեխաներին հիշեցրե՛ք, որ տեղեկատվություն որոնելու և համեմատություններ կատարելու համար հարկավոր է օգտվել առնվազն երեք կայքից և միշտ դպրոցական հանձնարարություն կատարելիս պետք է նշել համապատասխան աղբյուրը:

Ծնողների հետ միասին համացանցային զննարկիչում հավաքե՛ք http://kids.yahoo.com հասցեն: Այնուհետև որոնե՛ք տեղեկություններ, օրինակ Տիրոնազավրին վերաբերող: Ձեր նախընտրած երեք ամենահետաքրքիր կայքերը պահպանեք Favorites (Սիրելի կայքեր) ցանկում: Կարող եք նաև ստեղծել ձեր թղթապանակը:

Հետաքրքիր կայքերը Favorites թղթապանակում (զննարկիչի գործիքաշարի ընտրանք) պահպանելն ու դասակարգելը շատ լավ միջոց է, երեխաների մոտ համացանցում տեղեկատվություն փնտրելու անհրաժեշտությունը նվազեցնելու տեսանկյունից:

ԱՐԴՅՈ՞Ք ՃԻՇՏ ԵՔ ՀԱՍԿԱՑԵԼ

1: հակավիրուսային/հակալրտեսային ծրագիր 2: վիրուս, անծանոթ, ներբեռնեք, վարակված, հիշողության կրիչ, չպաշտպանված 3: տարօրինակ 4: անծանոթ, կից ֆայլեր, փոստաղբ 5: մեկ, փոստաղբի 6: առաջին իսկ, երեք, համեմատեք, յուրաքանչյուր մարդ, հրապարակել 7: հակավիրուսային և հակալրտեսային ծրագրերը 8: խոսեք, ծնողների 9: տեղեկացրեք

ԻՐԱՎԻՃԱԿԱՅԻՆ ՔԱՐՏԵՐԻ ՀԱՄԱՐ ԱՌԱՋԱՐԿՎՈՂ ԼՈՒԾՈՒՄՆԵՐ

Իրավիճակ 1. Երբեք մի նավարկեք համացանցում, եթե ձեր համակարգիչը պաշտպանված չէ թարմացված հակավիրուսային և հակալրտեսային ծրագրերով: Այն նման է առանց սահմանապահների սահմանի. ձեր համակարգիչը կարող է վարակվել վնասակար ծրագրերով, ինչպիսիք են վիրուսները, Տրոյական ձիերը, որդերը կամ լրտեսական ծրագրերը:

Իրավիճակ 2. Ուշադիր եղեք անծանոթ մարդկանցից ստացված կից հաղորդագրություններով էլեկտրոնային նամակների նկատմամբ, որ լի են խոստումներով՝ ամենայն հավանականությամբ դրանք փոստաղբ են: Փոստաղբը կարող է վարակել ձեր համակարգիչը վնասակար ծրագրերով, ինչպիսիք են վիրուսները, Տրոյական ձիերը, որդերը կամ լրտեսական ծրագրերը: Մի բացեք այդ էլ.նամակները: փոխարենը արգելափակեք ուղարկողին պահելով մկնիկի աջ կոճակը էլ.նամակի վրա և ընտրելով ‘Block sender’ (Արգելափակել ուղարկողին) հրահանգը կամ պարզապես ջնջեք այն:

Իրավիճակ 3. Երբ համացանցում որոնում եք կատարում, մի վստահեք անմիջապես առաջին իսկ պատահած կայքին: Ստուգեք առնվազն երեք տարբեր կայքեր և համեմատեք դրանցում գտած տեղեկույթը: Հիշեք՝ յուրաքանչյուր մարդ կարող է ստեղծել և տեղեկություններ հրապարակել համացանցում: Երբ զեկուցում եք գրում կամ հանձնարարություն եք կատարում, պետք է միշտ նշեք ձեր օգտագործված ինֆորմացիայի և նկարների աղբյուրը… արդպես կվարվեր իսկական գիտնականը:

2. Հաղորդակցվում ենք

ՎԱՐԺՈՒԹՅՈՒՆՆԵՐ

Նշե՛ք, թե հետևյալ տեղեկությունները որքանով են գաղտնի ձեզ համար. հեռախոսի համարը, մազերի գույնը, անունը, երկիրը, դպրոցը, հասցեն, ընտանի կենդանու անունը, ծնողների մասնագիտությունը, էլ. փոստը, նկարները, տարիքը:

Արդյո՞ք ձեր երեխաները անձնական տվյալների գաղտնիությունն ընկալում են այնպես, ինչպես՝ դուք: Նշված երեք գույները ցույց են տալիս թե արդյո՞ք տեղեկատվությունը խիստ գաղտնի է (կարմիր), բավականին գաղտնի (նարնջագույն) կամ ոչ այնքան գաղտնի (կանաչ):

Օգնե՛ք Աննային ստեղծել լավ գաղտնաբառ՝ հետևելով Հելենի հուշումներին:

Լավ գաղտնաբառերը պետք է բաղկացած լինեն պատահականորեն ընտրված տարբեր տառանշաններից (թվեր, տառեր և կետադրական նշաններ) և միշտ պետք է պահվեն գաղտնի:

Հետևելով Աննայի օրինակին՝ ստեղծե՛ք ապահով անձնական էջ: Այնուհետև ստեղծե՛ք այնպիսի անձնական էջ, որն ապահով չէ:

Թողե՛ք, որ ձեր երեխաները ստեղծեն մեկ ապահով և մեկ ոչ այնքան ապահով անձնական տեղեկությունները բացահայտող անձնական էջ: Հիշեցրե՛ք երեխաներին, որ ապահով անձնական էջ ստեղծելը չի պաշտպանի նրանց, եթե առցանց հաղորդակցման ժամանակ նրանք չպաշտպանեն իրենց անձնական տվյալների գաղտնիությունը:

Նկարագրե՛ք պատկերված մարդուն:

Նկարի վրա հիմնվելով՝ ի՞նչ անձնական տեղեկություններ կարելի է կորզել: Երեխաները հաճախ չգիտեն՝ որքան հզոր գործիք է նկարը:

Հիմնվելով Հելենի գաղափարների վրա՝ մտածե՛ք 3 այնպիսի խորհուրդների մասին, որն «Ալեքս կարմիր գլխարկը» կստանա Հելենից՝ համացանցային գայլերից պաշտպանվելու համար:

Պարզե՛ք արդյոք ձեր երեխաները հասկացել են, որ անծանոթների հետ առցանց հաղորդակցվելը կարող է վտանգավոր լինել:

Ինչպե՞ս կուզեիք, որ մարդիկ ձեզ հետ վարվեին առցանց համակարգում: (1….. 2….. 3…..):

Համոզվե՛ք, որ ձեր երեխաները հասկանում են, որ համացանցում այլ անձանց հետ պետք է վարվել այնպես, ինչպես կցանկանային, որ վարվեին իրենց հետ…

ԳԱՂՏՆԱԶԵՐԾԵ՛Ք ԿՈԴԸ. Գտե՛ք զրուցարաններում կիրառվող ամենատարածված բառային հապավումներից մի քանիսի իմաստը:

Կատերալագործե՛ք հապավումների ձեր իմացությունը՝ օգտվելով համացանցային էթիկայի և զրուցարանային լեզվին վերաբերող գլխից:

Ստեղնաշարի գրանիշների համադրությամբ պատկերե՛ք հետևյալ էմոթիկոնները՝ Ժպիտացող դեմք - Զարմացած դեմք - Տխուր դեմք – Մեծ ժպիտ - Թարթող աչքերով դեմք - Լեզուն դուրս հանած:

Ավելի մանրակրկիտ տեղեկությունների համար տե՛ս համացանցային էթիկայի և զրուցարանային լեզվի վերաբերյալ գլուխը:

ԱՐԴՅՈ՞Ք ՃԻՇՏ ԵՔ ՀԱՍԿԱՑԵԼ

1: Անձնական էջը 2: Մասնավորության, պատասխանատու 3: Անծանոթների, ասա 4: Համացանցային էթիկան, վարվել, վարվեին 5: Էմոթիկոնը 6: Գաղտնաբառը , կետադրական 7: Գաղտնի է 8: չեմ փոխանցում 9: ծանոթ

ԻՐԱՎԻՃԱԿԱՅԻՆ ՔԱՐՏԵՐԻ ՀԱՄԱՐ ԱՌԱՋԱՐԿՎՈՂ ԼՈՒԾՈՒՄՆԵՐ

ԻՐԱՎԻՃԱԿ 4. Երբ օգտագործում եք համացանցը, ձեր անձնական էջը կամ հրապարակված տեղեկությունները հասանելի են դառնում տասնյակ, հարյուրավոր կամ նույնիսկ հազարավոր մարդկանց: Այդ իսկ պատճառով կարևորվում է շատ ուշադիր ընտրել ձեր մասին հրապարակվող տեղեկությունները. Անհատական տեղեկություններ տվեք միայն այն մարդկանց ում վստահում եք և լավ եք ճանաչում արտացանցային կյանքում:

ԻՐԱՎԻՃԱԿ 5. Մայքը հավանաբար ասել է իր էլեկտրոնային փոստի գաղտնաբառը ընկերոջը, որը այնուհետև որոշել է վրեժ լուծել ընկերոջից և իր անունից զազրելի նամակներ է ուղարկել. Միշտ պահեք ձեր գաղտնաբառերը, եթե չեք ցանկանում, որ ուրիշները կարդան ձեր էլեկտրոնային նամակները կամ ձեր անունից ասեն այնպիսի բաներ , որ դուք երբեք չեիք ասի:

ԻՐԱՎԻՃԱԿ 6. Անծանոթ մարդու հանդիպելը այդքան էլ լավ գաղափար չէ. Սակայն եթե դուք կարծում եք, որ կարող եք վստահել ձեր համացանցային ընկերոջը եւ հանդիպել նրան, պատմեք ձեր ծնողներին այդ մասին, որպեսզի ծնողներից մեկը ուղեկցի ձեզ: Եթե ձեր ընկերը ազնիվ մտադրություններ ունի, նրա համար այս իրավիճակը խնդրահարույց չի լինի: Սա խնդիր է միայն այն մարդկանց համար, ով ինչ որ բան ունի թաքցնելու:

3. Կիբերհետապնդում

ՎԱՐԺՈՒԹՅՈՒՆՆԵՐ

Պատկերե՛ք այն հրավիրատոմսը, որն Ալեքսը ստացել է իր ուսուցիչներից: Ցույց տվե՛ք կիբերհետապնդումների դեմ շաբաթվա ընթացքում օգտագործվող հակահետապնդման խորհրդանշանը կամ կարգախոսը:

Թող երեխաները ստեղծագործեն և նկարեն դատարկ շրջանակում:

Հետևելով Ալեքսի օրինակին՝ նշե՛ք հինգ պատճառ, որոնք հիմք կհանդիսանան որևիցե մեկին կարմիր քարտ տալու համար:

Երեխաների հետ քննարկե՛ք, թե վարքագծի որ տեսակն են նրանք համարում անընդունելի:

ԱՐԴՅՈ՞Ք ՃԻՇՏ ԵՔ ՀԱՍԿԱՑԵԼ

1: արդար, փչացնում են 2: խոսելը 3: պարսավելի 4: կիբերհետապնդումը 5: արգելափակում եմ 6: ծանոթ 7: պատասխանում

ԻՐԱՎԻՃԱԿԱՅԻՆ ՔԱՐՏԵՐԻ ՀԱՄԱՐ ԱՌԱՋԱՐԿՎՈՂ ԼՈՒԾՈՒՄՆԵՐ

ԻՐԱՎԻՃԱԿ 7. Սա անշուշտ բջջային հեռախոսի օգտագործման ընդունելի ձև չէ: Մի տարածեք այն հաղորդագրությունները, նկարները կամ այլ նյութերը, որ կարող են վնաս պատճառել: Միշտ վերաբերվեք ուրիշներին այնպես ինչպես կցանկանայիք որ վերաբերվեին ձեզ: Նման իրավիճակում միշտ խոսեք ձեր ծնողների կամ այն մեծահասակների հետ, ում վստահում եք:

ԻՐԱՎԻՃԱԿ 8. Ալեքսը պետք է պատմի ընկերոջը, որ հետապնդողի վատ վարքագիծը իր մեղքը չէ: Նա չպիտի պատասխանի հետապնդողի հաղորդագրություններին, սակայն պահպանի դրանք որպես ապացույց ծնողներին կամ ուսուցիչներին ցուցադրելու համար: Ալեքսը նաև պիտի պատմի այս մասին ծնողներին, որոնք կարող են օգնել իր ընկերոջը:

ԻՐԱՎԻՃԱԿ 9. Նեթիկետի կամ ցանցային քաղաքավարության կանոնների համաձայն, այլ մարդկանց պետք է վերաբերվել այնպես, ինչպես կցանկանայիք, որ վերաբերվեն ձեզ: Վստահ ենք, որ դուք արդեն բավականին սովորել եք, որպեսզի օգնեք Աննային իր խնդրում:

4. Զվարճանք եվ ներբեռնում

ՎԱՐԺՈՒԹՅՈՒՆՆԵՐ

Բացե՛ք ձեր սիրելի որոնման համակարգը: Այնտեղ հավաքե՛ք free ringtones (անվճար հեռախոսազագերի երաժշտություն) արտահայտությունը և տեսե՛ք ինչպիսին կլինի ձեր որոնման արդյունքը: Ստուգեք մի քանի կայք-էջեր: Կարո՞ղ եք ինչ որ թակարդներ գտնել:

Կատարե՛ք վարժություններ՝ որոնելով գլխաբառերը և ստուգե՛ք՝ արդյո՞ք ձեր գտած կայքերում առկա է մարկետինգային թակարդ: Տեսե՛ք՝ ինչպես է մանր տառերով գրված տեղեկությունը բացակայում գովազդային կարգախոսներից:

Ո՞րն է քո սիրելի համակարգչային խաղը: Պարզիր՝ ծնողներդ գիտե՞ն արդյոք այդ մասին և կարո՞ղ են այն նկարագրել: Եթե նրանք ոչին չեն կարող հուշել, նախ նրանց բացատրի՛ր, իսկ հետո թո՛ղ, որ նրանք գրեն կարճ նկարագրություն: Արդյո՞ք ծնողներիդ համար ամեն ինչ պա՞րզ է:
Քանի միավոր կտաս նրանց 10 հնարավորից: …Այստեղ ծնողը պետք է տա երեխայի սիրելի խաղի կարճ նկարագիրը, իսկ երեխան այն նկարում է:

Դուք իսկապե՞ս տեղյակ եք՝ ինչ խաղեր են ձեր երեխաները խաղում առցանց և գիտե՞ք արդյոք՝ որն է նրանց սիրած խաղը: Թողե՛ք, որ երեխաները ստուգեն ձեր իմացությունը:

ԱՐԴՅՈ՞Ք ՃԻՇՏ ԵՔ ՀԱՍԿԱՑԵԼ

1: անվճար 2: ձևաթղթերը 3: թակարդ ընկնել 4: անօրինական 5: խաչը 6: մասնավորությունը 7: տարածել, ինքներդ 8: ներբեռնիր

ԻՐԱՎԻՃԱԿԱՅԻՆ ՔԱՐՏԵՐԻ ՀԱՄԱՐ ԱՌԱՋԱՐԿՎՈՂ ԼՈՒԾՈՒՄՆԵՐ

ԻՐԱՎԻՃԱԿ 10. Երաժշտության և ֆիլմերի մեծ մասը, որ գտնում եք համացանցում ապօրինի պատճեններ են: Բացի այդ, այն կայքերը, որոնց միջոցով մարդիկ փոխանակում են երաժշտություն կամ ֆիլմեր սովորաբար լի են վնասակար այնպիսի ծրագրերով, ինչպիսիք են վիրուսները, Տրոյական ձիերը, որդերն ու լրտեսական ծրագրերը: Աննայի համար լավագույն լուծումը կլինի ընտրել b կամ c տարբերակները: Իհարկե, վստահելի կայքից, ուր տեղադրված են օրինական երաժշտական ֆայլեր, երաժշտության ներբեռնումը

փոքր ինչ ավելի էժան կլինի, քան CD ձեռքբերումը: Լավ կլիներ, որ ծնողները հայտնեն իրենց կարծիքը և տան թույլտվություն:

ԻՐԱՎԻՃԱԿ 11. Համացանցում կան անվճար ծառայություններ, սակայն զանգերի մեղեդիները, պաստառները, MP3 ֆայլերը,ավատարներն ու նմանատիպ այլ բաներ հազվադեպ են անվճար լինում: Եթե Ալեքսը ավելի ուշադիր նայի կայքին, հավանաբար կնկատի մանր տառերով գրված տեքստին ուր ասվում է ծառայության իրական արժեքի մասին. Երաժշտական ֆայլերը, թեստերը, խաղերը և այլն հոյակապ միջոց են մարդկանց գայթակղելու «անվճար» ծառայությունը բաժանորդագրվելու, որը իրականում նրանց վրա շատ ավելի թանկ է նստում:

ԻՐԱՎԻՃԱԿ 12. Ալեքսը պետք է հիշի իր ինքնության գաղտնիության մասին, երբ խաղում է առցանց խաղեր անծանոթ մարդկանց հետ: Նա չպետքէ տեղեկություններ տրամադրի իր տան, դպրոցի, ընտանիքի անդամների, ազգանվան մասին:
Ալեքսը ծնողներին անպայման տեղեկացնում է այն մասին թե ինչ խաղեր է խաղում և առանց նրանց թույլտվության համացանցային խաղեր երբեք չի ներբեռնում, քանի որ դրանք կարող են վնասել համակարգիչը:

D. Բառարան

Account – Հաշիվ. Հաշիվը ձեզ հնարավորություն է տալիս, որպես լիազորված և իրավասու օգտվող, օգտագործել առցանց ծառայությունները՝ մուտքագրելով ձեր անունը և գաղտնաբառը: Ձեր օպերացիոն համակարգի միջոցով դուք կարող եք ընտանիքի յուրաքանչյուր անդամի համար ստեղծել առանձին հաշիվ:

Acronym - Տառային հապավում. Դարձվածքի կամ արտահայտության յուրաքանչյուր բառի առաջին տառերից կազմված հապավում: Տառային հապավումները հաճախ կիրառվում են չատերով /զրուցարաններով/ հաղորդակցվող անձանց կողմից՝ հաղորդակցությունն ավելի արագ դարձնելու նպատակով (տե ս հաղորդակցության մասին գլուխը):

Alert - Նախազգուշացում. Էկրանին հայտնվող փոքր պատուհան, որը տեղեկացնում է օպերացիոն համակարգի շահագործումից բխող հնարավոր վտանգի մասին: Դա կարող է լինել, օրինակ, նոր նամակ կամ հակավիրուսային ծրագրի աշխատանքի վերաբերյալ հաղորդագրություն:

Anti-virus – Հակավիրուսային ծրագիր. Համակարգչային ծրագիր, որի միջոցով փորձ է արվում ճանաչել, մեկուսացնել, արգելափակել կամ վերացնել վիրուսները և այլ «վնասակար ծրագրեր»: Սկզբում հակավիրուսը կատարում է ֆայլերի զննում՝ հայտնի վիրուսները փնտրելու նպատակով, այնուհետև ճանաչում է «վարակիչ» համակարգչային ծրագրերի կասկածելի «վարքագիծը»:

Anti-spyware -Հակալրտեսային ծրագիր. ծրագիր, որը պայքարում է լրտեսածրագրերի դեմ: Այն ստուգում է լրտեսածրագրերի առկայությունը ստացվող բոլոր տվյալներում և արգելափակում է հայտնաբերված վտանգները կամ տալիս է ցուցակ, որտեղից կարելի է ջնջել կասկածելի գրառումները:

Attachment - Կից փաստաթուղթ. Համակարգչային ֆայլ, որն ուղարկվում է էլեկտրոնային հաղորդագրության հետ միասին: Համակարգչային որդերը և վիրուսները հաճախ տարածվում

են կից հաղորդագրությունների տեսքով: Անհայտ անձանցից ստացված կից փաստաթղթերով էլեկտրոնային նամակները հարկավոր է դիտել որպես կասկածելի հաղորդագրություններ:
Author - Հեղինակ. գրական կամ տեսալսողական ստեղծագործություններ, համակարգչային ծրագրեր և այլ աշխատություններ ստեղծող անձ: Հեղինակային իրավունքը պաշտպանում է հեղինակների ստեղծագործությունները անօրինական բազմացումներից:
Avatar -Ավատար. Առցանց համակարգչային խաղերում կամ վիրտուալ աշխարհում ստեղծված օգտվողի նկարագիր /պրոֆիլ/, որը ներկայացվում է օգտվողի անվամբ, նկարով, պատկերանշանով կամ եռաչափ կերպարով:
Blog - Բլոգ. Ցանցային օրագիր (web log) բառակապակցության կրճատ տարբերակը: Կայք, որի բովանդակությունը գրեթե ամեն օր համալրվում է անհատի կամ խմբերի կողմից ստեղծված տեքստերով, նկարներով, տեսալսողական ֆայլերով և հղումներով:
Blogging - Բլոգինգ. Բլոգը գրելու կամ թարմացնելու գործընթացը:
Browser - Զննարկիչ. Ծրագիր, որն օգտագործվում է կայքեր դիտելու համար: Windows համակարգում գործող ամենատարածված զննարկիչներից են Internet Explorer-ը, Firefox-ը, իսկ Macs համակարգում առավել կիրառելի է Safari-ն: Այս զննարկիչների ամենավերջին տարբերակները ծնողներին առաջարկում են վերահսկողության նորարական եղանակներ:
Browsing - Զննարկում. Զննարկիչի օգտագործումը կայքեր դիտելու կամ ցանցում նավարկելու համար:
Bullying – Հետապնդում, ոտնձգություն. Մեկ կամ մի քանի «հետապնդողների» կողմից իրականացվող ագրեսիվ գործողություններ՝ բազմակի վնասների, սպառնալիքների, սեռական բնույթի ակնարկների, ֆիզիկական հարձակման կամ նվաստացուցիչ խոսքի տեսքով:
CD Rom - CD սկավառակ (CD Rom). Կոմպակտ դիսկի (compact disk) տառային հապավումն է: Այն տեղեկություն չգրանցող կոմպակտ սկավառակ է, որի տվյալները կարելի է ընթերցել համակարգչով: CD սկավառակները լայնորեն կիրառվում են ծրագրաշարեր տարածելու նպատակով:
Chat - Համաժամանակյա հաղորդակցում համացանցում՝ գրավոր հաղորդագրությունների և ակնթարթային հաղորդակցման ծրագրերի (օրինակ՝ MSN-ի) միջոցով:
Chat room – Զրուցարան, զրուցասենյակ. Վիրտուալ հասարակական վայր՝ իրական հաղորդակցման համար: Աշխարհի տարբեր մասերում բնակվող մարդիկ կարող են հանդիպել զրուցարաններում և ստեղնաշարի օգնությամբ փոխանակել հաղորդագրություններ: Եթե ձեր երեխաները օգտվում են զրուցասենյակներից, ղեկավարների և մոդերատորների հետ միասին համոզվե՛ք, որ դրանք նախատեսված են երեխաների համար:
Child pornography Մանկական պոռնկագրություն. Որոշ երկրներում այս երևույթը անվանում են «երեխայի բռնության պատկերում»՝ հաստատելու համար, որ մանկական պոռնկություն պատկերող նկարների հետևում թաքնված են իրական երեխաների հանդեպ կատարված ոտնձգությունների փաստերը: Մանկական պոռնկագրությունը տարբեր երկրներում ունի տարբեր իրավական սահմանումներ:
Computer file - Համակարգչային ֆայլ. Համապատասխան տեղեկությունների (փաստաթղթերի, ծրագրերի ևն) հավաքածու, որն ունի իր ուրույն անվանումը: Համակարգչային ֆայլերը կարող են համարվել գրասենյակային և գրադարանային քարտարկղերի մեջ նախկինում պահվող տպագիր փաստաթղթերի ժամանակակից կրկնորդները:
Computer program - Համակարգչային ծրագիր. սովորաբար կրում է ծրագրաշար անվանումը: Ծրագրաշարը կազմված է ծրագրավորողների կողմից գրված հստակ հերթականություն ունեցող հրամաններից, որոնք համակարգչին հնարավորություն են տալիս կատարել հանձնարարություններ: Համակարգչային ծրագիր գնելիս այն հաճախ ձեռք եք բերում CD սկավառակով (տե՛ս սահմանումը), որը հանդիսանում է ծրագրերի պահպանման ֆիզիկական միջոց:

Contact list -Հասցեացուցակ. Կոնտակտային տվյալների հավաքածու ակնթարթային հաղորդակցման և էլեկտրոնային փոստի ծրագրերում, առցանց խաղերում, բջջային հեռախոսներում, ևն: Կոնտակտային տվյալները կարող են ավելացվել, մերժվել /չգրանցվել/ կամ ջնջվել:

Cookies - Թխուկներ. Որևէ կայքից ձեր համացանցային զննարկիչում տեղադրված ֆայլ: Ամեն անգամ տվյալ կայքը կրկին բացելիս թխուկը հետ է ուղարկվում այն սերվերին, որի վրա պահպանված է կայքը: Թխուկները տեղեկություն են հաղորդում ձեր նախընտրած կայք(եր)ի մասին և օգտագործվում են առցանց գնումների համակարգերում: Թխուկների մերժումը կարող է անօգտագործելի դարձնել որոշ կայքեր:

Copyright -Հեղինակային իրավունք. Որևիցե գաղափարի, աշխատության կամ տեղեկատվության օգտագործոմը կանոնակարգող բացառիկ իրավունքների ամբողջություն: Հեղինակային իրավունքը ներկայացվում է «©» նշանով:

Cracker - Համակարգչային ենթգործդ. Մարդ, որը անօրինական կերպով ներխուժում է համակարգչային համակարգեր:

Crack-Հափշտակում. Հեղինակային իրավունքի ոտնահարմամբ՝ ծրագրաշարերի անօրինական բազմացում:

Cyberbullying - Կիբերհետապնդում. Ակնթարթային հաղորդագրությունների կամ էլեկտրոնային նամակների միջոցով կատարվող հետապնդումներ, ագրեսիվ գործողություններ: Կիբերհետապնդողները կարող են հրապարակել զոհերի անձնական տվյալները և նույնիսկ հանդես գալ վերջիններիս փոխարեն ու նրանց անունից հրապարակել նյութեր՝ այդ անձանց վարկաբեկելու կամ ծաղրելու նպատակով:

Directory - Ենթաբաժին Կառուցվածքային միավոր, որը ձեր համակարգիչն օգտագործում է թղթապանակներն ու ֆայլերը ստորակարգային կառուցվածքով դասավորելու համար (օրինակ՝ Իմ փաստաթղթերը (My Documents), Իմ նկարները (My Pictures) և այլն):

Download - Ներբեռնում. վերաբերում է առցանց համակարգից ֆայլը համակարգիչ փոխանցելու /արտագրելու/ գործընթացին:

Email - Էլեկտրոնային փոստ. էլեկտրոնային գրավոր հաղորդակցման միջոց, որը թույլ է տալիս ուղարկել հաղորդագրություններ ցանկացած տեսակի կից ֆայլով (տեքստ, նկար, աուդիո և այլն):

Email address -Էլեկտրոնային հասցե. Վիրտուալ վայր, որտեղից ուղարկվում կամ ստացվում են էլեկտրոնային հաղորդագրությունները: Էլեկտրոնային հասցեները բաղկացած են երկու մասից, որոնք իրարից բաժանվում են @ նշանագրով:

Emoticon - Էմոթիկոն. Պատկեր կամ նշան, որն օգտագործվում է զգացմունքներ կամ հույզեր արտահայտելու համար: Այն կարող է պատկերվել ստեղնաշարի գրանիշների և նշանների կամ էլ զրուցասենյակների և խաղասենյակների, ակնթարթային հաղորդակցման ծառայությունների, բջջային հեռախոսների և այլ ծառայությունների կողմից առաջարկվող գրանշաններով:

Family settings - Ընտանեկան կարգավորումներ. կարգավորումներ, որոնք օգտագործվում են զննարկիչը կամ այլ կարգավորումները երեխաների կարիքներին հարմարեցնելու համար: Առավել տարածված են բովանդակության ֆիլտրացման, ժամանակային սահմանափակման և խաղերի վերահսկման համակարգերը:

Favourites – Սիրելի կամ նախընտրելի. ձևափոխման ենթակա զննարկիչի թղթապանակ, որտեղ դուք կարող եք պահպանել հետաքրքիր հղումներ/էջանշաններ: Վերջիններիս կարելի է դասավորել ենթաթղթապանակներում կամ կցել այնպիսի թղթապանակների, որոնք պարունակում են հեշտ փնտրվող գլխաբառեր:

File sharing - Ֆայլերի փոխանակում. առցանց համակարգում ֆայլերի փոխանակում օգտվողների միջև: Այս հասկացությունը ներառում է ֆայլերը այլ օգտվողների առաջարկելու (վերբեռնում) և համացանցից դեպի համակարգիչ ֆայլերը արտագրելու (ներբեռնում)

գործընթացները: Ֆայլերը որպես կանոն փոխանակվում են P2P (ապակենտրոնացված) ցանցերի միջոցով:

File transfer - Ֆայլերի փոխանցում. ֆայլերի փոխանցումը համակարգչային ցանցերով: Օգտվողների շրջանում ֆայլերի փոխանցման գործընթացը հայտնի է որպես վերբեռնում կամ ներբեռնում:

Filter – Զտիչ. Համակարգչային ծրագրի հավելված, որը կանոնակարգում է համացանցային ծառայություններից օգտվելու գործընթացը, նախազգուշացնում է խնդրահարույց կայքերի մասին, հետևում է օգտվողի նավարկմանը, արգելափակում է վտանգավոր կայքերը և անգամ ամբողջությամբ անջատում է համակարգիչը: Զտիչային համակարգերը կարող են տեղադրվել ցանցին չմիացված համակարգիչներում, սերվերներում, համացանցին միացած հեռխոսներում և այլուր:

Firewall - Հրապատ. Ձեր երթուղղիչին միացված սարքաշար կամ համակարգչում տեղադրված ծրագրաշար, որի նպատակն է խափանել չլիազորված օգտվողների (օրինակ՝ համակարգչային նենգորդների և համակարգչահենների) մուտքը ձեր համակարգիչ կամ համացանցին միացված համակարգչային ցանց:

Flaming – Զազրախոսություն. Թշնամական կամ վիրավորական բնույթի հաղորդակցություն ինտերնետից օգտվողների միջև: Այն սովորաբար հանդիպում է քննարկման հարթակներում, զրուցասենյակներում և անգամ էլեկտրոնային փոստում:

Folder Թղթապանակ. Ֆայլային համակարգի միավոր, որը պարունակում է մի խումբ ֆայլեր կամ այլ ենթաբաժիններ: Թղթապանակները պարունակում են բազմաթիվ փատաթղթեր և օգտագործվում են տեղեկույթը դասակարգելու համար:

Form (online form) - Ձևաթուղթ (առցանց ձևաթուղթ). դատարկ դաշտեր պարունակող որոշակի ձևաչափ ունեցող փաստաթուղթ, որտեղ կարող եք լրացնել ձեր տվյալները: Էլեկտրոնային ձևաթուղթը կարող է լրացվել ազատ տեքստով կամ նախապես կազմված ցանկերից ընտրված այլընտրանքային բովանդակությամբ:

Forum - Ֆորում. Առցանց քննարկման խումբ, որտեղ ընդհանուր հետաքրքրություններ ունեցող մասնակիցները ազատ փոխանակում են թեմատիկ հաղորդագրությունները:

Freeware - Անվճար ծրագրեր. հիմնականում համակարգչային ծրագիրը պաշտպանված է հեղինակային իրավունքով, և հետևաբար այն հնարավոր չէ ներբեռնել: Անվճար համակարգչային ծրագիրը նշանակում է, որ հեղինակային իրավունքի սուբյեկտը համաձայն է, որ այդ ծրագիրն անվճար հասանելի լինի բոլորին:

Shareware - Պայմանականորեն անվճար ծրագիրը նշանակում է, որ հեղինակային իրավունք սուբյեկտը համաձայն է, որ ծրագիրն անվճար հասանելի լինի բոլորին փորձնական ժամանակահատվածով: Այդ ժամանակահատվածը լրանալուց հետո օգտվողը պետք է վճարի որոշակի գումար, որպեսզի շարունակի օգտվել տվյալ ծառայությունից:

Digital Game - Թվային խաղ. Ծրագրավորողների կողմից ստեղծված համակարգչային խաղ: Առցանց խաղերը այն թվային խաղերն են, որոնք խաղալու համար անհրաժեշտ է միացված լինել համացանցին: Առցանց խաղերը կարող են ապահովել բազմաթիվ խաղացողների փոխգործակցությունը:

Grooming - Գրումինգ, Սեռական ոտնձգություն կատարելու նպատակով վստահության ձեռքբերում. Զրուցարանների օգտագործումը մանկապիղծների կողմից՝ երեխաների հետ հուզական կապ հաստատելու համար: Ձևանալով երեխաներ՝ մանկապիղծները զրույցի մեջ են մտնում հավանական զոհերի հետ՝ նրանց գտնվելու վայրի, հետաքրքրությունների, նախընտրությունների և սեռական փորձառության մասին տեղեկություններ կորզելու նպատակով: «Գիշատիչները» հաճախ օգտագործում են տարբեր միջոցներ՝ երեխաներին սեռական թեմայով խոսակցություններում ներգրավելու համար:

Hacker - Համակարգչահեն. Լայնորեն կիրառվող հասկացություն, որը բնութագրում է

համակարգչային նենգորդի (անձին, որն անօրինական կերպով ներխուժում է համակարգչային համակարգեր - տե՛ս համակարգչային նենգորդ): Համակարգչից օգտվողների շրջանում այն կարող է օգտագործվել՝ համակարգչով տարված անձին նկարագրելու համար:

Hardware - Սարքաշար. Համակարգչի բաղկացուցիչ մաս, որը պետք է հստակ կերպով տարանջատել ծրագրաշարից (software): Այն կարող է լինել ներքին (մայր պլատաներ, կոշտ սկավառակներ և RAM, որոնք հաճախ կրում են «համակարգչի բաղկացուցիչ մասեր» անվանումը) և արտաքին (ցուցարկիչներ, ստեղնաշարեր, տպիչներ, որոնք հայտնի են նաև որպես համակարգչի «ծայրանդամներ»):

Harmful content - Վտանգավոր բովանդակություն. Նկարներ, տեքստեր և այլ նյութեր, որոնց բովանդակությունը կարող է հանգեցնել վնասակար հետևանքների (օրինակ՝ բռնություն պատկերող նկարները կարող են վնասել երեխաներին և անչափահասներին):

Helpline - Օգնության գիծ. երեխաների աջակցման կազմակերպությունների կամ Insafe ցանցի անդամների կողմից տրամադրվող էլեկտրոնային, երբեմն նաև հեռախոսային ծառայություններ: Երեխաները կարող են բարձրաձայնել իրենց մտահոգությունները առցանց տեխնոլոգիաների օգտագործման հետ կապված անօրինական և վնասակար բովանդակության և անհարմար ու սարսափազդու զգացողությունների շուրջ:

Homepage -Գլխավոր էջ. վեբ էջ, որը ավտոմատ կերպով բեռնվում է զննարկիչը թողարկելիս: Այս հասկացությունը կարող է վերաբերել նաև վեբ կայքի առաջին կամ հիմնական էջին (տես սահմանումը):

Hotline - Թեժ գիծ. հեռախոսային աջակցման գիծ կամ վեբ ծառայություն, որտեղ մարդիկ կարող են բողոքել ենթադրվող անօրինական բովանդակությունից և/կամ համացանցի անօրինական օգտագործումից: Թեժ գիծը պետք է ապահովի բողոքների ուսումնասիրության և մշակման արդյունավետ եւ թափանցիկ ընթացակարգ և ունենա կառավարության, իրավապահ մարմինների, ձեռնարկությունների և ինտերնետից օգտվողների աջակցությունը համապատասխան երկրում:

Identity theft - Անձնական տվյալների հափշտակում. անձնական տեղեկություններ (օրինակ՝ անուն, ծննդյան թիվ, կրեդիտ քարտի համար) գողանալը և դրանք անօրինական կերպով օգտագործելը:

Illegal content - Անօրինական բովանդակություն. առցանց բովանդակություն, որն ըստ ազգային օրենքների համարվում է անօրինական: Նման բովանդակության ամենատարածված տեսակներից են երեխաների սեռական շահագործում պատկերող նկարները, անօրինական գործունեությունը զրուցարաններում, ատելության սերմանումը առցանց համակարգում և քսենոֆոբիա տարածող կայքերը:

Instant Messaging (IM): Ակնթարթային հաղորդագրությունների փոխանակում. անմիջական և համաժամանկյա էլեկտրոնային հաղորդակցության տեսակ երկու և ավելի օգտվողների միջև: Երբ ձեր հասցեացուցակում գրանցված մարդիկ միանում են ցանցին, դուք այդ մասին անմիջապես տեղեկանում եք:

Internet Համացանց. Ամբողջ աշխարհում տարածված և ազատ օգտագործման համար նախատեսված համընդհանուր ցանց, որի միջոցով տեղի է ունենում տվյալների հաղորդում կամ փոխանակում: Այն բաղկացած է ավելի փոքր ներքին /տեղական/, ուսումնական, բիզնես և կառավարական ցանցերից, որոնք ապահովում են բազմատեսակ ծառայություններ, ինչպիսիք են տեղեկատվության տարածումը, էլեկտրոնային փոստը, առցանց զրուցարանները, ֆայլի փոխանցումը և այլն:

Internet connection Համացանցային /ինտերնետային կապ. Օգտվողների միացումը համացանցին ապահովող կապի միջոցներ: Համացանցին միանալու ամենատարածված եղանակներն են dial - up, հեռախոսագծային (T- lines), անլար (Wi-Fi), առբանյակային և բջջային:

Junk/Spam folder - Փոստարկղի/անպետք նամակների համար նախատեսված թղթապանակ. Էլեկտրոնային փոստարկղի այն մասը որտեղ պահվում են փոստարկղ կամ անպետք նամակներ համարվող հաղորդագրությունները:
Junk mail - Անպետք նամակներ. անցանկալի էլեկտրոնային հաղորդագրություններ: Քանի որ համացանցը հասանելի է հանրությանը՝ անպետք նամակների հոսքի կանխումը գրեթե անհնար է, ճիշտ այնպես ինչպես անհնար է փոստարկղի կանխումը:
Link - Հղում. առցանց համակարգում հասանելի որևէ փաստաթղթի (վեբ էջի, տեքստային փաստաթղթի, նկարի և այլն) արված հիշատակում: Հղմանը մկնիկով մատնազարկելիս բացվում է նոր էջ կամ բոլորովին նոր կայք: Տեքստային հղումները սովորաբար կապույտ գույնի են և ընդգծված, սակայն կարող են ունենալ նաև այլ գույն և ընդգծված չլինել: Նկարները նույնպես կարող են ծառայել որպես այլ կայքեր ուղղորդող հղումներ:
Malware - Վնասակար ծրագրեր. վնասակար ծրագրային ապահովում, որի նպատակն է թափանցել համակարգչային համակարգ կամ վնասել այն՝ առանց տիրոջ տեղեկացված համաձայնության: Այն ներառում է համակարգչային վիրուսներ, որդեր, տրոյական ձիեր, լրտեսածրագրեր, անազնիվ գովազդային ծրագրեր և այլ վնասակար և անցանկալի ծրագրաշարեր:
Manipulation - Մեքենայություն. Պատկերի, ֆայլի, նկարի ակնհայտ կամ ոչ ակնհայտ փոփոխելու գործընթաց: Ներկայումս կան բազմաթիվ միջոցներ, որոնք կարող են փոփոխության ենթարկել բովանդակությունը կամ տվյալների համակարգը՝ ստեղծելով իրականությանը չհամապատասխանող արդյունք:
Massively Multiplayer Games - Բազմաթիվ մասնակիցներ ունեցող խաղեր. եռաչափ համակարգչային խաղեր, որոնց մասնակցում են հորինված կերպարների դերեր ստանձնած և միմյանց դեմ մրցող մարդիկ: Այս անվանակարգում կարևորվում են դերախաղեր առաջարկող խաղերին, որոնց մասնակիցները համատեղ ջանքերով ստեղծում են պատմություններ կամ հետևում դրանց:
Memory/USB stick - Հիշողության/USB կրիչ. Տվյալների պահպանման սարք USB միացուցիչով համալրված: Հիշողության կրիչը որպես կանոն ունենում է փոքր չափեր, թեթև քաշ, շարժական է և փոփոխական բովանդակությամբ:
Mobile - Շարժական հեռախոս. էլեկտրոնային հեռահաղորդակցման սարք, որը հայտնի է որպես շարժական հեռախոս, բջջային հեռախոս, gsm, սմարթֆոն կամ ձեռքի հեռախոս անվանմամբ: Այն ունի նույն հիմնական հնարավորությունները, ինչ՝ սովորական ֆիքսված հեռախոսը: Այսօր շարժական հեռախոսների մեծ մասը ունեն տեսախցիկ, ինչպես նաև՝ ինտերնետին միանալու հնարավորություն (վճարովի ծառայություն):
Mp3: աուդիո հարմարեցմամբ կոդավորման ձևաչափ: Mp3 ձևաչափով ֆայլերն ունեն օրիգինալ աուդիո ֆայլի մեկ տասներորդ չափը, սակայն նրանց ձայնի որակը գրեթե չի զիջում կոմպակտ սկավառակին (CD): Իրենց փոքր ծավալի և լավ ձայնային հատկանիշների շնորհիվ, mp3 ֆայլերը դարձել են երաժշտական ֆայլերը համակարգչում և շարժական սարքերում պահպանելու հանրահայտ միջոց:
Net - Ցանց. համացանցի կրճատ տարբերակը:
Netiquette - Համացանցային էթիկա. առցանց հաղորդակցություններում քաղաքակրթության կանոններ թելադրող համացանցային էթիկա:
Newsgroup - Նորությունների խումբ. տես ֆորումի սահմանումը:
Nickname Մականուն. Այն ներկայացնում է առցանց ծառայությունից օգտվողին և սահմանվում է հենց այդ օգտվողի կողմից: Մականունը ներկայացնում է օգտվողին հասցեների ցուցակում, զրուցասենյակներում և այլուր: Ճիշտ ընտրության դեպքում մականունները կարող են պաշտպանել ձեր անանունությունը առցանց համակարգում:
Operating system - Օպերացիոն համակարգ. ծրագիր, որը կառավարում է համակարգչի հիմնական ֆունկցիաները և որի շնորհիվ այլ ծրագրերի աշխատանքը դառնում է հնարավոր:

Հայտնի օպերացիոն համակարգեր են Windows-ը, Linux-ը և Mac OS-ը:
Parental control - Ծնողական վերահսկողություն. տես ընտանեկան կարգավորումների սահմանումը:
Password - Գաղտնաբառ. տառանիշերի գաղտնի համակարգ, որն ապահովում է հասանելիությունը ֆայլին, համակարգչին, հասցեին կամ ծրագրին. այն հանդես է գալիս որպես ապահովության միջոց չլիազորված օգտվողներից (տե՛ս Հաղորդակցում գլուխը):
Personal data - Անձնական տվյալներ. ցանկացած տեղեկություն, որը կապ ունի անձի հետ: Անձնական տվյալների հավաքագրման, մշակման և պահպանման անհրաժեշտության դեպքում հարկավոր է հստակ նշել պատճառները:
Pop-up window - Դուրս լողացող պատուհան. պատուհան, որը կարող է հանկարծակի հայտնվել որևէ կայք այցելելիս կամ հատուկ գործառույթով օժտված որևէ ստեղ սեղմելիս: Դուրս լողացող պատուհանները սովորաբար ունենում են հրահանգացանկ և մնում են էկրանին այնքան, մինչև ընտրում եք այդ հրահանգներից որևէ մեկը կամ փակում պատուհանը՝ սեղմելով աջ անկյան խաչը:
Port - Պորտ. համակարգիչն այլ սարքի հետ միացնելու նպատակով օգտագործվող ինտերֆեյս: Պորտերը կարող են լինել ներքին կամ արտաքին: Ներքին պորտերը ապահովում են միացումը սկավառակատարին կամ ցանցին, իսկ արտաքին պորտերը միանում են արտաքին որևէ սարքի, օրինակ՝ տպիչի կամ ստեղնաշարի:
Privacy – Մասնավորություն, անձնական տվյալների գաղտնիություն. սեփական անձի մասին տեղեկատվության հոսքը վերահսկելու և դրանով իսկ սեփական ընտրությամբ անձնական տեղեկություններ բացահայտելու անհատի կամ խմբի ունակությունը:
Privacy setting – Մասնավորության, կամ գաղտնիության կարգավորումներ. տվյալ օգտվողի անձնական տվյալների բացահայտման կարգավորումներ, որոնք կարող եք խմբագրել՝ ձեր անձնական տվյալների, թխուկների և այլ տեղեկությունների գաղտնիությունը բացահայտումներից ավելի լավ պաշտպանելու նպատակով:
Private - Մասնավոր. անձին կամ խմբին վերաբերող տեղեկություններ, որոնք չեն բացահայտվում հանրությանը: Անձի կողմից սովորաբար գաղտնի են պահվում հատուկ նշանակություն ունեցող կամ անձնական տեսանկյունից զգայուն համարվող թեմաները:
Processor Պրոցեսոր /մշակիչ. նաև կենտրոնական մշակիչ հանգույց: Համակարգչի մաս, որը մշակում է տվյալներ, ստեղծում վերահսկման ազդանշաններ և պահպանում արդյունքներ: Հիշողության հետ միասին այն հանդիսանում է համակարգչի կենտրոնական հանգույցը:
Profi le Նկարագիր/Անձնական էջ. Օգտվողի անձնական տեղեկությունները սոցիալական ցանցերում, անմիջական հաղորդակցման համակարգերում, առցանց զրուցարաններում, առցանց խաղերում և այլուր: Դրանք կարող են լինել բաց և փակ /գաղտնի/ և փոփոխվել վիրտուալ համակարգում իրենց մասին տեղեկություններ ներկայացնող անձանց կողմից:
P2P network - P2P ցանց/Ապակենտրոնացած ցանց. Ցանց, որի շնորհիվ օգտվողները կարող են փոխանակել ֆայլեր՝ ներբեռնման կամ արտաբեռնման միջոցով (տես սահմանումը): Դա պարզապես համացանցով ֆայլեր փոխանակելու բազմաթիվ ձևերից մեկն է: Ֆայլերի փոխանակման որոշ ծրագրեր անօրինական են:
Recycle bin - Աղբարկղ. Համակարգչային դիրեկտորիա, որում ժամանակավորապես պահվում են ջնջված ֆայլերը: Դուք պետք է կանոնավոր կերպով աղբարկղից մաքրեք հին և ոչ ցանկալի տվյալները, որպեսզի տեղ ազատեք ձեր համակարգչի ներքին պահեստ հանդիսացող կոշտ սկավառակում:
Report - Տեղեկացում. Գործառույթ, որը հնարավորություն է տալիս հանրային վիրտուալ տարածքների օգտվողներին իրենց խնդիրների (տեխնիկական, օգտվողների անընդունելի վարքագծի, անօրինական բովանդակության ևն) մասին հայտնել մոդերատորին կամ կայքի կայքի սպասարկման անձնակազմին:
Ringtone - Հեռախոսազանգի մեղեդի. բջջային հեռախոսի ձայն կամ մեղեդի, որն ազդանշում է ստացվող զանգերը: Գոյություն ունեն փոփոխման ենթակա տարատեսակ մեղեդիներ և

երաժշտություններ, որոնք կարող են ներբեռնվել (հաճախ վճարելով գումար) և օգտագործվել հեռախոսի տերերի կողմից:

Safety settings (profile) - Ապահովության կարգավորումներ (նկարագիր). ձեր առցանց նկարագրի հետ կապված փոփոխման ենթակա ապահովության կարգավորումներ: Որպես կանոն դրանք վերաբերում են նկարների կամ ֆայլերի բացմանը, վստահելի տեղեկատվության ճանաչմանը և մեծահասակների համար նախատեսված բովանդակության սահմանափակումներին:

Scan - Սկանավորում /պատկերառում/. Սկաների միջոցով տպագիր նյութը թվային ֆայլի վերածելու գործողությունը: Այդ ձևափոխումը ձեզ թույլ է տալիս փաստաթղթերը դիտել որպես համակարգչում պահպանված էլեկտրոնային ֆայլեր և տարածել դրանք առցանց համակարգում:

Screen name - Էկրանային անուն. տես մականվան սահմանումը:

Search engine - Որոնման համակարգ. կայքերում պարունակվող տեղեկությունը փնտրելու նպատակով օգտագործվող գործիք: Ամենահայտնի որոնման համակարգերն են Google և MSN –ը:

Search Որոնում. Որոնման համակարգեր, որոնցում օգտվողները կարող են իրենց նախասիրությամբ ստեղծել հետաքրքիր ապահովության կարգավորումներ:

Second Life - Երկրորդ կյանք. ԱՄՆ Linden Labs ընկերության կողմից առաջարկվող հանրաճանաչ եռաչափ վեբ համայնք: Նրա վիրտուալ համակարգում օգտվողները կարող են հաղորդակցվել ավատարի (տես սահմանումը) միջոցով, ստեղծել տներ, միջավայրեր, առևտուր անել, անգամ վաստակել վիրտուալ արժույթ և այլն:

Sign-up – Գրանցում. Առցանց ծառայությունների (նորությունների, քննարկումների ֆորումի, էլեկտրոնային փոստի, զրուցարանների ևն) բաժանորդագրում: Որպես կանոն այս համակարգերից օգտվողներն ունեն իրենց ուզած պահին ծրագրից դուրս գալու (sign out) հնարավորություն:

SIP-Bench. Եվրոպական հանձնաժողովի կողմից աջակցություն ստացած ծրագիր, որի շրջանակներում ուսումնասիրվել են 30 վերահսկման և հակափոստաղբային գործիքներ՝ երեխաներին համացանցի վտանգավոր բովանդակությամբ նյութերից պաշտպանելու արդյունավետությունը ստուգելու նպատակով:

Social networking - Սոցիալական ցանցեր. Առցանց համայնքներ, որոնց անդամները ունեն ընդհանուր հետաքրքրություններ և առցանց համակարգում միմյանց հետ շփվում են օգտվելով համապատասխան ծառայություններից և ծրագրերից (տես սոցիալական ցանցերի կայքեր):

Social networking sites - Սոցիալական ցանցերի կայքեր. Վիրտուալ հարթակներ ընդհանուր հետաքրքրություններ ունեցող մարդկանց համայքների համար: Անդամները ստեղծում են իրենց անձնական էջերը և կարող են փոխանակել տարբեր տեքստեր, նկարներ և այլ ֆայլեր, ուղարկել հաղորդագրություններ, մասնակցել ֆորումներում: Սոցիալական ցանցերի շատ կայքեր ունեն անձնական էջի ապահովության կարգավորումներ և տարիքային սահմանափակումներ՝ մինչև 13 տարեկան:

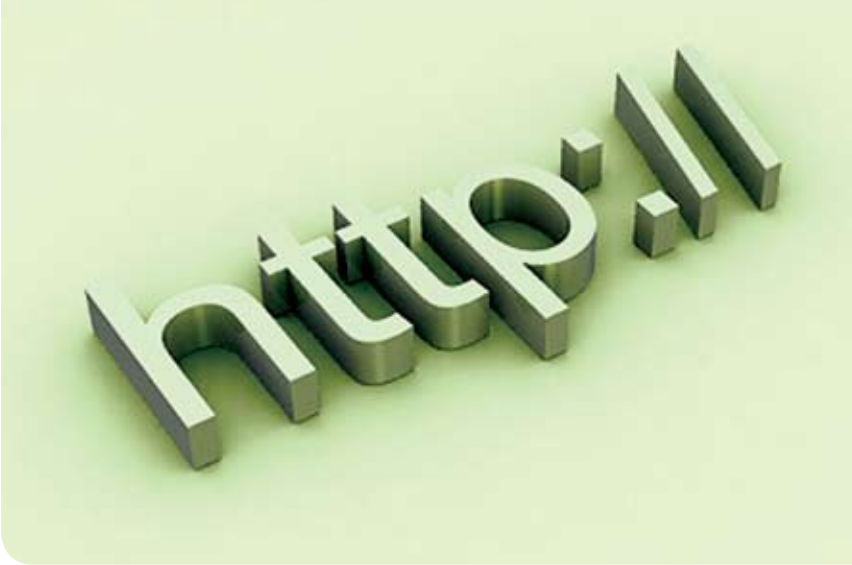
Software - Ծրագրաշար /ծրագրային ապահովում/. Տես համակարգչային ծրագրի սահմանումը:

Spam - Փոստաղբ. Մեծ քանակություններով առաքվող անցանկալի, սովորաբար առևտրային բնույթի էլեկտրոնային հաղորդագրություններ: Այլ անձանց փոստաղբ ուղարկելը միանշանակ հանդիսանում է համացանցից օգտվելու կանոնների խախտման ամենավառ դրսևորումներից մեկը:

Spam filter - Փոստաղբային զտիչ. Ծրագրային հավելված, որն արգելափակում է փոստաղբի մուտքը ձեր միջարկը:

Spyware - Լրտեսածրագիր. Համացանցից ներբեռնված ֆայլերին գաղտնի կերպով կցված վնասակար ծրագիր: Այն տեղեկությունն ուղարկում է երրորդ անձանց, որոնք գովազդելու կամ այլ տեղեկություններ տարածելու նպատակով հավաքագրում են անհատական տվյալներ: Ձեր տվյալները կարող են նաև ուղարկվել համակարգչային հանցագործների:

Subscribe - Բաժանորդագրվել. Որևէ ծառայության կամ լուրերի կամավոր բաժանորդագրություն:
Toolbar - Գործիքների վահանակ. Համակարգչային ծրագրի մաս կազմող պատկերանշանների կամ սեղմակների ամբողջություն: Գործիքների վահանակները ծառայում են որպես սովորական գործառույթների կատարման համար նախատեսված միշտ հասանելի և հեշտ օգտագործվող ինտերֆեյս:
Trial software - Փորձնական ծրագիր. Համակարգչային ծրագրիր, որը նախքան գնելը կարող եք փորձել: Ծրագրի փորձնական տարբերակները որպես կանոն օժտված են նույն գործառույթներով, ինչ՝ իսկական տարբերակները, սակայն նրանց օգտագործման ժամկետը սահմանափակ է:
Trojan horses - Տրոյական ձիեր. Արտաքուստ անվնաս թվացող համակարգերի (օրինակ՝ խաղերի և անգամ վիրուսներ որսացող ծրագրերի) անվան տակ ձեր համակարգիչ ներխուժող վնասակար ծրագիր: Տրոյական ձիերը ինքնուրույն չեն բազմանում, սակայն որպես կանոն հետապնդում են խոցելի համարվող տվյալները հասանելի դարձնելու կամ տվյալները ընդհանրապես ոչնչացնելու նպատակ: Նրանք կարող են ջնջել կոշտ սկավառակի պարունակությունը կամ գողանալ գաղտնի տեղեկություններ:
URL (Uniform Resource Locator): URL (պաշարների միասնական նշիչ). կոնկրետ կայքի կամ ֆայլի հասցե համացանցում: Այն չի պարունակում հատուկ գրանշաններ կամ ազատ տարածություններ, և օգտագործում է դեպի առաջ ուղղորդող թեք գծեր՝ տարբեր դիրեկտորիաները մատնանշելու համար: Հասցեի առաջին մասը ցույց է տալիս՝ ինչ հաղորդակարգից օգտվել, իսկ երկրորդը հստակեցնում է IP հասցեն կամ այն դոմենի (տիրույթի) անվանումը, որտեղ տեղակայված է ռեսուրսը:
User profile - Օգտվողի նկարագիր. համակարգչային ծրագրից, կայքից կամ այլ տեխնիկական գործիքներից օգտվող կոնկրետ անձին նկարագրող տեղեկություններ: Նրանք որպես կանոն ներառում են օգտվողի անունը, գաղտնաբառը և այլ մանրամասներ (ծննդյան թիվ, հետաքրքրություններ):
Virtual possession - Վիրտուալ սեփականություն. Խաղի յուրաքանչյուր մասնակցի համար նախատեսված առարկաների խումբ:
Virus - Վիրուս. Վնասակար կոդի տեսակ, վնասակար ծրագիր, որը տարածվում է օգտվողի միջնորդավորված մասնակցությամբ: Այն սովորաբար տարածվում է էլեկտրոնային նամակներին կցված հաղորդագրություններով, ինչպես նաև վարակված հիշողության արտաքին կրիչների (USB կրիչ, CD) միջոցով:
Voice over Internet Protocol (VoIP) - Ձայնի փոխանցման հաղորդակարգ. համապատասխան ծրագրի ներբեռնումից հետո օգտվողներին համացանցում խոսելու հնարավորություն տվող տեխնոլոգիա: VoIP միևնույն համակարգի միջոցով իրար հետ խոսող օգտվողների համար զանգերը կարող են լինել անվճար (օրինակ՝ Skype, Voicebuster): Նման ծրագրերն առաջարկում են նաև զրուցարանի և ֆայլեր փոխանակելու հնարավորություն:
Wallpaper - Պաստառ. Ձեր համակարգչի էկրանի ֆոնը ձևավորող նախշ, նկար կամ այլ գրաֆիկական պատկեր:
Web - Վեբ. Համաշխարհային սարդոստայնի կրճատ անվանումը (անգլերեն web - ոստայն): HTML (հիպեր տեքստի նշման լեզու) ձևաչափով առցանց փաստաթղթերի հավաքածու, որտեղ կան այլ փաստաթղթերի, ինչպես նաև գրաֆիկական պատկերների, աուդիո և վիդեո ֆայլերի արված հղումներ: Վեբը հանդիսանում է համացանցի մի մաս:
Website Կայք /կայքէջ/. Տեղակայում համաշխարհային սարդոստայնում: Յուրաքանչյուր կայք ունի գլխավոր էջ, որն առաջինն է երևում այնտեղ մուտք գործելիս: Կայքերում սովորաբար հանդիպում են լրացուցիչ ֆայլերի կամ այլ կայքերի արված հղումներ: Նրանց ղեկավարումն իրականացվում է կայքի սեփականատեր համարվող անհատների, ընկերությունների կամ կազմակերպությունների կողմից:
Webcam - Վեբ խցիկ/տեսախցիկ. տեսախցիկ, որը կարող է հեռարձակում իրականացնել վեբի, ակնթարթային հաղորդակցումների, տեսակոնֆերանսների և զրուցարանների միջոցով:
Worm - Որդ. ինքնուրույն բազմացող հատուկ տեսակի վիրուս, որն առանց տիրոջ միջամտության կարող է անցնել մեկ համակարգչից մյուսը և վնասել ցանցը, սպառել թողունակության հսկայական ծավալ, անջատել համակարգիչը նն:



Ե. Օգտակար հասցեներ

SAFE.AM

Այս կայքում կարելի է գտնել ռուսուցիչների, սովորողների և ծնողների համար համացանցային ապահովությանը վերաբերող խորհուրդներ *http://www.safe.am*

THE HOTLINE

Եթե համացանցում ինչ որ բան անհագստացնում է ձեզ, կամ կարծում եք, որ անօրինական բովանդակության եք հանդիպել հայտնեք Թեժ գիծ շուրջօրյա ծառայությանը: 24-ժամյա ծառայությունը 18-ից ցածր տարիքի անձանց առաջարկում է օգնություն՝ հեռախոսային (080061111) և առցանց խորհրդատվության միջոցով: *http://www.safe.am*

INSAFE

Համացանցային ապահովության իրազեկման Եվրոպական ցանց:
http://www.saferinternet.org

WATCH YOUR SPACE

Այս կայքում կսովորեք օգտագործել սոցիալական ցանցերը. Ինչպիսիք են Bebo-ն, MySpace-ը, YouTube-ը:
http://www.watchyourspace.ie

MAKEITSECURE

makeITsecure իրազեկության կենտրոն է Իռլանդիայում, որի կայքում կարող եք գտնել SS անվտանգության, մասնավորապես՝ լրտեսածրագրերի, անհատական տվյալների գողության և այլ խնդիրների վերաբերյալ օգտակար խորհուրդներ:
http://www.makeitsecure.ie

European Commission

MEDIA EDUCATION

ins@fe

World Vision Armenia

LIBERTYGLOBAL
Աջակցությամբ

Վերնագիր: Ընտանեկան համացանցային ապահովության հավաքածու • Ստեղծվել է Insafe/Liberty Global-UPC 2008 թ.
Prefix: 9789078209 • Id 51950 • ISBN-NUMBER: 9789078209577 • EAN: 9789078209577

Հեղինակային իրավունք: Այս աշխատանքն արտոնագրված է Creative Commons Attribution-No Derivative Works 3.0 Unported արտոնագրով:
Արտոնագրի ամբողջական տեսնելու համար այցելեք՝ http://creativecommons.org/licenses/by-nc-nd/3.0