ՀԱՄԱՑԱՆՑԻ ԱՊԱՀՈՎ ՕԳՏԱԳՈՐԾՄԱՆ ՁԵՌՆԱՐԿ

Ուսուցիչների, ծնողների եւ երեխաների համար

1.Սոցիալական Ցանց

Ինչ են Սոցիալական Ցանցերը

Սոցիալական ցանցերը ընդհանուր հետաքրքրություններ ունեցող մարդկանց վիրտուալ համայնքներ են: Օգտվողները այդ ցանցերում շփվելու եւ ինքնարտահայտվելու հնարավորություն են ստանում հաղորդակցական տարբեր՝ chat, messaging, բլոգ, էլեկտրոնային փոստ եւ այլ 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:

Սոցիալական Ցանցերի օգուտները

Սոցիալական ցանցերը սովորելու, ազատ արտահայտվելու եւ հաղորդակցվելու հնարավորություն են տալիս մարդկանց: Նրանց միջոցով ձեւավորվում են նաեւ ընդհանուր հետաքրքրություններ ունեցող ակտիվ մարդկանց համայնքներ:

Պատանիները ավելի շատ հակված են ինքնաարտահայտման եւ շատ արագ համախմբվում եւ քննարկում են հրատապ հարցերը:

Սոցիալական Ցանցի ռիսկերը

Ցանցերում ներկայացվող 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: Սոցիալական ցանցերում անձնական նկարագրերը կարող են հասանելի լինեն բոլոր օգտվողներին, իսկ երեխաները չեն կարողանում պաշտպանել իրենց անձնական տվյալները:

Սոցիալական ցանցերի վտանգները

ա/ Այլասերված մեծահասակները, որոնք երեխա են ձեւանում, կարող են վտանգ ներկայացնել: Չկան տեխնոլոգիաներ, որոնք կարող կանխել մեծահասակներին մանկա-պատանեկան ցանցերում գրանցվելուց:

բ/ Անհատական տեղեկատվության ու անձնական տվալների տարածում:

գ/ Ժամանակի վատնում եւ համացանցային կախվածություն:

Երեխաները կարող են օրեր շարունակ անցկացնել ցանցում անընդհատ փոփոխելով իրենց նկարագիրը (պրոֆայլը) եւ հաղորդակցվել:

ե/ Ագրեսիայի դրսեւորում:

զ/ Շատ կայքեր թույլ են տալիս այլ անդամների գնահատել ձեր նկարագիրը (պրոֆայլ), արդյունքում կարող են հայտնվել անպարկեշտ մեկնաբանություններ:

Խորհուրդ ծնողներին

Ձեռք բերեք երեխաների վստահությունը եւ ուղղորդեք նրանց:

Սոցիալական ցանցերում երեխաները պետք է հետեւեն որոշակի կանոնների: Սովորաբար դրանք նման են իրական աշխարհում գործող կանոններին, օրինակ քաղաքավարության կանոնները:

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

Անձնական տվյալների հրապարակվելուց հետո, դուք կորցնում եք այն վերահսկելու հնարավորությունը եւ չգիտեք թե ինչպես այն կօգտագործեն այլ մարդիկ:

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

Ցանցում հայտնվող մարդիկ միշտ չէ, որ այն են, ինչպես ներկայանում են: Ցանկացած մարդ կարող է բացել օգտվողի նկարագիր (պրոֆիլ), իրեն դնելով մեկ ուրիշի տեղ:

Կայքի հեղինակների հայտարարությունը, որ կայքը ծառայում է միայն դպրոցականների համար ոչինչ չի նշանակում: Ավելին յուրաքանչյուր մարդ կարող է հարյուրավոր կայքերում ներկա գտնվել:

Խորհուրդներ երեխաներին

Հնարավորինս փակ պահեք ձեր անձնական տվյալները:

Օգտագործեք ծածկագրեր, որպեսզի միայն ձեր ընկերները կարողանան կարդալ ձեր նկարագիրը:

Ձեր ծածկագրերը պահեք ապահով:

Մեկնաբանություն գրելուց առաջ 2 անգամ մտածեք, քանի որ այն համացանցում հայտնվելուց հետո, կարող է հավերժ մնալ այնտեղ:

Մի վստահեք այն ամենին ինչ ասում են Ձեզ օտար մարդիկ, նրանք կարող են կեղծ լուսանկարներ օգտագործել, կամ ստել: Ուշադիր եղեք, թե ում հետ եք շփվում: Եվ ուշադիր եղեք անծանոթ մարդկանց նկատմամբ, ովքեր Ձեզ հրավիրում են միանալ իրենց համայնքին: Պարզեք թե ինչ են ուրիշները գրում ցանցում Ձեր մասին եւ զգուշացրեք նրանց եթե դուք համաձայն չեք այդ տեղեկատվության հետ:

2. ԲԼՈԳ

Բլոգի մասին

Բլոգ բառը ծագել է "weblog"՝ առ-ցանց ամսագրերի անվանումից: Բազմաթիվ կայքեր տալիս են այն գործիքները, որոնցով մարդիկ կարող են ստեղծել բովանդակություն: Օրինակ՝ www.blogger.com. Դուք կարող եք նաեւ ստեղծել ինտերակտիվ բլոգներ եւ հրավիրել մարդկանց մեկնաբանելու ձեր հրապարակված ինֆորմացիան (տեղեկատվությունը):

Որոնք են բլոգերի օգուտները եւ ռիսկերը

Բլոգը ինքնադրսեւորման արտակարգ միջոց է եւ թույլ է տալիս օգտվողներին նաեւ համագործակցել եւ սովորել համագործակցելով:

Անձնական տվյալների հրապարակման ռիսկ: Ձեր անձնական տվյալները այլ մարդիկ կարող են օգտագործել շահադիտական եւ առեւտրային նպատակներով:

Հեղինակային իրավունքի ռիսկ: Ոչ մի դեպքում չի կարելի օգտագործել այլ մարդկանց նյութերը եւ նույնիսկ նրանց կայքերի դիզայնը առանց թույլտվության:

Այլ մարդկանց մասին տեղեկատվություն հրապակելուց առաջ ստացեք նրանց թույլտվությունը:

Երբեք չի կարելի ոչ պատշաճ բովանդակություն տեղադրել բլոգերում:

10 խորհուրդ, որոնք կարող եք տալ ձեր երեխաներին, որպեսզի նրանք ավելի ապահով օգտվեն համացանցից

- Քաջալերեք ձեր երեխաներին, որպեսզի կիսեն իրենց համացանցային փորձառությունը ձեզ հետ: Վայելեք համացանցը 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 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 համացանցում նույնն է, ինչպես իրական կյանքում:
- Ցույց տվեք ձեր երեխաներին, թե ինչպես հարգել ուրիշներին համացանց 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 համացանցում հարգեն ուրիշների սեփականության և հեղինակային իրավունքը: Բացատրեք, որ ուրիշների աշխատանքի անօրինական պատճենահանումը (երաժշտություն, վիդիո խաղեր և այլ ծրագրեր) նույնն է, ինչ դրանք խանութից գողանալը:

- Ասեք ձեր երեխաներին, որ նրանց չի կարելի անձամբ հանդիպել համացանցի միջոցով ծանոթացած ընկերների հետ: Բացատրեք, որ համացանցային 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 համացանցային վերահսկման տեխնոլոգիաներով: 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:

10 խորհուրդ երեխաներին համացանցի ապահովության մասին

- Ես ցանցում, երբեք չեմ բացահայտում իմ, մեր ընտանիքի եւ ընկերներիս մասին տեղեկատվությունը:

- Համացանցային ֆայլեր ներբեռնելու, ցանցային խանութից գնումներ կատարելու եւ համացանցային մրցույթի մասնակցելու համար ես դիմում եմ ծնողներիս օգնությանը:

- Երբ ես օգտագործում եմ համացանց, հարգում եմ նրա կանոնները ամենուրեք. տանը, դպրոցում և ընկերներիս շրջապատում:

- Ես ծնողներիս միշտ ցույց եմ տալիս համացանցային այն բովանդակությունը, որը տեսնելիս անհարմար եմ զգում:

- Բռնության տեսարաններով կայքերը ես չեմ գրանցում կամ նշում և չեմ ցուցադրում իմ ընկերներին:

- Ես երբեք չեմ հանդիպում իմ համացանցային 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 համացանցում:
- Համացանցում ծախսած ժամանակը փող արժե եւ այդ պատճառով ես միայն նպատակային եւ խնայողաբար եմ օգտագործում այն:

Եւս մի քանի խորհուրդ երեխաներին

- Անծանոթներին համացանցով մի փոխանցեք անձնական բնույթի ինֆորմացիա
- Երբեք միայնակ մի գնացեք “համացանցային ընկերների” հետ հանդիպման
- Երբեք անծանոթներին մի փոխանցեք ֆայլեր, երգեր կամ այլ ինֆորմացիա համացանցի միջոցով
- Երբեք մի սեղմեք անծանոթների կողմից ուղարկված համացանցային էջերի հղումների վրա և մի բացեք դրանք
- Հարգեք այլ անձանց հեղինակային իրավունքները:

- Համացանցային ծառայություններ տրամադրող ընկերությունները հիմնականում ջնջում են անցանկալի նամակները նախքան ձեզ հասնելը, այնուամենայնիվ ջնջեք **սփամը** առանց այն բացելու
- Երբեք մի պատասխանեք անծանոթ նամակներին;

Ուշադիր եղեք կասկածելի բովանդակությամբ նամակների եւ տեղեկատվության 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 ը նման է պատի, որը ստեղծում է պատնեշ համակարգչի և համացանցի 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 համացանցային կայքերը պահպանում են ձեր անձնական ինֆորմացիան

Այլ մարդկանց տվյալների որսում, եւ անհատական տվյալների գողություն

Ինքնության կողոպուտ կամ անհատական տվյալների գողություն տեղի է ունեցել երբ անհատի անձնական տվյալները գողացել են եւ օգտագործել ապօրինի ձեւով: Օրինակ, ոչ վստահելի կոմերցիոն կայքերը կարող են չկատարել պայմանագրով ստանձնած իրենց պարտավորությունները եւ 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՝

Ընկերության անունը, հասցեն, հեռախոսի համար եւ այլն,

Պայմանագրի ժամկետները թափանցիկ են,

Ապրանքի հատկանիշները եւ երաշխիքները հստակորեն սահմանված են,

Ապրանքի գնի մեջ ներառված են բոլոր լրացուցիչ ծախսերը,

Առաջարկվում է վճարման անվտանգ եղանակ,

Պատվերները հաստատվում են էլ.փոստով,

Գնորդը հնարավորություն ունի ետ վերցնելու իր գումարը,

Առաքման ժամկետը հստակ սահմանված է,

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:

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, ծածկագրերին եւ այլն:
Օրինակ, օգտվողները ստանում են էլեկտրոնային նամակ, 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 ձեր ծածկագրերը 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:

Ինչպես ճանաչել վճարման անվտանգ եղանակները՝ Վստահելի առեւտրային կայքերը գործառույթները իրականացնում են միայն “secure electrnic 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 գումարը:

Այլ մարդկանց տվյալների որսում, եւ անձնական տվյալների գողություն:

Հեղինակային իրավունքի խնդիրներ՝

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:

Copyright - Հեղինակային իրավունք

Ստեղծագործական գործունեության արդյունքի, ինչպես օրինակ՝ տեքստի, երաժշտական ստեղծագործության, նկարի կամ համակարգչային ծրագրի հեղինակի իրավունքներն օրենքով պաշտպանելու եղանակ: Գրագողությունը որևէ մեկի աշխատանքը պատճենելը և այն, առանց աղբյուրին հղում կատարելու, սեփական աշխատանքում օգտագործելը:

Cyber-bullying - Կիբեր սպառնալիքներ

Թե երեխաները, թե մեծահասակները կարող են օգտագործել համացանցը անհանգստացնելու կամ վախեցնելու համար այլ մարդկանց

Disturbing content - Անհանգստացնող բովանդակություն

Եթե երեխան օգտվում է համացանցից առանց վերահսկողության, ապա կարող է հանդիպել անցանկալի նկարների կամ տեղեկատվության

File sharing - Ֆայլերի փոխանակում

Երաժշտության, տեսաֆիլմերի և այլ ֆայլերի ինտերնետի միջոցով փոխանակումը անձանոթներին կարող են լինել անօրինական, և հնարավորություն տան մուտք գործելու ձեր համակարգիչ և փոխանցել վիրուսներ:

Hacker - Հակեր

Անձ, որն օգտվում է համակարգչի հետ աշխատելու գիտելիքներից՝ առանց թույլտվության համակարգիչ մուտք գործելու համար, և այնուհետև սխալ է օգտագործում ծրագրերը և համակարգչում պահեստավորված տվյալները կամ վնաս է հասցնում դրանց:

Hoaxes - Խորամանկություններ

Էլ. նամակներ, որոնք ուղարկվում են համացանցային հանցագործների կողմից, ովքեր փորձում են գումար կորզել

Identity Theft - Ինքնության գողություն

Ինքնության կողոպուտ տեղի է ունեցել երբ անհատի անձնական տվյալները գողացել են եւ օգտագործել ապօրինի ձեւով: Օրինակ, երբ խարդախները ձեռք բերելով անհատի բանկային քարտի համարը կարողանում են ներխուժել նրա բանկային հաշիվների մեջ և կորզել գումարներ:

Intellectual property - Մտավոր սեփականություն

Համացանցում հասանելի ցանկացած տեղեկություն համարվում է մտավոր սեփականություն, որն օրենքով այդ տեղեկությունը ստեղծողի սեփականությունն է: Մտավոր սեփականության իրավատերը այդ տեղեկությունների օգտագործումը վերահսկելու բացառիկ իրավունքներ ունի:

Internet Firewall - Համացանցային հրապատ

Համացանցային հրապատը վիրտուալ արգելափակոց է համակարգչի և համացանցի համացանցի միջև: Ջոիչ, 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:

Invasion of privacy - Ներխուժում անձնական կյանք

Երբ երեխան լրացնում է համացանցային հարցաթերթիկներ, կարող է փոխանցել տեղեկատվություն իր կամ իր ընտանիքիմասին, որն անցանկալի է փոխանցել անծանոթների կամ համացանցային ծանոթներին

Phishing - Որսում

Համակարգչից օգտվողներից անձնական տեղեկություններ, ինչպես օրինակ՝ գաղտնաբառեր և վարկային քարտի մանրամասներ կորզելը և դրանք չարամիտ նպատակներով օգտագործելը:

Spam - Անցանկալի նամակներ

Անցանկալի նամակներ, հաղորդագրություններ, էլ. բացիկներ և այլն

Spyware - Լրտես ծրագրեր

Համակարգչային ծրագրեր, որոնք աննկատ տեղադրվում են համակարգչում: Լրտես ծրագրերը կարող են ցանցի միջոցով և գաղտնի կերպով այլ համակարգիչ ուղարկել ոստայնում Համակարգչից օգտվողի նավարկելու սովորությունների մասին կամ այլ անձնական տեղեկություններ:

SSL - Տեղեկատվության պաշտպանության հաղորդակարգ

Համացանցի անվտանգության հաղորդակարգ, որն ապահովում է տվյալների անվտանգ հաղորդում՝ փոխանցվող տեղեկությունները գաղտնագրելու միջոցով: SSL հաղորդակարգը հաստատում է, որ կայքը իսկական է, և որ դրանով տրամադրված տվյալները սխալ չեն օգտագործվի։

Trojan Horses - Տրոյական ձիեր

Տրոյական ձին օգտակար ծրագրի, ինչպես օրինակ՝ խաղի, օժանդակ ծրագրի կամ ծրագրաշարի տակ քողարկված համակարգչային վնասարար ծրագիր է : “Տրոյական ձին” օգտակար գործողություն կատարելու պատրվակով վնասում է համակարգիչը :

Viruses - Վիրուսներ

Ծրագրեր, որոնք խաթարում եւ վտանգում են համակարգչի աշխատանքը, կամ վնասում պահեստավորված տվյալները:

Worms - Որդեր

Համակարգչային ծրագիր է , որը տարածվում է համակարգչից համակարգիչ՝ սովորաբար յուրաքանչյուր համակարգչի հիշողությունում ստեղծելով իր պատճենները: Որդը կարող է մեկ համակարգչում բազմաթիվ պատճեններ ստեղծել՝ ի վերջո շարքից հանելով այն:

The Internet Safety Guide for Teachers, Parents and Children was prepared by Media Education Center. Materials from Insafe (European Network of Awareness Centres), Australian Government (NetAlert) and Microsoft were used.

Ձեռնարկը պատրաստված է Մեդիակրթության կենտրոնի (www.mediaeducation.nt.am) կողմից: Օգտագործվել են Իրազեկության կենտրոնների եվրոպական ցանցի, Ավստրալիայի կառավարության եւ Մայքրոսոֆտ-Հայաստան կազմակերպությունների նյութերը: