Էլեկտրոնային գրագիտության և
թվային անվտանգության դպրոց

«ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ ԵՐԻՏԱՍԱՐԴՆԵՐԻ ՇՐՋԱՆՈՒՄ»

ՀՆԱՁԱՆԴ ՄԱՆՈՒԿՅԱՆ
ՄԱՐԻԱՄ ԱԴԱՄՅԱՆ

Շվեդիա Sverige
EURASIA PARTNERSHIP FOUNDATION
All Rights FOUNDATION
DIGITAL SCHOOL

Սույն ուսումնասիրությունն իրականացվել է «Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոց»» ծրագրի շրջանակում, «Բոլորը հանուն հավասար իրավունքների» հիմնադրամի կողմից, Եվրասիա համագործակցություն հիմնադրամի կողմից Շվեդիայի միջազգային զարգացման գործակալության, Միդայի աջակցությամբ իրականացվող «Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագրի շրջանակում:

Ուսումնասիրությունում ներկայացված բովանդակությունը կարող է չհամընկնել ծրագիրը ֆինանսավորող կողմերի դիրքորոշումների հետ:

Ուսումնասիրության աշխատանքային խումբ՝
Հնազանդ Մանուկյան, Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոցի շրջանավարտ,
Մարիամ Ադամյան, Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոցի շրջանավարտ:

Գյումրի, 2022

Բովանդակություն

Ներածություն

Համացանցը մեր կյանքի անբաժան մասն է: 21-րդ դարում մարդն առանց համացանցի չի կարող լիարժեք լինել: Համացանցի շնորհիվ մենք կարող ենք ակնթարթորեն տեղեկանալ աշխարհի ցանկացած այլ կետում տեղի ունեցող իրադարձության մասին: Այն մեզ օգնում է ձեռք բերել կապեր, գիտելիքներ, փորձ և մեր առաջ բացում է զարգացման և առաջընթացի անսահման հնարավորություններ:

Տեխնոլոգիաների զարգացումը, տեղեկատվական արագընթաց հոսքերը մեզ ստիպում են դառնալ համացանցի և մեդիայի անբաժան մաս: Statista-ի տվյալներով[1] 2021 թվականի դրությամբ 4,66 միլիարդ մարդ համարվում է համացանցի ակտիվ օգտատեր, մինչդեռ երկիր մոլորակի բնակչության 80%-ից ավելին ունի ազատ մուտք դեպի համացանցային տիրույթ:

Մերօրյա տեղեկատվական հասարակության և աշխարհի բնակչության համակեցությունը, կյանքի կարգավորման ոլորտները՝ տնտեսությունը, կրթությունը, առողջապահությունը, արդյունաբերությունը ամբողջությամբ հենված են համացանցի վրա: Բնակչության «արտագաղթը» օֆլայն միջավայրից օնլայն միջավայր իր հետ տեղափոխեց նաև վարքագծային բացասական դրսևորումներ, որը մեր օրերում արտահայտվում է թվային վտանգների՝ անձնական տվյալների, անձի ինքնության կողոպուտի, ֆինանսական և բարոյական վնասի, կյանքի գաղտնիության խախտման, բազմաթիվ իրավունքների ոտնահարման, կոնֆլիկտների հրահրման, անհանդուրժողականության և մի շարք այլ տեսքերով:

Թերևս մեր օրերում մեդիագրագիտությունը, համացանցային գիտելիքների տիրապետումը, թվային անվտանգության իմացությունը համարվում են առաջնահերթություններ: Միևնույն ժամանակ դրանց վերաբերյալ գիտելիքների և կարողությունների փոխանցումը մարտահրավեր է կրթական համակարգի համար և առաջնահերթ խնդիրներից մեկը նախակրթական, հանրակրթական և բարձրագույն կրթական համակարգերում այս թեմաների հանդեպ պատշաճ ուշադրության սևեռումն է:

Իրական պատկերը շոշափելու համար «Էլեկտրոնային գրագիտություն և թվային անվտանգություն» դպրոցի շրջանավարտները՝ Հնազանդ Մանուկյանը և Մարիամ Ադամյանը հանձն առան իրականացնելու սույն ուսումնասիրությունը:

Սույն ուսումնասիրությունն իրականացվել է Շիրակի մարզում, այն չի համարվում ներկայացուցչական և ենթադրում է շրջանավարտների կողմից կատարած փոքրիկ աշխատանք՝ ոլորտի և թեմայի առնչությամբ երիտասարդների շրջանում գիտելիքների ու փորձի դիտարկման նպատակով:

[1] Statista.com - https://www.statista.com/statistics/617136/digital-population-worldwide/

Թվային անվտանգության մասին

Անգլալեզու գրականության մեջ[2] «տեղեկատվական անվտանգություն» (information security) հասկացությունը սահմանվում է որպես տեղեկատվության և աջակցող ենթակառուցվածքների պաշտպանվածություն բնական կամ արհեստական բնույթի պատահական կամ կանխամտածված ազդեցություններից, որոնք տեղեկատվական հարաբերությունների սուբյեկտներին, այդ թվում՝տեղեկատվությունը տիրապետողին ու օգտագործողին, ինչպես նաև աջակցող ենթակառուցվածքին կարող են անուղղելի վնաս հասցնել:

Հասկացության մեկ այլ սահմանմամբ[3]՝ «Տեղեկատվական անվտանգությունը տեղեկույթի և տեղեկատվական համակարգերի՝չարտոնված մուտքից, օգտագործումից, հրապարակումից, փոփոխումից կամ ոչնչացումից պաշտպանությունն է, որպեսզի ապահովված լինեն գաղտնիությունը, ամբողջականությունը և մատչելիությունը: Այս իմաստով տեղեկատվական անվտանգության հոմանիշներն են «կիբերանվտանգությունը» (Cyber-security) և «համակարգչային անվտանգությունը» (Computer security):

Այլ կերպ ասած, տեղեկատվական անվտանգությունը նույն ֆիզիկական անվտանգությանն ուղղված գործողությունների համակցությունն է, որը գործում է առցանց տիրույթում: Միևնույն ժամանակ տեղեկատվությունը կարող է լինել օֆլայն միջավայրում՝ որևէ կրիչի, փաստաթղթի, ձայնագրության տեսքով, որը նույնպես ենթակա է համապատասխան պաշտպանության:

[2]Microsoft Word - banber153_6.doc (ysu.am)

[3] Glossary of Key Information Security Terms». Ed. by Richard Kissel. National Institute of Standards and Technology, May 2013, p. 94.

Ուսումնասիրության մեթոդաբանություն

Սույն ուսումնասիրությունն իրականացվել է «Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոց» ծրագրի շրջանակում: Ուսումնասիրությունն իրականացվել է Շիրակի մարզում, այն չի համարվում ներկայացուցչական և ենթադրում է դպրոցի շրջանավարտների կողմից կատարած փոքրիկ աշխատանք՝ ոլորտի և թեմայի առնչությամբ երիտասարդների շրջանում գիտելիքների ու փորձի դիտարկման նպատակով:

Շրջանավարտների կողմից ուսումնասիրության իրականացման համար հիմք է հանդիսացել Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոցի ընթացքում ձեռք բերած գիտելիքներն ու փորձը թվային անվտագության վերաբերյալ:

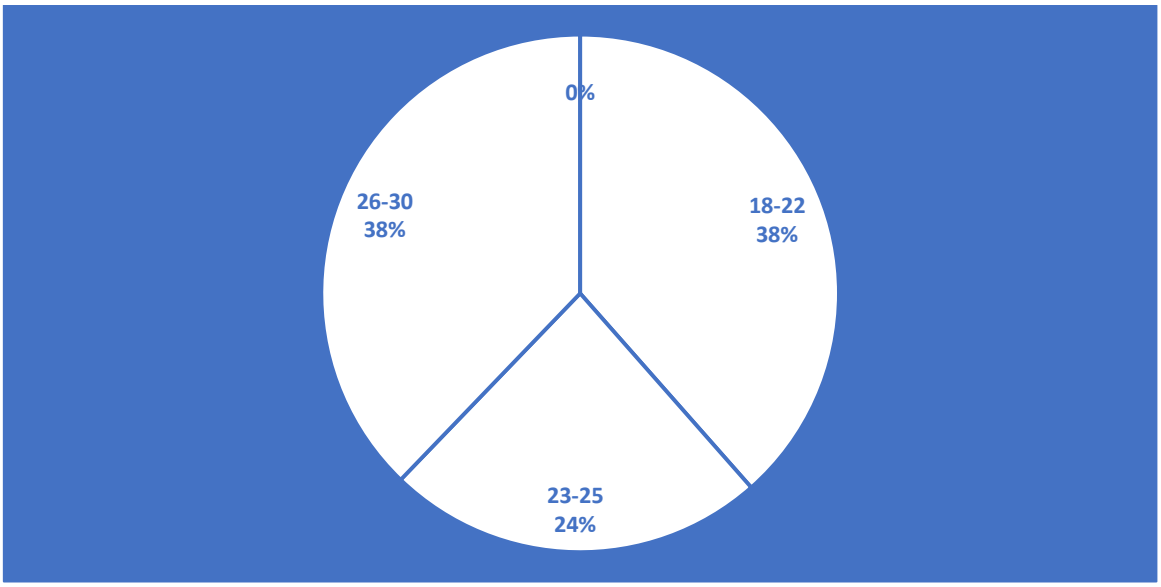
Ուսումնասիրության իրականացման համար կիրառվել է առցանց հարցումների մեթոդը Google Forms թվային գործիքի օգնությամբ:

Հարցման առցանց թերթիկի պատրաստման գործընթացում հաշվի է առնվել հարցաթերթի կարճ ծավալը և բովանդակային պատասխան ակնկալող հարցերի նվազագույն ծավալի տեքստ պահանջելու հանգամանքը: Հարցաթերթը պատրաստելիս հաշվի է առնվել սոցիոլոգիական մի քանի կարևոր բաղադրիչներ, որոնք մշտապես կիրառվում են հետազոտություններում՝

- յուրաքանչյուր պատասխանող իրավունք ունի հարցերին պատասխանել անանուն,
- յուրաքանչյուր պատասխանող իրավունք ունի չպատասխանելու ցանկացած հարցի,
- յուրաքանչյուր հարց, բացի բուն հարցին վերաբերող տարբերակներից ունեցել է նաև հետևյալ տարբերակները՝
    - Այլ,
    - Չգիտեմ,
    - Դժվարանում եմ պատասխանել,
    - Հրաժարվում եմ պատասխանել:

Հարցմանը մասնակցել է 135 հոգի, որոնցից 74.1%-ը՝ իգական սեռի ներկայացուցիչներ, 25.9%-ը՝արական սեռի ներկայացուցիչներ: Հարցմանը մասնակիցների 43%-ը Շիրակի մարզից են, 24.4%-ը՝ Գեղարքունիքից, 5.9%-ը՝ Կոտայքից, իսկ 26.7%-ը՝ այլ մարզերից և Երևան քաղաքից:

Հարցվողների տարիքային կազմը ներկայացված է հետևյալ գրաֆիկով։



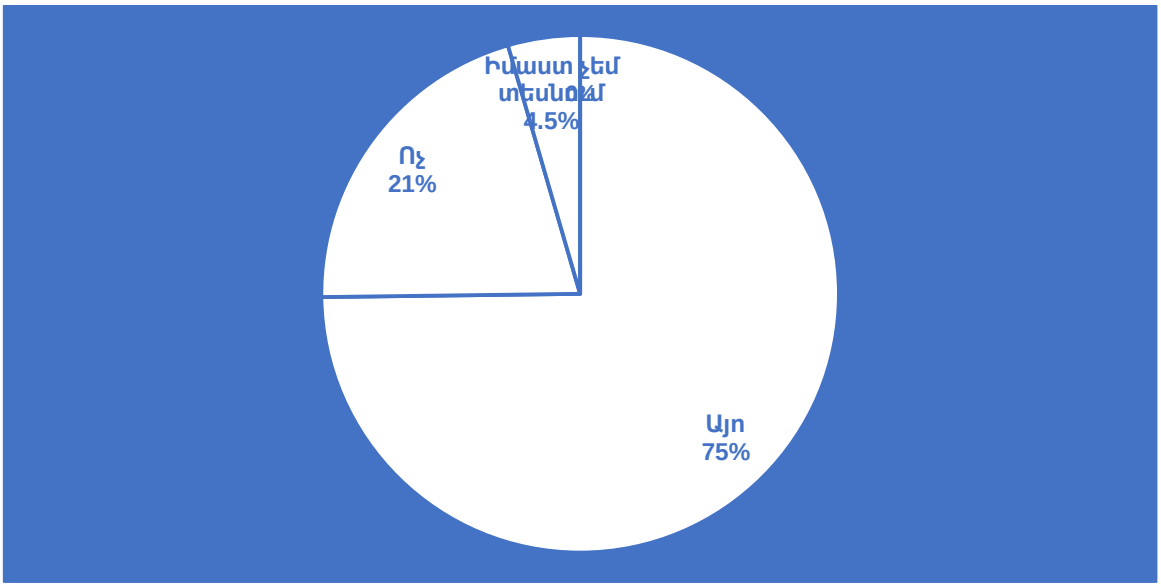
Հարցմանը մասնակցողների 58.5%-ն ունեցել է բարձրագույն կրթություն, 17.8%-ը՝ միջնակարգ մասնագիտական, 21.5%-ը՝ միջնակարգ, 2.2%-ը՝ թերի։ Հարցման թերթիկը բաց է եղել 3 օր։

Ուսումնասիրությունն իրականացվել է նաև սեղանային աշխատանքի մեթոդով, որի ընթացքում դիտարկվել են տեղական և միջազգային մի շարք փաստաթղթեր, զեկույցներ և գիտահանրամատչելի գրականություն։ Փաստաթղթերի ընտրության հարցում հիմք է վերցվել աշխարհի լավագույն փորձը։

Դաշտային ուսումնասիրության արդյունքներ

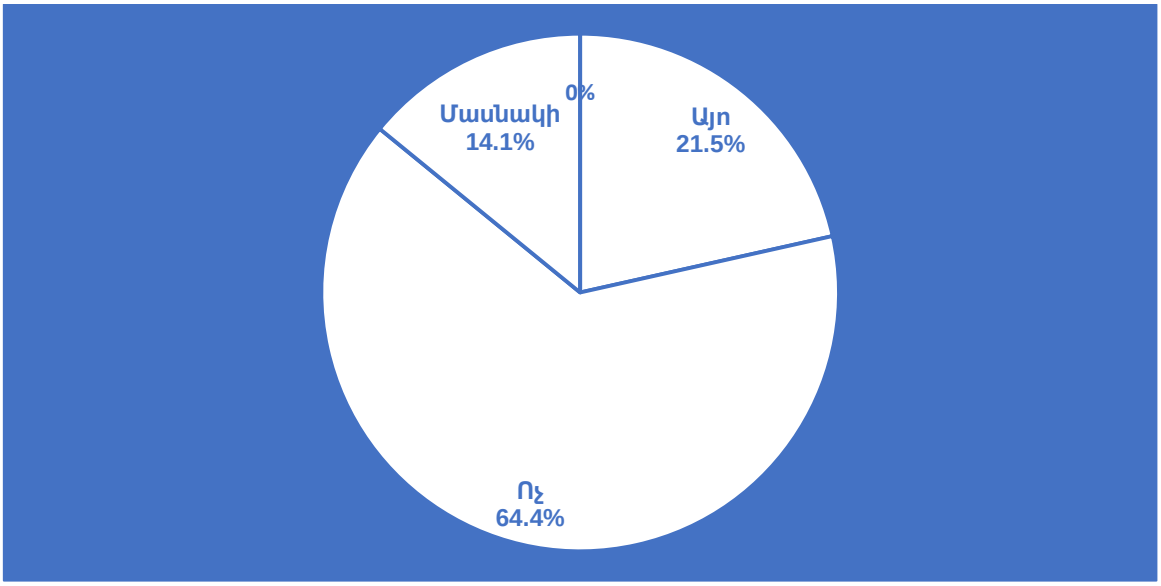
Հարց– Արդոք ունե՞ք գաղտնաբառ ձեր սմարթֆոնի էկրանին։
Հարցման մասնակիցների 74.8%-ը պատասխանել են, որ կիրառում են գաղտնաբառ, մինչդեռ 20.7%-ը՝ չի կիրառում, իսկ 4.5%-ը կարծում է, որ որևէ իմաստ չկա սմարթֆոնի էկարնին գաղտնաբառ դնելու համար։

Ընդհանուր առմամբ հարցման մասնակիցների շուրջ 25%-ը չի կիրառում գաղտնաբառ։ *Ստացվում է՝ յուրաքանչյուր չորրորդ ռեսպոնդենտն իր սմարթֆոնի վրա չունի գաղտնաբառ։*



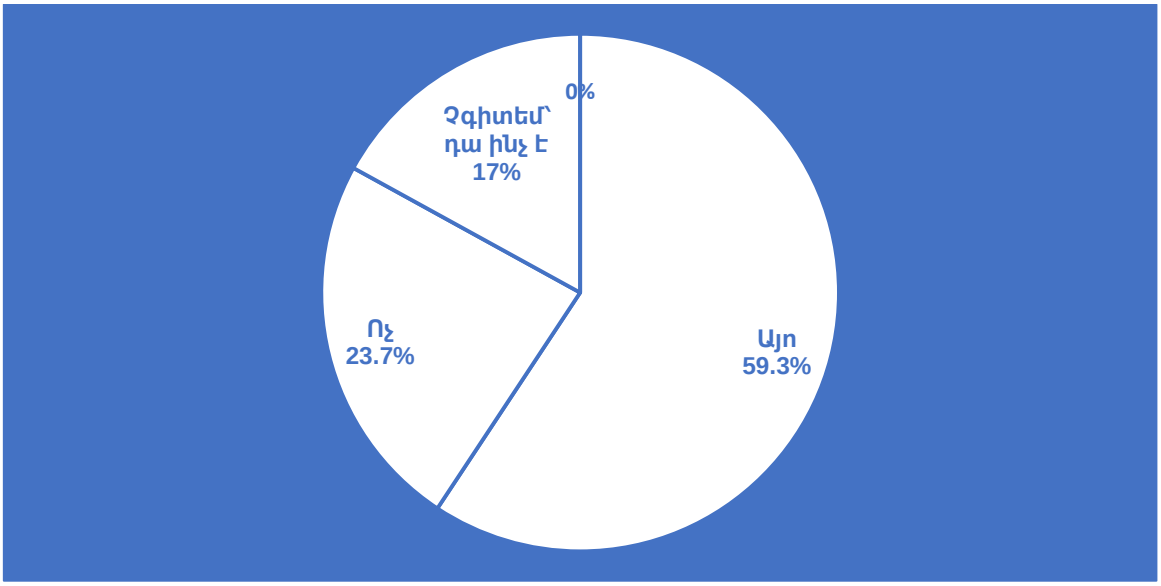
Հարց-Արդյո՞ք բջջային հավելվածների վրա ունեք գաղտնաբառ։

Հարցվողների 64.4%-ը պատասխանել են, որ չունեն գաղտնաբառ իրենց հեռախոսների վրա։ Հարցվողների 21.5%-ը պատասխանել են, որ այո ունեն գաղտնաբառ, իսկ 14.1%-ն ունեն մասնակի՝որոշ հավելվածների վրա՝ այո, որոշների վրա՝ ոչ։



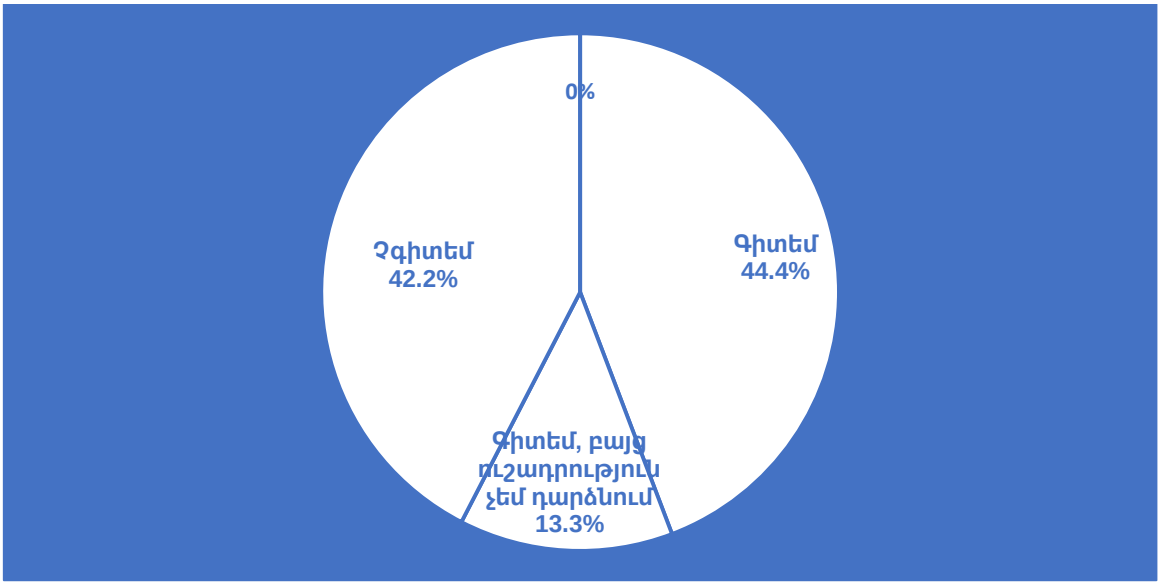
Հարց -Արդյո՞ք ձեր սոցիալական ցանցերի հաշիվներում միացված է երկուլ/երկաստիճան անվտանգության (two-step verification) համակարգը:

Հարցվողների 59.3% - ը պատասխանել են, որ միացված է սոցիալական ցանցերի հաշիվների մուտքի երկփուլային անվտանգությունը, 23.7%-ի մոտ այն միացված չէ, իսկ 17%-ը չգիտի, թե դա ինչ է իրենից ենթադրում:



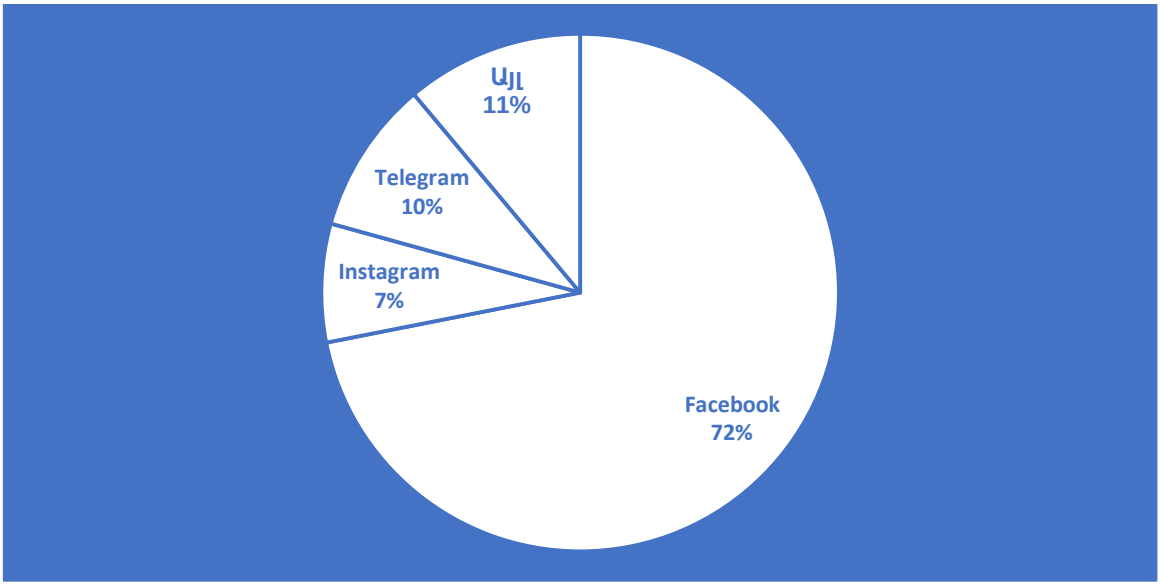
Հարց -Արդյոք գիտե՞ք, որ բաց՝ առանց գաղտնաբառի wi-fi-ները որոշակի վտանգ են պարունակում և որքանո՞վ եք ուշադրություն դարձնում այդ փաստին:

Հարցվողների 44.4%-ը պատասխանել են՝այո, 13.3%-ը գիտի, բայց ուշադրություն չի դարձնում այդ փաստին, 34.8%-ը չգիտի, իսկ 7.4%-ը չգիտեր բաց wi-fi սարքերի վտանգավոր լինելու փաստի մասին:



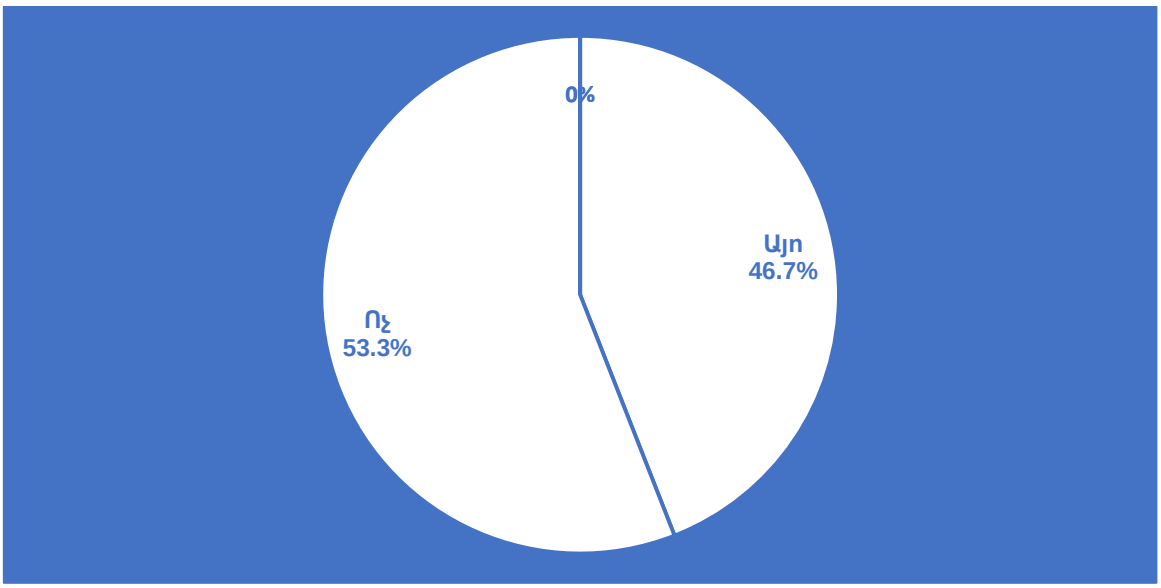
Հարց -Սոցիալական ո՞ր ցանցն է ձեզ համար հանդիսանում այն հիմնական օղակը, որի միջոցով ստանում եք նորություններ:

Հարցվողների 72%-ի համար որպես տեղեկատվության ստացման և նորությունների էջերի անցման կապող օղակ է հանդիսանում Ֆեյսբուկը, 9.6%-ի համար՝ Տելեգրամը, 7.4%-ի համար՝ Ինստագրամը, իսկ 11.1%-ի համար՝ այլ ցանցեր:



Հարց – Արդյո՞ք երբևէ ստացել եք հակերային բնույթի (phishing, spamming, spoofing, pharming) հաղորդագրություններ:

Հարցվողների 53.3%-ը նշել են, որ երբևէ չեն ստացել հակերային բնույթի հաղորդագրություն, իսկ 46.7%-ը հաստատել են, որ այն ստացել են:



Հարցվողներին ուղղված հաջորդ հարցը բխել է նախորդից՝ փորձելով պարզել՝եթե հարցվողը ստացել է հակերային բնույթի հաղորդագրություն, ապա ի՞նչ քայլեր է ձեռնարկել, իսկ եթե դեռ չի ստացել, ապա ստանալիս ինչպիսի՞ քայլեր կձեռնարկեր։

Այս հարցին հարցվողներից 25%-ը չեն պատասխանել առհասարակ։ Հիմնականում հնչել են հետևյալ պատասխանները. «կանտեսեմ», «չեմ բացի», «կջնջեմ», «կփորձեմ պարզել՝ ինչ է դա», «կբացեմ, հետո որոշում կկայացնեմ», «կախված է բովանդակությունից», «չգիտեմ՝ ինչ անել», «ուղարկում եմ սպամ»։

Հարկ է նշել, որ հարցվողներից մեկը նշել է, որ հաղորդագրության ստացման էլեկտրոնային փոստի հասցեն կարգելափակի (block), այնուհետև, կդիմի անձնական տվյալների պաշտպանության կոմիտեին, որտեղ կկարողանան ուսումնասիրել դեպքը և կտեղեկացնեն այլ օգտատերերի։

Սեղանային ուսումնասիրության արդյունքներ

Հասարակության շրջանում ինտերնետի, հետևաբար նաև թվային տեխնոլոգիաների օգտագործման մակարդակը բավականին բարձր է։

1) Հայաստանի բնակչության 96%-ն ունի ինտերնետի հասանելիություն տանը։ Ամրակցված ինտերնետ կապից օգտվում է բնակչության 68%-ը։ Ընդ որում, այս ցուցանիշը շատ ավելի բարձր է քաղաքային բնակավայրերում (76%)՝ ի համեմատություն գյուղական բնակավայրերի (60%)[4]։

2) Միևնույն ժամանակ հարկ է նշել, որ Հայաստանի բնակչությունը ինտերնետը հիմնականում օգտագործում է զվարճության կամ պարզագույն հաղորդակցության նպատակներով՝ ներառյալ զանգեր (90%), սոցիալական ցանցեր (68%), հաղորդագրություններ (60%), երաժշտություն (54%) և առցանց նորություններ (53%)։ Առավել կարևոր և արժեքաստեղծ գործառնությունների համար ինտերնետի օգտագործման ցուցանիշները համեմատաբար ավելի ցածր են. սեփական բովանդակության տեղադրում համացանցում (16%), աշխատանքի փնտրում համացանցում (11%), մասնակցություն առցանց քննարկումներին (8%), ապրանքների ու ծառայությունների վաճառք (7%) կամ գնում (13%), և այլն։

3) Էլեկտրոնային մասնակցության համաթվով Հայաստանը վերջին տարիներին տպավորիչ աճ է արձանագրել[5], սակայն իր դիրքով դեռևս հետ է մնում ԵԱՏՄ երկրներից։ 2018թ. տվյալներով Հայաստանի դիրքը 193 երկրների շարքում 57-րդն է, մինչդեռ նույն շարքում Ղազախստանը 26-րդն է, Ռուսաստանը՝ 27-րդը, իսկ Բելառուսը՝ 57-րդը։

[4] «Հայաստան. ՏՀՏ-ի օգտագործումը տնային տնտեսություններում և անհատների կողմից» հարցում (առաջիկա), Համաշխարհային բանկ, 2020թ.
[5]«Էլեկտրոնային կառավարում» հարցում, ՄԱԿ, 2020թ.

Կիբերանվտանգությունը որպես թվային անվտանգության հիմնական բաղադրիչ[6]

Ինչպես հայտնի է, այսօր ձևավորվել է հաքերային հարձակումների ծառայությունների հսկայական սև շուկա[7]: Մասնավորապես, այսպես կոչված «Մութ ցանցում» (Darknet) գործում են բազմաթիվ անոնիմ կայքեր, որտեղ կարելի է պատվիրել տարբեր տիպի հաքերային հարձակումներ՝ սկսած ընտանեկան բնույթի գործողություններից, ուղղված սոցցանցերի օգտատերերի դեմ, մինչև լուրջ կորպորատիվ հարձակումները, երբ կորզվում է գաղտնի տեղեկատվություն կամ էլ իրականացվում համակարգի խափանում: Նման խմբերը համացանցում գովազդում են իրենց ծառայությունները, ինչպես դա անում է բազմաթիվ երկրների ուժային կառույցներին հաքերային ծառայություններ մատուցող իտալական The Hacking Team հաքերային կազմակերպությունը, կամ էլ գործում են անոնիմ:

Հարձակումներ կատարող հաքերային խմբավորումները կարելի է բաժանել մի քանի տիպի[8].

- Իրենց «Սև գլխարկ» (Black Hat) անվանող վարձկան հաքերներ, որոնք պատրաստ են երրորդ կողմի պատվերով իրականացնել ցանկացած տիպի հարձակում:
- Սեփական պետությանը ծառայող հաքերներ, որոնք իրականացնում են հարձակումներ պետական պատվերով:
- Կիբերլրտեսներ, որոնք աշխատում են մեծ կորպորացիաների և կազմակերպված հանցավոր խմբերի պատվերով:
- Կիբերահաբեկիչներ, որոնք իրականացնում են գործողություններ նույն դրդապատճառներով, ինչ ավանդական ահաբեկչական խմբերը:
- Հաքտիվիստներ (hacktivist)՝ քաղաքական, կրոնական կամ հասարակական ոլորտների ակտիվիստներ, որոնք իրենց բողոքը դրսևորում են հաքերային հարձակումների միջոցով:

Հարձակվող խմբերի բազմազանությունն այնպիսին է, որ թիրախ կարող է հանդիսանալ յուրաքանչյուրը: Հաճախ օգտատերերը չեն պատկերացնում, թե ինչ պատճառով հաքերները կարող են իրենց թիրախավորել: Հասկանալի է, որ քաղաքական գործիչները, իրավապաշտպանները, բիզնեսմենները, լրագրողները կարող են հանդիսանալ անմիջական թիրախներ: Նույնիսկ համացանցի «շարքային» օգտատերը կարող է հանդիսանալ թիրախ, քանի որ. հաքերները հաճախ իրականացնում են զանգվածային ավտոմատացված հարձակումներ՝ հնարավորինս մեծ քանակի անձնական տվյալներին տիրանալու համար, և այդ պարագայում յուրաքանչյուրը կարող է տուժել հաքերային գրոհից:

---

[6] Ուսումնասիրությունը հիմնականում իրականացվել է «Նորավանք» գիտակրթական հիմնադրամի կողմից հրատարակված «Տեղեկատվական անվտանգություն» վերտառությամբ գրականությունից:

[7]Markets for Cybercrime Tools and Stolen Data. The RAND Corporation. 2014.
http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_ RR610.pdf

[8]Types of Hacker Motivations, https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

Այսօր շատերն էլեկտրոնային առևտուր են կատարում, և հարձակվողները փորձում են նրանցից գումար կորզել: Համացանցում ստեղծվում են տարատեսակ ծրագրեր և մեթոդներ, որոնց միջոցով հաքերները գումար են շորթում: Օրինակ, այսպես կոչված շորթող վիրուսների (Ransomware) միջոցով, որոնք համակարգչի ֆայլերը գաղտնագրում են, իսկ հաքերները դրանք վերադարձնում են տիրոջը միայն գումարի դիմաց, և նման հարձակումների թիվը ժամանակի հետ աճում է:

Հաքերային ծառայությունների սև շուկան այսօր բավական մատչելի է և թույլ է տալիս պատվիրել հարձակումներ յուրաքանչյուրին յուրաքանչյուրի դեմ:
Կիբերհանցագործություններ. Կիբերհանցագործությունները կիբերտարածքի ածանցյալն են՝ իրենց սև դրոշմը դնելով այն լավատեսության վրա, որն աշխարհին տվել էր համացանցը: Վերջին երկու տասնամյակներում նկատվել է կիբերհանցագործությունների, դրանցից բխող վնասների զգալի աճ[9]: «Գայթակղվելով մեծ շահույթներ ստանալու հեռանկարով՝ կիբերհանցագործությունների նորարարությունն ու մեթոդները հիրավի գերազանցել են անվտանգության ավանդական մոդելների և ստորագրության վրա հիմնված նույնականացման ժամանակակից տեխնոլոգիաների հնարավորությունները»[10]:

Առաջացել է ընդհատակյա բիզնեսի նոր տեսակ՝ կիբերհանցագործությունների կենտրոններ: Սրանք համացանցային կայքերի ստեղծման, ինտերնետային գովազդի, կայքերի տեղակայման և դոմենների գրանցման ծառայություններ առաջարկող օրինական ընկերություններ են, երբեմն մինչև 50 աշխատակիցներով: Վնասակար ծրագրեր ներբեռնելով իրենց միջոցով համացանցին միացած հարյուր հազարավոր համակարգիչներում՝ կիբերհանցագործ ընկերությունները հետզհետե այդ համակարգիչները վերածում են իրենց զոմբիների[11].

Վնասակար ծրագրի ներբեռնումը տեղի է ունենում տարբեր կեղծ առիթներով: Օրինակ, կիբերհանցագործներն ունեն մի շարք կայքեր, որտեղ այցելուներին առաջարկվում է իբրև թե անհրաժեշտ ծրագիր ներբեռնել առանց վճարման: Իրականում դա վնասակար ծրագիր է, որն ուղղորդում է դոմենի անվանման սերվերի ցուցիչը դեպի այլ տեղ՝ փոփոխելով օգտատիրոջ համացանցային գործողությունները և հանգեցնելով նրա գաղտնի տվյալների կորզման:

Որքան էլ զարմանալի է, կիբերհանցագործությունների զգալի մասը ոչ թե ֆինանսական օգուտներ քաղելու, այլ միայն վնաս հասցնելու նպատակով է կատարվում: Նույնքան զարմանալի է, որ կազմակերպություններից շատերն ավելի քիչ միջոցներ են հատկացնում կիբերպաշտպանությանը, քան իրենց սեփական աշխատակիցների կողմից

[9]55 FBI 2009 Cybercrime Statistics, ScamFraudAlert Blog, http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics/.
[10]Cyber Crime: A Clear and Present Danger, Deloitte, http://www.deloitte.com/view/en_GX/global/insights/thoughtleadership/c2ac85e761e58210VgnVCM100000ba42f00aRCRD.htm.
[11] Investigations on a Cybercrime Hub in Estonia, http://blog.trendmicro.com/investigationson-a-cybercrime-hub-in-Estonia.

համացանցի չարաշահման կանխմանը: Պահանջվող ռեսուրսների տեսանկյունից կիբերհանցագործությունը ոչ ծախսատար և ֆիզիկապես անվտանգ հանցագործությունն է: Դրանից բխող նորանոր վտանգներ են հայտնաբերվում: Համացանցի միջոցով կատարված հանցագործություն ների համապարփակ ցանկ կազմելն ուղղակի անհնար է: Ակնհայտ է, որ հաքերներին փոխարինման են գալիսկազմակերպված հանցախմբերը, իսկ կիբերպաշտպանության համար կատարած ծախսերը պարտադիր չէ, որ հանգեցնեն կիբերանվտանգության բարելավման:

Ստորև բերված աղյուսակ ներկայացված են համացանցի միջոցով կատարվող հանցագործությունների առավել տարածված տեսակները:

Գործողություն	***Նկարագրություն***
1. Կիբեռհեղինակազրկում	1. Զրույցներում (չաթերում), բլոգերում և կայքերում կեղծ տեղեկությունների տարածում:
2. Կիբեռհետևում	2. Անձի գործունեությանը հետևելը՝ համապատասխան տեղեկություններ պարունակող կայքեր կատարվող անկոչ այցելությունների միջոցով:
3. Կիբեռհետապնդում	3. Անձի նկատմամբ սպառնալիքներին հղումը՝ համացանցում կատարվող անանուն գրառումների միջոցով:
4. Վիրուսների տարածում	4. Էլեկտրոնային փոստի կամ կայքերի միջոցով վնասակար ծրագրերի տեղադրում:
5. Անձնավորում	5. Էլեկտրոնային փոստով կամ չաթում որպես այլ անձ ներկայանալը:
6. Անձի նույնականացման գողություն	6. Այլ անձանց մասին բավականաչափ անձնական տեղեկություններ հավաքելու միջոցով նրանց նույնականացման հափշտակումը:
7. Կեղծ աճուրդներ	7. Արժեքավոր ապրանքներ ցուցադրող, դրանց աճուրդներ կազմակերպող, վճարումներ հավաքող, բայց վաճառված ապրանքը երբեք չտրամադրող կայքեր:
8. Ֆինանսական բուրգ	8. Ներդրումների հավաքման սխեմա, որում տրված շռայլ խոստումները երբեք չեն կատարվում:
9. Կեղծ վիճակախաղեր	9. Վիճակախաղերի միջոցով վճարումների հավաքում հնարավոր շահումների դիմաց, որոնք երբեք չեն իրականանում:
10. Կեղծ առցանց խանութներ	10. Էլեկտրոնային առևտրի կայքեր, որոնք ստանում են վճարումները, սակայն փոխարենը ոչինչ չեն ուղակում գնորդին:
11. Վարկային քարտերի չարաշահում	11. Վավեր վարկային կամ դեբիտային քարտերի տվյալների օգտագործմամբ չարտոնված առցանց գնումների կատարում:
12. Կեղծ ծառայություններ	12. Բնորոշ տեսակներից են աստղագուշակությունը, տեխնիկական սպասարկումը, մասնավոր հետաքննության ծառայությունները, անձի տոհմաբանության հետազոտությունները, հակավիրուսային ծրագրերը:

Կիբերչարաշահումների միտումները. Միտումները ցույց են տալիս, որ կիբերհանցագործությունները տեղի են ունենում ոչ միայն կիբերչարաշահումների, այլ նաև նորարարական մեխանիզմներով իրականացվող անօրինականությունների ձևով, որոնք հայտնվում են համացանցում ամեն օր: Մեծ թվով շարժական հավելվածներ ստեղծվել են առանց անվտանգության նկատառումների, իսկ շատերը՝ կիբերհանցագործություն կատարելու նկատառումով[12]: Հանրությունն առանց երկար մտածելու ներբեռնում և տեղակայում է հավելվածներ, առանց իմանալու դրանց անվտանգության մակարդակը: Արդյունքում՝ վնասակար հավելվածները վարակում են օգտատիրոջ հեռախոսը, իսկ հետո նաև դրա հետ կապի մեջ գտնվող հեռախոսները՝ հասանելի դարձնելով դրանց պարունակությունը:

Ստորև բերված աղյուսակում ներկայացված են մեծ աճ արձանագրած կիբերչարաշահումները[13]:

Կիբեռհանցագործությունների կենտրոններ (կազմակերպված հանցախմբեր) Դոմենի անվանման կեղծ և վնասաբեր սերվերներ Ինտերնետ ծառայությունների կեղծ տրամադրողներ Գովազդների նենգափոխում «Զոմբիների» ստեղծում	**Թերագնահատում** Հնարավոր վնասի թերագնահատում Պաշտպանության ապահովման ծախսերի թերագնահատում
Ահաբեկչություն Հաղորդակցման ապահովում Անդամների հավաքագրում Ջրպարտում	**Չհրապարակվող իրադարձություններ** Պահպանվող տվյալների կորուստ Պահպանվող տվյալների բացահայտում
Լրտեսական գործունեություն Միջազգային Արդյունաբերական Քաղաքական	**Առցանց բանկային գործարքներ** Անօրինական գործարքներ Վնասակար ծրագրերի տեղադրում Անօրինականորեն ձեռք բերված դրամական միջոցների փոխանցում կատարողներ
Տեղեկությունների անօրինական հավաքում Միջազգային Ներքին Գործարար Անձնական	**Ընդհատակյա տնտեսական գործունեություն** Տեղեկատվության վաճառք Գրանցված տվյալների վաճառք Վնասակար ծրագրերի վաճառք Ստեղնաշարի հարվածները գրանցող ծրագրերի վաճառք
Փողերի լվացում Առցանց խաղամոլության միջոցով Առցանց բանկային գործարքների միջոցով Առցանց ներդրումների միջոցով	**Ընկերությունների իրազեկության բարձրացման կարիք** Պատրաստվածություն Ուսուցում Հանցագործությունների հայտնաբերում
Վավերացման ընթացքում որպես օրինական օգտատեր քողարկվելը Անձի նույնականացման գողություն Երթուղիչների (*URL*-ի՝ *Universal Resource Locator*-ի) սխալ ուղղորդում	**Կիբեռհանցագործություններ սոցիալական ցանցերում** Կեղծ ընկերներ Օգտատերերի տվյալների «որս» Վնասակար ծրագրերի տեղադրում Մոլորեցնող առաջարկություններ

[12] Best Practices for Designing Mobile Touch Screen Applications, User Centric News, http://www.usercentric.com/news/2011/06/15/best-practices-designing-mobile-touch-screen-applications., Mobile Application Design and Development, http://www.slideshare.net/ronnieliew/mo-bile-application-design-development-5465097.
Towards a Handbook for User-Centred Mobile Application Design, http://drops.dagstuhl.de/opus/voll-texte/2005/166/pdf/04441.SWM3.Paper.166.pdf.

[13] Cyber Crime: A Clear and Present Danger, Deloitte, http://www.deloitte.com/view/en_GX/glo-bal/insights/thought-leadership/c2ac85e761e58210VgnVCM100000ba42f00aRCRD.htm. Cybercriminals Target Online Banking Customers, M86 Security Lab, http://www.m86secu-rity.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf.

Կիբերհանցագործությունների դեմ պայքարը. Համացանցին միացած լինելն արդեն իսկ խոցելիություն է ստեղծում: Հետևապես, ճիշտ կլինի համացանցին միանալ միայն անհրաժեշտության դեպքում: Կիբերհանցագործությունների իրականացման դյուրինության պատճառով մարդկության ստեղծած հրաշալի գործիք համացանցը վերածվել է ականապատված դաշտի: Այնուհանդերձ, իրազեկությունը և պաշտպանող ծրագրերը կարող են նվազեցնել ռիսկերը: Կիբերհանցագործությունների դեմ պայքարը պետք է ուղղված լինի ոչ այնքան անվտանգության բարձրացմանը, որքան ռիսկերի նվազեցմանը: Այս երկու հասկացությունների միջև կա նուրբ, բայց էական տարբերություն: Առաջինը սահմանում է միայն միջոցները, իսկ երկրորդն՝ իրական նպատակն է:

Կորպորատիվ մակարդակում կիբերանվտանգությունը պետք է դիտարկել ոչ թե որպես տեխնիկական վարժություն, այլ որպես վերին օղակի ղեկավարության պարտականություն, որի կատարման համար պատասխանատվությունը դրվում է կազմակերպության անվտանգության համար պատասխանատու պաշտոնյայի վրա: Որպես այդպիսին՝ կիբերանվտանգությունը պետք է հանդիսանա վերին օղակի ղեկավարության ամենաառաջնահերթ խնդիրը:

Կիբերհանցագործություններից պաշտպանող համակարգչային բազմաթիվ ծրագրեր կան, որոնք զտում են կասկածելի կայքերը և թույլ տալիս միայն ընտրված կայքերի մուտքը և էլեկտրոնային փոստի հասցեատերերի հետ հաղորդակցումը: Այդ ծրագրերն ապահովում են «մուտքից և ելքից հաղորդագրությունների անվտանգությունը, արդյունավետ հակասպամային և հակավիրուսային պաշտպանությունը, պարունակության կատարելագործված զտումը, տվյալների կորստի կանխարգելումը և էլեկտրոնային փոստի գաղտնագրումը»[14]: Կորպորատիվ կիբերգործողություններից որևէ մեկը չի կարող աննշան համարվել կիբերանվտանգության տեսանկյունից: Այնուամենայնիվ, որոշ հարցեր հատուկ ուշադրություն են պահանջում կիբերհանցագործությունների մեծ ռիսկի պատճառով: Դրանցից մեկը գաղտնաբառերի կառավարումն է: Կիբերհանցագործությունների մի զգալի մասը տեղի է ունենում գաղտնաբառերի բացահայտման միջոցով: Կիբերհանցագործության այս տեսակի դեմ կարելի է պայքարել մեկանգամյա գաղտնաբառերի կիրառմամբ[15]:

[14] Brightmail Product Family, Symantec, http://www.symantec.com/business/products/fam-ily.jsp?familyid=brightmail.

[15] One-Time-Passwords, OTP, Nordic Edge, Inc., http://www.nordicedge.se.

Ստորև բերված աղյուսակում ներկայացված են կիբերհանցագործությունների համար առավել խոցելի չորս ուղղությունները.

Բնագավառը	*Մտահոգության առարկան*
Մուտքի կառավարում	Մուտքի լիազորությունների և մուտքի մեխանիզմների կառավարում, օրինակ՝ գաղտնաբառերի, կոդերի, օգտատերերի անունների տրամադրում և մեկանգամյա գաղտնաբառերի կիրառում:
Համացանցային ծրագրեր	Առցանց գործարքներ, կայքերի նավիգացիա, ինտրանետային (ներքին ցանցերի) պորտալներ: Մուտքի համակարգեր, միջինտերնետային կապ և համագործակցային գործիքներ, անվտանգության պարամետրեր:
Չվերահսկվող սարքեր և սարքավորումներ	Բանկոմատներ, ռադիոհաճախականային նույնականացման կապով քարտեր, *Wi-Fi* մուտքի սարքեր, *USB* կրիչներ:
Շարժական և ֆիքսված հեռախոսակապ	Շարժական հեռախոսակապի ծառայություններ, ձայնային կամ ստեղնաշարային ավտոմատացված փոխգործողություններ, ավտոմատ ձայնային պատասխան:

Կիբերհանցագործությունների դեմ պայքարում երկու ճակատ կա: Մեկը տեխնիկական հզորացումն է, այսինքն՝ մեր համակարգիչներում լավագույն հակավիրուսային լուծումներ տեղակայելը: Նման հուսալի ծրագրային լուծումներ կան անգամ համացանցի մուտքով բջջային հեռախոսների համար[16]: Ցավոք, կիբերհանցագործություններում կիրառվող վնասակար ծրագրերը տեխնոլոգիապես ավելի առաջադեմ են, իսկ դրանցից անվտանգություն ապահովող միջոցները 3-6 ամսով հետ են մնում: Պայքարի երկրորդ ճակատը համացանցով տարածվող խարդախությունների մասին մեր իրազեկությունն է և կիբերհանցագործների ծուղակներից խուսափելը:

Օրինակ, որոշ կայքերում ներկայացվում են ապրանքների և ծառայությունների աներևակայելի առաջարկներ: Ոմանք գումար են գանձում ձեր վարկային քարտից և երբեք չեն ուղարկում գնված ապրանքը: Այդ դեպքերում հարկավոր է տեղյակ պահել քարտը թողարկած ընկերությանը և փորձել հետ ստանալ գումարը: Սակայն էլեկտրոնային առևտրի որոշ այլ կեղծ կայքերում պատվերն ստանալուց հետո տեղեկացնում են, որ տվյալ ապրանքը վերջացել է և ձեր քարտից գումար չի գանձվի: Իսկապես, գումարը չի գանձվում, սակայն քարտի տվյալները վաճառվում են կիբերհանցագործներին: «Անվտանգության տեխնոլոգիաները մեզ կարող են միայն որոշակի տեղ հասցնել, իսկ մնացածը՝ համակարգիչների օգտատերերի քաջատեղյակության զգոնության հարց է»[17]:

[16] BullGuard Mobile Security 10, http://www.bullguard.com/products/bullguard-mobile-security-10.aspx.

[17] A Good Decade for Cybercrime, McAfee, http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf.

Կիբերհանցագործությունների դեմ պայքարին լծված բազմաթիվ կազմակերպություններ կան, և դրանց մասին տեղեկացվածությունը կարևոր է մեր սեփական պայքարում։

Ֆիզիկական աշխարհում կամ կիբերտարածքում կատարված հանցագործության բեռն ընկնում է տուժածի վրա։ Օրինակ, եթե ինչ–որ մեկը կեղծ քարտի միջոցով բանկոմատից գումար է գողանում ձեր հաշվից, ապա դրա պատասխանատվությունը պետք է կրի բանկը։ Սակայն եթե ինչ–որ մեկը, կիրառելով ստեղնաշարի սեղմումների հավաքածուի սխեման, ձեռք է բերում ձեր բանկային գաղտնագրերը և գումար շորթում ձեր հաշվից, ապա բանկը կարող է հրաժարվել կրած կորուստների համար պատասխանատվությունից, քանի որ «մուտքը համակարգ վավերական է եղել։ Բանկը պատասխանատու չէ հաճախորդի համակարգչի անվտանգության համար»[18]։

Ցանցային հիգիենայի կանոններ

Ինչպես հայտնի է, կիբերվտանգների 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 այլսարքերը 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 ծառա-յության գաղտնաբառը։ Նամակները կարող են գալ միանգամայն այլ հասցեից, ինչն ուշադիր լինելու պարագայում հեշտ բացահայտվում է։
- 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 դյուրինությամբ 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

[18]Cyber Crime Protection, http://www.safechecks.com/products/pdf/cyber_crime.pdf.

հասցեները՝ օգտվողի մոտ տպավորություն ստեղծելով, թե նա ուղղորդվում է դեպի լեգիտիմ կայք: Կեղծ կայքն արտաքնապես կարող է իդեալական կերպով նույնականացվել որևէ հայտնի սոցիալական ցանցի, էլեկտրո-նային փոստի, ինտերնետ խանութի արտաքին տեսքին: Իսկ հաս-ցեն 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)[19]: 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 «ֆեյսբուքյան վիրուսներ»:
- Ողջամտության սկզբունքից ելնելով՝ արժե հետևել հետևյալ պարզ կանոնին.նամակներով կամ մեսենջերով չուղարկել գաղտնաբառեր կամ անձնական գաղտնի այլ տվյալներ պարունակող տեղեկատ-վություն: Եթե ստիպված եք նման հաղորդագրություններ ուղար-կել, 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:

[19]How to recognize phishing email messages, links, or phone calls https://www.mi-crosoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx

Եզրակացություն և ամփոփում

Այսպիսով, 21-րդ դարում մարդիկ ապրում են միաժամանակ իրական և էլեկտրոնային կյանքում: Ինչպես իրական կյանքում, այդպես էլ էլեկտրոնայինում մենք ապահովագրված չենք հնարավոր սպառնացող վտանգներից:

Եթե իրական կյանքում մեզ կողոպտում են, սպառնում կամ ինչ-որ այլ վտանգի մեջ ենք հայտնվում, մենք ձեռնարկում ենք քայլեր և կիրառում ենք մեր հնարավոր բոլոր միջոցները՝ դրանցից պաշտպանվելու և խուսափելու համար: Այդպիսին է նաև էլեկտրոնային կյանքը, որտեղից կարող են կողոպտել մեր անձնական տվյալները, կոտրել մեր անձնական էջերը, սպառնալ, շանտաժի ենթարկել, ինչպես նաև տարբեր տեսակի խարդախությունների զոհ դարձնել:

Այս ամենից պաշտպանվելու և խուսափելու համար պետք է տիրապետ ենք համացանցային տարրական գիտելիքների, որոնց շնորհիվ պետք է ապահովենք մեր անվտանգությունը:

20-րդ դարի կեսերին տեղեկատվության դերի ու ծավալի աճին, ինչպես նաև տեղեկատվական տեխնոլոգիաների զարգացմանը զուգահեռ՝ավելացել են նաև տեղեկատվական անվտանգության սպառնալիքները, ուստի տեղեկատվության պաշտպանությունը դարձել է շատ պետությունների ներքին ու արտաքին քաղաքականության առաջնային ուղղություններից մեկը:

Տեղեկատվական անվտանգության ապահովման տեխնիկական մոտեցումը ենթադրում է առաջին հերթին մշակել կայքերի անվտանգության պահանջները, ինչպիսիք են՝ սերվերների պաշտպանությունը, լիցենզավորումը և այլն:

Քանի որ, համակարգիչները գնալով ինտեգրվում են բիզնեսի աշխարհում՝ անվտանգության փորձագետների համար աճում է պահանջարկը տվյալների անվտանգությունը պահպանելու և ընկերությունների սահուն գործունեությունը ապահովելու համար: ԱՄՆ աշխատանքի վիճակագրության բյուրոն գնահատում է[20], որ հաջորդ տասնամյակում Տեղեկատվական անվտանգության վերլուծաբանների պահանջարկը կաճի 28 տոկոսով: Դա շատ ավելի արագ է, քան բոլոր ոլորտների միջին աճը:

[20] Անվտանգության և տեղեկատվության ապահովում - Վիքիպեդիա՝ ազատ հանրագիտարան (wikipedia.org)

Առաջարկություններ

1. Մշակել պետության թվային անվտանգության ռազմավարություն, որից կբխի նաև կրթական հաստատություններում, մասնավորապես, տարրական, միջնակարգ և բարձրագույն ուսումնական հաստատություններում թվային անվտանգության ուսուցումը և ուսուցման կարգը։
2. Խրախուսել ոչ կառավարական կազմակերպությունների կողմից թվային անվտանգությանն ուղղված նախագծերի իրականացումը։
3. Դպրոցական դասագրքերի մեջ ներառել՝ թվային անվտանգությանը վերաբերող նյութեր՝ ինֆորմատիկա առարկայի ուսումնական պլանում։
4. Ուսուցիչներին հնարավորություն տալ վերապատրաստվելու և գիտելիքները փոխանցելու սերունդներին։
5. Իրականացնել գովազդային արշավներ և փողոցներում գովազդային պաստառների տեսքով փակցնել՝ «կարելի» և «չի կարելի»-ների մասին, որոնք վերաբերում են թվային անվտանգությանը։
6. Թվային անվտանգության վերաբերյալ ստեղծել ուսուցանող խաղեր և տրամադրել ուսումնական հաստատություններին, ժամանցի վայրերին, որտեղ այցելելով երիտասարդները կօգտվեն այդ հնարավորությունից։

Սույն ուսումնասիրությունն իրականացվել է «Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոց»» ծրագրի շրջանակում, «Բոլորը հանուն հավասար իրավունքների» հիմնադրամի կողմից, Եվրասիա համագործակցություն հիմնադրամի կողմից Շվեդիայի միջազգային զարգացման գործակալության, Միդայի աջակցությամբ իրականացվող «Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագրի շրջանակում:

Ուսումնասիրությունում ներկայացված բովանդակությունը կարող է չհամընկնել ծրագիրը ֆինանսավորող կողմերի դիրքորոշումների հետ:

Ուսումնասիրության աշխատանքային խումբ՝

Հնազանդ Մանուկյան, Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոցի շրջանավարտ,

Մարիամ Ադամյան, Էլեկտրոնային գրագիտության և թվային անվտանգության դպրոցի շրջանավարտ:

Գյումրի, 2022