Safe.am

ՀԱՄԱՑԱՆՑԻ ԱՊԱՀՈՎ ՕԳՏԱԳՈՐԾՄԱՆ ՄԱՍԻՆ

սովորողների, դասավանդողների եվ ծնողների համար

Համացանց

Հեռուստատեսային դարաշրջանում մեծացած ծնողների համար, ներկա ինտերնետային սերնդի դաստիարակությունը նոր մարտահրավերներ է նետել:
Երեխաները նոր տեխնոլոգիաների մասին ավելին գիտեն, ուստի զարմանալի չէ, որ ծնողները հաճախ ոչ շահեկան վիճակում են երեխաների համեմատ:

Քանի որ իսկապես վտանգներ կան, շատ կարևոր է ծնողների ներգրավումը երեխաների համացանցային կյանքի մեջ: Երեխաները կարող են շատ հմտորեն տիրապետել համակարգիչը, սակայն նրանք մեծահասակների կարիքն ունեն քննադատական մտածողություն ու դատողական հմտություններ տարբեր իրավիճակների համար զարգացնելու նոր ինֆորմացիայի և ցանցային շփումներում ժամանակ:

Մեզանից շատերը չգիտեն, թե ինչպես են երեխաները համացանց օգտագործում, երբ բազում պատուհաններ են բացվում համակարգչի էկրանին և նրանց մատները սահում են ստեղնաշարի վրայով վտանգավոր արագությամբ:

Մեր կայքում տեղադրված նյութերը կօգնեն ձեզ բացահայտել երեխաների կողմից սիրված տեխնոլոգիաներն ու զբաղմունքները:

Վեբ կայքեր

Համաշխարհային սարդոստայնը (կարճ՝ վեբը) երեխաների համար այցելության ամենահանրաճանաչ վայրն է համացանցում: Վեբ կայքը բաղկացած է ,,էջից" կամ էջերի հավաքածուից, որ պարունակում է տեքստ, նկարներ, խաղեր, երաժշտություն կամ համակարգչային ծրագրեր, ձայնային և տեսա-հոլովակներ ներբեռնելու հղումներ: Բառացիորեն միլիոնավոր կայքեր կան ցանցում, որ կարող է մատչելի լինել ձեր համակարգչային ծրագրի օգտագործմամբ, որ կոչվում է ցանցային ,,զննարկիչ":

Ցանցը տարբերվում է մեդիայի այլ տեսակներից նրանով, որ այն երեխաներին հնարավորություն է ընձեռում ստեղծելու իրենց սեփական բովանդակությունը: Երիտասարդներն օգտագործում են ցանցը բացահայտելու և ցուցադրելու իրենց ստեղծագործական կարողությունները զանազան ձևերով. ստեղծելով առցանցային ֆիլմեր, երաժշտություն, վեբ կայքեր, ամսագրեր (էլ-գրեր) և բլոգներ կամ առցանցային օրագրեր:

Այնուամենայնիվ, ցանցն իր վատ կողմերը նույնպես ունի: Ցանցում նավարկելիս հեշտ է հանդիպել կայքերի, որ պարունակում են պոռնոգրաֆիա, ատելություն, բռնություն, անօրինական ու վտանգավոր բովանդակություն, կամ առաջարկում են ապորինի ծառայություններ: Երեխաների անձնական ապահովությունը կարող է ռիսկի ենթարկվել թե՛ կոմերցիոն կայքերի կողմից, որոնք պահանջում են

անձնական ինֆորմացիա, թե՛ երբ երեխաներն իրենք են հրապարակում կոնտակտային տեղեկություններ կամ նկարներ իրենց վեբ կայքերում:

Չնայած հրապարակված միլիոնավոր էջերին և նրանց, որ ուղարկվում են ամեն օր հրապարակվելու, ներցանցային հավաստի ինֆորմացիա գտնելը դժվար խնդիր է: Քանի որ ամեն ոք կարող է հրապարակել իր սեփական տեսակետը ցանցում, ցանցը պարունակում է հսկայածավալ ոչ հավաստի և կեղծ ինֆորմացիա: Ուսումնասիրությունները ցույց են տալիս, որ երիտասարդներն հակված են հավատալու, որ ,,եթե էկրանի վրա է, ապա պետք է որ այն ճիշտ լինի, ուստի կարևոր է սովորեցնել ձեր երեխաներին կասկածանքով վերաբերել ցանցում կարդացածին:

Եթե երեխաներն ունեն սեփական էջեր, ստուգեք՝ ի՞նչ են նրանք հրապարակում: Սովորեցրեք նրանց հարգել հեղինակային իրավունքը՝ չգողանալ այլ կայքերից և ուրիշի մասին անպարկեշտ ու նրան սպառնացող որևէ բան չտեղակայել ցանցում:

Խորհուրդ. Ստեղծեք ձեր ընտանեկան վեբ կայքը ձեր երեխաների օգնությամբ, տեղեկացրեք ձեր ընկերներին ու ազգականներին ձեր զբաղմունքների մասին:

Էլ-փոստ

Եթե ձեզ մատչելի է համացանցը, ուրեմն դուք էլ-փոստի հնարավորություն ունեք: Էլ-նամակի ուղարկումն ու ստացումը, որ իրականացվում է էլեկտրոնային փոստի միջոցով, համացանցի թիվ մեկ կիրառությունն է: Էլ-նամակը արագ, արդյունավետ և էժան ձև է երեխաների համար կապի մեջ մնալու ընկերների և ընտանիքի հետ և նույնիսկ աշխարհասփյուռ գրչընկերների խումբ (e-pals) ստեղծելու:

Չնայած օգտակարությանը, ամեն ոք, ով էլ-փոստ է օգտագործում, վտանգված է համացանցային թափոնով կամ անցանկալի էլ-նամակներով, որ ներհոսում են փոստարկղեր ամեն օր, որոնցից շատերը տհաճ են ու անպարկեշտ: Պարզվել է, որ անցանկալի էլ-նամակները կազմում են համացանցում ճամփորդող նամակների 40 տոկոսը: Երեխաները, որ չեն կարող քննադատաբար մտածել ստացած հաղորդագրությունների մասին, խոցելի են մասնավորապես գովազդների, խարդախությունների և անհանգստացնող հաղորդագրությունների նկատմամբ, որ ի հայտնվում են էլեկտրոնային փոստարկղում:

Համացանցային ծառայությունների մատակարարները հիմնականում ապահովում են իրենց հաճախորդներին անվճար էլ- փոստային հասցեներով: Եթե ձեր երեխաները փոքր են, խնդրեք ձեր մատակարաներին տրամադրել համատեղ էլ-փոստային հասցե, որպեսզի դուք կարողանաք հսկել երեխաների հաղորդագրությունները: Պաշտպանելու համար փոքր երեխաներին անցանկալի հաղորդագրություններ ստանալուց, սովորեցրեք նրանց երբեք չտալ իրենց էլ-հասցեն մեկին, ում չեն ճանաչում:

Եթե ձեր երեխաները մեծ են, հավանական է նրանք ունեն իրենց սեփական անվճար հասցեները այնպիսի կայքերում, ինչպիսիք են Google-ը ու Yahoo!-ն: Օգնեք նրանց տեղադրել զտիչներ (ֆիլտրեր) այդ հասցեների վրա խուսափելու անցանկալի հաղորդագրություններից և համոզվեք, որ գրանցվելու ընթացքում նրանք ընտրել են գովազդատուներից առաջարկություններ չստանալու և համացանցային տեղեկագրքերում չներառվելու տարբերակը: Խրախուսեք նրանց պահպանել իրենց էլեկտրոնային հասցեն և այն երբեք համացանցում չթողարկել:

Խորհուրդ. Ստեղծեք “թիրախ” էլեկտրոնային հասցե ձեր երեխաների համար ցանցում: Այն կպաշտպանի նրանց իսկական հասցեն աղբ էլ-նամակներից:

Բլոգ

Բլոգը (որ ծագում է "Web log" -ից "weblog") ցանցային օրագիր կամ ամսագիր է: Երեխաների համար հայտնի շատ բլոգային կայքեր կան, որ հնարավորություն են ընձեռում օգտվողներին ստեղծելու իրենց օրագրերը, որոնք պարունակում են նաև նկարներ և նույնիսկ տեսաերիզներ: Կարելի է ստեղծել ինտերակտիվ բլոգեր եւ հրավիրել մարդկանց մեկնաբանելու հրապարակված ինֆորմացիան:

Բլոգերը հեշտ է ստեղծել ու թարմացնել, որի պատճառով էլ դրանք չափազանց հանրահայտ են – միջին հաշվով յուրաքանչյուր 5.8 վայրկյանը մեկ նոր բլոգ է ստեղծվում և ավելի քան 3 բլոգեր թարմացվում են ամեն վայրկյան, իսկ Հյուսիսային Ամերիկայում 2005–ի հետազոտությունները ցույց են տալիս, որ դպրոցական օրվա ընթացքում 4-րդ դասարանի աշակերտների 14 տոկոսը գրում են բլոգում կամ ցանցային օրագրում:

Nexopia, Piczo, Facebook և LiveJournal-ը հայտնի բլոգային կայքեր են ուսանողների շրջանում: Խնդիրներ կարող են ծագել այն ժամանակ, երբ երեխաները հրապարակում են իրենց անձնական ինֆորմացիան, նկարները կամ տեսաերիզները այդ կայքերում կամ օգտագործում են իրենց բլոգերը՝ հասակակիցների և ուսուցիչների մասին ասեկոսեներ ու բամբասանքներ տարածելու համար:

Խորհուրդ: Երեխաներին անհրաժեշտ է հիշեցնել, որ համացանցում ուղարկված ամեն ինչ մատչելի է յուրաքանչյուրին և իրապես կարող է լինել համացանցում տարիներ շարունակ, այնպես որ նրանք պետք է զգույշ լինեն, որ իրենց բլոգը չպարունակի անձնական տվյալներ՝ կամ պատկերներ, կոպիտ կամ անպարկեշտ մեկնաբանություններ կամ ցանկացած բան որ կանհանգստացնի իրենց կամ ուրիշներին:

Որոնք են բլոգի օգուտները

Բլոգը տալիս է անձնական դրսեւորման համար առտակարգ հնարավորություն, թույլ է տալիս օգտվողներին համագործակցել եւ սովորել համագործակցելով:

Որոնք են ռիսկերը

Ռիսկը կապված է անձնական տվյալները հրապարակելու հետ, որոնք կարող են օգտագործվել կոմերցիոն նպատակներով: Այս դեպքում կարելի է կեղծ անուն օգտագործել: Եթե դուք նախատեսում ենք տեղադրել այլ մարդկանց մասին ինֆորմացիա, նաեւ լուսանկարներ, անհրաժեշտ է սկզբից ստանալ նրանց թույլտվությունը: Կա հեղինակային իրավունքի ռիսկ:

Ոչ մի դեպքում չի կարելի օգտագործել այլ մարդկանց նյութերը եւ նույնիսկ այլ կայքերի դիզայնը առանց թույլտվության: Երբեք չի կարելի ոչ պատշաճ բովանդակություն տեղադրել բլոգերում:

Ակնթարթային հաղորդակցում

Այսօրվա ցանցային սերնդի համար ակնթարթային հաղորդակցումը փոխարինում է հեռախոսին որպես ընկերների հետ խոսելու ամենանախընտրելի եղանակ: Երեխաները շտապում են տուն, մտնում ցանց և շարունակում դպրոցական խոսակցությունները, հաճախ ժամեր շարունակ մնալով ցանցում: Ակնթարթային հաղորդակցումը ընկերների հետ հաղորդակցման, հեռավոր վայրերում գտնվող մարդկանց

հետ կապի մեջ լինելու և դպրոցական ծրագրերը համակարգելու լավագույն անվճար միջոցն է երեխաների համար:

Շատ ծնողներ ակնթարթային հաղորդակցումը շփոթում են զրուցասենյակների հետ, երբ նրանց երեխաներն ասում են, որ իրենք ,,զրուցում են,, ցանցում: Երկու տեխնոլոգիաների միջոցով էլ ,,ներկա ժամանակում,, են զրուցում, բայց կարևոր տարբերություններ կան, որոնք երեխաների ապահովությանն են վերաբերվում:

Զրուցասենյակը մի վայր է համացանցում, որտեղ կարելի է խոսել աշխարհի ցանկացած մարդու հետ: Պատկերացրեք, բացում եք միջազգային հեռախոսագիրքը, ընտրում պատահական անծանոթների ու զանգում նրանց: Ակնթարթային հաղորդակցումն ավելի ապահով միջավայր է, քանի որ հնարավորություն է ընձեռում օգտվողներին ընտրել այն մարդկանց ում հետ ուզում ես խոսել: Օգտվողները ստեղծում են կոնտակտային ցանկեր և նրանք կարող են արգելափակել այն մարդկանց, ում չգիտեն կամ չեն ուզում հաղորդակցվել:

Չնայած երեխաները կարրող են վերահսկել ում հետ զրուցել, այնուամենայնիվ, հնարավոր է ակնթարթային հաղորդակցման ընթացքում հանդիպել անծանոթների: Հեղինակությունից ելնելով որոշ երեխաներ ունեն մոտ 100 հաղորդակցման ընկերներ, որոնցից շատերին նրանք երբևէ չեն հանդիպել:

Երեխաները ցանցում ավելի անկաշկանդ են ասելու բաներ, որ երբեք դեմ առ դեմ չէին ասի, այնպես որ ակնթարթային հաղորդակցումը կարող է օգտագործվել ասեկոսեներ ու բամբասանք տարածելու համար: Շատ երեխաների համար տունն այլևս ապաստարան չէ դպրոցում հասակակիցների ճնշումներից:

Շատ ծրագրեր առաջարկում են լրացնել ,,անձնական կենսագրություն,, , որ պարունակում է ամբողջական անձնական ինֆորմացիա: Այդ տվյալները մատչելի են ցանկացած մեկին համացանցում, որ ցանկանում է կարդալ: Երեխաներին պետք է սովորեցնել երբեք նման կարգի անձնական կենսագրությունները չլրացնել ցանցում:

Խորհուրդ. Նստե՞ք ձեր երեխաների հետ և ծանոթացեք նրանց հաղորդակցման կապերին՝ համոզվելու համար, որ նրանք անձամբճանաչումեն յուրաքանչյուրին:

Զրուցարաններ

Զրուցարանները տեղեր են համացանցում, ուր դուք կարող եք ուղիղ, իրական ժամանակում խոսակցություններ ունենալ շատ մարդկանց հետ: Ասես հեռախոսազրույցներ լինեն, միայն թե դուք խոսելու փոխարեն գրում եք: Ամեն ոք կարող է տեսնել ինչ է ամեն մեկը գրում, բայց դուք կարող եք մնալ ծածկանունով, եթե ուզում եք:

Զրուցարանները կարող են մշտական հանդիպման վայր լինել նույն հետաքրքրություններ ունեցող մարդկանց համար, միևնույն ժամանակ դրանք կարող են դառնալ նաև փնտրտուքի տարածք այն գիշատիչների համար, ովքեր հետապնդում են երեխաներն և փորձում կապ հաստատել նրանց հետ: Այդ պատճառով, երեխաները չպետք է լինեն զրուցարաններում: Ճիշտ այնպես, ինչպես մենք սովորեցնում ենք երեխաներին չխոսել անծանոթների հետ փողոցում, նրանք չպետք է խոսեն անծանոթների հետ ցանցում: Երբ նրանք մեծանան (10-13), այդ ժամանակ միայն կարող են մտնել վերահսկվող մանկական զրույցարաններ, և այդ ժամանակ նույնիսկ՝ մեծահասակի հսկողության տակ:

Զրուցարանները վերահսկվում են տարբեր կերպ: Որոշ կայքեր ունեն ծրագրային համակարգեր, որոնք անմիջապես հեռացնում են մարդկանց, ովքեր անպարկեշտ լեզու են օգտագործում, մինչդեռ մյուսների

համար ընդունելի է անմիջական և իրական հսկողությունը: Հիշեք, որ նույնիսկ վերահսկվող զրուցարաններում ոչինչ չի կարող ետ պահել մեծահասակներին մասնակցելու և ներկայանալու որպես երեխա:

Դեռահասները հատկապես խոցելի են զրուցարաններում: Նրանք փորձարկում են իրենց զգացմունքները՝ հեռանալով ծնողական հսկողությունից և փորձում հաստատել նոր հարաբերություններ ընտանիքից դուրս: Զրուցարանների ծածուկ միջավայրում նրանք ազատ են զգում լինելու առավել բաց և անկեղծ և խոսակցություններն արագ կարող են դառնալ մտերմիկ, նրանց դարձնելով խոցելի ներցանցային հետապնդողների համար:

Այս պատճառով, դեռահասներին պետք է քաջալերել օգտվել միայն վերահսկվող զրուցարաններից՝ պաշտպանելու համար նրանց անձնական ինֆորմացիան երբ նրանք ցանցում են և միշտ մնալ զրուցարանների հասարակական մասում (որոշ զրուցարաններ օգտվողներին առաջարկում են նաև մտնել ,,անձնական,, սենյակ կամ փոխանակել անձնական հաղորդագրություններ, որ ոչ ոք չի կարող տեսնել կամ վերահսկել) :

Խորհուրդ. Դրե՞ք ձեր Ինտերնետին միացած համակարգիչը ձեր տան երևացող մասում և ըդհանուր օգտագործման սենյակներում, ոչ մի դեպքում՝ երեխայի սենյակում:

Խորհուրդներ զրուցարաններում ապահով լինելու համար

- Հնարավորինս փակ պահեք ձեր անձնական տվյալները:
- Օգտագործեք բարդ ծածկագրեր: Ձեր ծածկագրերը պահեք ապահով:
- Մեկնաբանություն գրելուց առաջ 2 անգամ մտածեք, քանի որ երբ այն հայտնվեց Ինտերնետում, այն կարող է հավերժ մնալ այնտեղ:
- Մի վստահեք այն ամենին ինչ ասում են Ձեզ այլ մարդիկ, նրանք կարող են կեղծ անուններով հանդես գալ, կամ ստել:

Խորհուրդներ ուսուցիչներին և ծնողներին

Երեխաները պետք է սովորեն որոշակի կանոններ, սովորաբար դրանք նույն կանոններն են, որ իրական աշխարհում են գործում, օրինակ քաղաքավարության կանոններ:

Երեխաները պետք գիտակցեն, որ այն ինչ իրենք հրապարակում են ցանցում, հասու է դառնում ողջ մարդկությանը:

Լավագույն խորհուրդը ծնողներին ձեռք բերեք երեխաների վստահությունը, եւ ուղղորդեք նրանց: Գիտակցեք, որ այն պահից երբ հրապարակվեցին ձեր անձնական տվյալները դուք կորցնում եք այն վերահսկելու հնարավորությունը եւ չգիտեք թե ինչպես կօգտագործվեն այդ տվյալները:

Ցանցում հայտնվող մարդիկ միշտ չէ, որ այն են, ինչպես ներկայանում են:

Կայքի ստեղծողների հայտարարությունը, որ կայքը ծառայում է միայն դպրոցականների համար ոչինչ չի նշանակում:

Ֆայլերի փոխանակում

Ֆայլերի փոխանակումը, որ հայտնի է նաև որպես ապակենտրոնացված տեխնոլոգիա, թույլ է տալիս օգտվողներին փնտրել և ներբեռնել ֆայլեր այլ օգտվողների համակարգիչներից: Երիտասարդները օգտագործում են այս տեխնոլոգիան հեռուստատեսային շոուներից և ֆիլմերից երաժշտական կամ տեսաձայնային ֆայլերի շտապ փոխանակման համար:

Երեխաները ներբեռնելու մշակույթը որդեգրել հենց սկզբից: Զարգացած երկրներում անցկացված ուսումնասիրությունները ցույց են տալիս, որ երեխաների 65 տոկոսը ներբեռնում և լսում է ներցանցային երաժշտություն: Ֆիլմերի և հեռուստատեսային շոուների ներբեռնման հեղինակությունը աճում է. 4-րդ դասարանի աշակերտների 17 տոկոսն է այդպես վարվում օրվա կտրվածքով: Այդ թիվը 11-րդ դասարանում աճում է մինչև 40 տոկոս:

Ծնողների ակտիվ մասնակցության կարիքը կա այս ասպարեզում, անհրաժեշտ է քննարկել ֆայլերի փոխանակման էթիկան իրենց երեխաների հետ: Սա բարդ թեմա է շատ մարդկանց համար, կան շատ ծնողներ և երաժիշտներ, որ օժանդակում են ստեղծագործությունների ազատ տարածմանը:
Դուք կարող եք հարցնել երեխաներին արդյո՞ք համոզված են, որ ֆայլերի փախանակումը թույլատրված է: Ասեք նրանց, որ մտածեն արդյո՞ք արվեստագետները չպետք է փոխհատուցվեն, երբ նրանց երգերը փոխանակվում են ցանցի միջոցով: Եթե ամեն մեկը ֆայլեր փոխանակի, գումար կլինի՞ նոր արվեստագետների աճման ու առաջադիմության համար:

Մուտք գործելու համար ֆայլերի փոխանակման ցանց, օգտվողները կարիք ունեն ներբեռնելու հատուկ համակարգչային ծրագրեր: Այս ծրագրերը ցանցում ազատ են: Բայց հայտնի ծրագրերից շատերը լիքն են լրացուցիչ համակարգչային ծրագրերով, ինչպիսիք են լրտեսային ծրագրերը (spyware, կամ adware): Մեկ անգամ տեղադրվելով ձեր համակարգչում, այս ծրագիրը կարող է «հետևել». ու՞ր եք գնում համացանցում՝ ստեղծելով կապեր ցանցային կայքերում, որոնք օգտվողներին ուղարկում են գովազդներ և նույնիսկ ինֆորմացիա հավաքում ձեր համակարգչից, ինչպիսիք են գաղտնաբառեր, կրեդիտ քարտերի համարներ և էլեկտրոնային հասցեներ:

Ֆայլերի փոխանակմանը վերաբերող մեկ այլ նկատառում այն է, որ շատ մարդիկ օգտագործում են այս ցանցերը պոռնոգրաֆիկ նկարների ու տեսաերիզների առևտրի համար, դյուրին դարձնելով երեխաների համար անպարկեշտ նյութերի հայտնաբերումը: Այս խնդրի առումով դժվարությունն այն է, որ ծնողական ֆիլտրերը, որ նախագծված են արգելափակելու պոռնոգրաֆիան, չեն աշխատում ֆայլերի փոխանակման ծրագրերի հետ: Ֆայլերի փոխանակման որոշ ծրագրեր այժմ առաջարկում են իրենց ներքին ֆիլտրող համակարգերը, այնպես որ, ստուգեք՝ համոզվելու արդյո՞ք ծրագիրը, որից օգտվում են ձեր երեխաները, կարող է արգելափակել սեքսուալ բովանդակությամբ նյութը:

Խորհուրդ. Իմանալու համար թե ինչպես հեռացնել լրտեսող միջոցները ձեր համակարգչից, այցելեք *http://antivirus.about.com/od/spywareandadware/tp/ adwarespyware.htm*.

Հրապատ

Զտիչ, որն արգելափակում է ոչ հուսալի տեղեկությունների ներթափանցումը Համացանցից՝ նախքան դրանք կհասնեն համակարգիչ կամ մասնավոր ցանց: Այն լրացուցիչ պաշտպանություն է ապահովում նաև հակերներից և վիրուսներից: Հրապատը ապահովում է նաև համակարգչի անհատական տվյալների պաշտպանությունը՝ արգելելով թույլտվություն չունեցող օգտվողների կողմից համակարգիչ մուտք գործելը:

Էլ. փոստի հաղորդագրությունների զտում

Անհայտ անձինք կարող են ուղարկել էլ. փոստի բազմաթիվ հաղորդագրություններ: Էլ. փոստի նման հաղորդագրությունները, որոնք կոչվում են սպամ կամ թափոնափոստի հաղորդագրություններ, հաճախ կարող են վիրուսներ կամ լրտես ծրագրեր պարունակել: Անձնական տեղեկություններ ձեռք բերելու փորձեր կատարող հակերները նույնպես կարող են թափոնափոստի հաղորդագրություններ ուղարկել: Հետևաբար, այդ հաղորդագրություններից պետք է զգուշանալ: Էլ. փոստի ծրագրաշարերը հնարավորություն են տալիս ստեղծել հաղորդագրությունների զտիչներ՝ թափոնափոստի հաղորդագրություններն արգելափակելու համար: Բացի այդ, երբեք պետք չէ պատասխանել թափոնափոստի հաղորդագրություններին, քանի որ դա կարող է հանգեցնել անցանկալի նամակների թվի աճին և անձնական տեղեկությունների պատահական տրամադրման:

Բջջային հեռախոսներ

Բջջային հեռախոսների նոր սերունդը ունի Ինտերնետին միանալու հնարավորություն և կարող է տեսանկարահանել: Այս հեռախոսները նվազեցնում են ծնողների՝ իրենց զավակների ցանցային զբաղմունքների վրա ազդեցություն ունենալու հնարավորությունը, որովհետև ի տարբերություն համակարգչի, որ տեղադրված է տան կամ դպրոցի երևացող մասում՝ բջջային հեռախոսները անձնական են, ունեն կապ և միշտ մատչելի են:

Կարճ հաղորդագրությունների ուղարկումը, որ հայտնի է որպես SMS (կարճ հաղորդագրության համակարգ) սիրված է երեխաների շրջանում՝ ավելի էժան է ուղարկել հաղորդագրություն, քան զանգել, և կարելի է ուղարկել հաղորդագրությունները միաժամանակ շատ մարդկանց:

Երեխաներն օգտագործում են SMS լեզուն, որում կարճ ձևեր են և հապավումներ են օգտագործվում, որ նույնպես ընդունված են զրուցասենյակներում և ակնթարթային հաղորդակցման ժամանակ: SMS ժարգոնով գաղնագրված խոսակցությունները մտահոգում են շատ մեծահասակների:

Օրինակ, սա կարճ SMS հաղորդագրություն է. ,,Ոնց էր Յվա քեֆը? Լավ :)? Պիտի գնամ: Ց.,, Թարգմանությունը. ,,Ո՞նց էր երեկվա քեֆը: Լավ ուրախացա՞ք: Պիտի գնամ: Ցտեսություն:,,

Ինչպես համացանցը՝ այս դեպքում ևս, ծնողներն ու երեխաները տարբեր կերպ են օգտագործում բջջային հեռախոսները: Շատ ծնողներ բջջային հեռախոսները գործիք են համարում, մինչդեռ երեխաների համար դրանք նրանց հասարակական կյանքի ու զվարճալիքների անբաժան մասն են: Ի տարբերություն ծնողների, որ համարում են բջջային հեռախոսները երբեմն ձանձրացնող, և անջատում ու միացնում են հեռախոսները ըստ անհրաժեշտության, երեխաները միշտ միացրած են պահում իրենց հեռախոսները, որ միշտ հասանելի լինեն իրենց ընկերների համար, և ոչ միայն ծնողների:

Մեծանում է այն երեխաներ թիվը, որ օգտագործում են բջջային հեռախոսները հասակակիցների հանդեպ ագրեսից վարքագիծ դրսևորելու համար: Քանի որ երեխաները հակված են իրենց հեռախոսները միշտ միացված պահել, վիճաբանությունները կարող են լինել անդադար՝ դպրոցում, տանը և նույնիսկ նրանց սեփական սենյակում: Եթե ձեր երեխան այդպեսի վիճաբանությունների մեջ է, այդ խնդրի մասին անմիջապես հայտնեք ձեր հեռախոսային ծառայությունների մատակարարին, եթե խնդիրը չի լուծվում կարող եք փոխել հեռախոսահամարը:

Սոցիալական ցանց

Սոցիալական ցանցերը ընդհանուր հետաքրքրքրություններ ունեցող մարդկանց վիրտուալ համայնքներ են: Օգտվողները այդ ցանցերում շփվելու եւ ինքնարտահայտվելու հնարավորություն են ստանում հաղորդակցական տարբեր՝ chat, messaging, բլոգ, էլեկտրոնային փոստ, տեսանյութ գործիքների միջոցով: Այսպիսի ցանցերը բնութագրում են WEB-2 ը, քանի որ բովանդակության զգալի մասը ստեղծվում եւ տարածվում են բուն օգտվողների կողմից: Ցանցերը կառուցվել են հետեւյալ սկզբունքով՝ ցանցի հիմնադիրները հրավիրում են մարդկանց միանալ, նոր անդամները նոր մարդկանց են հրավիրում եւ այդպես շարունակ: Անդամները կարող են ունենալ իրենց սեփական էջերը, նկարներով, բլոգերով եւ այլն:

Որոնք են ցանցերի օգուտները

Սոցիալական ցանցերը սովորելու, ազատ արտահայտվելու եւ հաղորդակցվելու հնարավորություն են տալիս: Նրանց միջոցով ձեւաորվում են նաեւ ընդհանուր հետաքրքրքրություններ ունեցող ակտիվ մարդկանց համայնքներ:
Նկարիչները կարող են ցուցադրել իրենց աշխատանքները, ցանկացած մարդ կարող է վաճառել կամ գովազդել իր աշխատանքի արդյունքները: Պատանիները ավելի շատ հակված են ինքնաարտահայտման եւ շատ արագ համախմբվում եւ քննարկում են հրատապ հարցերը:

Որոնք են ռիսկերը

Այս ցանցերը հասարակական վայրեր են եւ ցուցադրվող բովանդակությունը հասանելի է ողջ հասարակությանը: Ցանկացած մարդ կարող է տարածել ոչ պատշաճ բովանդակություն եւ երեխան կարող է ոչ միայն է զոհ դառնալ ագրեսիվ վարքագծի, այլ նաեւ ներքաշվել այլ մարդկանց դեմ ուղղված գործողությունների մեջ: Ցավոք սրտի սոցիալական ցանցերի մեծ մասը այնպես են կառուցված որ, անձնական նկարագրերը հասանելի են օգտվողներին, երեխան պետք արդեն հմուտ օգտվող լինի, որպեսզի իմանա ինչպես պաշտպանել իր անձնական տվյալները:

Որոնք են վտանգները

- Այլասերված մեծահասակներ, որոնք երեխա են ձեւանում
- Չկան տեխնոլոգիաներ, որոնք կարող կանխել մեծահասակներին մանկա-պատանեկան ցանցերում գրանցվելուց:
- Անհատական տեղեկատվության տարածում
- Ժամանակի վատնում, Ինտերնետից կախվածություն: Երեխաները կարող են օրեր շարունակ անցկացնել ցանցում անընդհատ փոփոխելով իրենց նկարագիրը (պրոֆայլը) եւ հաղորդակցվելով:
- Ագրեսիայի դրսեւորում:
- Շատ կայքեր թույլ են տալիս այլ անդամների գնահատել ձեր նկարագիրը (պրոֆայլ), արդյունքում կարող են հայտնվել անպարկեշտ մեկնաբանություններ:

Ինչ խորհուրդ կարելի է տալ ծնողներին

Երեխաները պետք է սովորեն որոշակի կանոններ, սովորաբար դրանք նույն կանոններն են, որ իրական աշխարհում են գործում, օրինակ քաղաքավարության կանոններ: Երեխաները պետք գիտակցեն, որ այն ինչ իրենք հրապարակում են ցանցում, հասու է դառնում ողջ մարդկությանը: Լավագույն խորհուրդը ծնողներին ձեռք բերեք երեխաների վստահությունը, եւ ուղղորդեք նրանց:
Գիտակցեք, որ այն պահից երբ հրապարակվեցին ձեր անձնական տվյալները դուք կորցնում եք այն վերահսկելու հնարավորությունը եւ չգիտեք թե ինչպես կօգտագործվեն այդ տվյալները: Լուսանկարները

կարող են մեկ մատի շարժումով բազմացվել եւ հասու դառնալ հազարավոր մարդկանց: Նկարների թվանշային բնույթը թույլ է տալիս դրանք փոփոխությունների ենթարկել եւ աղճատել:
Ցանցում հայտնվող մարդիկ միշտ չէ, որ այն են, ինչպես ներկայանում են: Ցանկացած մարդ կարող է բացել օգտվողի պրոֆիլ, իրեն դնելով մեկ ուրիշի տեղ: Կայքի ստեղծողների հայտարարությունը, որ կայքը ծառայում է միայն դպրոցականների համար ոչինչ չի նշանակում: Ավելին յուրաքանչյուր մարդ կարող է հարյուրավոր կայքերում ներկա գտնվել:

Խորհուրդներ երեխաներին սոցիալական ցանցում ապահով լինելու համար

Հնարավորինս փակ պահեք ձեր անձնական տվյալները եթե որոշել եք դրանք հրապարակել: Օգտագործեք ծածկագրեր, որպեսզի միայն ձեր ընկերները կարողանան կարդալ: Ձեր ծածկագրերը պահեք ապահով:

Մեկնաբանություն գրելուց առաջ 2 անգամ մտածեք, քանի որ երբ այն հայտնվեց Ինտերնետում, այն կարող է հավերժ մնալ այնտեղ: Մի վստահեք այն ամենին ինչ ասում են Ձեզ այլ մարդիկ, նրանք կարող են կեղծ լուսանկարներ օգտագործել, կամ ստել: Ուշադիր եղեք թե ում հետ եք շփվում, հատկապես երբ ձեր ընկերների ցանկում ընդգրկում եք նոր մարդու: Եվ ուշադիր եղեք անծանոթ մարդկանց նկատմամբ, ովքեր Ձեզ հրավիրում են միանալ իրենց համայնքին: Պարզեք թե ինչ են ուրիշները տեղադրում ցանցում Ձեր մասին եւ զգուշացրեք նրանց եթե դուք համաձայն չեք այդ ինֆորմացիայի հետ:

Phishing, կամ որսում

Phishing-ը դա անհատին հնարքների միջոցով թյուրիմացության մեջ գցելն է, ստիպելով նրան կամավոր տրամադրել իր անձնական տվյալները. Արդյունքում գողանում կամ կեղծում են անհատի տվյալները եւ ստանում մուտք նրա հաշվեհամարներին, էլեկտրոնային փոստին, PIN կոդերին եւ այլն:

Օրինակ, օգտվողները ստանում են email, որը թվում է թե բանկից է եկել. Այդ նամակում հաճախակի խոսում են բանկային համակարգի անվտանգության մասին եւ խնդրում են մուտք գործել որոշակի վեբ կայք, որը նույնպես այնպիսի տեսք ունի կարծես ձեր բանկին է պատկանում եւ մուտքագրել ձերծածկագրերը եւ այլն. Պետք միշտ հիշել որ ոչ մի բանկ երբեք իր հաճախորդներից չի հարցնի անձնական տվյալները էլեկտրոնային նամակով կամ հեռախոսով:
Նման նամակների մասին անմիջապես տեղյակ պահեք ձեր բանկին:
Ստուգեք բանկի դոմեյնը եւ նրա հղումը տվյալ կայքի վրա:

Ուշադիր եղեք խարդախությունների նկատմամբ

Որոշ նշանների միջոցով կարելի է տարբերակել նմանատիպ նամակները

- Մեծ շահման մասին հայտարարություններ
- Հայտնի ընկերությունների կողմից արվող առաջարկություններ
- Առաջարկներ, որոնք շատ գրավիչ են ճշմարիտ լինելու համար
- Տառասխալներ կամ քերականական սխալներ նամակներում

Օգտագործեք Anti-Phishing և anti-spam տեխնոլոգիաներ նմանատիպ նամակներից խուսափելու համար

Հեղինակային իրավունք

Կայքերի մեծ մասում առկա նյութերը հիմնականում պաշտպանված են հեղինակային իրավունքով, և դրանց օգտագործումն առանց թույլտվության կարող է իրավական խնդիրներ առաջացնել:Համացանցում կարելի է գտնել տարատեսակ տեղեկություններ՝ նորություններ, հոդվածներ, նկարներ, երգեր, տեսանյութեր և ծրագրեր:
Կայքերից տեղեկություններ ներբեռնելը հիմնականում անվճար է: Սակայն, կայքերում տեղեկությունը համարվում է հեղինակի կամ կայքի սեփականությունը: Այդ պատճառով, այդ տեղեկություններն օգտագործելու համար անհրաժեշտ է ստանալ հեղինակի կամ կայքի սեփականատիրոջ թույլտվությունը: Որևէ մեկի աշխատանքը պատճենելը և այն, առանց աղբյուրին հղում կատարելու, օգտագործելը սեփական աշխատանքում կոչվում է *գրագողություն*: Շատ կայքեր երգերի ներբեռնման և համատեղ օգտագործման հնարավորություն են տալիս: Սակայն, դրանց մի մասը կարող է երգերն անվճար ներբեռնելու հնարավորություն տրամադրելու իրավունք չունենալ: Այդ կայքերից երգերի ներբեռնումը հեղինակային իրավունքով պաշտպանված երաժշտության օգտագործման կանոնների խախտում է:

Առանց հեղինակային իրավունքի իրավատիրոջ կողմից լիցենզիա կամ թույլտվություն ստանալու հեղինակային իրավունքով պաշտպանված ծրագրաշարի չթույլատրված պատճենումը համարվում է ծրագրաշարի գողություն:Պատկերանշանը հեղինակային իրավունքով պաշտպանված նյութ է, որն օգտագործվում է հեղինակային իրավունքի իրավատիրոջ կողմից որպես նույնացման նշան: Առանց իրավատիրոջ թույլտվության պատկերանշանի պատճենումը կամ օգտագործումը անօրինական է:
Հեղինակային իրավունքով պաշտպանված նյութերից փոքր մասերի՝ ուսումնական նպատակներով օգտագործումը և դրանց աղբյուրը նշելը համարվում է հեղինակային իրավունքով պաշտպանված նյութի բարեխիղճ օգտագործում: Կայքերից նյութեր պատճենելու և աշխատանքում օգտագործելու փոխարեն կարելի է այդ նյութերին հղումներ կատարել: Այդ կերպ կարելի է ընդհանրապես խուսափել հեղինակային իրավունքով պաշտպանված նյութի գրագողությունից:

Pharming, կամ դոմեյնի կեղծում

Pharming- ը դոմեյնի անվանվան կեղծում է, որի արդյունքում օգտվողներին ուղղորդում է կեղծ կայքը: Օգտվողները սկսում են իրականացնել գործառույթներ կեղծ կայքի միջոցով , ինչը ենթադրում է անձնական տվյալների մուտքագրում, ինչպես նաեւ հաշվեհամարների եւ վարկային քարտերի տվյալների մուտքգրում: Այս դեպքում կեղծ կայքի հեղինակները կարող են օգտագործել տվյալները սեփական նպատակների համար:

Այլ մարդկանց տվյալների որսում, անձնական տվյալների գողություն

Ոչ վստահելի կոմերցիոն կայքերը կարող են չկատարել պայմանագրով ստանձնած իրենց պարտավորությունները, կարող են ոչ նպատակային օգտագործել ձեր անձնական տվյալները եւ ֆինանսական տեղեկությունները: Կոմերցիոն վեբ-կայքերը կարող են նաեւ երեխաներին առաջարկել ծառայություններ, որոնք ապօրինի են: Հաճախակի նման կայքերը ստեղծվում են այն երկրներում ուր չկան իրավական արգելող մեխանիզմներ:
Ինչպես տարբերակել նման կայքերը. իրական կյանքում ճանաչված եւ կայացած ընկերությունները վստահելի են նաեւ առ-ցանցում: Այլ նշաններ՝
Առկա են՝

1. Ընկերության անունը, հասցեն, հեռախոսի համար եւ այլն

2. Պայմանագրի ժամկետները թափանցիկ են
3. Ապրանքի հատկանիշները եւ երաշխիքները հստակորեն սահմանված են
4. Ապրանքի գնի մեջ ներառված են բոլոր լրացուցիչ ծախսերը
5. Առաջարկվում է վճարման անվտանգ եղանակ
6. Պատվերները հաստատվում են էլ.փոստով
7. Գնորդը հնարավորություն ունի ետ վերցնելու իր գումարը
8. Առաքման ժամկետը հստակ սահմանված է

Տեղական էլեկտրոնային խանութներից օգտվելը նվազեցնում է ռիսկերը:

Ինչպես ճանաչել վճարման անվտանգ եղանակները

Վստահելի առեւտրային կայքերը գործառույթները իրականացնում են միայն “secure electronic transaction” միջոցով. Ձեր ֆինանսական ինֆորմացիան մուտքագրելիս , միշտ ստուգեք արդյոք ձեր այցելած կայքի հասցեն սկսվում է “https://” թե “http://”. Այդ դեպքում դուք կիմանաք իրականացնում է արդյոք տվյալ կայքը անվտանգ գործառույթ:

Ինչպես խուսափել առ-ցանց գնումների ռիսկերից

Առ-ցանց վաճառքի հիմնական ռիսկը կանխավճարն է: Եթե ձեր գործընկերը ստանում է փողը, բայց չի կատարում մատակարարումը, շատ դժվար է ետ ստանալ ձեր գումարը:

Ինչ է ինքնության գողությունը

Ինքնության կողոպուտ տեղի է ունեցել երբ անհատի անձնական տվյալները գողացել են եւ օգտագործել ապօրինի ձեւով:

Համացանցի մասին հաճախակի տրվող հարցեր

1. Ո՞ր տարիքից կարելի է թույլ տալ երեխաներին համացանց մտնել:
2. Պե՞տք է թույլ տալ երեխաներին ունենալու իրենց անձնական էլեկտրոնային հասցեն:
3. Ի՞նչ տնային կանոններ պիտի ունենալ համացանցի օգտագործման համար:
4. Քանի՞ տարեկան պիտի լինի երեխան Ակնթարթային հաղորդակցման ծրագրեր օգտագործելու համար:
5. Կարո՞ղ եմ ես կարդալ իմ երեխայի հաղորդագրությունները:
6. Պետք են արդյո՞ք երեխաները օգտագործեն բլոգներ կամ սոցիալական ցանցեր, ինչպիսիք են Facebook-ը ևOdnoklassniki-ն:
7. Արդյո՞ք վեբխցիկները հուսալի են երեխաների օգտագործման համար:
8. Ինչպե՞ս կարող եմ կանխել pop - up պատուհանների մուտքը իմ համակարգիչ:
9. Կարո՞ղ են երեխաները կախվածություն ձեռք բերել համացանցից:
10. Ի՞նչ պետք է իմանան իմ երեխաները համակարգչային վիրուսների մասին:
11. Ինձ անհագստացնում է ինչպե՞ս են իմ երեխաները համացանց օգտագործում: Կարո՞ղ եմ տեսնել ինչ կայքեր են նրանք այցելում ցանցում:
12. Ի՞նչ պետք է անեմ, եթե իմ երեխային անհանգստացնում են համացանցում:
13. Արդյո՞ք օգտակար են ֆիլտրող ծրագրերը:
14. Իմ փոքրիկը ցանկանում է գնումներ կատարել համացանցում: Ինչպես կարող եմ համոզված լինել, որ կայքն ապահով է:

15.Ի՞նչ կետեր պետք է պարունակի մանկական կայքի քաղաքականությունը անձնական տվյալների պաշտպանության առումով:

1. Ո՞ր տարիքից կարելի է թույլ տալ երեխաներին համացանց մտնել:

Հետզհետե երեխաները համացանց են մտնում ավելի վաղ տարիքից. Զարգացած երկրներում համացանցից օգտվող նախադպրոցականների թիվը աննախադեպ աճում է: Շատ երեխաներ համացանցից օգտագործում նաև դպրոցում՝ վեց տարեկանից, այնպես որ, իրականում նրանք պիտի որ ցանկանան համացանց մտնել այդ տարիքից: Այնուամենայնիվ, տաս տարեկանից փոքր երեխաները հիմնականում քննադատական հմտություններ չունեն համացանցում մենակ լինելու համար, հետևաբար, մինչ այս տարիքը դուք պետք է մշտապես մասնակցեք նրանց համացանցային գործունեությանը: Եղեք երախաների հետ, երբ նրանք համացանցում են: Համոզվեք, որ նրանք օգտնվում են ձեր նախընտրած կայքերից: Սովորեցրեք նրանց երբեք չբացահայտել անձնական ինֆորմացիան համացանցում:

2. Պե՞տք է թույլ տալ երեխաներին ունենալու իրենց անձնական էլեկտրոնային հասցեն:

Փոքր երեխաները նախընտրելի է, որ օգտվեն ընտանեկան էլեկտրոնային հասցեներից, քան թե ունենան իրենց սեփականը: Երբ նրանք մեծանան և ցանկանան լինել ավելի անկախ, կարող եք նրանց տալ անձնական հասցե: Այն կարող է տեղակայված լինել ընտանեկան փոստարկղում, որպեսզի դուք կարողանաք տեղեկանալ ստացած կասկածելի թվացող հաղորդագրությունների մասին: Հարցրեք ձեր համացանցային ծառայության մատակարարին, թե ի՞նչ ծառայություններ է ապահովում ընտանեկան էլեկտրոնային հասցեների համար:

7 դասարանում արդեն շատ երեխաներ ուզում են ունենալ իրենց սեփական համացանցային հասցեն, այն կորող է լինել Gmail, Yahoo! ազատ համակարգերում: Համոզվեք, որ նրանք ձեռնարկել են բոլոր նախազգուշական միջոցառումները՝ պահպանելու համար իրենց էլեկտրոնային հասցեն օտարների կողմից էլ-հաղորդագրություններ ստանալուց:

3. Ի՞նչ տնային կանոններ պիտի ունենալ համացանցի օգտագործման համար:

Կարևոր է իմանալ, որ կանոնները դրական ազդեցություն ունեն երեխաների վարքի վրա: Հետազոտությունները ցույց են տալիս, որ օրինակ՝ 'իրական կյանքում չի կարելի ինտերնետային ծանոթին հանդիպել' կանոնին ծանոթանալուց հետո մեկուկես անգամ կրճատվում է սխալ վարվելու հավանականությունը: Չնայած երեխաները հակված են խախտելու կանոնները, սակայն դրանց գոյությունը դրական դեր է ունենում իրենց վարքագծի վրա:

Օրինակ՝այն 8-9 դասարանցիները, որոնց ընտանիքներում ընդունված չեն համացանցից օգտվելու կանոնները, կրկնակի անգամ ավելի հակված են մտնելու անպատշաճ բովանդակությամբ կայքեր:

Կարևոր է իմանալ, որ կանոնները դրական ազդեցություն ունեն երեխաների վարքի վրա: Հետազոտությունները ցույց են տալիս, որ օրինակ՝ 'իրական կյանքում չի կարելի ինտերնետային ծանոթին հանդիպել' կանոնին ծանոթանալուց հետո մեկուկես անգամ կրճատվում է սխալ վարվելու հավանականությունը: Չնայած երեխաները հակված են խախտելու կանոնները, սակայն դրանց գոյությունը դրական դեր է ունենում իրենց վարքագծի վրա:

Օրինակ՝ այն 8-9 դասարանցիները, որոնց ընտանիքներում ընդունված չեն համացանցից օգտվելու կանոնները, կրկնակի անգամ ավելի հակված են մտնելու անպատշաճ բովանդակությամբ կայքեր:

Համաձայնության եկեք համացանցի օգտագործման կանոնների մասին ձեր երեխաների հետ՝ ձևակերպելով տանը համակարգչից օգտվելու իրավունքներն ու պարտականությունները: Համոզվեք, որ համաձայնությունը հստակ է. որտե՞ղ կարող են ձեր երեխաները գնալ ցանցում և ի՞նչ կարող են անել նրանք այնտեղ, որքա՞ն ժամանակ կարող են նրանք անցկացնել համացանցում, ի՞նչ անել, երբ ինչ-որ բան անհանգստացնում է նրանց, ինչպե՞ս պահպանել սեփական ինֆորմացիան, ինչպե՞ս ապահովել անվտանգությունը ինտերակտիվ միջավայրերում և ինչպե՞ս վարվել բարեկիրթ և պատասխանատվորեն, երբ ցանցում են:

Ձեր երեխաների մասնակցությունը կարևոր է համաձայնության գալու համար: Տպեք և ունեցեք այն տնային համակարգչի մոտ՝ հիշեցնելու բոլորին այդ կանոնների մասին: Պարբերաբար վերանայեք այն և թարմացրեք՝ ձեր երեխաների մեծանալուն զուգընթաց:

4. Քանի՞ տարեկանից թույլ տալ երեխային օգտվել ակնթարթային հաղորդակցման ծրագրերից:

Զարգացած երկրներում ակնթարթային հաողրդակցումը փոխարինել է հեռախոսին որպես հաղորդակցության հիմնական միջոցի նույնիսկ 4-րդ դասարանի աշակերտների համար: Հետազոտությունները ցույց են տալիս, որ այդ երկրների 5-րդ դասարանի աշակերտների 43 տոկոսը օրվա ընթացքում հաղորդակցվում է հաղորդագրություններով, այնպես որ այս ընդունված միջոցի չընդունումը կսահմանափակի ձեր երեխայի հասարակական կյանքը: Այն պահից երբ երեխաները սկսում են օգտագործել ակնթարթային հաղորդակցությունը, մեծանում է ծնողների դերը՝ ապահովելու համար նրանց անձնական տվյալների ապահովությունը և օգնելու նրանց պատասխանատվությամբ կիրառել այդ տեխնոլոգիան:

Անկթարթային հողորդակցման կանոնները պետք է ընդգրկեն հետևյալը.

- չլրացնել անձնական կենսագրությունը,
- երբեք չխոսել անծանոթի հետ (պետք է պարբերաբար ստուգել նրանց զրուցակիցների ցանկը՝ համոզվելու համար, որ երեխաները գիտեն յուրաքանչյուրին),
- չուղարկել ասեկոսեներ, բամբասանքներ կամ չարակամ և ագրեսիվ հաղորդագրություններ՝ օգտագործելով ծառայությունը:

5. Կարո՞ղ եմ ես կարդալ իմ երեխայի հաղորդագրությունները:

Այո՛: Ակնթարթային հաղորդակցման ծրագրերը կարող են զրույցը ավտոմատ պահպանել է ձեր համակարգչում: Գտեք "My chat logs" թղթապանակը, սովորաբար այն լինում է C:\My Documents\. –ում է: Սակայն եթե երեխաները գիտեն այս հնարավորության մասին, նրանց համար դժվար չէ արգելափակել այս հատկանիշը: Ի վերջո, բաց զրույցներ ունենալը երեխաների հետ ավելի նախընտրելի է նրանց լրտեսելուց: Ինչ վերաբերում է տեխնոլոգիաներին՝ երեխաները միշտ մի քայլ առաջ են ծնողներից: Ավելի լավ է երեխայի հետ միասին կանոններ մշակել և վստահ լինել, որ երեխան կհետևի դրանց:

6. Պետք են արդյո՞ք երեխաները օգտագործեն բլոգներ կամ սոցիալական ցանցեր, ինչպիսիք են Facebook-ը և Odnoklassniki-ն:

Հետազոտությունները ցույց են տալիս, որ սոցիալական ցանցերը մեծ սեր են վայելում երեխաների շրջանում, զարգացած երկրներում այդ կայքերը հատկապես շատ են սիրված 8-11 տարեկան աղջիկների

կողմից: Օգտվողները ստեղծում են իրենց կենսագրությունները այս կայքերում, հաճախակի մուտքագրելով անձնական ինֆորմացիա և նկարներ: Facebook-ը և Odnoklassniki-ն մեծահասակների համար նախատեսված սոցիալական ցանեցեր են, և եթե երախան գրանցվում է այդ ցանցերում, ապա կա ռիսկ, որ կարող է հանկարծակի ոչ պատշաճ բովանդակություն հանդիպել: Եթե ձեր երեխաները օգտվում են բլոգներից և սոցիալական ցանցերից, պետք է հետևեք, որ ոչ մի անձնական ինֆորմացիա կամ նկար չի հրապարակվում:

7. Արդյո՞ք վեբխցիկները հուսալի են երեխաների օգտագործման համար:

Մատչելի գներն ու օգտագործելու դյուրին լինելը վեբխցիկները հետզհետե ավելի հեղինակավոր են դառնում երեխաների շրջանում: Ուսումնասիրությունները ցույց են տալիս, որ զարգացած երկրներում երեխաների 22 տոկոսը ունեն վեբխցիկներ (11 տարեկանների 31%): Ապահովության և անվտանգության համար վեբխցիկները չպիտի միացված լինեն համակարգիչներին երեխաների սենյակում, որտեղ նրանց օգտվելը չի վերահսկվում: Կարևոր է հաստատել ընտանեկան կանոններ վեբխցիկների համար, որոնք ներառում են հետևյալը.

- օգտագործել վեբխցիկից ծանոթ մարդկանց հետ,
- միշտ պահել ոսպնյակի գլխիկը փակ կամ վեբխցիկը հոսանքից անջատած, երբ համակարգիչը չի օգտագործվում,
- երբեք չանել որևէ բան վեբխցիկի դիմաց, եթե չեք ուզում ողջ աշխարհը տեսնի,
- ցանց չուղարկել վեբխցիկի տեսաերիզներ:

8. Ինչպե՞ս կարող եմ կանխել pop-up պատուհանների մուտքը իմ համակարգիչ:

Pop-up պատուհաններից խուսափելու ամենահեշտ ձևը արգելափակող ծրագրերի օգտագործումն է, որ կարող եք գնել կամ ներբեռնել համացանցից: Կարող եք օգտագործել նաև հատուկ "գործիքներ" ձեր զննարկիչով: Շատ գործիքներ թույլ են տալիս սեղմելով կոճակը՝ արգելափակում pop-up պատուհանները և ապա կրկին սեղմելով վերացնել արգելափակումը: Հատուկ գործիքների կիրառումը անհատական տվյալների պաշտպանության առումով որոշակի խնդիրներ է հարուցում, քանի որ այն կարող է օգտագործվել ձեր համացանցային պատմությունը գրանցելու համար:

Դուք կարող եք որևիցե համակարգչային խանութից pop-up պատուհանների արգելափակման գործիքներ ձեռք բերել կամ ներբեռնել հետևյալ կայքից՝

http://download.cnet.com/1770-20_4-0.html?searchtype=downloads&query=Pop-up+blocker&tg=dl-20

9. Կարո՞ղ են երեխաները կախվածություն ձեռք բերել համացանցից:

Համացանցը հրաշալի միջոց է երիտասարդների համար, հատկապես նրանց, ովքեր իրենց հասակակիցների հետ հաղորդակցման դժվարություններ ունեն: Համակարգչին լավ տիրապետող երեխաները կարող են փայլել համացանցում, որովհետև տեսքն ու մարզական կարողությունները կարևոր չեն և այն կարող է օգնել բարձրացնելու իրենց ինքնագնահատականը: Այնուամենայնիվ, չափից ավելի համակարգչի օգտագործումը կարող է նպաստել ինքնամփոփ երեխաների ավելի մեկուսացմանը իրենց հասակակիցներից կամ խանգարել ուսումնառությանը:

Ծնողները և ուսուցիչները սովորաբար տեղյակ չեն լինում այս զարգացումների մասին, մինչ լուրջ խնդիրներ ի հայտ չեն գալիս: Մի կողմից ցանցային գործունեությունը հեշտ է թաքցնել ծնողների

ուշադրությունից, մյուս կողմից համացանցից կախվածության վտանգը լայնորեն ճանաչում չի ստացել առ այսօր:

Սահմանեք համակարգչի օգտագործման կանոններ և փորձեք համատեղել այն ավելի ակտիվ ֆիզիկական գործունեությամբ: Մի մոռացեք, որ համացանցին միացած համակարգիչը պետք է լինի երևացող տեղում, այլ ոչ թե երեխայի սենյակում:

Եվ վերջապես, հետևեք որքան ժամանակ եք ինքներդ օգտագործում համացանցը: Արդյո՞ք դուք ժամեր չեք անցկացնում ցանցում: Եթե այո, ապա ձեր երեխաները, բնականաբար, կհետևեն ձեր օրինակին:

10. Ի՞նչ պետք է իմանան իմ երեխաները համակարգչային վիրուսների մասին:

Վիրուսը վնասակար համակարգչային ծրագիր է, որ «վարակում է» համակարչի ֆայլերը բազմաթիվ պատճեններ թողնելով: Երեխաների կողմից համացանցի որոշ կայքերի օգտագործումը կարող են խոցելի դարձնել համակարգիչները վիրուսների նկատմամբ: Էլ-փոստին կցված ֆայլերը վիրուսների փոխանցման ամենատարածված ձևն են, բայց վիրուսները կարող են ներբեռնվել նաև ֆայլերի փոխանակման և ակնթարթային հաղորդակցման ծրագրերի միջոցով: Տեղեկացրեք երեխաներին, որ չի կարելի բացել անծանոթ մարդկանցից ստացած էլեկտրոնային նամակները և կցված ֆայլերը; չի կարելի ներբեռնեն ֆայլեր, որ վերջանում են ".exe"-ով, երբ օգտագործում են ֆայլերի փոխանակման ծրագրերը; ակնթարթային հաղորդակցման ծրագրերը պետք է կարգավորվեն այնպես, որ հնարավոր չլինի ստանալ ֆայլեր այլ օգտվողների կողմից; երբեք չի կարելի ներբեռնել ծրագրեր առանց ծնողների թույլտվության: Դուք կարող եք պաշտպանել ձեր համակարգիչը ժամանակակից հրապատ (firewall) և հակավիրուսային ծրագրերի օգնությամբ:

11. Ինձ անհագստացնում է ինչպե՞ս են իմ երեխաները համացանց օգտագործում: Կարո՞ղ եմ տեսնել ինչ կայքեր են նրանք այցելում ցանցում:

Այո, դուք կարող եք տեսնել նրանց “ինտերնետային պատմությունը”, բայց համակարգչին լավ տիրապետող երեխաները գիտեն՝ ինչպես թաքցնել իրենց “համացանցային հետագծերը”: Համացանցի օգտագործման կանոնները պարզաբանելն ու բաց երկխոսությունը երեխաների հետ ավելի օգտակար են, քան նրանց անձնական աշխարհի ներխուժելը:

Երբ դուք նավարկում եք համացանցում, ձեր վեբ զննարկիչը (Microsoft Internet Explorer կամ Google Chrome) հավաքում է տեղեկություն այն տեղերի մասին, ուր այցելել եք և պահում այն համակարգչում:

Զննարկիչները սովորաբար պահպանում են վերջին այցելած կայքերի “պատմությունը”: Internet Explorer-ի շատ տարբերակներ ունեն History կոճակ՝ վերևի գործիքների մեջ: Եթե դուք չեք տեսնում կոճակը կամ Netscape օգտվող եք, պարզապես սեղմեք Ctrl (control) և H կոճակները միաժամանակ , որը նույնպես ցույց կտա պատմության ցանկը: Կրկնակի սեղմումով կկարողանաք տեսնել կայքը:

Զննարկիչները նույնպես վեբ էջերի ժամանակավոր կրկնօրինակներ են ստեղծում, որ հայտնի են որպես cache files (թաքնված ֆայլեր) և պահպանում են դրանք ձեր համակարգչում: Internet Explorer-ում օգտվողները կարող են սեղմել Tools կամ View, այնուհետև ընտրել Internet Options և սեղմել General և ապա՝ Settings. Վերջապես, սեղմելով View Files՝ կտեսնեք ձեր համակարգչում բոլոր թաքցված Վեբ էջերը:

Կան նաև շատ համակարգչային ծրագրեր, որ թույլ են տալիս հսկել տարբեր առցանցային գործողությունները: Ավելին իմանալու համար կարող եք այցելել GetNetWise

կայք. http://kids.getnetwise.org/tools/: Բացեք էջի "Find Tools for Your Family"մասը և փնտրեք "monitors"-ի տակ.

Կարելի է նաև դիմել համակարգչային մի խանութ և հարցնել թե ի՞նչ արտադրանք նրանք կառաջարկեն:

12. Ի՞նչ պետք է անեմ, եթե իմ երեխային անհանգստացնում են համացանցում:

Այս դեպքում դուք կարող եք "արգելափակել" այն անձին, որ անհանգստացնող կամ ագրեսիվ հաղորդագրություններ է ուղարկում: Կան "արգելափակող" միջոցներ էլ- փոստի և ակնթարթային հաղորդագցման ծրագրերում: Պահեք բոլոր անհանգստացնող հաղորդագրությունները և ուղարկեք այն ձեր երեխայի էլ-փոստի սպասարկումն ապահովողին: Շատ ծառայություններ ունեն համապատասխան միջոցներ, որ թույլ չեն տալիս օգտվողներին համացանցում անհանգստացնել ուրիշներին:

Եթե անհանգստացնող հաղորդագրությունը հրապարակված է որևէ վեբ կայքում, կապվեք ձեր Ինտերնետային ծառայության մատակարարին և խնդրեք պարզել, ում կողմից է տրամադրված հոստինգը: Այնուհետև, կարելի է կապվել հոստինգ տրամադրող ծառայության մատակարարին և վիրավորական հաղորդագրությունները ներկայացնել նրանց ուշադրությանը: Դուք կարող եք դիմել նաև ոստիկանություն: Շատ երկրներում ագրեսիայի նման դրսևորումները հանցանք են համարվում, թե՛ իրական աշխարհում, թե՛ համացանցում: Ապօրինի է համարվում այն հաղորդակցումը, որը հարցի տակ է առնում մի այլ մարդու ապահովության զգացումը:

13. Արդյո՞ք օգտակար են ֆիլտրող ծրագրերը:

Ֆիլտրող գործիքները, կամ զտիչները կարող են օգտակար լինել փոքր երեխաների համար լրացնելու – ոչ փոխարինելու – ծնողական հսկողությունը: Ֆիլտրերը և արգելափակիչները, այնուամենայնիվ, վերջնական լուծումներ չեն և հաճախ նրանք ձախողվում են՝ թույլ տալով անպատշաճ նյութի մուտք: Համաձայն 2001-ի սպառողների զեկույցի՝ ֆիլտրերը չեն արգելափակել առարկելի կայքերի 20 տոկոսը: Նրանք կարող են արգելափակել նաև շատ օգտակար նյութեր, որոնք անհրաժեշտ են երեխաներին ուսման գործընթացում:

Թեպետ ֆիլտրերը օգտակար կարող են լինել, երբ երեխաները փոքր են, մեծանալուն զուգընթաց անհրաժեշտ է, որ նրանք որոշակի կանոններ սովորեն՝ համացանցում ապահով ու պատասխանատու վարքագիծ դրսևորելու համար: Ծնողները և ուսուցիչները լավագույնս կարող են ուղղորդել երեխաներին, թե ինչպես պատասխանատվությամբ օգտագործել համացանցը:

14. Իմ փոքրիկը ցանկանում է գնումներ կատարել համացանցում: Ինչպես կարող եմ համոզված լինել, որ կայքն ապահով է

Եթե երեխաները կամ դեռահասները ցանկանում են գնումներ կատարել համացանցում, նրանց պետք է լրջորեն ուղղորդել որպեսզի փոխանցումները ապահով և անվտանգ եղանակով կատարվեն: Երեխաները պետք է իմանան, որ դեպքերում կարելի է տրամադրել վարկային քարտի ինֆորմացիան՝ երբ առկա է Better Business Bureau որակի երաշխիքի կնիք, "https", "http" –ի փոխարեն, գննարկիչի հասցեների մասում: Համոզվեք, որ գննարկիչը ապահովում է 128-բիթ կոդավորում, որպեսզի վարկային քարտի համարը ավտոմատ կերպով կոդավորվի նախքան ուղարկվելը: (Internet Explorer վերջին տարբերակները ապահովում են 128 բիթ կոդավորում:

15 . Ի՞նչ կետեր պետք է պարունակի մանկական կայքի քաղաքականությունը անձնական տվյալների պաշտպանության առումով:

Կայքերի անձնական տվյալների պաշտպանության պայմանները հաճախակի անորոշ են կամ անիրական: Երբ կարդում եք անձնական տվյալների պաշտպանության մասին, առաջին հերթին պետք է պարզեք՝ որ տվյալներն են կուտակվում և ինչպե՞ս է այդ ինֆորմացիան օգտագործվում (հատկապես, արդյոք այն վաճառվում է երրորդ կողմին); ունե՞ք արդյոք հնարավորություն փոխելու կամ ջնջելու ձեր երեխայից ստացած տեղեկությունները , ի՞նչ միջոցներ են կիռարվում պաշտպանելու երեխաներին զրուցարաններում , նրանց հաղորդագրությունները; արդյո՞ք տվյալ կայքը փորձում է ստանալ ծնողի համաձայնությունը նախքան երեխան կհրապարակի իր անձնական տվյալները համացանցում:

10 խորհուրդ երեխաներին համացանցում ապահով լինելու համար

- Ես ցանցում, երբեք չեմ բացահայտում իմ, մեր ընտանիքի եւ ընկերներիս մասին տեղեկատվությունը
- Ինտերնետային ֆայլեր ներբեռնելու, ցանցային խանութից գնումներ կատարելու եւ ինտերնետային մրցույթի մասնակցելու համար ես դիմում եմ ծնողներիս օգնությանը:
- Երբ ես օգտագործում եմ ինտերնետ, հարգում եմ նրա կանոնները ամենուրեք. տանը, դպրոցում և ընկերներիս շրջապատում:
- Ես ծնողներիս միշտ ցույց եմ տալիս ինտերնետային այն բովանդակությունը, որը տեսնելիս անհարմար եմ զգում:
- Բռնության տեսարաններով կայքերը ես չեմ նշում և չեմ ցուցադրում իմ ընկերներին:
- Ես երբեք չեմ հանդիպում իմ ինտերնետային ընկերոջը, առանց ծնողներիս տեղյակ պահելու:
- Իմ գաղտնաբառը գաղտնիք է բոլորի համար՝ նաև իմ ընկերների, երբեմն ես փոխում եմ այն:
- Մերթ ընդ մերթ ես բացատրում եմ իմ ծնողներին, թե ինչ եմ անում ցանցում:
- Ես ազնիվ և բարեկամաբար եմ վարվում ուրիշ մարդկանց հետ ինտերնետ ցանցում:
- Ժամանակը, որ ես ծախսում եմ ինտերնետ ցանցում ՝ փող արժե, այդ պատճառով էլ ես օգտագործում եմ ինտերնետը խնայողաբար:

Եւս մի քանի խորհուրդ երեխաներին

- Անծանոթներին ինտերնետով մի փոխանցեք անձնական բնույթի տեղեկատվություն
- Երբեք միայնակ մի գնացեք “ինտերնետային ընկերեների” հետ հանդիպման
- Երբեք անծանոթներին մի փոխանցեք ֆայլեր, երգեր կամ այլ ինֆորմացիա ինտերնետի միջոցով
- Երբեք մի սեղմեք անծանոթների կողմից ուղարկված ինտերնետային էջերի հասցեների վրա և մի բացեք դրանք
- Հարգեք այլ անձանց սեփականությունը:

Խորհուրդներ պատանիներին սոցիալական ցանցերում ապահով լինելու համար

Հնարավորինս փակ պահեք ձեր անձնական տվյալները եթե որոշել եք դրանք հրապարակել:

Օգտագործեք ծածկագրեր, որպեսզի միայն ձեր ընկերները կարողանան կարդալ: Ձեր ծածկագրերը պահեք ապահով:

Մեկնաբանություն գրելուց առաջ 2 անգամ մտածեք, քանի որ երբ այն հայտնվեց Ինտերնետում, այն կարող է հավերժ մնալ այնտեղ:

Մի վստահեք այն ամենին ինչ ասում են Ձեզ այլ մարդիկ, նրանք կարող են կեղծ լուսանկարներ օգտագործել, կամ ստել:

Ուշադիր եղեք թե ում հետ եք շփվում, հատկապես երբ ձեր ընկերների ցանկում ընդգրկում եք նոր մարդու:

Եվ ուշադիր եղեք անծանոթ մարդկանց նկատմամբ, ովքեր Ձեզ հրավիրում են միանալ իրենց համայնքին:

Պարզեք թե ինչ են ուրիշները տեղադրում ցանցում Ձեր մասին եւ զգուշացրեք նրանց եթե դուք համաձայն չեք այդ ինֆորմացիայի հետ:

Այլ խորհուրդներ

- Շատ ինտերնետ ծառայություններ տրամադրողներ ջնջում են անցանկալի նամակները նախքան ձեզ հասնելը: Այնուամենայնիվ Ջնջեք “spam”-ն առանց այն բացելու:
    - Երբեք մի պատասխանեք անծանոթ նամակներին;
    - Տեխնոլոգիաները կօգնեն ձեզ պաշտպանվել անցանկալի նամակներից:

10 խորհուրդ ծնողներին երեխաների առցանց ապահովության վերաբերյալ

- Քաջալերեք ձեր երեխաներին, որպեսզի կիսեն իրենց ինտերնետային փորձառությունը ձեզ հետ: Վայելեք ինտերնետը ձեր երեխաների հետ:

- Սովորեցրեք ձեր երեխաներին վստահել իրենց ներքին զգացողությանը: Եթե որևէ բան նրանց նյարդայնացնում է ցանցում, հարկ է որ նրանք ասեն ձեզ այդ մասին:

- Անձի հաստատում պահանջող կայքեր (չատ, տեսախաղեր եւ այլն) մտնելիս, օգնեք երեխաներին ընտրել այնպիսի անուն, որ չբացահայտվի անձնական տեղեկատվությունը:

- Օգտագործեք instant messaging (IM) ծրագրերը. Պնդեք, որ երեխաները չբացահայտեն ձեր հասցեն, հեռախոսի համարը կամ այլ անձնական տեղեկատվություն, ներառյալ այն, թե որ դպրոցն են հաճախում կամ որտեղ են սիրում խաղալ:

- Սովորեցրեք ձեր երեխաներին, որ ճշտի և սխալի միջև եղած տարբերությունը ինտերնետում նույնն է, ինչպես իրական կյանքում:

- Ցույց տվեք ձեր երեխաներին, թե ինչպես հարգել ուրիշներին ինտերնետ ցանցում: Համոզված եղեք այն բանում, որ նրանք գիտեն, որ լավ վարքագծի կանոնները չեն փոխվում հենց այն պատճառով, որ նրանք համակարգչի առջև են:

- Պնդեք, որ ձեր երեխաները ինտերնետ ցանցում հարգեն ուրիշների սեփականությունը և հեղինակային իրավունքը: Բացատրեք, որ ուրիշների աշխատանքի անօրինական

պատճենահանումը (երաժշտություն, տեսախաղեր և այլ ծրագրեր) նույնն է, ինչ դրանք խանութից գողանալը:

- Ասեք ձեր երեխաներին, որ նրանց չի կարելի անձամբ հանդիպել ինտերնետ ցանցի միջոցով ծանոթացած ընկերների հետ: Բացատրեք, որ ինտերնետային ընկերները հնարավոր է չլինեն այնպիսին ինչպիսին ներկայանում են ցանցում:

- Սովորեցրեք ձեր երեխաներին, որ ճիշտ չէ այն ամենը, ինչ որ կարդում կամ տեսնում են ցանցում: Քաջալերեք նրանց հարցնել ձեզ, եթե համոզված չեն:
-
- Վերահսկեք ձեր երեխաների ցանցային գործունեությունը ինտերնետային առաջավոր տեխնոլոգիայով: Ծնողական վերահսկողությունները կարող են օգնել ձեզ զտելու վնասակար բովանդակությունը, հետևելու այն կայքերը, որոնք երեխան այցելում է և պարզելու, թե այդ պահին ինչ է նա անում այդտեղ:

Եւս մի քանի խորհուրդ ծնողներին

Ձեռք բերեք երեխաների վստահությունը, եւ ուղղորդեք նրանց:

Երեխաները պետք է սովորեն որոշակի կանոններ, սովորաբար դրանք նույն կանոններն են, որ իրական աշխարհում են գործում, օրինակ քաղաքավարության կանոններ:

Երեխաները պետք գիտակցեն, որ այն ինչ իրենք հրապարակում են ցանցում, հասու է դառնում ողջ մարդկությանը:

Գիտակցեք, որ այն պահից երբ հրապարակվեցին ձեր անձնական տվյալները դուք կորցնում եք այն վերահսկելու հնարավորությունը եւ չգիտեք թե ինչպես կօգտագործվեն այդ տվյալները:

Լուսանկարները կարող են մեկ մատի շարժումով բազմացվել եւ հասու դառնալ հազարավոր մարդկանց: Նկարների թվանշային բնույթը թույլ է տալիս դրանք փոփոխությունների ենթարկել եւ աղճատել:

Ցանցում հայտնվող մարդիկ միշտ չէ, որ այն են, ինչպես ներկայանում են:

Ցանկացած մարդ կարող է բացել օգտվողի պրոֆիլ, իրեն դնելով մեկ ուրիշի տեղ:

Կայքի ստեղծողների հայտարարությունը, որ կայքը ծառայում է միայն դպրոցականների համար ոչինչ չի նշանակում:

Ավելին յուրաքանչյուր մարդ կարող է հարյուրավոր կայքերում ներկա գտնվել:

Խորհուրդներ ուսուցիչներին

Երեխաները պետք է սովորեն որոշակի կանոններ, սովորաբար դրանք նույն կանոններն են, որ իրական աշխարհում են գործում, օրինակ քաղաքավարության կանոններ:

Երեխաները պետք գիտակցեն, որ այն ինչ իրենք հրապարակում են ցանցում, հասու է դառնում ողջ մարդկությանը:

Լավագույն խորհուրդը ծնողներին ձեռք բերեք երեխաների վստահությունը, եւ ուղղորդեք նրանց: Գիտակցեք, որ այն պահից երբ հրապարակվեցին ձեր անձնական տվյալները դուք կորցնում եք այն վերահսկելու հնարավորությունը եւ չգիտեք թե ինչպես կօգտագործվեն այդ տվյալները:

Լուսանկարները կարող են մեկ մատի շարժումով բազմացվել եւ հասու դառնալ հազարավոր մարդկանց: Նկարների թվանշային բնույթը թույլ է տալիս դրանք փոփոխությունների ենթարկել եւ աղճատել:

Ցանցում հայտնվող մարդիկ միշտ չէ, որ այն են, ինչպես ներկայանում են:

Ցանկացած մարդ կարող է բացել օգտվողի պրոֆիլ, իրեն դնելով մեկ ուրիշի տեղ:

Կայքի ստեղծողների հայտարարությունը, որ կայքը ծառայում է միայն դպրոցականների համար ոչինչ չի նշանակում:

Ավելին յուրաքանչյուր մարդ կարող է հարյուրավոր կայքերում ներկա գտնվել:

Խորհուրդներ բոլորին

Ջնջեք “spam”-ն առանց այն բացելու

- Երբեք մի պատասխանեք անծանոթ նամակներին
- Տեխնոլոգիաները կօգնեն ձեզ պաշտպանվել անցանկալի նամակներից
- Շատ ինտերնետ ծառայություններ տրամադրողներ ջնջում են անցանկալի նամակները նախքան ձեզ հասնելը:

Ուշադիր եղեք խարդախությունների նկատմամբ

Որոշ նշանների միջոցով կարելի է տարբերակել նմանատիպ նամակները

- Մեծ շահման մասին հայտարարություններ
- Հայտնի ընկերությունների կողմից արվող առաջարկություններ
- Առաջարկներ, որոնք շատ գրավիչ են ճշմարիտ լինելու համար
- Տառասխալներ կամ քերականական սխալներ նամակներում:

Օգտագործեք anti-phishing և anti-spam տեխնոլոգիաներ նմանատիպ նամակներից խուսափելու համար:

Օգտագործեք "բարդ" գաղտնաբառեր

- Պահպանեք ձեր անձնական ինֆորմացիան գաղտնի և ստեղծեք այնպիսի գաղտնաբառեր որոնք դժվար կլինեն գուշակել
- Երբեք մի ասեք ձեր գաղտնաբառը նույնիսկ ձեր ընկերներին:

Պահպանեք Ձեր համակարգիչը՝ ակտիվացրեք Համացանցային հրապատը՝

Համացանցային հրապատը նման է պատի, որը ստեղծում է պատնեշ համակարգչի և ինտերնետի միջև:

Պահեք ձեր համակարգիչը ժամանակին համընթաց

- Տեղակայեք ձեր համակարգչի անվտանգության համար անհրաժեշտ բոլոր ծրագրային թարմացումները
- Ավտոմատ թարմացումները ամենալավ միջոցն է համակարգիչը պահպանելու համար:

Տեղակայեք հակավիրուսային ծրագիր

- Հակավիրուսային ծրագիրը կարող է հայտնաբերել և ոչնչացնել համակարգչային վիրուսները նախքան դրանք կհասցնեն վնասել ձեր համակարգիչը
- Հակավիրուսային ծրագրերն անհրաժեշտ է միշտ թարմացնել:

Տեղակայեք հակալրտեսային ծրագրային գործիքներ

Օգտագործեք հակալրտեսային ծրագրային ապահովում, որպեսզի անծանոթ մարդիկ չկարողանան ներխուժել ձեր համակարգիչ և գողանալ ձեր համակարգչի ինֆորմացիան:

Մտածեք նախքան սեղմելը

- Երբեք մի բացեք անծանոթ մարդկանց կամ կազմակերպությունների կողմից ուղարկված էլեկտրոնային նամակները և դրանց կցված ֆայլերը
- Ֆայլեր քաշեք միայն այն կայքերից որոնք ձեզ ծանոթ են և վստահում եք:

Փակեք Pop-up պատուհանները օգտագործելով կարմիր “X”-ը

- Pop-up պատուհանները փակելու համար միշտ օգտագործեք տվյալ պատուհանի վերևի անկյունում գտնվող կարմիր “X”-ը
- Երբեք մի սեղմեք “yes,” “accept” կամ նույնիսկ “cancel”, քանի որ այն կարող է լինել խորամանկություն որևիցէ անցանկալի ծրագիր տեղակայելու համար
- Սկզբում մտածեք հետո սեղմեք
- Եղեք ուշադիր և պահպանողական ձեր անձնական ինֆորմացիայի նկատմամբ
- Համոզվեք, որ ինտերնետային կայքերը պահպանում են ձեր անձնական ինֆորմացիան: