Թեմա 1 - Համակարգիչը և հասարակությունը

1. Էլեկտրոնային ապահովություն

Կիբեռանվտանգությունն արդի աշխարհի կարևորագույն հարցերից մեկն է, քանի որ աշխարհում լայն տարածում է գտել տեղեկատվական տեխանլոգիաների կիրառումը տարբեր տիպի հիմնախնդիրների լուծման համար: Եվ դրան զուգահեռ աստիճանաբար աճում է կիբեռհարձակումների ենթարկվելու հավանականությունը:

Կիբերհարձակվող խմբավորումները կարելի է բաժանել մի քանի դասի.

- «Սև գլխարկ» հաքերներ, որոնք աշխատում են պատվերով և իրականացնում են ցանկացած տիպի հարձակում:
- Պետական հաքերներ, որոնք իրականացնում են հարձակումներ պետական պատվերով:
- Կիբեռլրտեսներ, որոնք աշխատում են մեծ կազմակերպությունների և կազմակերպված հանցավոր խմբերի համար:
- Կիբեռահաբեկիչներ, որոնք իրականացնում են առցանց ահաբեկչություններ:
- Հաքտիվիստներ, քաղաքական, կրոնական կամ հասարակական ոլորտներում գործող ակտիվիստներ, որոնք իրենց բողոքն արտահայտում են հաքերային հարձակումների միջոցով:

Այսօր գրեթե յուրաքանչյուր մարդ կարող է դառնալ հարձակման թիրախ, ինչի պատճառով կիբեռպաշտպանությունը յուրաքանչյուրի համար կարևոր է դառնում: Կիբեռվտանգների մեծ մասից կարելի է խուսափել մի շարք պայմանների հետևելով: Դրանք ներառում են համակարգչի, հեռախոսի, հաշիվների պաշտպանությանը վերաբերող քայլեր:

Այս ուղեցույցի միջոցով մենք կփորձենք պատասխանել հետևյալ արդիական հարցերին.

- ինչու՞ է անհրաժեշտ առցանց անվտանգության ապահովումը,
- ինչի՞ է հնարավոր հասնել առցանց անվտանգության ապահովման միջոցով,
- ի՞նչ օգուտ այն կտա երեխաներին,
- ինչպե՞ս պաշտպանվել առցանց ոտնձգություններից:

Ինտերնետի օգտագործումից բխող վտանգները

Համակարգչային անվտանգության խնդիրներն այսօր առավել արդիականներից են, քանի որ մենք ապրում ենք այսպես կոչված «տեղեկատվական հասարակությունում», որտեղ տեղեկատվությունն առաջնային կարևորություն ունի: Հետևաբար, տեղեկատվական անվտանգության համար պատասխանատվության հարցերը պետք է երեխաների հետ անընդհատ քննարկման առարկա լինեն:

Ֆայլերի փոխանակման վտանգներ

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

Կիբեր հարձակումներ

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

Ինտերնետային խաբեբայություններ

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

Ներխուժում անձնական կյանք

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

Խորամանկություններ

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

Անհանգստացնող բովանդակություն

Ինտերնետում հաճախ հանդիպող անցանկալի նկարներ կամ տեղեկատվություն:

Շարժական սարքերի պաշտպանությունը

Շարժական սարքերը՝ հեռախոսները և պլանշետները, անձի վերաբերյալ զգայուն տեղեկատվության կրողներ են:

Այսօր շարժական սարքերում հիմնականում տեղադրվում է երկու օպերացիոն համակարգ՝ Android և iOS: Դրանք անվտանգ են, եթե պահպանվում են մի շարք կանոններ: Հարկավոր է հավելվածներ տեղադրել Google Play-ից և App Store-ից: Համացնացում առկա այլ կայքերից բեռնված ծրագրերը կարող են պարունակել թաքնված հնարավորություններ, որոնք թույլ կտան հաքերներին տիրանալ ձեզ վերաբերող տեղեկատվությանը: Հավելված տեղադրելիս միշտ հետևեք, թե ինչ տիպի տեղեկատվություն է ուզում ստանալ ձեզանից հավելվածը: Եթե, օրինակ, բառարանը, պահանջում է ձեր SMS-ների վերաբերյալ տեղեկատվություն կամ ուզում է միացնել խոսափողը, ապա հեռացրեք տվյալ ծրագիրը, քանի որ այն կարող է օգտագործվել լրտեսելու համար:

Android-ի **Device Manager** հավելվածը թույլ է տալիս գտնել ձեր սարքավորումը քարտեզի վրա, ինչպես նաև վերացնել դրանում առկա ողջ անձնական տեղեկատվությունը, իսկ iOS-ի դեպքում դա Find My iPhone հավելվածն է:

Կայքերի հաշիվների պաշտպանությունը

Այսօր մարդկանց բոլոր հաշիվները հիմնվում են հիմնականում էլեկտրոնային հասցեներում, որոնք հանդիսանում են մարդուն իդենտիֆիկացնելու միջոց: Էլեկտրոնային հասցեն կրիտիկական խոցելի կետ է. դրա վրա հաջողված հարձակումն անմիջապես վտանգի տակ է դնում մարդու բոլոր մնացած հաշիվները: Այդ պատճառով գերադասելի է ունենալ մի քանի էլեկտրոնային հասցե.

- հանրային շփումների համար,
- անձնական, ընկերների և բարեկամների հետ շփվելու համար,
- գաղտնի էլեկտրոնային հասցե, որն օգտագործվում է այլ կայքերում գրանցվելու համար, օրինակ՝ Facebook, Twitter, Instagram և այլն,
- տեխնիկական օգտագործման հասցե, որը կիրառվում է անծանոթ, ոչ վստահելի կայքերում գրանցվելու համար:

Հեռախոսների հաղորդագրությունների և զանգերի պաշտպանությունը

SMS հաղորդագրությունները վտանգավոր են, քանի որ դրանք կարող են հասանելի դառնալ բոլորին: Դրանց միջոցով ոչ մի տեսակի գաղտնի կամ անձնական տեղեկատվություն չպետք է ուղարկել: Էդվարդ Սնոուդենի բացահայտումները խոսում են նրա մասին, որ ցանկացած ինֆորմացիա կարելի է վերահսկել: Հաղորդագրությունները պահպանվում են տվյալ ծառայությունների սերվերների վրա՝ նույնիսկ ձեր կողմից դրանք ջնջելուց հետո, ինչը նշանակում է, որ դրանք կարող են հայտնվել ցանցում՝ բոլորին հասանելի տեսքով, այդ ծառայության վրա հաքերային հարձակման հետևանքով:

Այսօր գաղտնագրման հնարավորություն են ներմուծել Whatsapp, Viber մեսենջերները: Facebook-ն իր մեսենջերում նույնպես ներմուծել է գաղտնագրված հաղորդագրությունների տարբերակ՝ Secret Conversation հատուկ տարբերակի միջոցով:

Աննկատելի լրտես

Վեբ-տեսախցիկը մեծագույն հայտնագործություն է հատկապես նրանց համար, ում ընկերները և հարազատները գտնվում են շատ հեռու: Միջոցներ ձեռնարկեք, որպեսզի ձեր սարքերի տեսախցիկները հանցագործներին չպատմեն ձեր անձնական կյանքի մանրամասները: Ցանցահենները այդ մանրամասները կարող են տարբեր կերպ օգտագործել՝ վաճառել պոռնոկայքերին կամ էլ շանտաժի ենթարկել նկարահանված մարդկանց: Եթե չեք ուզում անհարմար դրության մեջ հայտնվել՝ օգտվեք պաշտպանական միջոցներից, այսօրյա հակավիրուսները կարողանում են հսկել վեբ-տեսախցիկների հասանելիությունը:

Օգտագործե՛ք բրաուզերի հատուկ ապահով ռեժիմը

Վտանգներից խուսափելու համար ոչ անձնական համակարգչից կամ շարժական սարքից օգտվելիս բրաուզերը պետք է օգտագործել հատուկ ռեժիմով, որը չի պահպանում տվյալները՝ պատուհանը փակելուց հետո: Google Chrome-ի դեպքում դա New Incognito Window հրամանն է (կամ ստեղնաշարով Ctrl+Shift+N), իսկ Firefox-ի դեպքում՝ New Private Window-ը (կամ ստեղնաշարով Ctrl+Shift+P):

Հաշվին կցե՛ք բջջային հեռախոսի համար

Հաշվի պաշտպանությունն ավելի է ուժեղանում, երբ դրան կցվում է բջջային հեռախոսի համարը, ինչը թույլ է տալիս արագ տեղեկանալ հարձակումների մասին և վերականգնել հաշիվը: Մյուս կողմից՝ սա կարող է նաև լրացուցիչ խոցելիություն դառնալ, քանի որ արդեն հայտնի են ձևեր, որոնք թույլ են տալիս մուտք գործել օգտատիրոջ հաշիվ՝ կեղծելով համարը կամ այլ կերպ կորզելով SMS-ները: Այդ պատճառով, եթե հաշվին կցվում է հեռախոսահամարը, ապա պետք է կիրառվեն նաև լրացուցիչ միջոցներ, որոնցից ամենավստահելին այսօր երկփուլային պաշտպանությունն է: Այսօր ամենախորացված պաշտպանության միջոցը

երկփուլային մուտքի ընթացակարգն է (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի երկրորդ քայլով անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ սարքի, կամ կարճ հաղորդագրությունների միջոցով: Նման ֆունկցիա կարելի է միացնել Gmail, Yahoo, Yandex, Dropbox, Facebook, Twitter և տասնյակ այլ ծառայություններում: Դրանց ցանկը կարելի է գտնել www.twofactorauth.org կայքում: Two-factor authentication-ի ակտիվացումն ու կիրառումն անհամեմատ պաշտպանված են դարձնում օգտվողին: Այս համակարգը նշանակում է, որ եթե ուրիշն անգամ ունի ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվը՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է:

Կիբեռանվտանգությունն արդի աշխարհի կարևորագույն հարցերից մեկն է, քանի որ աշխարհում լայն տարածում է գտել տեղեկատվական տեխանլոգիաների կիրառումը տարբեր տիպի հիմնախնդիրների լուծման համար: Եվ դրան զուգահեռ աստիճանաբար աճում է կիբեռհարձակումների ենթարկվելու հավանականությունը:

Կիբերհարձակվող խմբավորումները կարելի է բաժանել մի քանի դասի.

- «Սև գլխարկ» հաքերներ, որոնք աշխատում են պատվերով և իրականացնում են ցանկացած տիպի հարձակում:
- Պետական հաքերներ, որոնք իրականացնում են հարձակումներ պետական պատվերով:
- Կիբեռլրտեսներ, որոնք աշխատում են մեծ կազմակերպությունների և կազմակերպված հանցավոր խմբերի համար:
- Կիբեռահաբեկիչներ, որոնք իրականացնում են առցանց ահաբեկչություններ:
- Հաքտիվիստներ, քաղաքական, կրոնական կամ հասարակական ոլորտներում գործող ակտիվիստներ, որոնք իրենց բողոքն արտահայտում են հաքերային հարձակումների միջոցով:

Այսօր գրեթե յուրաքանչյուր մարդ կարող է դառնալ հարձակման թիրախ, ինչի պատճառով կիբեռպաշտպանությունը յուրաքանչյուրի համար կարևոր է դառնում: Կիբեռվտանգների մեծ մասից կարելի է խուսափել մի շարք պայմանների հետևելով: Դրանք ներառում են համակարգչի, հեռախոսի, հաշիվների պաշտպանությանը վերաբերող քայլեր:

Այս ուղեցույցի միջոցով մենք կփորձենք պատասխանել հետևյալ արդիական հարցերին.

- ինչու՞ է անհրաժեշտ առցանց անվտանգության ապահովումը,

- ինչի՞ է հնարավոր հասնել առցանց անվտանգության ապահովման միջոցով,
- ի՞նչ օգուտ այն կտա երեխաներին,
- ինչպե՞ս պաշտպանվել առցանց ոտնձգություններից:

Ինտերնետի օգտագործումից բխող վտանգները

Համակարգչային անվտանգության խնդիրներն այսօր առավել արդիականներից են, քանի որ մենք ապրում ենք այսպես կոչված «տեղեկատվական հասարակությունում», որտեղ տեղեկատվությունն առաջնային կարևորություն ունի: Հետևաբար, տեղեկատվական անվտանգության համար պատասխանատվության հարցերը պետք է երեխաների հետ անընդհատ քննարկման առարկա լինեն:

Ֆայլերի փոխանակման վտանգներ

Երաժշտության, տեսանյութերի և այլ ֆայլերի ինտերենետի միջոցով փոխանակումը անծանոթներին կարող են լինել անօրինական, և հնարավորություն տան մուտք գործելու ձեր համակարգիչ և փոխանցել վիրուսներ:

Կիբեր հարձակումներ

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

Ինտերնետային խաբեբայություններ

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

Ներխուժում անձնական կյանք

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

Խորամանկություններ

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

Անհանգստացնող բովանդակություն

Ինտերնետում հաճախ հանդիպող անցանկալի նկարներ կամ տեղեկատվություն:

Շարժական սարքերի պաշտպանությունը

Շարժական սարքերը՝ հեռախոսները և պլանշետները, անձի վերաբերյալ զգայուն տեղեկատվության կրողներ են:

Այսօր շարժական սարքերում հիմնականում տեղադրվում է երկու օպերացիոն համակարգ՝ Android և iOS: Դրանք անվտանգ են, եթե պահպանվում են մի շարք կանոններ: Հարկավոր է հավելվածներ տեղադրել Google Play-ից և App Store-ից: Համացնացում առկա այլ կայքերից բեռնված ծրագրերը կարող են պարունակել թաքնված հնարավորություններ, որոնք թույլ կտան հաքերներին տիրանալ ձեզ վերաբերող տեղեկատվությանը: Հավելված տեղադրելիս միշտ հետևեք, թե ինչ տիպի տեղեկատվություն է ուզում ստանալ ձեզանից հավելվածը: Եթե, օրինակ, բառարանը, պահանջում է ձեր SMS-ների վերաբերյալ տեղեկատվություն կամ ուզում է միացնել խոսափողը, ապա հեռացրեք տվյալ ծրագիրը, քանի որ այն կարող է օգտագործվել լրտեսելու համար:

Android-ի **Device Manager** հավելվածը թույլ է տալիս գտնել ձեր սարքավորումը քարտեզի վրա, ինչպես նաև վերացնել դրանում առկա ողջ անձնական տեղեկատվությունը, իսկ iOS-ի դեպքում դա Find My iPhone հավելվածն է:

Կայքերի հաշիվների պաշտպանությունը

Այսօր մարդկանց բոլոր հաշիվները հիմնվում են հիմնականում էլեկտրոնային հասցեներում, որոնք հանդիսանում են մարդուն իդենտիֆիկացնելու միջոց: Էլեկտրոնային հասցեն կրիտիկական խոցելի կետ է. դրա վրա հաջողված հարձակումն անմիջապես վտանգի տակ է դնում մարդու բոլոր մնացած հաշիվները: Այդ պատճառով գերադասելի է ունենալ մի քանի էլեկտրոնային հասցե.

- հանրային շփումների համար,
- անձնական, ընկերների և բարեկամների հետ շփվելու համար,
- գաղտնի էլեկտրոնային հասցե, որն օգտագործվում է այլ կայքերում գրանցվելու համար, օրինակ՝ Facebook, Twitter, Instagram և այլն,
- տեխնիկական օգտագործման հասցե, որը կիրառվում է անծանոթ, ոչ վստահելի կայքերում գրանցվելու համար:

Հեռախոսների հաղորդագրությունների և զանգերի պաշտպանությունը

SMS հաղորդագրությունները վտանգավոր են, քանի որ դրանք կարող են հասանելի դառնալ բոլորին: Դրանց միջոցով ոչ մի տեսակի գաղտնի կամ անձնական տեղեկատվություն չպետք է ուղարկել: Էդվարդ Սնոուդենի բացահայտումները խոսում են նրա մասին, որ ցանկացած ինֆորմացիա կարելի է վերահսկել: Հաղորդագրությունները պահպանվում են տվյալ ծառայությունների սերվերների վրա՝ նույնիսկ ձեր կողմից դրանք ջնջելուց հետո, ինչը նշանակում է, որ դրանք կարող են հայտնվել ցանցում՝ բոլորին հասանելի տեսքով, այդ ծառայության վրա հաքերային հարձակման հետևանքով:

Այսօր գաղտնագրման հնարավորություն են ներմուծել Whatsapp, Viber մեսենջերները: Facebook-ն իր մեսենջերում նույնպես ներմուծել է գաղտնագրված հաղորդագրությունների տարբերակ՝ Secret Conversation հատուկ տարբերակի միջոցով:

Աննկատելի լրտես

Վեբ-տեսախցիկը մեծագույն հայտնագործություն է հատկապես նրանց համար, ում ընկերները և հարազատները գտնվում են շատ հեռու: Միջոցներ ձեռնարկեք, որպեսզի ձեր սարքերի տեսախցիկները հանցագործներին չպատմեն ձեր անձնական կյանքի մանրամասները: Ցանցահենները այդ մանրամասները կարող են տարբեր կերպ օգտագործել՝ վաճառել պոռնոկայքերին կամ էլ շանտաժի ենթարկել նկարահանված մարդկանց: Եթե չեք ուզում անհարմար դրության մեջ հայտնվել՝ օգտվեք պաշտպանական միջոցներից, այսօրյա հակավիրուսները կարողանում են հսկել վեբ-տեսախցիկների հասանելիությունը:

Օգտագործե՛ք բրաուզերի հատուկ ապահով ռեժիմը

Վտանգներից խուսափելու համար ոչ անձնական համակարգչից կամ շարժական սարքից օգտվելիս բրաուզերը պետք է օգտագործել հատուկ ռեժիմով, որը չի պահպանում տվյալները՝ պատուհանը փակելուց հետո: Google Chrome-ի դեպքում դա New Incognito Window հրամանն է (կամ ստեղնաշարով Ctrl+Shift+N), իսկ Firefox-ի դեպքում՝ New Private Window-ը (կամ ստեղնաշարով Ctrl+Shift+P):

Հաշվին կցե՛ք բջջային հեռախոսի համար

Հաշվի պաշտպանությունն ավելի է ուժեղանում, երբ դրան կցվում է բջջային հեռախոսի համարը, ինչը թույլ է տալիս արագ տեղեկանալ հարձակումների մասին և վերականգնել հաշիվը: Մյուս կողմից՝ սա կարող է նաև լրացուցիչ խոցելիություն

դառնալ, քանի որ արդեն հայտնի են ձևեր, որոնք թույլ են տալիս մուտք գործել օգտատիրոջ հաշիվ՝ կեղծելով համարը կամ այլ կերպ կորզելով SMS-ները: Այդ պատճառով, եթե հաշվին կցվում է հեռախոսահամարը, ապա պետք է կիրառվեն նաև լրացուցիչ միջոցներ, որոնցից ամենավստահելին այսօր երկփուլային պաշտպանությունն է: Այսօր ամենախորացված պաշտպանության միջոցը երկփուլային մուտքի ընթացակարգն է (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի երկրորդ քայլով անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ սարքի, կամ կարճ հաղորդագրությունների միջոցով: Նման ֆունկցիա կարելի է միացնել Gmail, Yahoo, Yandex, Dropbox, Facebook, Twitter և տասնյակ այլ ծառայություններում: Դրանց ցանկը կարելի է գտնել www.twofactorauth.org կայքում: Two-factor authentication-ի ակտիվացումն ու կիրառումն անհամեմատ պաշտպանված են դարձնում օգտվողին: Այս համակարգը նշանակում է, որ եթե ուրիշն անգամ ունի ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվը՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է: