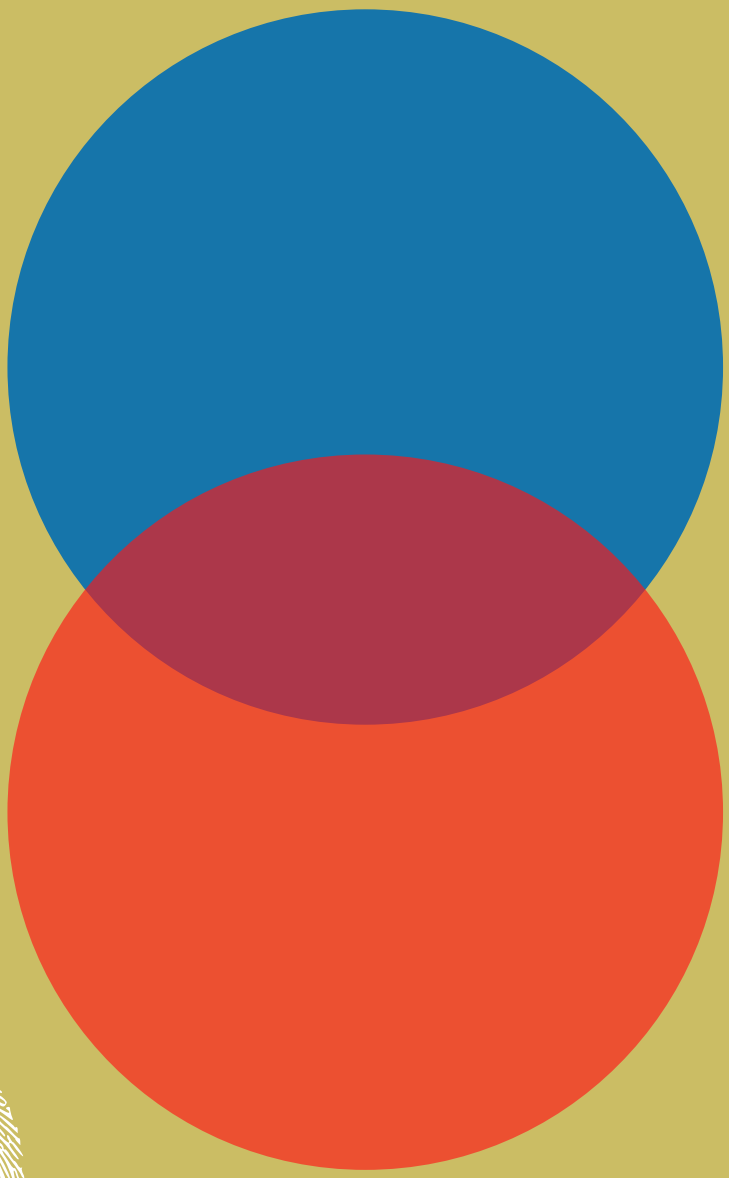
ԲՈԼՈՐԸ ՀԱՆՈՒՆ ՀԱՎԱՍԱՐ ԻՐԱՎՈՒՆՔՆԵՐԻ ՀԻՄՆԱԴՐԱՄ



ԹՎԱՅԻՆ ՀԵՏՔ.

ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ՁԵՌՆԱՐԿ

All Rights FOUNDATION

Ձեռնարկը ստեղծվել է Բոլորը հանուն հավասար իրավունքների հիմնադրամի (ԲՀՀԻ հիմնադրամ) կողմից «Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագրի շրջանակում: Նյութի բովանդակության համար պատասխանատու է միայն ստեղծողը: Ձեռնարկում արտահայտված տեսակետները/ բովանդակությունը կարող են չհամընկնել Շվեդիայի կառավարության տեսակետների հետ:

«Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագիրն իրականացվում է Եվրասիա համագործակցություն հիմնադրամի կողմից Շվեդիայի կառավարության աջակցությամբ:

Web: www.allrights.am
Email: info@allrights.am

ԹՎԱՅԻՆ ՀԵՏՔ.
ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ՁԵՌՆԱՐԿ

Ձեռնարկի էլեկտրոնային գրագիտության բաղադրիչը մշակվել է ԲՀՀԻ հիմնադրամի կողմից, թվային անվտանգության և որոնողական համակարգերի բաղադրիչներում առկա նկարագրությունների որոշ հատվածներ վերցված են ստորև բերված հրապարակումներից՝

Հանրային լրագրության ակումբ, «Փաստերի ռադար» առցանց ուղեցույց:

World Vision Armenia, «Անվտանգ համացանց» ձեռնարկ, Արտակ Հարությունյան, Վահե Երիցյան, 2011:

Նորավանք գիտակրթական հիմնադրամ, «Տեղեկատվական անվտանգություն», ՀՏԴ 004(07), ԳՄԴ 32.81y7, ISBN 978-9939-825-34-2 «Նորավանք» ԳԿՀ, 2017, ՀՀ ԿԳՆ ԳՊԿ, 2017:

Գյումրի (2022)

ԹՎԱՅԻՆ ՀԵՏՔ

ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ՁԵՌՆԱՐԿ

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՄԱՍ 2. ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

ՆԵՐԱԾՈՒԹՅՈՒՆ

Այսօր մենք համարվում ենք տեղեկատվական հասարակություն: Հասարակության տեսակ, որտեղ տեղեկատվության և գիտելիքի ստեղծումը, օգտագործումն ու մշակումը հանդիսանում են կարևոր տնտեսական, քաղաքական և մշակութային գործոններ:

Մի քանի տարրեր կան, որոնք վերահաստատում են մեր անցումը տեղեկատվական հասարակություն, և դրանք ստուգելը դժվար չէ:

Տեղեկատվական տեխնոլոգիաների դերի մեծացումը հասարակական կյանքում. դժվար է պատկերացնել կյանքն առանց տեխնոլոգիաների: Կրթության, աշխատանքի և գործունեության ամենատարբեր ոլորտներում առաջնային դիրք զբաղեցնելու համար մենք ուղղակի և անուղղակի կերպով առնչվում ենք տեխնոլոգիաների հետ, իսկ առանց դրանց անհամեմատ հետ ենք մնում արագ զարգացող աշխարհին առաջ տանող վազքուղուց:

Տեղեկատվական տեխնոլոգիաների, ապրանքների ու ծառայությունների, ինչպես նաև հաղորդակցության ոլորտներում աշխատող մարդկանց թվի աճը. Անհամեմատ մեծացել են տեխնոլոգիաների ոլորտում աշխատող մարդկանց պահանջարկն ամբողջ աշխարհում: Տեխնոլոգիաների ոլորտում աշխատանքն այսօր ամենապահանջվածն է նաև ֆրիլանս ոլորտում և անկախ անհատի գտնվելու վայրից, տվյալ պահին բնակության վայրի սոցիալական ու տնտեսական վիճակից, մարդը կարող է ունենալ աշխատանք և վաստակել ավելին, քան՝ մյուսները:

Հասարակության տեղեկատվայնացման (informatization) աճը՝ հեռախոսակապի, ռադիոյի, հեռուստատեսության, համացանցի, ավանդական ու էլեկտրոնային ԶԼՄ-ների կիրառմամբ. բազմաթիվ հետազոտություններ են իրականացվել, և մենք ինքներս էլ կարող ենք վերահաստատել, որ շատերն օրվա մեծ մասն անցկացնում են էկրանների դիմաց՝ նորություններ կարդալով, սոցիալական մեդիան թերթելով, հեռախոսով և հաղորդակցության այլ միջոցներով շփվելով և, առհասարակ, գլոբալ մեդիա սպառելով: Բավական է, որ մենք մեկ ժամ կտրվենք արտաքին աշխարհի հետ հաղորդակցության միջոցներից, և արդեն հետ ենք մնում աշխարհի զարգացումներից:

Գլոբալ տեղեկատվական միջավայրի զարգացումը. վերոթվարկյալ բոլոր տենդենցները մեզ տանում են դեպի գլոբալ տեղեկատվական միջավայրի զարգացման, մեր կենցաղային տեխնիկան, ավտոմեքենաները, անգամ տներն այսօր խելացի (smart) են, հեռախոսներն հենց այդպես էլ կոչվում են՝ սմարթֆոն, աճում է արհեստական բանականության կիրառման պահանջները, մարդկային գործունեությունն ավտոմատիզացվում է, ռոբոտներն աշխատում են մարդկանց փոխարեն, հրթիռները գնում են դեպի Լուսին ու Մարս, նանոտեխնոլոգիաները գալիս են փրկելու աշխարհը, կլոնավորումն ու համակարգչային մոդելավորումը գերակա նշանակություն ունեն գիտության և տնտեսության զարգացման հիմքում, անգամ պատերազմներն առավել հաճախ, մասշտաբային և ազդեցիկ կերպով տեղի են ունենում կիբերտիրույթում: Այս ամենը մեզ տանում է գլոբալ տեղեկատվական միջավայրի զարգացման, որտեղ մարդը, որպես բանական էակ, հաճախ զիջում է իր տեղը տեխնոլոգիաներին, չնայած որ համարվում է դրա ստեղծողն ու կառավարողը: Սակայն միշտ չէ, որ մենք վստահ ենք այն նպատակների մեջ, որոնցով առաջնորդվում են տեխնոլոգիաներ ստեղծողներն ու կառավարողները, և մենք երբեք չենք

կարող կանխատեսել, թե ստեղծված շնորհն ում ձեռքերում և ինչպես կարող է դառնալ հակահարված մարդասիրությանը, բնությանը, մարդու իրավունքներին ու ժողովրդավարությանը, հավատքին ու կենսակերպին և աշխարհի համակեցությանը:

Այս և մի շարք այլ նպատակներով այժմ, ավելի քան երբևէ առաջնահերթություն է տեղեկատվական հասարակությունում տիրապետել տեխնոլոգիաներին, իմանալ դրանցից ճիշտ և գրագետ օգտվելու ձևերն ու մեթոդները, կիրառել դրանք ի նպաստ մարդկության և աշխարհի բարօրության: Զուգահեռ կարիքը թելադրում է նաև այս ոլորտում անվտանգության հիմնահարցերին տիրապետելը և դրանցով առաջնորդվելը, որովհետև այսօր տեղեկատվական հասարակության համար որքան դրական ու նշանակալի են տեխնոլոգիաները, այնքան դրանք կրկնակի և շեշտակի բացասական ազդեցություն կարող են ունենալ «սխալ» մարդու ձեռքերում: Այդ իսկ նպատակով այսօր թվային անվտանգության մարտահրավերներին դիմակայելը տեխնոլոգիական աշխարհի առաջնահերթություններից են: Երբեմն անգամ մարդիկ հրաժարվում են տեխնոլոգիական բեկման տանող նորարարական գործիքներից, քանի դեռ դրանք բավարար չափով չեն ապահովում թվային անվտանգությունը, անձնական տվյալների պաշտպանությունը:

Այս ձեռնարկը ստեղծվել է խթանելու մարդու էլեկտրոնային գրագիտության և թվային անվտանգության գիտելիքներն ու հմտությունները, որոնք հնարավորություն կտան տեղեկատվական հասարակության ներսում լինել առավել իրազեկված և պաշտպանված գլոբալ տեղեկատվական միջավայրի զարգացման համատեքստում: Ձեռնարկում տեղ գտած տեղեկությունները վերցված են «Բոլորը հանուն հավասար իրավունքների» հիմնադրամի կողմից իրականացված

«Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոց» ծրագրի շրջանակում ոլորտի փորձառու մասնագետների կողմից վարած դասընթացների և վերապատրաստումների բովանդակությունից:

ՄԱՍ 1.
ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅՈՒՆ

ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ՀԻՄՈՒՆՔՆԵՐ

Ի՞նչ է էլեկտրոնային գրագիտությունը.

Էլեկտրոնային գրագիտությունը համակարգչով, սմարթֆոնով կամ տեխնիկական այլ միջոցով առցանց միջավայրում գործունեություն իրականացնելու առավել արդյունավետ և ընդունելի մեթոդների կիրառմամբ լավագույն արդյունքի հասնելու ճանապարհն է: Այլ կերպ ասած, էլեկտրոնային գրագիտությունը համակարգչային միջնորդավորված և ինտերնետային միջավայրերում գրագետ և վստահորեն հաղորդակցվելու, անվտանգ կարդալու, գրելու, ստեղծելու, ստեղծագործելու և հետազոտություններ իրականացնելու ունակություն է:

Ինչո՞ւ է մեզ պետք էլեկտրոնային գրագիտությունը.

Էլեկտրոնային գրագիտությունը թույլ է տալիս մեզ ճիշտ և արդյունավետ կիրառել տեխնոլոգիաները, դրանք օգտագործել ցանցային հաղորդակցության, արտադրանքներ ստեղծելու գործընթացում՝ որպես հիմնական և անփոխարինելի գործիքներ, ավանդական հաղորդակցության տարբերակները փոխարինել ժամանակակից մեթոդներով, որոնք, այլ կերպ ասած, թույլ են տալիս անցնել ժամանակով և տարածությունով, խնայել ժամանակ, միջոցներ և ռեսուրսներ, ընդլայնել գործունեության և ազդեցության շրջանակը:

Էլեկտրոնային գրագիտությունը մերօրյա՝ տեղեկատվական հասարակությունում թույլ է տալիս գրավել առաջնային դիրքեր, քանի որ այն ընձեռում է բազմաթիվ առավելություններ, ինչպես անհատական և անձնական գործունեությունում, այնպես էլ աշխատանքային շուկայում և

առավել լայն շրջանակում, քան անձնական և աշխատանքային գործունեության ավանդական փոխգործակցությունում:

Որո՞նք են էլեկտրոնային գրագիտության հիմնական առավելությունները, և ո՞րն է դրանց շնորհը.

Էլեկտրոնային գրագիտությունը մերօրյա միջավայրում անփոխարինելի կարողությունների ամբողջություն է և տեղեկատվական հասարակությունում ուրույն տեղ զբաղեցնելու միջոց:

Կան հիմնական պատճառներ, որոնք միանշանակ առավելություն և առանձնահատկություն են տալիս էլեկտրոնային գրագիտությանը.

- մենք գնում ենք դեպի գիտելիքահեն տնտեսություն, որն ամենուրեք օգտագործում է էլեկտրոնային գործիքներ,
- կրթությունն այլևս գտել է իր ժամանակակից հունը՝ էլեկտրոնային եղանակով կապելով և՛ սովորողին, և՛ սովորեցնողին, և՛ սովորեցնելու միջոցներն ու գործիքները, և՛ բովանդակությունը՝ ստեղծելով ահռելի և անսպառ հնարավորությունների հսկայական տիրույթ,
- տանը, դպրոցում, համալսարանում, աշխատավայրում, տնտեսության բոլոր ոլորտներում, գիտության, բժշկության, անգամ բնության մեջ, ամենուր պահանջվում են ունիվերսալ էլեկտրոնային հմտություններ,
- այն հեշտացնում է մեր աշխատանքը, հնարավորություն է տալիս որոնել առցանց տվյալներ, կապ պահել ընկերների հետ, հաղորդակցվել լայն հասարակության հետ, ստեղծել սեփական բովանդակությունը, հետևել մյուսների, այդ թվում նաև՝ զանգվածային լրատվության միջոցների և մեդիաների բովանդակությանը:

Ինչպիսի՞ մարտահրավերներ կան էլեկտրոնային միջավայրում.

Էլեկտրոնային միջավայրում մարտահրավերներն ուղիղ այնքան են,

որքան հնարավորությունները: Յուրաքանչյուր նոր գործիք սովորելու և կիրառելու ճանապարհը միշտ չէ, որ հարթ է ընթանում: Հաճախ, մեզ շատ ժամանակ է անհրաժեշտ որևէ գործիք կամ մոտեցում յուրացնելու և կիրառելու համար, երբեմն տեխնիկական հնարավորությունները սահմանափակում են մեզ որևէ գործիքի կամ մոտեցման կիրառման հնարավորության տեսանկյունից:

Էլեկտրոնային գրագիտությունը միանշանակ կարողությունների և հմտությունների ամբողջություն չէ, քանի որ այն իր մեջ ներառում է բազմաթիվ փոփոխականներ: Ամեն օր կայքերը, հավելվածները, գործիքներն ու մեթոդները թարմանում են, և մեր խնդիրն է տեղեկատվական արագ հոսքերի աշխարհում ունենալ բավարար ժամանակ, և այն հատկացնել այդ թարմացումների զարկերակը հսկելու համար:

Էլեկտրոնային գրագիտության առաջնահերթ մարտահրավերներից է նաև լեզուն: Բազմաթիվ հնարավորությունների տիրապետելու համար միայն մայրենի լեզվի իմացությունը բավարար չէ: Տեխնոլոգիաների ոլորտում այսօր ամբողջ աշխարհն է մեծ առաջընթաց ապրում, և ամեն օր ստեղծվում են ռեսուրսներ, որոնք այլ լեզվի կրող աշխարհի համար են: Այս տեսանկյունից շատ կարևոր է առնվազն անգլերենի յուրացումն ու կիրառումն էլեկտրոնային հաղորդակցության գործընթացում, քանի որ այն կարևոր է նախ՝ որևէ գործիք ուսումնասիրելու և կիրառման ճիշտ ձևերը սովորելու, հետո՝ այդ գործիքը գործնականում կիրառելու համար:

Թերևս, պետք է նշել, որ էլեկտրոնային գրագիտության մերօրյա

ամենամեծ մարտահրավերը թվային անվտանգությունն է: Առցանց տիրույթում ստեղծվել և ստեղծվում են բազմաթիվ որոգայթներ, որոնց նպատակն է մարդկանց անձնական տվյալների միջոցով շահեկան դիրք ունենալն ու տեղեկատվությանը տիրապետելը, որոնք անձնական և վերանձնային, մինչև իսկ պետական և հաքերային խմբերի մակարդակներում կարող են կիրառվել ամենատարբեր նպատակներով: Այս մասին առավել մանրամասն կանդրադառնանք ձեռնարկի թվային անվտանգության վերաբերյալ բաժնում:

Ի՞նչ է հաղորդակցությունը.

Հաղորդակցությունը տեղեկատվության փոխանցումն է մեկ վայրից մեկ այլ վայր: Էլեկտրոնային հաղորդակցությունն էլեկտրոնային եղանակով տեղեկատվության շրջանառումն է գրավոր, բանավոր և այլ եղանակներով:

Գրագետ հաղորդակցությունը ենթադրում է նաև հետադարձ կապ, ինչը բնորոշ է երկկողմ և բազմակողմ հաղորդակցությանը, որը նաև անվանում են տրանզակցիոն հաղորդակցություն: Հաղորդակցության մեկ այլ մոտեցում է գծային հաղորդակցությունը, երբ այն վարվում է մեկ ուղղությամբ և չի ակնկալում հետադարձ կապ: Թերևս, այս ձեռնարկում մենք կխոսենք միայն տրանզակցիոն հաղորդակցության մասին, որը փոխադարձ շփումերի, արձագանքների, հարցուպատասխանի և պլանավորման վրա հիմնված մոտեցում է:

Այս առումով հաղորդակցությունը մարդու վարքագծի վրա ազդելու և պատասխան ազդակ ստանալու միջոց է: Վարքագծի վրա ազդել ասելով ի նկատի չունենք մանիպուլյացիան կամ հոգեբանական, կամ ֆիզիկական նպատակային որևէ գործիքի ու մեթոդի կիրառում: Սակայն անկախ մեր կամքից, շատ ժամանակ ինքներս կիրառում ենք բազմաթիվ գործիքներ, որոնք ամրապնդվում են մեր մեջ լույս աշխարհ գալուց ի վեր: Այդուհանդերձ, ասել, թե հաղորդակցության գործընթացում չեն կիրառվում հոգեբանական ազդեցության նպատակով մշակված գործիքներ, սխալ կլինի, քանի որ այն կառուցված է մարդու հոգեբանական և վարքային առանձնահատկությունների վրա:

Հաղորդակցության տեսակներն ու նպատակները.

Հաղորդակցության տեսակներն ու ըստ այդմ նաև նպատակները կարող են լինել խիստ բազմազան և բազմաժանր: Այս ձեռնարկում մենք կառանձնացնենք ներքին և արտաքին հաղորդակցության հիմնական տեսակները, որոնք կիրառվում են աշխատանքային հարաբերություններում:

Ներքին հաղորդակցություն.

Ներքին հաղորդակցությունը հիմնականում ուղղված է թիմի ներսում հաղորդակցային կապերի և ենթակառուցվածքների ստեղծմանը, որի նպատակն է աշխատանքի համատեղ, արդյունավետ և համաժամանակյա իրականացումը: Շատ հաճախ ներքին հաղորդակցությունը տեղի է ունենում բանավոր եղանակով, քանի որ հաղորդակցության կողմերը գտնվում են ֆիզիկական միևնույն տարածքում, սակայն խորհուրդ է տրվում, որ անգամ բանավոր հաղորդակցության շրջանակում ձեռք բերված համաձայնությունը ճշգրտել և ամրագրել գրավոր եղանակով՝ թյուրըմբռնումներից, տարընկալումներից և հետագա հակասություններից զերծ մնալու նպատակով:

Հաղորդակցության կարողությունների զարգացման՝ բովանդակության մատուցման և ընկալման վերաբերյալ բազմաթիվ խաղեր կան, որոնք զարգացնում են մեր կարողությունները: Խաղերից մեկի օրինակը բերված է ստորև.

Խաղի նկարագրություն

Խաղացողները նստում են դեմ դիմաց՝զույգերով: Առաջին խաղացողը

երկրորդին պատմում է որևէ պատմություն, դրվագ կամ նկարագրում է որևէ բան: Երկրորդ խաղացողը, լսելով առաջինի բովանդակությունը, պետք է ասի՝ «Ես ճիշտ հասկացա՞, դուք ի նկատի ունեք, որ....» և շարունակի վերարտադրել այն բովանդակությունը, որը ստացել է առաջին խաղացողից՝ վերապատմելով այն իր ընկալումներով: Այնուհետև, հակառակը՝ երկրորդ մասնակիցն է որևէ բան պատմում առաջինին, և առաջինը վերարտադրում է այն: Այս ընթացքում զրուցակիցները միմյանց ուղղում են և կատարում նշումներ նկատված սխալների և վրիպակների վերաբերյալ:

Նմանատիպ վարժանքները մեզ օգնում են հասկանալու հաղորդակցությունն իր ողջ բարդությամբ և նպաստում է դիմացինին հասկանալու ու մեր ընկալումների օբյեկտիվությունը գնահատելու հարցում:

Ներքին՝ գրավոր հաղորդակցության նպատակով կիրառվում են էլեկտրոնային փոստերը, սակայն տեխնոլոգիաների զարգացմանը և տեղեկատվական հոսքերի մեծացմանը զուգահեռ հաղորդակցային էվոլյուցիան տեղափոխվել է նաև ժամանակակից սոցիալական մեդիաներ և մեսենջերներ, որտեղ հնարավոր է ստեղծել խմբային չատեր:

Հաղորդակցության ընթացքը գնահատելը բարդ գործընթաց է, սակայն եթե այն բերել է երկկողմ ցանկալի արդյունքի, ապա այն կարելի է համարել հաջողված, քանի որ հաղորդակցության գնահատման հիմնական ցուցիչը նպատակային արդյունքի արձանագրումն է: Ներքին հաղորդակցությունը մեծ ազդեցություն ունի արտաքին հաղորդակցության վրա, և սխալ չի լինի ասել, որ հաճախ, արտաքին

հաղորդակցության հաջողությունը կայանում է ներքին հաղորդակցության արդյունավետության մեջ:

Արտաքին՝ ռազմավարական հաղորդակցություն.
Արտաքին հաղորդակցությունն ամբողջապես հիմնված է դրա ռազմավարական պլանավորման վրա: Ռազմավարական հաղորդակցությունը ենթադրում է հաղորդակցության ողջ գործընթացի մշակում և իրականացում:

Հաղորդակցային ցանկացած գործընթաց մեկնարկելուց առաջ այն պետք է պլանավորել՝ լավագույն արդյունքի հասնելու նպատակով: Հաղորդակցությունը պլանավորելիս պետք է անդրադառնալ հետևյալ հարցերին՝

- Որո՞նք են հաղորդակցության նպատակները և խնդիրները:
- Ովքե՞ր են հաղորդակցության լսարանը, շահառուներն ու շահակիցները, թիրախ խումբը:
- Որո՞նք են այդ լսարանին հասնելու հաղորդակցային ալիքները, խողովակները:
- Որո՞նք են տվյալ լսարանի կարիքները և հետաքրքրությունները: Ինչպե՞ս բավարարել դրանք:
- Ո՞ր հարթակներով և ի՞նչ միջոցներով է հնարավոր արագորեն և արդյունավետ կազմակերպել հաղորդակցությունը տվյալ լսարանի հետ:
- Որո՞նք են այն բանալի ուղերձները, որոնք պետք է ուղղվեն լսարանին:

Այս հարցերի պատասխանները կհանդիսանան հաղորդակցության փոքրիկ ռազմավարություն, որը կօգնի ձեզ ճիշտ և արդյունավետ կերպով

կազմակերպել այն՝ հասնելով լավագույն արդյունքին:

Հիմա, ավելի մանրամասն. արտաքին՝ ռազմավարական հաղորդակցությունը որպես նախագիծ (պրոյեկտ): Ռազմավարական հաղորդակցության նպատակը պետք է սահմանի, թե ինչի համար է այն իրականացվում, ինչ արդյունքի ենք ուզում հասնել հաղորդակցության միջոցով, որն է այն կետը, որին ուզում ենք հասնել: Նպատակը պետք է հստակ ձևակերպվի և ցույց տա Ա կետից Բ կետ գնալու մեր ներքին շարժառիթն ու վերջնարդյունքի նկարագրությունը, որը զուգահեռ պետք է լինի չափելի և գնահատելի: Չափելի և գնահատելի լինելու կարևորությունը պայմանավորված է հաղորդակցության ռազմավարության իրականացման ընթացքը հսկելու և դրա արդյունավետությունը հասկանալու համար: Եթե, օրինակ, մենք գիտենք, որ մեր նպատակն է մեկ օրում ձեռք բերել հինգ խնձոր, ապա այստեղ ամեն բան ակնհայտ է, չափելի և գնահատելի, քանի որ գիտենք, որ գնահատումն իրականացնելիս ստուգելու ենք այդ նպատակին հասնելու համար ծախսված ժամանակը և խնձորների քանակը: Բացի այդ, երբ նպատակը չափելի է, այն մեզ օգնում է իրականացման ընթացքում չշեղվել և հավատարիմ մնալ նախանշված պայմաններին: Երբեմն, հաղորդակցության նպատակը ձևակերպվում է իբրև գերնպատակ կամ տեսլական, որն այս առումով ո՛չ գնահատելի է, ո՛չ չափելի: Գերնպատակի և տեսլականի ձևակերպումը ևս ռազմավարական պլանավորման մաս է, սակայն դրանք չպետք է ձևակերպվեն որպես միակ նպատակ, որպեսզի թույլ տան հասկանալու ռազմավարական հաղորդակցության հաջողությունները: Օրինակ, տեսլականում և գերնպատակում կարող է ձևակերպված լինել, որ հինգ տարի հետո Հայաստանում պետք է լինի մարդու իրավունքների և ազատությունների իրացման համար բոլոր

մեխանիզմները, և դրանք պետք է ամրապնդված լինեն արդարադատության համակարգում, կամ, որ Հայաստանում մեդիագրագիտության մակարդակը հասարակության լայն շերտերի մոտ կլինի բավարար մակարդակի վրա: Այս ձևակերպումները կարևոր են, սակայն միայն սրանց վրա հիմնվելը բավարար չէ: Այդ իմաստով կարևոր է ձևակերպել հաղորդակցության հիմնական նպատակը:

Խնդիրները ձևակերպելիս պետք է հիմնվել նպատակի և արդյունքների վրա: Խնդիրները նույնպես պետք է լինեն չափելի ու շոշափելի, և դրանց իրականացումը պետք է հանգեցնի նպատակի իրագործմանը: Այլ կերպ ասած, խնդիրները դրանք մեր փոքր նպատակներն են, որոնցից յուրաքանչյուրի իրականացումը մեզ մոտեցնում է մեր գլխավոր նպատակին: Ե՛վ նպատակի, և՛ խնդիրների ձևակերպումը ենթադրում է նախագծերի նպատակ-խնդիրների ձևակերպման մեթոդաբանության կիրառումը, սակայն այստեղ շեշտը դրվում է հաղորդակցության և լսարանի ներգրավման վրա:

Լսարանը ձևակերպելիս պետք է ֆիլտրացնել շահառուների այն խումբը, որին ուղղված է լինելու հաղորդակցությունը: Շատերը շահառուների խումբը սահմանելիս վերացական մոտեցում են ցուցաբերում և տալիս ընդհանրական ձևակերպումներ, օրինակ, որ իրենց լսարանը Հայաստանում ապրող մարդիկ են: Արտաքին հաղորդակցության տեսանկյունից սա համարվում է ոչ արդյունավետ, որովհետև Հայաստանում ապրում են ամենատարբեր տարիքի, կրթության, հետաքրքրությունների և զբաղվածության մարդիկ: Որպեսզի հաղորդակցությունն արդյունավետ իրականացվի պետք է ձևակերպել կոնկրետ և հստակ լսարան, օրինակ, Շիրակի մարզի բուհերի

իրավաբանական բաժնում սովորող ուսանողներ: Սա չափելի է և հստակ, ինչպես նաև օգնում է, որպեսզի մենք հեշտորեն մշակենք գործիքներ սահմանված լսարանին հասնելու համար: Եթե մենք գիտենք՝ որն է մեր լսարանը, մենք կկարողանանք ուսումնասիրել և հասկանալ նաև տվյալ լսարանի կարիքներն ու հետաքրքրությունները և, ըստ այդմ, մշակել հաղորդակցության նպատակները, խնդիրները, ուղերձներն ու դրանք հասցեավորելու եղանակները:

Երբ արդեն ձևակերպել ենք լսարանը, սկսում ենք աշխատել բանալի ուղերձների (key messages) վրա: Յուրաքանչյուր նպատակի հասնելու համար հարկավոր է ներգրավել լսարանին, իսկ լսարանին ներգրավելու համար հարկավոր է մշակել ուղերձներ, որոնք հիմնված են տվյալ լսարանի կարիքների ու հետաքրքրությունների վրա: Արտաքին հաղորդակցության ռազմավարական պլանավորումը նման է մարքեթինգի, որի նպատակը գովազդային արշավն է և դրա հաջողությունը: Այստեղ ևս լսարանն ու լսարանի կարիքներն առաջնային են, և, եթե մեր հաղորդակցությունը ներառում է լսարանի հետաքրքրությունները, ապա հաջողությունն անխուսափելի է:

Ռազմավարական հաղորդակցության հաջորդ և վերջին կարևոր կետն ուղերձները հասցեավորելու ալիքներն են: Այսինքն, այն հարթակները, գործիքներն ու այս պարագայում համացանցային միջոցները, որոնցով մենք հեշտորեն կարող ենք հասնել լսարանին: Օրինակ, եթե մեր լսարանը երիտասարդներն են, ապա սոցիալական մեդիայի ժամանակակից հարթակները և այդ հարթակներին համահունչ մշակված ուղերձները լավագույն ճանապարհն են հաղորդակցությունը հաջողությամբ պսակելու համար: Եթե երիտասարդներն առավել ակտիվ են

Ինստագրամում, ապա մենք կիրառում ենք այս հարթակը և ժամանակ ու ռեսուրսներ չենք ծախսում Լինկդինում սոցիալական մեդիայի արշավներ իրականացնելու վրա:

Այսպիսով, արտաքին՝ ռազմավարական հաղորդակցությունն էլեկտրոնային գրագիտության և էլեկտրոնային հաղորդակցության անբաժանելի մաս է և ենթադրում է նախապես պլանավորված ու մշակված գործողությունների իրականացում: Հաղորդակցության նպատակի իրագործումը խթանում է մեր նախագծի նպատակի իրագործմանը: Այս առումով դրանք միմյանց նման են մեթոդաբանորեն, սակայն միմյանցից տարբերվում են իրենց մոտեցումներով:

Արտաքին հաղորդակցության գնահատումը ներկայացնելու համար պատկերացնենք պայմանական կազմակերպություն, որում այն տեղի է ունենում: Արտաքին հաղորդակցությունը համարվում է ցանկացած նախագծի գործունեության հիմնական մասը: Արտաքին հաղորդակցությունն ապահովում է գործունեության տեսանելիությունը, ներկայացուցչականությունը և կապը գործընկերների ու այլ ցանցերի հետ: Բացի այդ, այն հնարավորություն է տալիս զարգացնել նախագծի մոտեցումները և համակարգման գործընթացները:

Արտաքին հաղորդակցությունը հնարավորություն է տալիս գնահատել լսարանը, լսարանի կարիքները և առավել խորքային ընկալել լսարանի կապն ու գոհունակությունը նախագծի հետ հարաբերություններում: Լսարանի հետ տարվող աշխատանքներում շատ կարևոր է հետադարձ կապի ապահովումը: Այն կարող է լինել և՛ գրավոր, և՛ բանավոր, կախված իրավիճակից և անհրաժեշտությունից: Ընդ որում, հարկ է նշել, որ

գնահատումները և հետադարձ կապի ապահովումը կարող է լինել ինչպես անվանական, այնպես էլ անանուն: Ստորև բերված է գնահատման ընթացակարգի մեկ օրինակ՝ գնահատման թերթիկների կիրառման պրիզմայով:

Գնահատման թերթիկների պատրաստման գործընթացում հարկավոր է հաշվի առնել, որ դրանք պետք է լինեն հնարավորինս կարճ և պահանջեն նվազագույն ծավալի տեքստ: Գնահատումը կարող է լինել միավորների տեսքով: Սակայն, հարկավոր է հաշվի առնել նաև տեքստի և որակական գնահատականի կարևորությունը, որովհետև քանակական և թվային գնահատումները չեն կարող բացահայտել խորքային խնդիրներն ու զարգացման հնարավոր հեռանկարները, ի տարբերություն տեքստի և նկարագրությունների:

Գնահատումների հարցաթերթերը պատրաստելիս հարկավոր է նաև հաշվի առնել սոցիոլոգիական մի քանի կարևոր բաղադրիչներ, որոնք մշտապես կիրառվում են հաղորդակցության ոլորտում և հետազոտություններում՝

- յուրաքանչյուր գնահատող իրավունք ունի գնահատումն անել անանուն,
- յուրաքանչյուր գնահատող իրավունք ունի չպատասխանելու ցանկացած հարցի, եթե նախապես այլ համաձայնագրով չի պարտավորվում մասնակցել գնահատմանը լիարժեքորեն,

յուրաքանչյուր հարց պիտի ունենա հետևյալ տարբերակները՝ այլ, չգիտեմ, դժվարանում եմ պատասխանել, հրաժարվում եմ պատասխանել: Գնահատման գործընթացի համար կիրառվող ամենահայտնի գործիքը Google Forms-ն է, որը նախատեսված է հարցումների, հայտաթերթերի և

գնահատման գործընթացների ու տվյալների հավաքագրման և վերլուծության համար:

Էլեկտրոնային հաղորդակցության տեխնիկական առանձնահատկությունները.

Մեր օրերում հաղորդակցությունը լսարանի հետ առավել հաճախ և ինտենսիվ կերպով տեղի է ունենում հեռավար և էլեկտրոնային եղանակով, ինչը ենթադրում է էլեկտրոնային գործիքների կիրառում: Այս առումով շատ կարևոր է տեխնիկական տեսանկյունից էլեկտրոնային եղանակով գրագետ հաղորդակցության վարումը լսարանի հետ:

Ցանցում շրջանառվող փաստաթղթեր և էլեկտրոնային գրագրություն.

Ստորև բերված են շրջանառվող փաստաթղթերի և գրագրության տեխնիկական չափանիշներ, որոնք ընդունելի են համարվում շատերի կողմից, սակայն միանշանակ չեն:

Գրագրությունում դրանք պետք է համապատասխանեն տեխնիկական հետևյալ չափանիշներին՝

- Տառատեսակը՝ «Sylfaen» (հայերենի դեպքում), «Times New Roman» (անգլերենի և ռուսերենի դեպքում): Այս տառատեսակների կիրառումը շատ կարևոր է, քանի որ դրանք ամենատարածված գործարանային տառատեսակներն են համակարգիչներում: Այլ տառատեսակով ուղարկվող նամակները ստացող կողմի մոտ կարող են լինել ոչ ընթեռնելի (դատարկ ուղանկյուններ, «ճիճուներ»), եթե տվյալ տառատեսակը համակարգչում կարգավորված չէ: Այդ պատճառով լավ է օգտվել այն տառատեսակներից, որոնք գործարանային (by default) սկզբունքով առկա են համակարգիչներում:

- Տառաչափը՝ 12 անգլերենի և ռուսերենի դեպքում, 11 հայերենի դեպքում: Հայերեն տառերի նիշերն իրենց չափերով առավել մեծ են, քան ռուսերենն ու անգլերենը: Այդ պատճառով լատինատառ և կյուրեղատառ կիրառելիս մեկ նիշով ավելի մեծ տառաչափ է կիրառվում, քան հայերենում:
- Վերնագրերի տառաչափը՝ 12 կամ 14: Շատ կարևոր է, որ տեքստում կիրառվող տառաչափերը մեկը մյուսի նկատմամբ շատ մեծ տարբերություն չունենա: Այն տգեղ է համարվում նաև վիզուալ առումով:
- Լրացումների, ծանուցումների (footnote) տառաչափը՝ մինչև 10, առանձնահատուկ շեշտադրումները՝ մուգ տառատեսակով և/կամ ընդգծված: Հարկ է հիշել, որ միևնույն տեքստում գույնզգույն նշումները և ուշադրությունը գրավելու համար միաժամանակ մի քանի տարբերվող գործիքների կիրառումը վիզուալ առումով վանող է դարձնում տեքստը:
- Տեքստի գույնը՝ մուգ սև: Սա նպաստում է տեքստի տեսանելիությանն ու ընթեռնելիությանը, եթե այն գրված է սպիտակ ֆոնի վրա:
- Բառերի միջև հեռավորությունը՝ 1 բացատ (space): Հաճախ մենք հանդիպում ենք տեքստերի, որոնց բառերի միջև եղած հեռավորությունը միմյանցից տարբերվում է. մի տեղ երկու բացատ, մի տեղ երեք և այլն: Էլեկտրոնային հաղորդակցությունն ուղղակիորեն պահանջում է գրագրության ընթացքում յուրաքանչյուր բառից հետո թողնել մեկ բացատ, այլապես ստեղծված տեքստը վիզուալ առումով կլինի տգեղ, տպագրման ոչ ենթակա, ոչ ներկայացուցչական և ոչ գրագետ: Հանդիպե՞լ կամ կարդացե՞լ եք երբևէ գրքեր, որտեղ բառերի միջև բացատների քանակը տարբերվում է միմյանցից: Իհարկե՝ ոչ:

- Փաստաթղթերի ձևաչափը՝ «A4»: Սա Հայաստանում և աշխարհում ամենաշատ կիրառվող տպագրական ձևաչափն է: Հարկ է նշել, որ «Microsoft Office Word»-ում նոր փաստաթուղթ ստեղծելիս այն գործարանային սկզբունքով ստեղծում է «Letter» ձևաչափի թուղթ, ինչը տարբերվում է «A4»-ից: Այդ պատճառով «Layout» մենյուի «Size» ենթաբաժնում հարկավոր է ընտրել ճիշտ և կիրառելի ձևաչափը:
- Լուսանցքները՝ ստանդարտ կամ ստանդարտ նեղ: Սա կարևոր է պահպանել, քանի որ հակառակ դեպքում տեքստը ստացող կողմի համար կարող է այն ընթեռնելի չլինել համակարգչի կամ սմարթֆոնի սահմանված լուսանցքներից դուրս լինելու պատճառով և չտպագրվել տպիչ սարքերի տպագրման սահմանների սահմանափակումների պատճառով:
- Միջտողային հեռավորությունը՝ 1.0–1.5: Այս հեռավորությունը կիրառվում է տպագրական գործընթացում և ֆիզիկական առումով համարվում է աչքի համար ընթեռնելիության լավագույն տիրույթը:
- Էջերի համարակալումը պարտադիր է: Էջերի համարակալումը գրագրության գործընթացում նախապայման է:
- Հղումները պետք է ներառված լինեն տեքստի մեջ, բաց հղումները կարող են դրվել ծանոթագրությունում՝ յուրաքանչյուր էջի վերջում՝ տվյալ էջինը, կամ փաստաթղթի վերջում՝ ամբողջ փաստաթղթինը: Դրանք պետք է լինեն ավտոմատ համարակալված: Սովորաբար այդ կարգավորումները լինում են մենյուի «Reference» բաժնի «Insert Footnote» ենթաբաժնում: Այն հղումները, որոնք իրենց մեջ պարունակում են ոչ լատինական նիշեր և դրանով պայմանավորված ավելի երկար են, քան մեկ տողը, հարկավոր է կրճատել օնլայն անվճար ծրագրերի միջոցով (Link shorterner):

- Փաստաթղթերի պատրաստման ամսաթվի և հեղինակի անվան զետեղումը փաստաթղթի վերջին էջի աջ անկյունում կամ փաստաթղթի անվան մեջ ցանկալի է:
- Փաստաթղթերի վերնագրերը գրվում են անգլերեն՝ լատինական այբուբենի տառերով, ոչ հոդային բառերի առաջնատառերը մեծատառ, իմաստային բառերը միմյանց կապած՝ ներքևի գծիկով (_), իսկ իմաստային առումով միմյանցից տարբերվող հատվածներն առանձնացվում են մեջտեղի գծիկով (-), օրինակ, «Digital_Security-Book_2022»:

Փաստաթղթերը Հայաստանում հիմնականում վարվում են «Microsoft Office» ծրագրային փաթեթի կողմից (հիմնականում «Windows» օպերացիոն համակարգի պարագայում), օնլայն փաստաթղթերը՝ «Google Online Office»-ի և «Microsoft Office 365»-ի կողմից:

Անկախ փաստաթղթի բովանդակության լեզվից, փաստաթղթի վերնագիրը (ֆայլի անունը) պետք է լինի գրված անգլերենով/ լատինատառ: Սա անհրաժեշտ է, որպեսզի ֆայլի օնլայն տարբերակը, չդառնա շատ երկար և կազմված տգեղ նշաններից (%%%), ինչը տեղի է ունենում և՛ հայերենի, և՛ ռուսերենի դեպքում: Ինչպես նաև, չնայած համակարգչային տեխնոլոգիաների զարգացմանը, դեռևս կան դեպքեր, երբ հայերեն կամ ռուսերեն անվանումներով ֆայլերը չեն բացվում, հատկապես աշխարհի այլ ծայրերում գտնվող համակարգիչների դեպքում:

Կարևոր է ֆայլի անվանման մեջ դնել հիմնական բանալի բառերը (կազմակերպության, նյութի վերնագրի, հեղինակի հապավումները) և

վերջին խմբագրման ամսաթիվը, ինչը կօգնի հետագայում փաստաթուղթը հեշտ գտնել, հասկանալ՝ մշակման որ փուլում է գտնվում, ինչպես նաև փնտրողը կամ ստացողն առաջին հայացքից կհասկանա՝ մոտավորապես ինչի մասին է նյութը:

Էլեկտրոնային փոստեր և աշխատանք փոստերի միջոցով.
Աշխարհում կան բազմաթիվ գործիքներ և հարթակներ, որոնք մարդկանց տրամադրում են անվճար տարածքներ (hosting) և նույնականացված հասցեներ (domain)՝ էլեկտրոնային փոստի ստեղծման և վարման համար: Օրինակ, բազմաթիվ մատակարարներ (provider) տրամադրում են անվճար մեյլային ծառայություններ, ինչպիսիք են՝ Gmail, AOL, Outlook, Yahoo Mail, iCloud Mail, Mozilla, Mail.ru, Rambler Mail, Yandex Mail, Zoho Mail, Proton Mail, GMX Mail և այլն: Չնայած այս հարթակներն անվճար են, բայց սրանցից յուրաքանչյուրն ունի որոշակի սահմանափակումներ՝ մեյլերի քանակի, օգտագործված հիշողության չափի և այլն: Զուգահեռ մեյլային ծառայությանն, այս հարթակներին կցված են մատակարարների այլ ծառայություններ ևս: Օրինակ, եթե դուք ստեղծում եք Գուգլի «Gmail»-ի հաշիվ, ավտոմատ՝նույն մուտքանունով և գաղտնաբառով, դուք կարողանում եք մուտք ունենալ Գուգլի այլ հարթակներ և օգտագործել դրանք որպես հաշվետեր: «Gmail»-ին զուգահեռ ստեղծվում են հաշիվներ YouTube, Bolgspot, Google Drive, Google Clasroom, Google Contacts, Google Maps, Google Calendar, Google Photos, Google Meet, Google Duo, Google Books, Google Ads, Google Business, Google Hangouts, Google Arts and Culture, Google Earth, Google Finance, Google Podcasts և բազմաթիվ այլ հարթակներում ու գործիքներում, որոնք ստեղծված են կազմակերպության կողմից: Այս իմաստով, Գուգլի կարգախոսն է՝ «Մեկ հաշիվ՝ Գուգլի ամբողջ աշխարհ»:

Անդրադառնալով էլեկտրոնային փոստերին՝ փորձենք հասկանալ դրանց գրագետ կիրառման մոտեցումները:

Գործընկեր կառույցներին և անհատներին նամակներ գրելիս հարկավոր է «Թեմա/Subject» դաշտում լրացնել նամակի էությանը վերաբերող վերնագիրը: Որոշակի ծրագրի շրջանակներում գրվող նամակների պարագայում ցանկալի է, որ «Թեմա/Subject» դաշտում նշվի նաև ծրագրի անվանումը կամ հապավումը: Այն հնարավորություն կտա հետագայում նամակների որոնելիության արդյունավետությունը բարձրացնել և հեշտությամբ կառավարել էլեկտրոնային փոստի հաղորդագրությունները:

Գործընկեր կառույցներին և անհատներին նամակներ գրելիս հարկավոր է կիրառել «to», «cc» դաշտերը՝ դրանցում դասակարգելով էլ. հասցեներն ըստ նամակի էության՝ «to» դաշտում ներառելով այն էլ. հասցեները, ում ուղղված է նամակը, «cc» դաշտում ներառելով այն հասցեները, ովքեր որոշակի (ուղղակի կամ անուղղակի) կապ ունեն այդ նամակի կամ հաղորդագրության հետ:

Հաղորդակցության և հանրային կապերի կառավարման տեսանկյունից սխալ է համարվում սեփական/անձնական էլ. փոստի կիրառումն աշխատանքային նպատակներով: Աշխատանքային պարտականություններից բխող հաղորդագրությունները պետք է ուղարկվեն աշխատանքային էլ. հասցեից: Այն կարևոր է անձնական տվյալների (շահառուներ, գործընկեր կառույցներ) և կոնֆեդենցիալ փաստաթղթերի պաշտպանության տեսակետից, առավել ներկայացուցչական է գործընկերների հետ հաղորդակցության առումով:

Աշխատանքային էլ. փոստի կիրառումը մեծ իմաստով կապ ունի նաև ինստիտուցիոնալ հիշողության հետ: Օրինակ, մեկ աշխատակցի փոխարինումն այլ աշխատակցով, չի այրում տեղեկատվական կամուրջները, այն շարունակում է պահպանել տեղեկություններ նախկինում արված աշխատանքի վերաբերյալ և հասանելի է լինում նոր աշխատակցին:

Կազմակերպության և անհատի անունից մի քանի կառույցների կամ անհատների ուղարկվող նամակների պարագայում, եթե դրանք իրենցից ենթադրում են հայտարարություններ, նորություններ և նման կատեգորիայի այլ տեղեկություններ, ապա պարտադիր է հասցեատերերի էլ. փոստերը գրել «bcc» դաշտում՝ երրորդ անձին չբացահայտելով քաղաքացիների անձնական տվյալները (էլ. փոստի հասցեները): Անձնական տվյալների պաշտպանությունը կարգավորվում է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով, որն արգելում է առանց տվյալների սուբյեկտի համաձայնության հավաքագրել, կիրառել վերաբերական տվյալները, և այն հասանելի դարձնել երրորդ անձին:

Նամակներին արձագանքելիս հարկավոր է օգտվել «Պատասխանել / Reply» և «Պատասխանել բոլորին / Reply All» կոճակներից որևէ մեկից՝ ելնելով արձագանքի նպատակից և այն լսարանից, որին ուղղվում է արձագանքը: Եթե պատասխան նամակն ուղղված է կոնկրետ անձի, ապա պետք է միայն օգտագործել «Պատասխանել/Reply» տարբերակը, հակառակ դեպքում բոլորը կտեսնեն միմյանց արձագանքը, մինչդեռ դրա անհրաժեշտությունը չկա, և այն կարող է համարվել հավելյալ ծանրաբեռնվածություն:

Միջազգային գործընկերներին էլ. փոստով նամակներ գրելիս հարկավոր է դրանք ուղարկել պլանավորման կոճակի (schedule) միջոցով՝ ելնելով տվյալ երկրում և Հայաստանում ժամային գոտիների տարբերությունից՝ առաջնահերթություն դիտարկելով հասցեատիրոջ երկրում աշխատանքային ժամի մեկնարկը և ավարտը: Առավել ակտիվ գործընկերային հարաբերությունների պարագայում նամակներն ուղարկվում են՝ անտեսելով ժամային գոտիների տարբերությունը:

Էլեկտրոնային փոստով նամակ ուղարկելիս հարկավոր է կրկնակի ստուգել՝ հասցեատերերի էլ. փոստերի համապատասխան դաշտերում լրացված լինելու ճշտությունը, հաղորդագրության «Թեմա/Subject» դաշտում զետեղված տեքստի կամ վերնագրի ճշտությունը, բովանդակության և կից ֆայլերի առկայությունը: Առանց բովանդակության և/կամ «Թեմա» դաշտի լրացման, նամակներ ուղարկելն արգելվում է: Դրանք կարող են հայտնվել նաև ոչ ցանկալի (Spam/Junk) նամակների պանակում, ինչի պարագայում կարող են անտեսվել և մնալ անարձագանք:

Էլեկտրոնային փոստով հաղորդակցվելիս հարկավոր է պահպանել տեխնիկական նույն կանոնները, որոնք թվարկված են այս ձեռնարկի փաստաթղթաշրջանառության և էլեկտրոնային գրագրության վերաբերյալ հատվածում:

Էլեկտրոնային փոստով նամակներ գրելիս հարկավոր է յուրաքանչյուր նոր միտք կամ միմյանցից անկախ ձևակերպումներ տարանջատել պարբերություններով: Դա օգնում է, որպեսզի տեքստը լինի դյուրընթեռնելի: Հարկավոր է ցուցաբերել ենթակարգություն

(սուբորդինացիա) և հարգանք, ինչը գործնականում արտահայտվում է դիմելաձևի մեջ, օրինակ՝

«Հարգելի Անի, հուսամ՝ լավ եք,
Կից ֆայլով Ձեզ եմ ուղարկում միջոցառման վերաբերյալ հայտարարության տեքստը և օրակարգի նախնական՝ սևագրային տարբերակը:
Կսպասեմ Ձեր դիտարկումներին և արձագանքներին:
Արդյունավետ աշխատանքային օր եմ մաղթում:
Հարգանքով՝
Արամ»

Յուրաքանչյուր օգտատիրոջ էլեկտրոնային փոստ պետք է ունենա ստորագրություն (signature), որտեղ պետք է արտացոլվի տվյալ մարդու անունը, ազգանունը, պաշտոնը կամ մասնագիտությունը, եթե դա կարևոր է, և կոնտակտային տվյալները՝ հետադարձ կապի համար: Օրինակ,

Lilit Hakobyan
Communication Specialist

_____

Address: ...., Yerevan, Armenia 0002
E-mail: lhakobyan@gmail.com
Tel.: +374 _ _ _
+ 374 _ _ _
Facebook: ...
Webpage: ...

Էլեկտրոնային փոստերով գրագետ հաղորդակցությունը մեծ նշանակություն ունի աշխատանքային գործունեություն ծավալելիս: Շատ գործընկերներ և անհատներ կարող են կարծիք կազմել մարդու մասին՝ գրված նամակի տեխնիկական մոտեցումներից, կոկիկությունից և մեդիագրագետ վարքագծից:

Facebook, Instagram, Twitter, LinkedIn, Tik-Tok, Telegram, Snapchat, Pinterest, Messenger, WhatsApp, Viber, Creator Studio, YouTube, Vimeo, Social Media Management գործիքներ և այլն:

Սոցիալական ցանցերը շատ են և բազմազան: Մեր օրերում տարեկան կտրվածքով կարելի է բացահայտել մի քանի նոր սոցիալական ցանց, գրանցվել դրանցում և դառնալ ակտիվ օգտատեր: Սոցիալական ցանցերը հայտնի են իրենց ժամանակատարությամբ, երբ օգտատերը կարող է մուտք գործել ու ժամերով թերթել նորությունների ժապավենը: Միևնույն ժամանակ սոցիալական ցանցերը նպաստում են ժամանակային խնայողությանը, քանի որ թույլ են տալիս միաժամանակ և արագ հաղորդակցվել շատ մարդկանց հետ: Ամեն ինչ կախված է օգտատերից:

Մի կողմ թողնելով սոցիալական մեդիայի հուզական ազդեցությունները և թե հոգեբանական ինչպիսի վիճակի կարող է այն բերել մարդկանց՝ միանգամից անցում կատարենք դրանց գրագետ և նպատակային օգտագործմանը:

Նախ, շատ կարևոր է հասկանալ, թե սոցիալական որ ցանցն ինչ նպատակով է ստեղծված, և որն է տվյալ ցանցի հաղորդակցային ձևաչափը: Օրինակ, Ինստագրամը նախատեսված է հիմնականում լուսանկարների, կարճ տեսանյութերի, սթորիների և ուղիղ հեռարձակումների համար, Տիկ-Տոկը՝ կարճ տեսանյութերի, Ֆեյսբուկը՝ առավել երկար գրառումների, հրապարակումների, խմբերի ձևավորման, միջոցների հայթայթման, միջոցառումների առցանց պլանավորման և

իրականացման, ուղիղ հեռարձակումների և լուրերի, Թվիթերը՝ կարճ գրառումների, տեսանյութերի և լուրերի, Լինկդինը՝ աշխատանքային ցանցերի ստեղծման, աշխատանքային փոխգործակցության, աշխատանքային կենսագրության ստեղծման և վարման, չատերը և մեսենջերները՝ հաղորդակցության, նորությունների փոխանակման, արագ կապի:

Շատ կարևոր է այս հարթակների նպատակային կիրառումը թե՛ անձնական, թե՛ գործնական նպատակներից ելնելով: Օրինակ, Ֆեյսբուկը լուսանկարների համար կիրառելը նույնչափ արդյունավետ չէ, որքան Ինստագրամը, Փինթերեսթը կամ լուսանկարների համար նախատեսված այլ հարթակներ:

Սոցիալական մեդիաներն աշխատում են հստակ կոդավորված ալգորիթմներով: Դրանց իմացությունը ևս անհրաժեշտություն է: Ալգորիթմը կանոնների մաթեմատիկական շարք է, որը սահմանում է, թե ինչպես է տվյալների խումբը հավաքագրվում, պահվում, շրջանառվում, վերլուծվում և այլն: Սոցիալական ցանցերում ալգորիթմներն օգնում են կարգուկանոն պահպանել և օգնում են դասակարգել որոնման արդյունքները և գովազդները: Օրինակ, Ֆեյսբուկում կա մի ալգորիթմ, որն ուղղորդում է էջերն ու բովանդակությունը, որոնք ցուցադրվում են որոշակի հերթականությամբ: Ալգորիթմ է նաև այն, որ դուք ավելի հաճախ եք տեսնում ձեր ընկերներից մեկի գրառումը, իսկ մյուսներինը՝ առհասարակ ոչ, կամ, երբ Գուգլում իրականացնում եք որոշակի որոնում, այնուհետև, սոցիալական մեդիայում տեսնում գովազդ՝ որոնման և դրա արդյունքների վերաբերյալ:

«Վուդու» տիկնիկը կամ «Խամաճիկ»-ը՝ համացանցային աշխարհում.

Մենք չենք պատկերացնում մեր կյանքն առանց համացանցի և սոցիալական մեդիայի: Ամեն օր համացանց է վերբեռնվում միլիարդավոր գրառումներ՝ տեքստային, ֆոտո և վիդեո ձևաչափի նյութեր, աշխարհագրական դիրքի վերաբերյալ նշումներ, անձնական, ընտանեկան և գործնական ձեռքբերումների մասին տեղեկություններ: Զուգահեռ այս ամենին մենք դիտում և հավանում ենք համացանցում հրապարակված հազարավոր բովանդակություններ: Մեկ մարդն օրական կտրվածքով կարող է կատարել հարյուրավոր գրառումներ սոցիալական մեդիայի իր հաշիվներում իր կյանքին վերաբերող իրադարձությունների, քաղաքական և այլ համատեքստերում: Զուգահեռ, նույն մարդը կարող է ընթերցել իր ընկերների գրառումները, դիտել լուսանկարներ, տեսանյութեր, ընթերցել հոդվածներ, շրջել սոցիալական մեդիայով և Յություբով, որոնումներ կատարել դիտարկիչներում (browser): Այս գործողությունների արդյունքում տվյալ անձի վերաբերյալ հավաքագրվում է բազմաթիվ տեղեկատվություն իր նախընտրությունների, հետաքրքրությունների, համացանցում օգտագործած ժամանակի, ուժեղ և թույլ կողմերի, հոգեբանական խոցելի կողմերի, հույզերի տիրապետման վերաբերյալ: Հավաքագրված ողջ տեղեկատվությունը վերլուծվում է ալգորիթմների միջոցով, որոնք ստեղծում են անհատի առցանց կերպարը, որին հաճախ անվանում են «Վուդու» տիկնիկ կամ «Խամաճիկ»: Հավաքագրված և վերլուծված տեղեկատվությունն օգնում է սոցիալական մեդիային հասկանալ մարդուն և ունենալ տվյալ անհատի նախատիպը (prototype): Նախատիպի ստեղծումը թույլ է տալիս հիմնվել մարդու հետաքրքրությունների, հույզերի և արժեքների հիման վրա առաջարկել անհրաժեշտ տեղեկատվություն և մշտապես պահել կախված վիճակում:

Կախվածությունն առաջանում է, երբ անհատի հետաքրքրությունները բավարարող բովանդակությունները հաջորդում են մեկը մյուսին՝ կտրելով մարդուն իրականությունից և թույլ չտալով հեռանալ իրականությունից: Զուգահեռ այս ամենին, համացանցում իրացվում է գովազդը, և այն ակտիվորեն սպառվում օգտատերերի կողմից: Մենք ինքներս մեզ պետք է հարց տանք. ինչո՞ւ են սոցիալական ցանցերը մեզ համար անվճար, մատչելի և հասանելի: Չէ՞ որ այդ համակարգերի ստեղծման և պահպանման վրա ծախսվում են միլիոնավոր և միլիարդավոր դոլարներ, մարդկային հսկայական ռեսուրսներ և անգնահատելի ժամանակ: Պատասխանն ակնհայտ է: Այս ամենի միջոցով ցանցերը կարողանում են կառավարել անհատին, մինչդեռ անհատը մտածում է, որ ինքն է կառավարում իր ժամանակը և բովանդակությունը, որը ստանում է ու վերլուծում:

Սոցիալական մեդիաների ալգորիթմներ.

Տիկ-Տոկ. մեր օրերում անկանոն իմաստով ամենաբարդ ալգորիթմն ունի Տիկ-Տոկը: Եթե սոցիալական մեդիայի մյուս հարթակներում ձեր նորությունների ժապավենում հիմնականում հայտնվում է այն, ինչը դուք հավանել եք նախապես, ձեր ընկերների գրառումները և նրանց ռեակցիաներն այլ գրառումներին, ապա Տիկ-Տոկում դա այդպես չէ: Այն օգտատերերին կարող է առաջարկել ցանկացած տեսանյութ և միշտ չէ, որ դրանց ընտրությունը պայմանավորված է օգտատիրոջ հետաքրքրություններով: Սոցիալական մեդիայում նորությունների ժապավենում հայտնվող տեղեկատվությունը ֆիլտրացնելու հիմնական ալգորիթմն օգտատիրոջ հետաքրքրություններն են: Օրինակ, եթե դուք դիտում եք գրառումներ, լուսանկարներ և տեսանյութեր կենդանիների՝

շների և կատուների մասնակցությամբ, ապա ալգորիթմն աշխատում է ձեր օգտին՝ ֆիլտրացնելով և ձեզ բերելով համապատասխան բովանդակություն: Տիկ-Տոկում սա ևս աշխատում է, սակայն բացի դրանից, այն կարող է ձեզ առաջարկել տեսանյութեր, որոնք բացարձակ կապ չունեն ձեր հետաքրքրությունների, որոնումների պատմության հետ: Տիկ-Տոկի «rec»-ը՝ բոլորին հայտնի գործընթաց է, երբ հրապարակված տեսանյութն ունենում է հազարավոր և միլիոնավոր դիտումներ, անգամ եթե դուք չունեք հետևորդներ (followers): Սա մի ալգորիթմ է, որը միշտ չէ, որ հաշվարկելի և կանխատեսելի է օգտատերերի կողմից:

Տիկ-Տոկն ի սկզբանե թույլ էր տալիս բեռնել մինչև մեկ րոպե տևողությամբ տեսանյութեր, այժմ այդ սահմանափակումն ընդլայնվել է, և այն թույլ է տալիս բեռնել մինչև հինգ րոպե տևողությամբ տեսանյութեր: Հարթակում հաջողության հասնելու համար հարկավոր է ինտենսիվորեն և ամենօրյա ռեժիմով ուշադրություն դարձնել և բեռնել տեսանյութեր: Տիկ-Տոկի հիմնական հաջողությունը կայանում է կարճ և միաժամանակ ինտերակտիվ տեսանյութերի մեջ: Շատերն այն անգամ օգտագործում են մասնագիտական առաջխաղացման համար և աշխատանքային նպատակներով: Օրինակ, հոգեբանները կիսվում են խորհուրդներով, Լրատվականները ներկայացնում են կարճ նորություններ և այլն: Հարկ է նշել, որ Տիկ-Տոկում հաջողված պատմություններ կան նաև առանց որևէ լեզվի և բանավոր խոսքի կիրառման տեսանյութերի շրջանում, և պարտադիր չէ լսարանին ներկայացնել բովանդակություն, որտեղ կլինի խոսք: Տիկ-Տոկի գործիքներից է համարվում նաև տեսանյութի հետ ընտրվող թրենդային երաժշտությունը և հեշթեգերը, որոնք կարող են խթանել բովանդակության առավել լայն տարածմանը:

Ինստագրամ. այս հարթակն ի սկզբանե կիրառվել է լուսանկարների և սթորիների համար, սակայն Տիկ-Տոկի ազդեցության ներքո այն ստեղծեց նաև «Instagram reels» գործիքը, որը նախատեսված է կարճ տեսանյութերի համար և ապահովում է մեծ տեսանելիություն: Այս հարթակում տեքստային գրառումները տեսանելի չեն, և այն առաջնահերթություն չի տալիս տեքստերին, սակայն օգտատերերը ժամանակի ընթացքում գտել են լուծումը՝ տեքստերը վերածելով վիզուալ նյութերի և պաստառների պատրաստման և հրապարակման միջոցով լսարանին են հասցնում տեքստային բովանդակությունը: Այստեղ ևս տեսանյութերի հետ ուղեկցվող երաժշտությունը և հրապարակվող բովանդակությունների հետ կիրառվող հեշթեգերը խթանում են բովանդակության առաջխաղացմանը:

Փինթերեսթ. այս հարթակը նախատեսված է միայն լուսանկարների և վիզուալիզացված տեքստերով նկարների համար: Այստեղ կարելի է ֆիլտրացնել և տեսնել լուսանկարներ ամենատարբեր թեմաներին և ոլորտներին առնչվող, օրինակ, կրթության, բնության, կենդանիների, ֆիզիկայի, ճարտարապետության, լեզուների և այլնի վերաբերյալ: Երբ օգտատերը որոնում և ֆիլտրացնում է որևէ բնույթի բովանդակություն, Փինթերեսթն առաջարկում է նույնաբովանդակ բազմաթիվ այլ նյութեր՝ բեռնված աշխարհի ամենատարբեր ծայրերից:

Ֆեյսբուք. հարթակն ի սկզբանե ստեղծվել է անձնական հաշվի կիրառման, ընտանեկան և ընկերական շրջանակների ձևավորման նպատակներով: Ավելի ուշ Ֆեյսբուկը ստեղծել և առաջխաղացրել է բազմաթիվ գործիքներ, որոնք սահմանված չեն եղել հարթակի

առաքելությունում և նպատակներում: Այժմ Ֆեյսբուկը համարվում է ոչ միայն անձնական, ընտանեկան և ընկերական շրջանակի համար նախատեսված միջավայր, այլ կիրառվում է մեդիաների կողմից լուրերի շրջանառման, մասնավոր սեկտորի կողմից բիզնեսի առաջխաղացման, ուղիղ եթերների, միջոցառումների պլանավորման և ստեղծման, միջոցների և ռեսուրսների հայթայթման, քրաուդֆանդինգի և ֆանդրեյզինգի, նախաձեռնությունների, արշավների կազմակերպման, հասարակական ոլորտում գործունեությունը հանրայնացնելու, անգամ պետական կառավարման մակարդակում հանրության հետ հաղորդակցությունը վարելու և բազմաթիվ այլ նպատակների համար: Ժամանակին համընթաց Ֆեյսբուկը ստեղծել է նաև Տիկ-Տոկի և Ինստագրամի կարճ տեսանյութերի բեռնման և շրջանառման գործիքը:

Հարկ է նշել, որ այս հարթակը պատկանում է «Meta» ընկերությանը, որն ավելի վաղ ձեռք է բերել Ինստագրամ և Վոթսափ հարթակները: Ֆեյսբուկի մերօրյա ամենամեծ մարտահրավերն այժմ ավելի անձնականացված և փակ (private) ռեժիմի վերադառնալն է: Այլ կերպ ասած, Ֆեյսբուկը փորձում է վերադառնալ արմատներին՝ սահմանափակելով գովազդը, օգտատերերի համար ստեղծելով գաղտնիության և անվտանգության համար առավել արդյունավետ գործիքներ, պայքարելով ատելության խոսքի, բոտերի, վիրուսների, կեղծ հաշիվների դեմ:

Ֆեյսբուկի ամենամեծ նախաձեռնություններից մեկն ուղղված է վիրտուալ իրականության ստեղծմանը և հեռահաղորդակցության ոլորտում հեղաշրջում մտցնելուն: Այժմ ընկերության աշխատակիցներն աշխատում

են հարթակի միջոցով տեսազանգերի կատարելագործմանը՝ վիրտուալ ակնոցների, ձեռնոցների և հագուստի միջոցով այն իրականությանը մոտ դարձնելուն:

Ֆեյսբուկը ստեղծել է հավելյալ գործիքներ, որոնք նպաստում են հաշիվների, էջերի և խմբերի կառավարմանը, գովազդ մշակելուն և դրանց առաջխաղացմանը: Այդ գործիքներից է՝ «Creator Studio»-ն որը միավորում է Ֆեյսբուկն ու Ինստագրամը և համարվում է հարթակների կառավարման, բովանդակության վերլուծության միասնական հարթակ:
Ֆեյսբուկի կողմից է ստեղծվել նաև «Messenger»-ը, որն իրենից ենթադրում է հաղորդակցության գործիք, որտեղ կարելի է շփվել ֆեյսբուկյան ընկերների հետ, ստեղծել չատեր, տեսազանգի սրահներ, գաղտնի և ինքնամաքրվող չատեր և այլն:

Թվիթեր. այս հարթակն առավել կիրառվում է կարճ գրառումների, լուսանկարների և տեսանյութերի համար: Այժմ հարթակը թույլ չի տալիս կատարել գրառումներ, որոնք գերազանցում են 280 նիշի սահմանները: Սրանով այն ավելի արագ է դարձնում տեղեկատվական հոսքերը՝ սահմանափակելով ավելորդ և երկար բովանդակությունների շրջանառումը: Այն նման է Տիկ-Տոկի, որտեղ կիրառվում են միայն կարճ տեսանյութեր, սակայն այս դեպքում՝ տեքստեր: Թվիթերում ակտիվ կիրառելի են հեշթեգերը, և դրանք մեծ նշանակություն ունեն բովանդակության ֆիլտրացման և որոնման հարցում: Թվիթերը համարվում է նաև քաղաքական պաշտոն զբաղեցնող անձանց համար պաշտոնական էջ վարելու միջավայր: Այդուհանդերձ, այստեղ իրենց պաշտոնական էջերն են վարում նաև բազմաթիվ մեդիա

կազմակերպություններ, SS ընկերություններ և այլ ուղղություններով գործունեություն իրականացնող կառույցներ և անհատներ:

Լինկդին. այն համարվում է «B2B» հարթակ, նախատեսված է աշխատանքային գործունեություն իրականացնելու համար: Հարթակի նպատակն է մասնագիտական ուղղություններով ցանցեր ստեղծելն ու ցանցերում սեփական պորտֆոլիոն վարելը: Այստեղ օգտատերերը կարող են կիսվել իրենց կենսագրական տվյալներով՝ կրթության, աշխատանքի և զբաղվածության վերաբերյալ մանրամասներով՝ կազմելով սեփական ինքնակենսագրականը և ռեզյումեն: Այստեղ ամենուր կարելի է փնտրել և գտնել աշխատանքի մասին հայտարարություններ, մասնագիտական տարբեր ուղղություններով հետաքրքիր, կրթական բովանդակություններ: Այստեղ դուք կարող եք ստանալ նամակներ անծանոթ մարդկանցից, ովքեր կարող են լինել ընկերությունների ղեկավարներ, ՄՌԿ մասնագետներ, որոնք, տեսնելով ձեր ռեզյումեն, ձեզ կառաջարկեն աշխատանք:

Հեղինակային իրավունքը սոցիալական մեդիայում.
Հեղինակային իրավունքի վերաբերյալ հարցերը Հայաստանում կարգավորվում են «Հեղինակային իրավունքի և հարակից իրավունքների մասին» ՀՀ օրենքով:

Շարժվենք բացառման սկզբունքով և սկսենք նրանից, թե որ ստեղծագործությունները չեն համարվում հեղինակային իրավունքի օբյեկտ.

- ժողովրդական բանահյուսության և արվեստի ստեղծագործությունները,

- օրվա նորությունների կամ ընթացիկ իրադարձությունների և փաստերի մասին տեղեկատվությունը,
- պաշտոնական փաստաթղթերը՝ իրավական ակտերը, պայմանագրերը և դրանց պաշտոնական թարգմանությունները,
- պաշտոնական խորհրդանիշերն ու նշանները (դրոշներ, զինանշաններ, շքանշաններ, դրամանիշներ),
- քաղաքական ելույթները, դատավարության ընթացքում արտասանված ճառերը,
- առանց մարդու ստեղծագործական գործունեության՝ տեխնիկական միջոցների օգնությամբ ստացված արդյունքները,
- հեղինակային իրավունքը չի տարածվում գիտական հայտնագործությունների, գաղափարների, սկզբունքների, մեթոդների, ընթացակարգերի, տեսակետների, համակարգերի, արարողակարգերի, գիտական տեսությունների, մաթեմատիկական բանաձևերի, վիճակագրական դիագրամների, խաղի կանոնների վրա, եթե անգամ դրանք արտահայտված, նկարագրված, բացահայտված, լուսաբանված են ստեղծագործություններում:

Ելնելով բացառություններից՝ կարելի է ասել, որ մնացյալ ամեն ինչը համարվում է հեղինակային իրավունքի օբյեկտ: Եկե՛ք այդ մեծ «բազմությունն» անվանենք՝ «ստեղծագործություն»:

Օրենքն ասում է, որ հեղինակ է ճանաչվում այն ֆիզիկական անձը, ով ստեղծել է ստեղծագործությունը:

Այժմ դիտարկենք հեղինակային իրավունքը սոցիալական մեդիայի համատեքստում:

Սոցիալական մեդիայի բազմաթիվ հարթակներ օգտատերերին ընձեռում են սեփական լսարանի ընտրության և ֆիլտրացիայի մի շարք գործիքներ: Օրինակ, Ֆեյսբուկում որևէ գրառում անելիս այն թույլ է տալիս ընտրել հասանելիությունը լսարանին, մասնավորապես՝ հանրային հասանելի, հասանելի ընկերներին և ընկերների ընկերներին, հասանելի միայն ընկերներին, հասանելի միայն ընկերներից ընտրված ցանկին, հասանելի ընկերներին, բացառությամբ ընտրված ցանկի, հասանելի միայն հրապարակողին:

Այս և նմանօրինակ գործիքներն առնչություն ունեն և՛ անձնական տվյալների պաշտպանության հետ, և՛ հեղինակային իրավունքի հետ: Հարկ է նշել, որ այդուհանդերձ, եթե օգտատերը հանրային եղանակով գրառում է կատարում և գրառման տեքստում չի հիշատակում հեղինակային իրավունքով պաշտպանված լինելու մասին, ապա այստեղ դադարում են գործել մեխանիզմները, և հարցն անցնում է էթիկայի դաշտ, այսինքն, դաշտ, որտեղ մարդիկ են իրենց խղճի, վարվեցողության, ցանցային էթիկայի կանոնների հիման վրա որոշում կայացնում՝ ինչպես տարածել տեղեկատվությունը: Նույնը վերաբերում է լուսանկարներին, տեսանյութերին և ստեղծագործական ու մուլտիմեդիա այլ արտադրանքներին:

Հեղինակը նաև ազատ է նշելու, որ գրառումը, հրապարակումը կամ ստեղծված բովանդակությունը կարող է տարածվել ցանցում երեք հիմնական եղանակով՝

- կարող է տարածվել՝ հղում տալով հեղինակին,
- կարող է արգելվել հրապարակման տարածումն առհասարակ՝ պաշտպանելով այն հեղինակային իրավունքով,

- կարող է հրապարակվել ազատ տարածման իրավունքի շնորհմամբ:

Ընդ որում, հարկ է նշել, որ հեղինակը կարող է արգելել ստեղծագործության ոչ միայն տարածումը, այլ դրա հետ առնչվող ցանկացած գործողություն՝ մշակում, արտահանում, ներմուծում, խմբագրում, նմանակում, տպում, վերատպում, ցուցադրում, հանրային ցուցադրում, ձայնագրում, թարգմանում և այլն:

Ստեղծագործության նկատմամբ հեղինակային իրավունքը ծագում է ստեղծագործության ստեղծման փաստով և կախված չէ այդ իրավունքի պաշտոնական հաստատագրումից, ստեղծագործության գրանցումից և որևէ այլ ձևականության պահպանումից:

Հեղինակային իրավունքի իրավատերն իր հեղինակային իրավունքի մասին ծանուցելու նպատակով կարող է օգտագործել հեղինակային իրավունքի պահպանության նշանը, որը տեղադրվում է ստեղծագործության յուրաքանչյուր օրինակի վրա և կազմված է՝

- շրջանակի մեջ վերցված լատինական «C» տառից,
- հեղինակային իրավունքի իրավատիրոջ անունից,
- ստեղծագործության առաջին հրատարակության տարեթվից:

Իրավատեր է համարվում հեղինակային իրավունքի պահպանության նշանում հիշատակված անձը, եթե այլ բան ապացուցված չէ:

Անանուն կամ կեղծանունով լույս ընծայված ստեղծագործության (բացառությամբ դեպքերի, երբ կեղծանունով հանդես եկող հեղինակի

անձը կասկած չի հարուցում) հրատարակիչը, որի անունը կամ անվանումը նշված է ստեղծագործության վրա, այլ ապացույցների բացակայության դեպքում համարվում է հեղինակի ներկայացուցիչ, որն իրավունք ունի պաշտպանել հեղինակի իրավունքները և ապահովել դրանց իրականացումը: Այս դրույթն ամրագրված է հեղինակային իրավունքի մասին օրենքով և գործում է այնքան ժամանակ, մինչև նման ստեղծագործության հեղինակը կբացահայտի իր անձը և կհայտարարի իր հեղինակության մասին:

Հետաքրքրական է, որ հեղինակի գույքային իրավունքները փոխանցվում են ժառանգաբար: Օրենքն ասում է, որ հեղինակի գույքային իրավունքները գործում են հեղինակի ամբողջ կյանքի ընթացքում և նրա մահից հետո 50 տարի՝ հաշված հեղինակի մահվանը հաջորդող տարվա հունվարի 1-ից:

Այդուհանդերձ, նշենք, հեղինակի տվյալ ստեղծագործության հեղինակը լինելու հանգամանքը հարատև է ու անժամկետ և հեղինակը լինելու մասին վկայությունն առնչություն չունի հեղինակային իրավունքի հետ:

Ցանցային էթիկետ կամ նեթիկետ.

Ինչպես իրական կյանքում, այնպես էլ առցանց կյանքում և տիրույթում կան գրված և չգրված կանոններ: Հաղորդակցվելիս շատ կարևոր է պահպանել այդ կանոնները, որոնք կոչվում են էթիկայի կանոններ, իսկ համացանցում՝ ցանցային էթիկա (network ethics, այստեղից էլ՝ նեթիկետ) կամ ցանցային վարվեցողության կանոններ:

Փորձագետների կողմից մշակվել է ցանցային էթիկայի 10 կանոն, որոնք թվարկված են ստորև.

- 1-ին կանոն. Հիշե՛ք, որ դուք մարդու հետ եք խոսում:
- 2-րդ կանոն. Հետևե՛ք վարվեցողության ճիշտ նույն կանոններին, ինչ իրական կյանքում:
- 3-րդ կանոն. Հիշե՛ք, թե կիբերտարածության որ մասում եք գտնվում: Նեթիկետը փոխվում է համակարգչից համակարգիչ:
- 4-րդ կանոն. Հարգե՛ք դիմացինի ժամանակն ու հնարավորությունները:
- 5-րդ կանոն. Պահե՛ք սեփական դեմքը, արժանապատվությունը:
- 6-րդ կանոն. Եթե կարող եք, ապա օգնե՛ք ուրիշներին:
- 7-րդ կանոն. Մի՛ մտեք կոնֆլիկտի մեջ:
- 8-րդ կանոն. Հարգե՛ք դիմացինի անձնական հաղորդակցման իրավունքը:
- 9-րդ կանոն. Ձեր հնարավորությունները մի՛ չարաշահեք:
- 10-րդ կանոն. Սովորե՛ք ներել ուրիշների սխալները:

Որոնողական համակարգեր.

Որոնողական համակարգերից հիմնական օգտագործվող գործիքը «Google»-ն է շատ պարզ պատճառով. այս համակարգն ունի տվյալների ամենամեծ շտեմարանը համացանցի մասին: Բայց պետք է հաշվի առնել, որ ոչ մի որոնողական համակարգ չունի ամբողջական տվյալներ ողջ համացանցի բոլոր էջերի մասին: Այդ պատճառով, խորացված որոնումների ժամանակ գերադասելի է օգտվել նաև այլընտրանքային որոնողական մեքենաներից, քանի որ ինչ-որ տվյալներ կարող են չլինել «Գուգլ»-ում, բայց կգտնվեն մեկ այլ համակարգում: Ռուսալեզու, իսկ ավելի ճիշտ, կյուրեղատառ էջերի որոնման համար կարելի է կիրառել «Yandex» համակարգը, քանի որ շատ հարցերում այն ավելի լավ է հասկանում

ռուսերենը: Նաև թուրքերեն որոնումների ժամանակ է կիրառելի «Յանդեքս»-ը: Այս կազմակերպությունն առանձին աշխատում է թուրքական լսարանի ուղղությամբ և նույնիսկ ունի հատուկ թուրքերեն տարբերակ: Մեկ ուրիշ այլընտրանք է նաև «Bing.com»-ը: Եթե անսպասելի պետք լինի չինական հատվածի որոնում, ապա կարելի է օգտվել նաև Չինաստանի «Գուգլ»-ից՝ «Baidu.com»-ից:

Որոնողական մեքենաներն ունենում են լրացուցիչ գործիքներ, որոնցից սովորաբար մարդիկ ոչ միայն չեն օգտվում, այլև նույնիսկ տեղյակ չեն դրանց մասին: Իսկ հետաքննական լրագրության, փաստերի ստուգման համար հենց այդ գործիքներն են կարևոր:

«Գուգլ»-ն ունի լրացուցիչ որոնողական օպերատորներ, որոնք թույլ են տալիս ցանցի զննումը նեղացնել մինչև մեկ կայքի սահմաններում, հեռացնել «բանալի» բառերը, գտնել ուզած ձևաչափի ֆայլեր և այլն:

Օգտակար օպերատորները.

·site:example.com - որոնում որոշակի կայքում,

·filetype:pdf - հստակ տեսակի ֆայլերի որոնում, օրինակ՝ pdf, doc, ppt, txt,

·-բառ - բառի վերացում որոնումից,

·"հստակ արտահայտության որոնում",

·cache:example.com - «Գուգլ»-ում էջի պահպանված տարբերակի դիտարկում:

Բացի դրանից, համակարգն ունի լրացուցիչ գործիքակազմ, որը հասանելի է «Tools» կոճակի միջոցով: Այստեղ կարելի է հրահանգել

ցուցադրել նյութեր միայն տրված ժամանակահատվածից, ընտրել կոնկրետ չափսի լուսանկարներ, հստակ տևողության տեսանյութեր և այլն:

«Yandex»-ն ունի խորացված որոնման համակարգ, որը նույնպես թույլ է տալիս փնտրել հստակ արտահայտություն, գտնել էջի ջնջված կամ հին տարբերակը և այլն:

Հաճախ անհրաժեշտ է լինում փնտրել ու գտնել հրապարակված նյութի նախնական տարբերակը, քանի որ այն, օրինակ, ձևափոխվել է, վերացվել կամ կորսվել է կարևոր տեղեկատվություն: Կամ հնարավոր է՝ էջը ջնջվել է, մեկ այլ պատճառով էլ՝ տվյալ պահին անհասանելի է: Նման դեպքերում այս տեղեկատվությունը հասանելի է դառնում որոնողական համակարգերի միջոցով, քանի որ դրանք հաճախ պահպանում են էջն իր նախնական տեսքով: Որոնողական համակարգում պահպանված էջը կոչվում է քեշ: Քեշերը վերականգնելու համար Գուգլում կիրառվում է «cache»: օպերատորը ամեն մի հղման համար:

Գուգլում քեշերից հանած էջը պարունակում է այն օրը, ժամն ու րոպեն, երբ համակարգն իր մոտ ֆիքսել է տվյալ էջը: Պետք է հաշվի առնել, որ համակարգը ներկայացնում է ժամանակն ըստ «GMT», այսինքն՝ Լոնդոնի ժամանակով: Երևանի ժամանակին անցնելու համար հարկավոր է հաշվի առնել ամառային և ձմեռային ժամանակների փոփոխությունները, ինչի համար կարելի է օգտվել http://www.timebie.com/std/gmt.php ժամանակի կոնվերտորից:

Միշտ չէ, որ սա աշխատող տարբերակ է: Լինում են դեպքեր, երբ որոնողական համակարգը չի հասցնում պահպանել քեշը կամ, հակառակը, փոփոխութունից հետո վերանայում է էջը, և քեշում պահպանվում է արդեն վերջին տարբերակը, որն առանց այդ էլ հասանելի է ցանցում: Այդ պատճառով, հարկավոր է փնտրել քեշերը միանգամից մի քանի համակարգերում, օրինակ՝ «Google», «Bing», «Yandex»:

Պետք է հաշվի առնել, որ ջնջված հին էջերի քեշը հաճախ վերացվում է նաև որոնողական համակարգերից: Այդ դեպքում օգտվում ենք այլընտրանքային աղբյուրներից: Օրինակ, կան կայքեր, որոնք պահպանում, իրենց մոտ արխիվացնում են համացանցը: Այնպես որ, ջնջված, նույնիսկ քեշերից վաղուց վերացված էջերը հնարավոր է, որ գտնվեն համացանցային արխիվում՝ https://archive.org/web/ :

Բաց աղբյուրներ և բաց տվյալների շտեմարաններ.
Համացանցում կան բազմաթիվ բաց աղբյուրներ և բաց տվյալների շտեմարաններ: Բաց աղբյուրները և տվյալների շտեմարանները հարթակներ են, որոնք իրենց մեջ պարունակում են տվյալների բազաներ և մատչելի են հասարակության համար:

Հայաստանում այդպիսի աղբյուրներն ու շտեմարանները շատ են: Դրանից մի քանիսը թվարկված են ստորև:

Կենտրոնական ընտրական հանձնաժողով, ընտրողների ռեգիստր: Այստեղ հասանելի են 18 տարին լրացած և ընտրելու իրավունք ունեցող քաղաքացիների վերաբերյալ տեղեկությունները, մասնավորապես, անուն, ազգանուն, ծննդյան տարեթիվ, գրանցման հասցե և նույն հասցեում

գրանցված քաղաքացիների տվյալները - https://www.elections.am/ :
Դատական տեղեկատվական համակարգում հնարավոր է որոնել դատական գործեր, տեսնել նիստերի ժամանակացույցը, ծանոթանալ վճռաբեկ դատարանի նախադեպային որոշումներին, իրականացնել Մարդու իրավունքների եվրոպական դատարանի կողմից կայացված որոշումների և գործերի ընթացքի որոնումներ - http://datalex.am/ :

Արդարադատության նախարարության իրավաբանական անձանց պետական ռեգիստրը նախատեսված է Հայաստանի Հանրապետությունում և Լեռնային Ղարաբաղի Հանրապետությունում գրանցված իրավաբանական անձանց վերաբերյալ տեղեկությունների որոնման համար: Լեռնային Ղարաբաղի Հանրապետությունում գրանցված իրավաբանական անձանց վերաբերյալ տեղեկատվության համար Հայաստանի Հանրապետության արդարադատության նախարարության իրավաբանական անձանց պետական ռեգիստրի գործակալությունը պատասխանատվություն չի կրում- https://www.e-register.am/am/search :

Հայաստանի Հանրապետության Կադաստրի կոմիտեի էլեկտրոնային կառավարման համակարգ - https://www.e-cadastre.am/ :

ARMEPS էլեկտրոնային գնումների առցանց համակարգը նախատեսված է թափանցիկ և արդյունավետ գնումների գործընթացների կազմակերպման և իրականացման համար - https://armeps.am :

Հայաստանի Հանրապետության Կադաստրի կոմիտեի գրադարան - https://www.cadastre.am/ :

ՀՀ Ֆինանսների նախարարության գնումների համակարգը նախատեսված է գնումների մասին հայտարարությունների, գնումների մասին միասնական անվանացանկի ստուգման, էլեկտրոնային աճուրդի միջոցով ձեռքբերվող գնման առարկաների թվային ծածկագրերի ստուգման, գնումների բողոքարկման խորհրդի նիստերի առցանց հեռարձակման, գնումների գործընթացին մասնակցելու իրավունք չունեցող մասնակիցների ցուցակի, ԵԱՏՄ երկրների գնումների գործընթացին մասնակցելու իրավունք չունեցող մասնակիցների ցուցակի ուսումնասիրության և ԵԱՏՄ անդամ-պետությունների արդյունաբերական ապրանքների եվրասիական ռեեստրի հասանելիություն ունենալու համար - https://gnumner.am/ :

Իրավական ակտերի միասնական համակարգը ՀՀ Սահմանադրության, օրենքների և ենթաօրենսդրական ակտերի, կառավարության, ԱԺ և տեղական մակարդակում կայացված որոշումների համակարգ է, որտեղ կարելի է տեսնել գործող բոլոր օրենքներն ու որոշումները, ինչպես նաև դրանց փոփոխությունները - https://www.arlis.am/ :

Գով էյէմ-ը կառավարության որոշումների և նախագծերի միասնական հարթակ է - https://www.e-gov.am/ :

Ի-դրաֆթ-ն իրավական ակտերի նախագծերի միասնական հարթակ է, որտեղ քաղաքացիները կարող են ծանոթանալ նախագծերին և կատարել առաջարկություններ բարելավումների և փոփոխությունների համար - https://www.e-draft.am/ :

Տնտեսական գործունեության տեսակների դասակարգիչ - https://www.petekamutner.am/tsOS_EAClassifier.aspx :

Հարկ վճարողների փնտրման համակարգ - https://www.petekamutner.am/tsOS_Taxpayers.aspx :

Հայաստանի Հանրապետության Վիճակագրական կոմիտե - https://armstat.am/am/ :

Հայտարարագրերի ռեեստր - http://cpcarmenia.am/hy/declarations-registry/ :

Պաշտոնական հայտարարություններ - https://www.azdarar.am/ :

Բաց աղբյուրների և տվյալների շտեմարանների ցանկն այսքանով չի սահմանափակվում, և դրանք գտնելու համար հարկավոր է խորացված որոնում իրականացնել Գուգլի դիտարկչում:

ՄԱՍ 2.
ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԵՐՆ ՈՒ ԴՐԱՆՑ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ

Բազմաթիվ փորձագետների և օգտատերերի նպատակն է համացանցը դարձնել անվտանգ, սակայն մեր օրերում դա անհնար է:

Տարեցտարի ավելանում է վնասակար ծրագրերի քանակը, անընդհատ նոր մեթոդներ են ստեղծվում շրջանցելու համար հակավիրուսային համակարգերի արգելքներն ու պաշտպանական մեխանիզմները: Այս ամենը ստիպում են օգտատերերին նոր լուծումներ փնտրել պաշտպանելու համար իրենց համակարգչի անվտանգությունը:

Անվտանգության ապահովման համար դուք կարող եք կամ օգտագործել օպերացիոն համակարգերի հնարավորությունները, կամ էլ տեղադրել հատուկ ծրագրեր, որոնց միջոցով կարող եք ապահովել հակավիրուսային և այլ պաշտպանություն ձեր համակարգչի համար:

Մասնագետներն այս հարցում միակարծիք չեն. փորձագետների մի մասը կարծում է, որ առավել հուսալի է ոչ թե պաշտպանել խոցելի կետերը, այլ ուղղակի անջատել (փակել) դրանք: Նրանք խորհուրդ են տալիս օգտագործել օպերացիոն համակարգի հնարավորությունները փակելու համար այս կամ այն «անցքը»: Մյուս մասը կարծում է, որ սա բավարար չէ լիարժեք պաշտպանության համար և առաջարկում են հակավիրուսային և արգելապատնեշ (firewall) հանդիսացող ծրագրեր:

Անվտանգության ծրագրային սպառնալիքներ.

Ներկայումս գոյություն չունի անվտանգության ծրագրային

սպառնալիքների միասնական և համընդհանուր դասակարգում: Սակայն առավել տարածված դասակարգման համաձայն՝ սպառնալիքները բաժանվում են երեք խմբի՝

1. Վնասակար ծրագրեր,
2. Վնասակար ցանցային տեխնոլոգիաներ,
3. Խոցելի գործառույթներ:

Վնասակար ծրագրեր.

Վնասակար ծրագրերն (malicious software, malware) այն բոլոր ծրագրերի միասնական անվանումն է, որոնց նպատակն է այս կամ այն կերպ վնասել վերջնական օգտագործողի համակարգիչը: Չնայած որոշ տարակարծություններին՝ փորձագետներն առանձնացնում են 5 հիմնական տարատեսակներ:

1.Trojan (trojan horse, «տրոյական ձիեր», «տրոյաններ») - վնասակար ծրագրերի այս տարատեսակը սկսել է առանձնացվել, երբ հայտնվեցին առաջին վիրուսները, որոնք, «դիմակավորվելով» որպես օգտակար ծրագիր, ստիպում են օգտատիրոջը բացել դրանք: Ներկայումս այս խմբին են դասվում տեղեկությունների գողության, ոչնչացման, փոփոխման ծրագրերը, առանձին համակարգիչների և ցանցերի աշխատանքը խաթարող տարբեր ծրագրեր: Այս ծրագրերի մեծ մասի գործունեությունն ուղղված է հասցված վնասից ֆինանսական օգուտ քաղելուն: Տրոյաններն հիմնականում առանձին ծրագրեր են, որոնք տարածվում են համացանցային «կոտրված» կայքերի, էլ. փոստի, ակնթարթային հաղորդակցման ծրագրերի և այլ միջոցներով: Ներկայումս տրոյանները կազմում են ծրագրային սպառնալիքների ամենամեծ խումբը: Տրոյանների մեջ են մտնում նաև այս երկու ենթախմբերը.

- Rootkit. համակարգչի օգտագործողից կամ հակավիրուսային ծրագրից թաքցնում կամ վերափոխում են ֆայլերը, պրոցեսները, ռեեստրի մասնիկները և այլն:
- Backdoor. վարակված համակարգչի հեռավար կառավարման ծրագիր, որն աշխատում է առանց օգտագործողի համաձայնության:

2. *Worm (որմ)* - այս տիպի վնասակար ծրագրերը նախ և առաջ առանձնանում են նրանով, որ ինքնաբազմանալու ունակություն ունեն, այսինքն ստեղծում և տարածում են իրենց կրկնօրինակները: Տարածման ավանդական ուղիներից բացի (էլեկտրոնային փոստ, ակնթարթային հաղորդակցման համակարգեր, ֆայլերի փոխանակման ցանցեր), որդերն իրենց կրկնօրինակները տարածում են ցանցային ռեսուրսների (ընդհանուր հասանելիությամբ թղթապանակների) և տեղեկույթի դյուրակիր կրիչների վրա: Որդը, որպես կանոն, նույնպես հանդես է գալիս որպես առանձին ծրագիր, բացառությամբ որոշ «անմարմին» տեսակների, որոնք հանդես են գալիս ցանցային փաթեթների տեսքով: Այս ծրագրերի գործունեության դաշտն ավելի նեղ է, քան տրոյաններինը և հիմնականում ուղղված է տեղեկության ոչնչացմանը, օպերացիոն համակարգի ռեեստրի անսարքությանը, որոշ ծրագրերի աշխատանքի խանգարմանը:

3. *Virus (վիրուս, դասական վիրուս)* - այս վնասակար ծրագրերն առաջացել են մյուսներից ավելի առաջ և սկիզբ են դրել «վիրուս» հասկացությանը: «Վիրուս» տերմինը ներկայումս լայնորեն կիրառվում է որպես բոլոր վնասակար ծրագրերին տրվող ընդհանուր անվանում: Դասական վիրուսը «վարակում» է կիրառական ֆայլերը՝ ծրագրային կոդի մեջ կատարելով այնպիսի փոփոխություն, որը թույլ է տալիս ապահովել իր սկիզբն ու աշխատանքը: Սովորաբար դասական վիրուսի

գործունեությունը սահմանափակվում է կոնկրետ մեկ օպերացիոն համակարգի շրջանակներում և տեղաշարժվելու համար անհրաժեշտ է մարդկային միջամտություն (վարակված ֆայլերի տեղափոխում էլ. փոստի կամ տեղեկույթի կրիչների միջոցով):

4. *Other malware (այլ վնասակար ծրագրեր)* - սովորաբար այս բաժնին են դասվում այն ծրագրերը, որոնք կամ չունեն երեք հիմնական խմբերից կոնկրետ որևէ մեկի բոլոր հատկանիշները, կամ էլ անմիջական վնաս չեն պատճառում համակարգչին, սակայն նպաստում են վնասակար ծրագրերի տարածմանը:

5. *Potentially unwanted software, riskware (անցանկալի ծրագրաշար)* - այս խմբին են դասվում պոտենցիալ վտանգ ներկայացնող ծրագրերը, որոնք տարբեր հակավիրուսային համակարգերի կողմից բնութագրվում են որպես անցանկալի, պոտենցիալ վտանգ ներկայացնող, պոտենցիալ անցանկալի և այլն: Սովորաբար այս խմբին են դասվում.

- Adware (գովազդային ծրագիր) - սրանց գործունեությունը սահմանափակվում է գովազդային բնույթի տեղեկատվության բեռնմամբ և ցուցադրմամբ:
- Spyware (լրտեսական ծրագիր) - օգտագործվում է անձնական տեղեկատվության հավաքման և պատվիրատուին փոխանցելու համար:
- Riskware (ռիսկային ծրագրեր) - օրինական ծրագրեր, որոնք, սակայն, կարող են օգտագործվել նաև որպես վնասակար ծրագրեր:

Վնասակար ծրագրերի տարածման ճանապարհներն են.

1. Էլեկտրոնային փոստ, ակնթարթային հաղորդակցման ծրագրեր, ֆայլերի փոխանակման համակարգեր. Վնասակար ծրագիրը կարող է տեղադրվել էլեկտրոնային նամակում, ինչպես նաև նամակի կամ հաղորդագրության օգնությամբ հնարավոր է ուղարկել վնասակար ծրագրին տանող հղում:

2. Վնասակար կամ կոտրված կայքեր. այս կայքերն ի սկզբանե ունեն վնասակար պարունակություն և կարող են վարակել համակարգիչը զննարկիչի պատուհանում այն բացելուն պես:

3. Տեղեկույթի կրիչներ (սկավառակներ, կամ դյուրակիր կրիչներ) դյուրակիր կրիչի միացման կամ սկավառակի գրման արդյունքում վնասակար ծրագիրը կարող է կրկնօրինակվել և հետագայում «վարակել» նաև «առողջ» համակարգիչը:

4. Ծրագրաշարերի հեղինակային հավաքածուներ, ոչ արտոնագրված ծրագրերի սկավառակներ. վնասակար ծրագրային կոդը կարող է տեղադրվել ծրագրային փաթեթում և խնամքով քողարկել որպես օգտակար ծրագրի:

5. Խոցելի ծրագրաշարի կամ օպերացիոն համակարգի խոցելի գործառույթների օգտագործում. մասնագիտական վերջին ուսումնասիրությունները ցույց են տվել, որ այն համակարգիչները, որոնք օգտագործում են «անպաշտպան» ծրագրեր, կամ չեն օգտվում պաշտպանության համակարգերից, (արգելապատնեշային (Firewall) և

հակավիրուսային ծրագրերից) կարող են վարակվել ընդամենը 5-10 րոպեի ընթացքում:

Վնասակար ցանցային տեխնոլոգիաներ.

Spam (փոստաղբ) ընդունված է դասակարգել որպես հաղորդագրությունների զանգվածային ուղարկում, որոնց հասցեատերերը ցանկություն կամ համաձայնություն չեն հայտնել ստանալու դրանք. այս հաղորդագրությունները սովորաբար ունենում են գովազդային կամ վնասատու բնույթ: Ներկայումս փոստաղբի տարածման համար լայնորեն կիրառվում են համացանցի հետևյալ գործիքները՝ էլեկտրոնային փոստ, ակնթարթային հաղորդակցման ծրագրեր, ֆորումներ և այլն:

Համացանցային խարդախություն այս տեխնոլոգիաներն ունեն տարբեր տարատեսակներ. Ֆինանսական բուրգերի ստեղծում, կեղծ հակավիրուսային ծրագրերի վաճառք, ֆիշինգ (phishing) և այլն: Ֆիշինգ ընդունված է անվանել այն գործունեությունը, որի նպատակը խաբեությամբ օգտագործողի անձնական տվյալների ստացումն է: Սովորաբար ֆիշինգն իրականացվում է այնպիսի կայքերի ստեղծման և շահագործման միջոցով, որոնք ճշտությամբ կրկնօրինակում են համացանցային խանութների, բանկերի, հոսթինգի վաճառքով զբաղվող և այլ կոմերցիոն գործունեություն ծավալող ընկերությունների կայքերը: Օգտագործողին ուղարկվում է փոստաղբ նամակ, որում պարունակվում է խնդրանք ծառայություն մատուցող ընկերությունից բացել հաշիվը և կատարել որոշակի գործողություններ: Նամակում պարունակվում է նաև հղում, որը սեղմելով՝ օգտագործողն ընկնում է կեղծ կայք: Եթե

ժամանակին չհասկանանք կեղծիքը և մուտքագրենք մեր տվյալները, չարամիտները հնարավորություն կստանան հավաքել անձնական տեղեկություններ, կատարել ֆինանսական գործարքներ, կոտրել անձնական էջեր և այլն:

Սովորաբար ֆիշինգային կայքերը տեղադրվում են այնպիսի դոմեյններում, որոնք շատ նման են իրական կայքերին:

Խոցելի գործառույթներ.

1. Ֆայլեր և թղթապանակներ առավել հաճախ վնասակար ծրագրերը հանգրվանում են հետևյալ հասցեներում

- Տրամաբանական սկավառակների արմատներում. C:\ և այլն:
- Օգտատերերի (User) թղթապանակներում. օրինակ՝ C:\Documents and settings Windows XP-ի համար:
- Օպերացիոն համակարգի թղթապանակում. C:\Windows:

Վարակի համար հիանալի հնարավորություն են ստեղծում ընդհանուր օգտագործման թղթապանակները (Shared folder), որոնք կիրառվում են միևնույն տեղային ցանցում միավորված մեկից ավելի համակարգիչների կողմից: Ցանցի համակարգիչներից մեկի վարակվելը բերում է բոլոր համակարգիչների վարակմանը:

2. Ռեեստր. սա օպերացիոն համակարգի ռեեստրային բազան է, որտեղ պահվում են համակարգչում առկա ծրագրերի պարամետրերն ու օպերացիոն համակարգի որոշ բաղադրիչներ:

3. Օպերացիոն համակարգի ցանցային գործառույթներ. ըստ էության՝ այս

ֆունկցիան ստեղծվել է համակարգիչների միջև կապ ապահովելու համար, սակայն միաժամանակ չարամիտներն այն օգտագործում են իրենց «արտադրանքի» տարածման նպատակով:

4. Զննարկիչ (browser). Ժամանակակից զննարկիչներն ունեն տեխնոլոգիական այնպիսի հնարավորություններ, որոնք համացանցում աշխատանքը հարմարավետ դարձնելուն զուգահեռ կարող են օգտագործվել վնասակար ծրագրերով համակարգիչը վարակելու համար.

- Սկրիպտներ, որոնք կարող են ինքնուրույն տեղադրել վնասակար ծրագրեր,
- Թաքնված վերանվանարկում,
- Զննարկիչների համար նախատեսված տարբեր լրացումներ, որոնք քողարկվելով օգտակար «դիմակ»-ով, տեղեկություններ են փոխանցում պատվիրատուին,
- Ակտիվ բաղադրիչներ, որոնք կարող են լինել նաև անօրինական և հնարավորություն տալ զննարկիչի միջոցով իրականացնել համակարգչի ֆայլերի կառավարում:

Օգտակար է իմանալ.

Հակավիրուսային ծրագրերը, կախված իրենց տեսակից, վնասակար ծրագիր հայտնաբերելու դեպքում կատարում են տարբեր գործողություններ: «Տրոյանները» և «Որդերը» ամբողջությամբ բաղկացած են վնասակար կոդից և որևէ օգտակար ինֆորմացիա չեն պարունակում, այդ իսկ պատճառով էլ դրանք ուղղակի ջնջվում են հակավիրուսի կողմից: Իսկ դասական վիրուսներն իրենց կոդով գտնվում են մյուս ֆայլերի մեջ և

հետևաբար դրանց նկատմամբ կիրառվում է «բուժում», այսինքն՝ ֆայլի կոդը մաքրվում է վիրուսային հատվածից: Անհրաժեշտ է նշել, որ «Տրոյանների» և «Որդերի» դեպքում հակավիրուսը ոչ միայն ջնջում է դրանք, այլև վերականգնում է օպերացիոն համակարգի ռեեստրն ու ֆայլային կառուցվածքը: Հակավիրուսների որոշ տեսակներ նաև այդ մասին հայտնում են օգտատիրոջը՝ օգտագործելով «cure» (բուժել) տերմինը: Մյուս տեսակները նշում են միայն ջնջման փաստի մասին, օգտագործում են «delete» (ջնջել) տերմինը՝ ինքնըստինքյան ենթադրելով նաև համակարգի վերականգնում: Սակայն այդ մասին տեղեկատվության բացակայությունը ստիպում է օգտատիրոջը ենթադրել, որ «իքս» հակավիրուսն ավելի լավն է, քան «իգրեկը», քանի որ այն ոչ միայն ջնջում է, այլև բուժում: Սակայն բոլոր հակավիրուսներն էլ պրակտիկորեն նույն գործողությունն են կատարում:

Խոսելով պաշտպանության մասին՝ մենք այն կդիտարկենք ըստ սպառնալիքների տեսակների: Ներկայումս սպառնալիքների յուրաքանչյուր խմբի համար առկա են հակազդեցության համարժեք միջոցներ:

Անվտանգության ծրագրային սպառնալիքները դասակարգվում են հետևյալ կերպ՝

Պաշտպանությունը վնասակար ծրագրերից

Հակավիրուսային ծրագրեր.

«Հակավիրուսային ծրագիր» հասկացությունը սահմանվում է որպես «Տրոյանների», «Որդերի», դասական վիրուսների և այլ վնասակար ծրագրերի հայտնաբերման և մշակման համակարգ: Որոշ հակավիրուսներ հայտնաբերում և աշխատում են նաև անցանկալի ծրագրերի հետ: Հակավիրուսային ծրագրերի կողմից կիրառվում է երկու հիմնական մեթոդ՝ վնասակար ծրագրերի հայտնաբերման համար:

Ռեակտիվ մեթոդ. այս մեթոդն իր անվանումը ստացել է «ռեակցիա» բառից: Այս մեթոդով հայտնաբերումը հնարավոր է այն դեպքում, երբ վնասակար ծրագրի կոնկրետ մի օրինակ ուսումնասիրվում է հակավիրուսային ծրագիր մշակող ընկերության լաբորատորիայում: Երբ մեր համակարգչում տեղադրած հակավիրուսային ծրագրի տվյալների բազան թարմացնում ենք, նոր վնասակար ծրագրի կոդի մասին ինֆորմացիան ևս ավելանում է այնտեղ: Ստուգման ժամանակ հակավիրուսային ծրագիրը համեմատում է համակարգչի ֆայլերն իր

տվյալների բազայի հետ: Համընկնման դեպքում ծրագիրը ճանաչվում է որպես վնասակար:

Այս մեթոդով աշխատող հակավիրուսային ծրագիր տեղադրելու դեպքում անհրաժեշտ է պարբերաբար թարմացնել (update) տվյալների բազան, որպեսզի մեր համակարգչում գործող հակավիրուսը կարողանա հայտնաբերել նորաստեղծ վնասակար ծրագրերը:

Պրոակտիվ մեթոդ. այս մեթոդով աշխատանքը թույլ է տալիս նկատել վնասակար ծրագիրը մինչև նրա ուսումնասիրումը ընկերության լաբորատորիայում և տվյալների բազայի թարմացումը: Այս մեթոդի ընթացքում հակավիրուսային ծրագիրն ուսումնասիրում է կասկածելի ծրագրի կոդը և, եթե այնտեղ նկատում է գործողություն, որը բնորոշ է վնասակար ծրագրերին, կամ, եթե կասկածելի ծրագիրն ունի չափազանց երկար անուն, ունի բազմակի կոդավորման համակարգ և այլն, այն ճանաչում է որպես վնասակար ծրագիր: Այս մեթոդի մեջ մտնում է նաև վարքի ուսումնասիրությունը. երբ հակավիրուսն ուսումնասիրում է այս կամ այն կոնկրետ ծրագրաշարի գործողությունները և իր կասկածների մասին տեղեկատվություն է տրամադրում օգտագործողին: Այս մեթոդն ունի ինչպես առավելություններ, այնպես էլ թերություններ: Առավելությունը ռեակտիվ մեթոդի համեմատ այն է, որ հնարավորություն է տալիս նկատել վնասակար ծրագիրը մինչև մշակող ընկերության կողմից տվյալների բազայի թարմացումը: Իսկ թերությունն այն է, որ, ի տարբերություն ռեակտիվ մեթոդի, վնասակար ծրագիրը հայտնաբերվում է այս կամ այն հավանականությամբ:

Անկախ հայտնաբերման մեթոդից՝ դուք միշտ կարող եք կասկածելի ֆայլն

ուղարկել մշակող ընկերություն, որտեղ այն մանրամասն կուսումնասիրեն և կպարզեն՝ արդյոք դա վնասակար ֆայլ է, թե ոչ: Հակավիրուսային ծրագրեր մշակող ընկերության կայքում դուք կարող եք պարզել, թե որ հասցեով է պետք ուղարկել կասկածելի ֆայլը:

Ցանկացած հակավիրուսային ծրագիր ներառում է մի քանի մոդուլներ. ֆայլային և փոստային մոնիտորինգ (վերջինս ստուգում է ֆայլերը դրանց բացելու պահին), ըստ պահանջի ստուգիչ, կարանտին և թարմացման ծառայություն:

Կախված տեսակից, այն կարող է պարունակել նաև այլ բաղադրիչներ, օրինակ՝ վեբ-մոնիտորինգ: Այս բաղադրիչը ստուգում է համացանցային էջերը, մինչև դրանց բացելը, որը թույլ է տալիս այս կերպ կանխել վարակը համացանցային էջերի միջոցով:

Այսօր գոյություն ունեն ինչպես անվճար, այնպես էլ վճարովի հակավիրուսային ծրագրեր: Անվճար տարբերակներից բավական տարածված են Avast, Avira, AVG, Microsoft Security Essentials և այլ նմանատիպ ծրագրերը, որոնք չեն զիջում վճարովիներին: Սակայն պետք է հիշել, որ ոչ մի հակավիրուսային ծրագիր չի տրամադրում լիակատար պաշտպանություն: Բոլոր դեպքերում լինում են նորաստեղծ վիրուսներ, որոնց վերաբերյալ հակավիրուսային լաբորատորիաները դեռևս տեղեկատվություն չունեն, այդ պատճառով դրանք չեն նույնականացվում: Կասկածելի ֆայլերի կամ հղումների առկայության դեպքում դրանք կարելի է ներբեռնել Virustotal.com կայքում, որն իրականացնում է ստուգում 54 հայտնի հակավիրուսային ծրագրերի միջոցով՝ ավելի նվազեցնելով վարակվելու հնարավորությունը:

Արգելապատնեշներ (Brandmauer, firewall,).

Բառացի թարգմանելու դեպքում գերմաներեն «brandmauer» և անգլերեն «firewall» բառերն ունեն նույն իմաստը՝ «արգելապատնեշ»: Հայալեզու որոշ գրականության մեջ կիրառվում է նաև «հրապատ» տերմինը: Հրդեհի տարածումը կանխելու համար նախկինում շինությունների արանքում կառուցում էին արգելապատնեշներ:

Համակարգչային տեխնոլոգիաներում արգելապատնեշն ապահովում է համակարգչի ցանցային միացումների նկատմամբ վերահսկողությունը:

Նրա հիմնական հնարավորություններն են.

- Խոցելի ծառայությունների մուտքի ֆիլտրում,
- Ցանցային ռեսուրսների մուտքի վերահսկում,
- Դրսից ներքին ցանց մուտք գործելու և հակառակ ուղղությամբ բոլոր փորձերի հաշվառման և կարգավորման իրականացում,
- Պաշտպանվող օբյեկտների, ինչպես նաև իր վրա կատարված հարձակումների մասին տեղեկության տրամադրում:

Արգելապատնեշի պաշտպանողական գործողությունների հետևանքով կարող են արգելափակվել նաև մի շարք օգտակար ծրագրեր և ծառայություններ. Օրինակ՝ «telnet», «ftp» և այլն: Դրա համար էլ արգելապատնեշի տեղադրման և կարգավորման ժամանակ ցանկալի է մասնագետի ներկայությունը: Արգելապատնեշի օգտագործումը նվազեցնում է համացանցից օգտվելու արագությունը և ցանցի թողունակությունը՝ անընդհատ ֆիլտրացիա իրականացնելու պատճառով:

Բացի արգելապատնեշային ծրագրերից, գոյություն ունեն նաև սարքային արգելապատնեշներ, որոնք սովորաբար կցվում են ցանցային սարքավորումներին, օրինակ, երթուղիչներին՝ ապահովելու համար ցանցի անվտանգությունը դրսի հարձակումներից:

Հակագովազդային և հակալրտեսական ծրագրեր.
Այս ծրագրերը կարողանում են պայքարել վնասակար ծրագրերի որոշ տեսակների հետ: Սովորաբար իրենց կառուցվածքով նման են հակավիրուսային ծրագրերին և ունեն մասնակի կամ ամբողջական մոնիտորինգի, ըստ պահանջի ստուգելու և տվյալների բազայի թարմացման հնարավորություն: Մասնագիտական հետազոտությունները ցույց են տվել, որ այս ծրագրերն իրենց հնարավորություններով զիջում են հակավիրուսային ծրագրերին, և ցանկալի է դրանք օգտագործել միայն որպես լրացում, եթե ձեր ընտրած հակավիրուսը չունի նման հնարավորություն:

Առցանց գովազդի արգելափակման համար օգտակար հավելվածներ ունի Գուգլ զննարկիչը, օրինակ՝ «Adblock», «AdblockPlus», «AdGuard» և այլն:

Ներխուժման կանխարգելման համակարգեր (Host(ed) Intrusion Prevention System, HIPS).
Այս խմբի արտադրանքներն իրականացնում են տարատեսակ ծրագրերի վերահսկողություն իրականացնելու այս կամ այն գործողությունը: Արգելապատնեշային ծրագրերի նմանությունը բերում է նրան, որ սովորաբար այս համակարգերն ինտեգրվում են արգելապատնեշային ծրագրերի հետ: Այս ծրագրերն աշխատում են պրոակտիվ մեթոդով և չունեն տվյալների բազա: Այս կամ այն ծրագրին թույլատրելով կամ

արգելելով ցանցային գործառույթներ՝ կարող է ընդհուպ մինչև 100%-անոց արդյունավետություն ապահովել՝ օպերացիոն համակարգը զերծ պահելով վնասվելուց կամ վարակվելուց: Սակայն, ինչպես և արգելապատնեշային ծրագրերը, սրանց օգտագործումը ևս որոշակի գիտելիքներ է պահանջում:

Հակափոստաղբային ծրագրեր կամ փոստաղբի զտիչներ.
փոստաղբային զտիչը կարելի է բնորոշել որպես օգտակար և վնասակար հաղորդագրությունների զտման գործիք: Այս զտիչները կարելի է դասակարգել երկու խմբի.

1. Փոստային զտիչներ. փոստային զտիչները դիտարկում են էլեկտրոնային նամակները՝ դասակարգելով որպես օգտակար, անցանկալի և կասկածելի:

Կախված ծրագրային կարգավորումներից՝ կասկածելի և անցանկալի նամակները կարող են ինքնուրույն ոչնչացվել, տեղափոխվել առանձին թղթապանակ կամ նշվել հատուկ նշումով:

Փոստային զտիչներն օգտագործում են տարբեր տեխնոլոգիաներ. բովանդակության վերլուծում, նամակի ձևական հատկանիշների վերլուծում, «սև» և «սպիտակ» ցուցակների հետ համեմատում և այլն: Փոստային զտիչներ տեղադրվում են ինչպես փոստային ծառայություն մատուցող ընկերության սպասարկիչների վրա, այնպես էլ կարող են տեղադրվել համացանցային ծառայություններ մատուցող ընկերության սերվերում կամ օգտա-գործողի համակարգչում: Վերջին դեպքում զտիչն ինտեգրվում է փոստային հաճախորդ հանդիսացող ծրագրին և աշխատում է նրա հետ զուգահեռ:

2. Փոստաղբային զտիչներ՝ նախատեսված ակնթարթային հաղորդակցման ծրագրերի և հրապարակումների վեբ հարթակների (ֆորումներ, հայտարարությունների տախտակներ և այլն) համար:

Ի տարբերություն փոստային զտիչների՝ այս զտիչներն աշխատում են ոչ թե արդեն ուղարկված հաղորդագրությունների հետ, այլ կանխում են դրանց ավտոմատ ուղարկումը և ստացումը: Այս նպատակով ստեղծվում են գործիքներ, որոնք կտարբերեն մարդ-օգտագործողին ծրագիր-ռոբոտից, որին կրճատ անվանում են «բոտ»:

Ակնթարթային հաղորդակցման ծրագրերի և որոշ վեբ հարթակների համար հակափոստաղբային զտիչն իրենից ներկայացնում է լրացում, որը հնարավորություն է տալիս գրողին հարց ուղարկել, և միայն ճիշտ պատասխանից հետո ստանալ նրա հաղորդագրությունները: Մյուս տարածված ձևը, որը կիրառվում է հիմնական վեբ հարթակներում CAPTCHA-ն է, որը կիրառվում է մարդուն համակարգչից տարբերելու համար:

CAPTCHA (անգլերեն «Completely Automated Public Turing test to tell Computers and Humans Apart անվանման հապավում) Թյուրինգի մեթոդով Լրիվ Ավտոմատացված Ստուգում Մարդկանց և Համակարգիչներին Տարբերելու համար (ԹԼԱՍՄՀՏ): Այս թեստն օգտագործողին առաջարկում է ճանաչել նկարի վրայի սիմվոլները և մուտքագրել համապատասխան դաշտում:

Պետք է հաշվի առնել, որ համակարգչային ծրագրային ապահովման սխալ ընտրությունն արդեն իսկ կարող է պարունակել լուրջ վտանգներ: Բացի այդ, կարևոր է նաև ծրագրային ապահովման հետ ճիշտ աշխատանք վարել, և այն պարբերաբար թարմացնել:

Համակարգչի պաշտպանությունը. այս խնդրում առաջնային դերակատարում ունի օպերացիոն համակարգը (Operation System): Այսօր ամենատարածված և ամենախոցելի օպերացիոն համակարգն է «Microsoft Windows»-ը: Այս համակարգի կառուցվածքային յուրահատկությունները հանգեցնում են նրան, որ հաքերային խմբերը հիմնական վիրուսները ստեղծում են հենց «Windows»-ի համար, և այս համակարգում են փնտրում խոցելի կետեր: Հարկ է նշել, որ այսօր պետք է խուսափել «Windows»-ի XP տարբերակից, քանի որ այն այլևս չի թարմացվում, և դրա տեղադրումը՝ համակարգիչը դարձնում է շատ խոցելի հարձակումների համար:

Համեմատաբար ավելի անվտանգ են «OS X» և «Linux» օպերացիոն համակարգերը: Դրանցից ամենաանվտանգը մատչելի կիրառման համար համարվում են «Linux» օպերացիոն համակարգերը: Մասնավորապես, այդ ընտանիքի «Ubuntu» օպերացիոն համակարգն անվճար է և կարող է ներբեռնվել ubuntu.com կայքից: Տվյալ համակարգն ինքնին շատ ավելի պաշտպանված է, քան մնացած ավելի տարածված օպերացիոն համակարգերը: Հարձակումների մեծ մասը տվյալ համակարգի համար վտանգավոր չէ:

Իսկ «Apple» արտադրանքի լայն տարածումը շուկայում կենտրոնացնում է

իր հանդեպ հաքերների ուշադրությունը: Արդյունքում՝ վերջին տարիներին «Apple»-ի դեմ հարձակումների թիվը կտրուկ աճել է: Իհարկե, կատարյալ պաշտպանված օպերացիոն համակարգ չկա, միշտ հնարավոր են թաքնված խոցելի կետեր, որոնք կարող են օգտագործել հաքերները: Բայց այն կարելի է դարձնել առավել պաշտպանված, այսպես կոչված, կիբերանվտանգության հիգիենայի կանոններին հետևելու պարագայում:

Օպերացիոն համակարգի պաշտպանությունը ենթադրում է երկու կարևոր կետ.

- Այն պետք է լինի լիցենզիոն, եթե խոսքը վճարովի համակարգերի մասին է:
- Համակարգը պետք է մշտապես թարմացնել:

Հակառակ պարագայում օպերացիոն համակարգում կարող են հայտնվել վտանգավոր խոցելի կետեր, որոնք թիրախ կհանդիսանան հանցագործների համար: Ինչ վերաբերում է թարմացումներին, ապա միշտ պետք է համոզված լինել, որ անջատված չեն ավտոմատացված թարմացումները (Update): Եթե օպերացիոն համակարգը չի կատարում թարմացումներն ինքնուրույն, ավտոմատացված կարգով, ինչպես դա կատարվում է «Windows»-ի դեպքում, ապա հարկավոր է պարբերաբար ստուգել թարմացումների բաժինը, և դրանք ներբեռնել ու տեղադրել համակարգչի վրա: Թարմացումների միջոցով օպերացիոն համակարգ ստեղծող կազմակերպությունները վերացնում են նոր հայտնաբերված խոցելի կետեր: Մինչդեռ երկար ժամանակ չթարմացված օպերացիոն համակարգը կարող է դառնալ խիստ խոցելի հարձակումների համար: Նույնիսկ մի քանի շաբաթ չթարմացված օպերացիոն համակարգը կարող է լուրջ վտանգ ներկայացնել, քանի որ պարբերաբար հայտնի են

դառնում վտանգավոր խոցելի կետեր, որոնք զանազան հաքերային խմբեր սկսում են կիրառել իրենց հարձակումներում:

Ոչ լիցենզիոն, «կոտրված» «Windows» օպերացիոն համակարգն ինքնին մեծ խնդիր է օգտագործողի համար, քանի որ նմանատիպ համակարգերն ինչ-որ պահից դադարում են թարմացվել: Նույնիսկ լինում են դեպքեր, երբ նման «Windows»-ները տարածվում են հենց հաքերների կողմից և պարունակում են ներդրված վիրուսներ կամ այլ վտանգներ:

Այսպիսով, պետք է օգտագործել միայն օրինական «Windows», և համակարգիչ գնելիս պետք է համոզվել, որ ձեզ տրվում է լիցենզիոն օպերացիոն համակարգով սարք: Նույնը վերաբերում է համակարգչի վրա տեղադրված ծրագրային ապահովմանը. այն պետք է լինի լիցենզիոն և թարմացված: Միևնույն ժամանակ, կարելի է օգտվել նաև անվճար «Linux» օպերացիոն համակարգերից: Այս հարցում պետք է հաշվի առնել, որ լիցենզիոն վճարովի ծրագրերը հաճախ օգտագործում են «կոտրելուց» հետո, որպեսզի դրանք անվճար տեղադրվեն համակարգչի վրա: Նման դեպքում օգտվողը վտանգի տակ է հայտնվում, քանի որ այդպիսով ծրագրային ապահովումը կարող է խոցելի լինել և, ի լրումն, կարող է պարունակել հաքերների կողմից ներդրված վտանգավոր ծրագրեր ու վիրուսներ: Այս խնդիրը հիմնականում առաջանում է տնային համակարգիչների հետ կապված, քանի որ օգտվողները գերադասում են չծախսել մեծ գումարներ ծրագրերի համար:

Սակայն վերոնշյալ խնդիրն ունի այլ, ավելի խոհեմ լուծում. տնային պայմաններում օգտագործելու համար գրեթե բոլոր վճարովի ծրագրերն ունեն անվճար փոխարինողներ (իհարկե, խոսքը լուրջ, պրոֆեսիոնալ

գործիքների մասին չէ): Այսպես, օրինակ, ամենատարածված «Microsoft Office»-ն ունի անվճար փոխարինող տարբերակ՝ «LibreOffice», «Photoshop»-ի փոխարինող տարբերակ՝ «Gimp» և այլն: Հնարավոր է նաև գտնել փոխարինող անվճար ծրագրեր, որոնք գործում են այսպես կոչված «ամպային» տեխնոլոգիաների միջոցով, ցանցային տարբերակով: Օրինակ, «Microsoft Office»-ի անվճար փոխարինող կարող է հանդիսանալ ցանցային «Google Drive» փաթեթը, որն անվճար հասանելի է «Gmail»-ում գրանցված բոլոր օգտատերերին:

Համակարգչի անվտանգության առանձնահատուկ հարցերից մեկը դրա ֆիզիկական հասանելիությունն է այլ անձանց համար:

Եթե տանը մեկ համակարգչից օգտվում են մի քանիսը, ապա գերադասելի է յուրաքանչյուրի համար բացել առանձին հաշիվ (user profile)՝ ամեն մեկը պաշտպանված գաղտնաբառով: Այն դեպքում, երբ համակարգչի վրա կա հաշիվների բաժանում, մեկ անձի դեմ հարձակումը չի անդրադառնում մյուսների վրա: Եթե օգտագործվում է շարժական համակարգիչ՝ լափթոփ, ապա գերադասելի է այն ֆիզիկապես վերահսկել: Սարքը պետք է լինի ձեր մշտական հսկողության տակ:

Համակարգիչը պարտադիր պետք է պաշտպանված լինի գաղտնաբառով, որի մուտքագրման ժամանակ ցանկալի է խուսափել այլ անձանց ներկայությունից, թիկունքում առկա հայելիներից և այլն: Խնդիր կարող են հանդիսանալ նաև հանրային վայրերում տեղադրված վերահսկողության տեսախցիկները, որոնցից նույնպես կարող են գրանցել գաղտնաբառերը:

Շարժական սարքերի պաշտպանությունը. շարժական սարքեր են հանդիսանում սմարթֆոնները և պլանշետները, որոնք նույնպես պարունակում են անձի վերաբերյալ շատ զգայուն տեղեկություններ: Ավելին, հաճախ շարժական սարքերի վրա ավելի զգայուն տեղեկատվություն է պահեստավորվում, քան անձնական համակարգիչների՝ լուսանկարներ, բանկային տվյալներ և այլն: Բացի այդ, հեռախոսը շատ դեպքերում մարդու անձը հաստատելու, միանշանակ նույնականացնելու գործիք է:

Այսօր շարժական սարքերի վրա հիմնականում տեղադրվում է երկու օպերացիոն համակարգ՝ «Android» և «iOS»: Այլ օպերացիոն համակարգերն այսօր աստիճանաբար լքում են համաշխարհային շուկան, այդ պատճառով դրանց անվտանգության խնդիրներին անդրադառնալը նպատակահարմար չէ:

«Android» և «iOS» սարքերը հիմնականում անվտանգ են, եթե պահպանվեն հետևյալ կանոնները.

- Հավելվածներ (application) տեղադրել միայն պաշտոնական համացանցային խանութներից՝ «Google Play» և «App Store»: Այլ կայքերից բեռնված ծրագրերը կարող են պարունակել թաքնված հնարավորություններ, որոնք թույլ կտան հաքերներին տիրանալ տեղեկատվությանը կամ հետևել ձեզ: Այսինքն՝ դուք կարող եք ներբեռնել ծրագրեր, որոնք իրականում վիրուսային բնույթ ունեն:
- Հավելված տեղադրելիս հետևեք, թե ինչ տիպի տեղեկատվություն է ուզում ստանալ ձեզանից հավելվածը: Եթե այն պահանջում է ձեր SMS-ների վերաբերյալ տեղեկատվություն կամ ուզում է միացնել խոսափողը, ապա հեռացրեք տվյալ ծրագիրը, քանի որ այն կարող է օգտագործվել լրտեսելու համար: Ցավոք, այսօր սոցիալական ցանցերի կամ նմանատիպ այլ հավելվածներն այնքան հնարավորություններ են պահանջում հեռախոսից, որ այս միջոցով միշտ չէ, որ հնարավոր է վտանգավոր ծրագիրը զատել անվտանգից:
- Սարքը «կոտրել» (jailbreak, root) խորհուրդ չի տրվում, քանի որ այդ դեպքում սմարթֆոնը կամ պլանշետը դառնում են ավելի խոցելի: Հիմնականում այս գործողությանը դիմում են զանազան վճարովի ծրագրերին կամ ծառայություններին անվճար տիրապետելու համար,

բայց որպես հետևանք թուլացնում են հեռախոսի կամ պլանշետի պաշտպանողական համակարգը:

- Շարժական սարքի վրա պետք է միացված լինի այն հեռավար գտնելու և պարունակվող տեղեկատվությունը ոչնչացնելու հնարավորությունը: «Android»-ի դեպքում դա «Device Manager» հավելվածն է, որը պետք է լրացուցիչ ներբեռնվի, քանի որ հեռախոսների և պլանշետների մեծ մասի վրա այն չկա հիմնական փաթեթի մեջ: «iOS»-ի դեպքում դա «Find My iPhone» հավելվածն է: Այս «Device Manager» հավելվածը թույլ է տալիս ինչպես գտնել ձեր սարքավորումը քարտեզի վրա, այնպես էլ վերացնել դրա վրա եղած անձնական ողջ տեղեկատվությունը: Այս հավելվածները կառավարվում են անձնական հաշիվներով, համակարգչից կամ այլ շարժական սարքից և թույլ են տալիս ինչպես տեսնել սարքի հստակ տեղը, այնպես էլ վերացնել դրա վրայի տեղեկատվությունը, որպեսզի այն հասանելի չլինի այլ անձանց: Հարկ է նշել, որ տեղեկատվության վերացումը տվյալ հավելվածների միջոցով լիարժեք չէ, եթե սարքավորման վրա առկա են արտաքին հիշողություն, փոփոխվող ֆլեշ քարտ: Այդ դեպքում հեռացված տեղեկատվությունը բավական հեշտ հնարավոր է վերականգնել բոլորին հասանելի ծրագրերի միջոցով:
- Սարքին պետք է միացված լինի սարքի արգելափակումը կոդի միջոցով, որպեսզի այլ անձինք հնարավորություն չունենան հեշտությամբ ներթափանցել: Կարևոր է սարքը ֆիզիկապես վերահսկողության տակ պահել, եթե չեք գտնվում ձեր տանը, այն միշտ պետք է ձեզ մոտ լինի, քանի որ չվերահսկվող նույնիսկ մի քանի վայրկյանը բավական է դրա մեջ լրտեսական ծրագրեր ներդնելու համար:

Հարկ է իմանալ, որ տեղեկատվությունը համակարգչի, հեռախոսի կամ պլանշետի վրա չի անհետանում այն ջնջելուց հետո: Իրականում ջնջելուց հետո ֆայլերը մեծ հավանականությամբ հնարավոր է վերականգնել: Որքան ավելի երկար է ֆայլը մնում ջնջված, որքան ավելի շատ է աշխատում սարքը ջնջելուց հետո, այնքան վերականգնելու հավանականությունը նվազում է:

Ջնջված ֆայլերը վերականգնելու համար գոյություն ունեն բազմաթիվ վճարովի և անվճար ծրագրեր: Անվճարներից կարելի է նշել «Recuva» ծրագիրը «Windows»-ի համար, «Mac»-երի համար՝ «TestDisk» և «PhotoRec», «Linux»-ի համար՝ «R-Linux» ծրագիրը:

Քանի որ ֆայլերը հնարավոր է վերականգնել, համակարգիչը կամ հեռախոսն ուրիշ մարդու փոխանցելուց կամ վաճառելուց առաջ պետք է վրայի տեղեկատվությունը ոչնչացնել հիմնովին: Հեռախոսների կամ պլանշետների վրա դա հնարավոր է կատարել գործարանային կարգավորումներին վերադառնալով. այդ դեպքում ֆայլերը վերականգնելի չեն, եթե դա չի իրականացվում մասնագետի կողմից հատուկ սարքավորումների միջոցով: Ինչպես արդեն նշվել է, այս գործողության հետևանքով տեղեկատվության վերացումը լիարժեք չէ, եթե սարքավորման վրա առկա են արտաքին հիշողություն, փոփոխվող ֆլեշ քարտ: Այդ դեպքում հեռացված տեղեկատվությունը կարելի է վերականգնել վերոնշյալ «Recuva» ծրագրով՝ քարտը միացնելով համակարգչին:

Ֆայլերը լիարժեք վերացնելու համար նույնպես պետք է կիրառվեն հատուկ ծրագրեր: Այսպես, «Windows»-ի համար գոյություն ունի «Ccleaner», «Mac»-երի համար գոյություն ունի ներդրված «Disk Utility» ծրագիր, «Android» համակարգի համար՝« Secure Wipe», «Secure Delete» ծրագրերը, «iOS»-ի համար՝ «iPhone Data Eraser» և այլ նմանատիպ հավելվածներ:

Այսօր օգտատերերի բոլոր հաշիվները (accounts)՝ առցանց բանկինգ (on-line banking), էլեկտրոնային փոստ, սոցիալական ցանցեր և այլն, հիմնվում են հիմնականում էլեկտրոնային հասցեների վրա, որոնք հանդիսանում են մարդուն նույնականացնելու միջոց: Էլեկտրոնային հասցեն կրիտիկական խոցելի կետ է հանդիսանում. դրա դեմ հաջողված հարձակումն անմիջապես վտանգի տակ է դնում մարդու մյուս բոլոր հաշիվները: Այդ պատճառով գերադասելի է ունենալ մի քանի էլեկտրոնային հասցե. գործնական և 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 կայքերի վրա գրանցվելու համար:

Գաղտնաբառերը հաշիվների պաշտպանության հիմնական բանալին են: Գաղտնաբառերի դեպքում կան մի քանի հիմնական կանոններ.

- գաղտնաբառը պետք է պարունակի առնվազն 10 նիշ՝ ներառյալ փոքր և մեծ տառեր, թվեր և սիմվոլներ,
- գաղտնաբառը չպետք է պարունակի հեշտ գուշակվող տեղեկատվություն, օրինակ՝ ձեր ծննդյան թիվը, հեռախոսահամարը, երեխաների անունները և այլն,
- տարբեր հաշիվների գաղտնաբառերը երբեք չպետք է կրկնվեն:

Գաղտնաբառերի չկրկնվելու պահանջն ունի իր տրամաբանությունը: Պարբերաբար հաքերներին հաջողվում է կորզել օգտատերերի տվյալները շտեմարանների տարբեր կայքերից: Նման շտեմարանները

պարբերաբար բոլորի համար հասանելի են դառնում համացանցում: Եվ նման հարձակումների ենթարկվում են նույնիսկ վստահելի և մեծ կայքեր, օրինակ՝ «Yahoo», «Dropbox» և այլն: Եթե մարդը բոլոր հաշիվների վրա կիրառում է նույն գաղտնաբառը, ապա նման բացահայտումը վտանգում է նրա բոլոր հաշիվները: Haveibeenpwned.com կայքից կարելի է տեղեկանալ՝ կա՞ արդյոք ձեր գաղտնաբառն արդեն իսկ հաքերների կողմից հրապարակված շտեմարաններում, թե՞ ոչ: Այստեղ հնարավոր է նաև գրանցվել և նոր հաքերային բացահայտումների դեպքում տեղեկանալ էլեկտրոնային նամակի միջոցով, եթե ձեր գաղտնաբառը հայտնվի համացանցում բոլորին հասանելի տարբերակով:

Հասկանալի է, որ այսօր միջին օգտատերն արդեն իսկ ստիպված է հիշել տասնյակ գաղտնաբառեր: Եվ բավական դժվար է լինում մտապահել, մանավանդ եթե մարդը պետք է տարբերվող գաղտնաբառեր ունենա: Եթե չունեք իդեալական հիշողություն, այստեղ կա երկու հիմնական լուծում.

- կիրառել գաղտնաբառերի ստեղծման հատուկ մեթոդներ, որոնք հասկանալի են միայն ձեզ,
- օգտագործել գաղտնաբառերի կառավարման հատուկ ծրագրեր (password manager), որոնք մի տեղ են պահում դրանք, և պարտադիր չէ դրանք բոլորն անգիր հիշել: Այդպիսի ծրագրեր են, օրինակ, «LastPass»-ը, «Dashlane»-ը, «KeePassX»-ը և այլն:

Այսօր գաղտնաբառերը կորցնելու մի շարք մարտահրավերներ կան: Այսպես.

- Վիրուսներով վարակված համակարգիչն արդեն իսկ վտանգ է, քանի որ դրանց միջոցով հաքերները կարողանում են ստանալ բոլոր գաղտնաբառերը: Այս դեպքերից փրկում են հակավիրուսային ծրագրերը:

- Հանրային Wi-Fi կետերից օգտվելը նույնպես կարող է հանգեցնել հաշվի կորստի:

Ինտերնետ ակումբներից, հանրային գրադարանների, կրթական հաստատությունների համակարգիչներից օգտվելը նույնպես կարող է բերել հաշիվների կորստի, քանի որ նմանատիպ համակարգիչները հաճախ լինում են վարակված և կորզում են ձեր տվյալները: Պետք է խուսափել նման համակարգիչներով անձնական հաշիվները մուտքագրելուց: Իսկ եթե ստիպված եք եղել, ապա գերադասելի է հնարավորինս շուտ վստահելի սարքից փոխել գաղտնաբառերը: Իսկ ավելի գերադասելի է միշտ ունենալ միացված երկփուլային մուտքի ընթացակարգը, ինչի մասին կխոսվի ստորև:

Հաշվի կորուստը կարող է տեղի ունենալ նաև այլ, ոչ անձնական համակարգչից մուտք գործելու դեպքում՝ բրաուզերի (դիտարկիչ, browser) մեջ էլեկտրոնային հասցեն և գաղտնաբառը պահպանելու կամ հաշվից դուրս գալ մոռանալու պարագայում: Նման վտանգներից խուսափելու համար ոչ անձնական համակարգչից կամ շարժական սարքից պետք է բրաուզերով մուտք գործել հատուկ ռեժիմով, որը չի պահպանում տվյալները պատուհանը փակելուց հետո: «Google Chrome»-ի դեպքում դա միանում է որպես «New Incognito Window» (կամ ստեղնաշարով Ctrl+Shift+N), իսկ «Firefox»-ի դեպքում՝ որպես «New Private Window», կամ ստեղնաշարով՝ Ctrl+Shift+P:

Այսօր ամենահուսալի պաշտպանության միջոցն է հանդիսանում երկփուլային մուտքի ընթացակարգը (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի՝ երկրորդ քայլով

անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ կարճ հաղորդագրությունների միջոցով: Նման տարբերակով երկար ժամանակ աշխատում էին բանկերը, որոնք տրամադրում էին առցանց հաշիվների հետ աշխատելու հնարավորություն (on-line banking): Սակայն այսօր անհատների դեմ հարձակումներն այնքան են հաճախակիացել, որ բազմաթիվ ցանցային ծառայություններ ներմուծում են երկփուլային մուտքի տարբերակը բոլորի համար: Այսօր նման ֆունկցիա կարելի է միացնել «Gmail», «Yahoo», «Yandex», «Dropbox», «Facebook», «Twitter» և տասնյակ այլ ծառայություններում, դրանց ցանկը կարելի է գտնել twofactorauth.org կայքում: Two-factor authentication-ի ակտիվացումը և կիրառումն անհամեմատ ավելի պաշտպանված է դարձնում օգտվողին: Այս համակարգը նշանակում է, որ եթե ուրիշի մոտ կա նույնիսկ ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվ՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է:

Ինչպես արդեն ասվեց, SMS-ներն այսօր արդեն վստահելի տարբերակ չեն հանդիսանում, և գերադասելի է օգտվել միայն հավելվածներից: «Google»-ն ունի հատուկ հավելված երկփուլային մուտքի համակարգի համար՝ «Google Authenticator»: Այս հավելվածը թույլ է տալիս գեներացնել կոդն ինչպես «Gmail»-ի համար, այնպես էլ կցել դրան այլ կայքերի հաշիվները: Այսպիսով, մեկ հավելվածով հնարավոր է կարգավորել մուտքերը դեպի բազմաթիվ այլ հաշիվներ մյուս սոցիալական ցանցերում կամ այլ ծառայություններում, որոնք թույլ են տալիս նմանատիպ ծրագրերի կիրառումը: Կան ծառայություններ, որոնք թույլ չեն տալիս օգտվել երրորդ կողմի հավելվածներից և պահանջում են կիրառել միայն սեփական արտադրության ծրագիր: Նմանատիպ մոտեցում ունի

«Yandex»-ը, որը հատուկ թողարկել է «Yandex Key» հավելվածը: «Facebook» հավելվածն ունի հենց իր մեջ ներդրված նման համակարգ, սակայն թույլ է տալիս օգտվել նաև երրորդ կողմի հավելվածներից, օրինակ՝ «Google Authenticator»-ից:

Որպես օրինակ ներկայացնենք «Facebook» հաշվի պաշտպանության հիմնական քայլերն ու կանոնները.

- Վստահելի էլեկտրոնային հասցեին կցել հաշիվը: Հանրային հասանելի էլեկտրոնային հասցեների ծառայություններից այսօր ամենավստահելիներից են «Gmail»-ը, «Hotmail»-ը և «Protonmail»-ը: Գերադասելի է, որ դա լինի հատուկ միայն սոցիալական ցանցերի և այլ կայքերի գրանցումների համար էլեկտրոնային հասցե, որը դուք ուրիշներից գաղտնի եք պահում:
- Էլեկտրոնային բոլոր հասցեների և «Facebook»-ի գաղտնաբառերը պարտադիր պետք է տարբերվեն:
- Այցելել «Facebook» settingsmobile և ավելացնել ձեր բջջային հեռախոսի համարը: Սա թույլ կտա հեռախոսն անվտանգ օգտագործել և ստանալ հաղորդագրություններ հնարավոր հարձակումների վերաբերյալ, արագ վերականգնել հաշիվը, եթե այն ենթարկվի հաքերային հարձակման:
- Մտնել «Facebook»-ի անվտանգության բաժին վերևի աջ անկյունից՝ settings բաժնից, ընտրելով security հատվածը և միացնել Login notifications: Այդ գործողությունից հետո, եթե ինչ-որ մեկն ուրիշ սարքից մուտք կգործի ձեր հաշիվ, դուք կստանաք հաղորդագրություն մուտքի մասին: Օգտատերն ինքը կարող է որոշել, թե ինչպես ստանա զգուշացումը՝ SMS-ով, թե էլեկտրոնային հասցեով, կամ երկուսը միասին:

- Ամենակարևոր գործողությունը Two-factor authentication երկփուլային մուտքերի համակարգի միացումն է: Միացվում է Login Approvals, այնուհետև ամեն անգամ նոր սարքով գաղտնաբառը մուտքագրելուց հետո անհրաժեշտ է մուտքագրել նաև հատուկ կոդ:
- Նշենք, որ եթե սմարթֆոնի վրա տեղադրված է «Facebook» հավելվածը, ապա այս դեպքում միացվում է «Code Generator»-ը, և հավելվածն ինքը 30 վայրկյանը մեկ գեներացնում է նոր կոդ: Հնարավոր է նաև միացնել այլ հավելվածներ, օրինակ՝ «Google Authenticator»-ը, որը 20 վայրկյանը մեկ գեներացնում է նոր կոդ:

Ինչպես հայտնի է, կիբեռվտանգների տեսակները բավական արագ են բազմանում, իսկ հաքերները ձգտում են գտնել հարձակման նոր ձևեր, պաշտպանության համակարգերը շրջանցելու նպատակով: Այսինքն՝ այս պահին նկարագրված անվտանգության խնդիրները և դրանց լուծումները կես տարի հետո արդեն կարող են թարմացման կարիք ունենալ: Այս համատեքստում որպես անվտանգության գլխավոր կանոն պետք է ընդունել նոր գիտելիքների ձեռքբերումը և ոլորտի նորություններին հետևելը: Ցանցային հիգիենայի մյուս կանոններն են.

Երբեք չշտապել, ամեն քայլը կատարելուց առաջ մի պահ մտածել, չկատարել մեխանիկական գործողություններ. օգտվողները հաճախ վարակում են համակարգիչները կամ այլ սարքերը վիրուսներով, քանի որ ավտոմատ գործողություններ են կատարում, ինչից էլ օգտվում են ցանցահենները:

Միշտ հաշվի առնել այն հանգամանքը, որ վիրտուալ աշխարհում հաքերները կարող են նմանակել ձեր ծանոթ կայքերը կամ օգտատերերին և նրանց անունից հաղորդակցվել ձեզ հետ:

Օգտատիրոջ անձնական տվյալները, գաղտնաբառերը կորզելու համար հաքերներն օգտագործում են մի շարք տարածված մեթոդներ: Դրանք ներառում են կեղծ նամակներ, որոնք առաջարկում են մտնել հղումով և մուտքագրել այս կամ այն ծառայության գաղտնաբառը: Նամակները կարող են գալ միանգամայն այլ հասցեից, ինչն ուշադիր լինելու պարագայում հեշտ բացահայտվում է:

Սակայն հաքերները կարող են նույնիսկ կեղծել էլեկտրոնային փոստի հասցեն և տպավորություն ստեղծել, թե նամակը ստացվել է, օրինակ, «Facebook», «Yahoo» ծառայություններից: Էլեկտրոնային հասցեների մի շարք ծառայություններ թույլ են տալիս հեշտությամբ կեղծել հասցեն, նման դեպքերում իրական առաքողի հասցեն կարելի է գտնել միայն էլեկտրոնային նամակի կոդը դիտելիս: Ընդ որում, նամակի մեջ հնարավոր է կեղծել ոչ միայն առաքողի հասցեն, այլ նաև հղումների հասցեները՝ օգտվողի մոտ տպավորություն ստեղծելով, թե նա ուղղորդվում է դեպի օրինական կայք: Կեղծ կայքն արտաքնապես կարող է իդեալական կերպով նույնականացվել որևէ հայտնի սոցիալական ցանցի, էլեկտրոնային փոստի, ինտերնետ խանութի արտաքին տեսքին: Իսկ հասցեն կարող է պարունակել ծանոթ բառեր, օրինակ՝ facebook.com-ի փոխարեն կարող է լինել http://facedook.co.gp, որտեղ նմանակվում են լատիներեն b և d տառերը: Կամ հասցեն կարող է պարունակել facebook բառը, օրինակ՝ http://www.facebook.pcriot.com : Անուշադիր օգտատերը նման կայքում ներմուծում է իր էլեկտրոնային հասցեն և գաղտնաբառը՝ այդպիսով հանձնելով դրանք հաքերներին: Այս կիբերմեքենայությունն ընդունված է կոչել ֆիշինգ (phishing): Նման հարձակումներից խուսափելու համար պետք է հիշել, որ ոչ մի որակյալ ծառայություն չի պահանջում նամակով մուտքագրել գաղտնաբառը:

Չի կարելի անզգուշորեն բացել հղումներ, որոնք եկել են անգամ ձեր վստահելի ընկերներից, քանզի հնարավոր է, որ ընկերոջ հաշիվն արդեն իսկ գտնվում է հաքերների վերահսկողության տակ, և տվյալ նամակը նա չի կազմել, այլ ուղարկվել է ձեզ չարագործների կողմից: Նման մեթոդներով ձեր ընկերների անունից նամակագրություն տարածելով՝

հաքերները վարակում են սոցիալական ցանցերի մեծաթիվ օգտատերերի: Դրանք հասարակության լայն շրջանակներում ավելի հայտնի են որպես «ֆեյսբուկյան վիրուսներ»:

Ողջամտության սկզբունքից ելնելով՝ արժե հետևել հետևյալ պարզ կանոնին. նամակներով կամ մեսենջերով չուղարկել գաղտնաբառեր կամ անձնական գաղտնի այլ տվյալներ պարունակող տեղեկատվություն: Եթե ստիպված եք նման հաղորդագրություններ ուղարկել, ապա փորձեք դրանք բաժանել մի քանի մասի և հատվածներ ուղարկել տարբեր տիպի ծառայություններով: Ուղարկելուց հետո դրանք անպայման ջնջեք, իսկ հետո պարտադիր մաքրեք աղբամանը, նույնը պահանջեք նաև ստացող կողմից:

Ծրագրային անվտանգության ապահովման 12 խորհուրդ.

1. Պետք չէ բացել և աշխատեցնել էլեկտրոնային նամակներին կից ֆայլերը, եթե դրանք ունեն exe, vbs, js և այլ ընդլայնումներ: Ընդ որում, էական չէ, թե ով է ուղարկել այս նամակը: Քանի որ վարակի դեպքում վնասակար ծրագիրն ինքնուրույն է ուղարկում նամակները հասցեատիրոջ անունից: Եթե դուք ստացել եք նամակ ձեզ ծանոթ անձնավորությունից, ճշտեք թե ի՞նչ ֆայլ է նա ուղարկում: Անծանոթ հասցեներից ստացված նամակներն անմիջապես ջնջեք:

2. Պետք չէ անցնել այն էջերի հղումներով, որոնք դուք ստացել եք ակնթարթային հաղորդակցման ծրագրերի, սոցիալական ցանցերի, ֆորումներում անձնական հաղորդագրությունների միջոցով, հատկապես, եթե չեք ճանաչում ուղարկողին: Եթե ուղարկողը ձեզ ծանոթ անձնավորություն է, ապա ցանկալի է հարցնել նրան այն էջի

բովանդակության մասին, որի հղումը ուղարկել է: Միշտ պետք է հիշել, որ վնասակար ծրագիրը կարող է ինքնուրույն ուղարկել հաղորդագրություններ կոտրված հաշիվներից:

3. Եթե դուք ստացել եք նամակ սոցիալական ցանցի, առցանց խանութի կամ բանկի, ֆորումի կամ այլ ռեսուրսի ադմինիստրացիայի անունից, որտեղ ձեզ խնդրում են բացել ձեր հաշիվը, ցանկալի է բացել զննարկիչը և հավաքել այդ ռեսուրսի գլխավոր էջի հասցեն՝ հղմանը կտտացնելու (click) փոխարեն: Իսկ եթե, այնուամենայնիվ, բացել եք հղումը, ապա համոզվեք, որ դուք իրական կայքում եք, դրա համար ստուգեք ձեր բացած կայքի հասցեն՝ հասցեների տողից:

4. Ցանկալի է միշտ միացնել ֆայլերի ընդլայնումների ցուցադրումը թյուրիմացություններից խուսափելու համար: Օրինակ, ձեզ կարող են ուղարկել «picture.jpg» անվանումով ֆայլ, որին նայելով կարելի է կարծել, թե սա նկար է, այնինչ, երբ միացնեք ընդլայնումը կհասկանաք, որ սա «picture.jpg.exe» ֆայլ է, որն իրենից ներկայացնում է վնասակար կիրառական ծրագիր:

5. Ցանկալի է օգտվել հաղորդակցման այլընտրանքային ծրագրերից և փոստային մատակարարներից (Providers), քանի որ, ի տարբերություն հիմնականների, դրանք ավելի քիչ են ենթարկվում հարձակումների, քանի որ ավելի փոքր տարածվածություն ունեն:

6. Ցանկալի է հանել ակնթարթային հաղորդակցման ծրագրերն ինքնաբեռնավորումից, այսինքն միացնել այն ձեռքով՝ համակարգչի միանալուց հետո:

7. Ցանկալի է փոստային մատակարարի ծրագիրը կարգավորել այնպես, որ նամակներին կից ֆայլերն ինքնուրույն (Automat) չներբեռնվեն համակարգիչ, այլ դա կատարվի միայն ձեռքով (Manual):

8. Ձևնարկիչն անհրաժեշտ է կարգավորել այնպես, որ բացառվի ֆայլերի ինքնուրույն ներբեռնումը համակարգիչ: Իսկ ներբեռնելուց էլ հավաստիացեք, որ արժե վստահել այն ռեսուրսին, որտեղից պատրաստվում եք ներբեռնել: Ներբեռնելուց հետո անպայման ստուգեք հակավիրուսային ծրագրով՝ մինչև ֆայլը բացելը:

9. Ցանկալի է անջատել ինքնագործարկման համակարգը բոլոր տիպի սկավառակների և տեղեկույթի կրիչների համար: Համակարգչում սկավառակ կամ կրիչ տեղադրելուց հետո անպայման ստուգեք այն, նոր բացեք պարունակությունը:

10. Համակարգիչը մի՛ թողեք միացված մնա ցանցին, եթե այն չեք օգտագործում, անգամ եթե օգտվում եք անսահմանափակ տրաֆիկով համացանցից:

11. Ծրագրեր ներբեռնելու համար օգտագործեք միայն արտադրողի պաշտոնական կայքը, մյուսները, ինչքան էլ գրավիչ լինեն, չեն երաշխավորում անվտանգությունը:

12. Ցանկալի է միշտ թարմացնել օպերացիոն համակարգի և ծրագաշարի անվտանգության թարմացումները, սրանց մշակող ընկերություններն անընդհատ հրապարակում են անվտանգության

փաթեթներ, որոնք, ինտեգրվելով օպերացիոն համակարգին և այս կամ այն ծրագրին, ձեր համակարգչի համար ապահովում են անվտանգության առավել բարձր մակարդակ:

Ձեռնարկը ստեղծվել է Բոլորը հանուն հավասար իրավունքների հիմնադրամի (ԲՀՀԻ հիմնադրամ) կողմից «Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագրի շրջանակում: Նյութի բովանդակության համար պատասխանատու է միայն ստեղծողը: Ձեռնարկում արտահայտված տեսակետները/ բովանդակությունը կարող են չհամընկնել Շվեդիայի կառավարության տեսակետների հետ:

«Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագիրն իրականացվում է Եվրասիա համագործակցություն հիմնադրամի կողմից Շվեդիայի կառավարության աջակցությամբ:

ԹՎԱՅԻՆ ՀԵՏՔ.

ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ՁԵՌՆԱՐԿ

Ձեռնարկի էլեկտրոնային գրագիտության բաղադրիչը մշակվել է ԲՀՀԻ հիմնադրամի կողմից, թվային անվտանգության և որոնողական համակարգերի բաղադրիչներում առկա նկարագրությունների որոշ հատվածներ վերցված են ստորև բերված հրապարակումներից՝

Հանրային լրագրության ակումբ, «Փաստերի ռադար» առցանց ուղեցույց:

World Vision Armenia, «Անվտանգ համացանց» ձեռնարկ, Արտակ Հարությունյան, Վահե Երիցյան, 2011:

Նորավանք գիտակրթական հիմնադրամ, «Տեղեկատվական անվտանգություն», ՀՏԴ 004(07), ԳՄԴ 32.81y7, ISBN 978-9939-825-34-2 «Նորավանք» ԳԿՀ, 2017, ՀՀ ԿԳՆ ԳՊԿ, 2017:

Գյումրի (2022)