Կիբերանվտանգություն.

միջավայրի վերլուծություն և կանխարգելիչ մեխանիզմներ

Կիբերանվտանգություն.

միջավայրի վերլուծություն և կանխարգելիչ մեխանիզմներ

Հեղինակներ՝ Դավիթ Շավքվելիձե եւ Գիորգի Գուրգենիձե

Վրացերենից աղբբեջաներեն թարգմանություն եւ խմբագրում. Ռամիլիա Ալիեւա

2023

Դասագրքի մասին

Սույն դասագիրքը մշակվել է «Վրաստանի տեղեկատվական և տեխնոլոգիաների վերլուծության կենտրոն»-ի կողմից (GITAC)՝ «Վրաստանի ռազմավարության և զարգացման կենտրոն»-ի պատվերով:

«Իրազեկ համայնքներ հանուն հզոր հասարակության» նախագիծն իրականացվում է ԱՄՆ դեսպանատան Ժողովրդավարության հանձնաժողովի Փոքր դրամաշնորհային ծրագրի աջակցությամբ, որի նպատակն է աջակցել Վրաստանում ազգային փոքրամասնությունների և բռնի ուժով գաղթականներով բնակեցված շրջաններում (Սամեգրելո, Սամցխե-Ջավախեթի, Քվեմո Քարթլի, Շիդա Քարթլի) ապրող հասարակության իրազեկվածության հզորացմանը՝ կիբեր և ապատեղեկատվական սպառնալիքների դեմ:

Դասագրքի մշակման ժամանակ կիրառվել է հանրությանը հասանելի, ոչ առևտրային գրականություն: Դասագրքի հիմնական մեթոդաբանական հիմքն է.

- ԱՄՆ կիբերանվտանգության և ենթակառուցվածքների գործակալության (US CISA) դասագրքեր
- ԱՄՆ Ստանդարտների և տեխնոլոգիաների ազգային ինստիտուտի (US NIST) դասագրքեր և եզրույթների պարզաբանումներ

- Մեծ Բրիտանիայի ազգային կիբերանվտանգության կենտրոնի (UK NCSC) դասագրքեր
- Կանադայի կիբերանվտանգության կենտրոնի (Canadian Centre for Cybersecurity) դասագրքեր
- Եվրոպական խորհրդի (CoE) դասագրքեր

Դասագրքի մշակման ընթացքում կիրառվել է նաև Վրաստանի գործող օրենսդրությունը՝ տեղեկատվական անվտանգության և անձնական տվյալների պաշտպանության վերաբերյալ:

Դասագրքում ներկայացված կիբերանվտանգության վերահսկումները և խորհուրդներն օգնում են նվազեցնել կիբեր ռիսկերը և կառավարել սպառնալիքները: Կարևորն այն է, որ դասագիրքը չի երաշխավորում պաշտպանություն բոլոր տեսակի կիբերհարձակումներից, սակայն ստորև նշված քայլերը զգալիորեն կնվազեցնեն Ձեր, Ձեր բիզնեսի կամ կազմակերպության կիբերհանցագործության զոհ դառնալու հավանականությունը:

Վրաստանի ռազմավարության և զարգացման կենտրոնի մասին

Վրաստանի ռազմավարության և զարգացման կենտրոնը (GCSD) անաչառ և չեզոք հասարակական կազմակերպություն է: Կազմակերպության արժեքները հիմնված են համահավասարության, մարդու ազատության, հարգանքի, հաշվետվողականության և թափանցիկության սկզբունքների վրա: Կենտրոնի հիմնական նպատակներն են՝ նպաստել Վրաստանի ազգային անվտանգությանը, երկրի արդյունավետ և ժողովրդավարական կառավարման սկզբունքների ամրապնդմանը, նրա եվրոպական և եվրատլանտյան

ինտեգրմանն աջակցմանը և երկրի կայուն զարգացման համար պայմանների ստեղծմանը:

Մանրամասն տեղեկությունների համար այցելեք՝
https://www.gcsd.org.ge/ge

Բովանդակություն

Եզրույթների պարզաբանում

Կիբերանվտանգություն - ներկայացնում է ցանցերի, սարքերի և տվյալների պաշտպանություն անօրինական գործողությունից, հասանելիությունից կամ հանցավոր օգտագործումից, որը բացահայտվում է տեղեկատվության գաղտնիության, ամբողջականության և մատչելիության ապահովման գործընթացով:

Գաղտնիություն - ապահովում է տվյալների հասանելիությունը միայն այն մարդկանց համար, որոնց այդ տեղեկատվությունն անհրաժեշտ է: Օրինակ, եթե Դուք համացանցում տեղեկատվություն տեղադրեք, ապա այն ընդմիշտ գոյություն կունենա:

Ամբողջականություն - ապահովում է տվյալների ճշգրտությունն ու ամբողջականությունը: Օրինակ՝ փոփոխված/խեղաթյուրված տվյալներն արժեք չունեն նրանց համար, որոնց անհրաժեշտ է այդ տեղեկատվությունը:

Մատչելիություն - ցանկացած պահին ապահովում է տեղեկատվության հասանելիություն բոլորի համար, որոնց անհրաժեշտ է այդ տեղեկատվությունը: Օրինակ, արագ և հուսալի կապն օգնում է համակարգչային ծրագրերին ավելի արդյունավետ աշխատել:

Հուզական տեղեկատվություն - կորցված տեղեկատվության չարաշահումը, փոփոխումը կամ չարտոնված մուտքը կարող է բացասաբար ազդել անհատի գաղտնիության, բարեկեցության, բիզնես-առևտրային գաղտնիքների կամ նույնիսկ ազգային անվտանգության կամ միջազգային հարաբերությունների վրա:

Անձնական տվյալներ - ցանկացած տեղեկատվություն, որով կարելի է պարզել անձի իսկությունը: Օրինակ՝ Ձեր անունը, ազգանունը, անձնական համարը, լուսանկարը, տեսագրությունը, էլ. փոստի հասցեն, բանկային հաշվեհամարը, սոցիալական ցանցի հաշիվը, անձնական նամակագրությունը: Անձնական տվյալ է նաև Ձեր աշխատավայրի, եկամուտի, ընտանեկան կարգավիճակի և այլնի մասին տեղեկատվությունը:

Հատուկ կատերգորիայի անձնական տվյալներ - տեղեկատվություն, որը կապված է անձի ռասայական կամ էթնիկ պատկանելիության, քաղաքական հայացքների, կրոնական կամ փիլիսոփայական համոզմունքների, մասնագիտական միության անդամակցության, առողջական վիճակի, սեռական կյանքի, դատվածության, վարչական կալանքի, խափանման միջոցի կիրառման, խափանման միջոցի կիրառման հետ կապված տեղեկատվության, հանցագործության զոհ ճանաչվելու կամ տուժող ճանաչվելու հետ:

Կենսաչափական ու գենետիկ տվյալներ - անձնական տվյալների հատուկ կատեգորիա, որը թույլ է տալիս ֆիզիկական անձին

նույնականացնել կենսաչափական և գենետիկական հատկանիշներով:

Mis-information (սխալ տեղեկատվություն) - ապատեղեկատվություն, որը տարածվել է առանց վնաս պատճառելու հիմունքով:

Dis-information (ապատեղեկատվություն) - ապատեղեկատվություն, որը տարածվել է վնաս պատճառելու հիմունքով:

Mal-information (վնասակար տեղեկատվություն) - վստահելի տեղեկատվություն, որը տարածվել է վնաս պատճառելու հիմունքով:

Վնասակար կոդ (Malware) - սահմանվում է որպես վնասակար ծրագիր, որը ներառում է լրտեսային ծրագիր (Spyware), թալանող ծրագիր (Ransomware), վիրուսներ (Virus) և (Worm) ճիճուներ:

Թալանող ծրագիր (Ransomware) - վնասակար ծրագրի ապահովման տեսակ, որը նախատեսված է արգելափակելու մուտքը համակարգչային ծրագիր՝ մինչև վճարումը կատարելը:

Սոցիալական ճարտարապետություն - զոհին մանիպուլյացիայի ենթարկելու, ազդելու կամ խաբելու մարտավարություն, որպեսզի հարձակվողը կարողանա վերահսկողություն հաստատել համակարգչային ծրագրի վրա, գողանալ անձնական կամ ֆինանսական տեղեկատվություն: Սոցիալական ճարտարագիտությունը կիրառում է հոգեբանական մանիպուլյացիա, որպեսզի հարձակվողը կարողանա հուզական

տեղեկատվության հասանելիություն ձեռք բերել կամ ստիպելու զոհին խախտել անվտանգության կանոնները/նորմերը:

Ֆիշինգ - վստահելի սուբյեկտ դառնալու նպատակով էլ. փոստի, SMS տեքստային հաղորդագրության կամ հեռախոսի միջոցով հուզական տեղեկատվություն, այդ թվում՝ սպառողի անուններ, գաղտնաբառեր և վարկային քարտի մանրամասներ, ստանալու փորձի գործընթացը կոչվում է Ֆիշինգ:

Վիշինգ (Vishing) - սոցիալական ճարտարագիտության տեսակ, որի ժամանակ կիրառվում է ձայնային հաղորդակցություն:

Սմիշինգ (Smishing) - սոցիալական ճարտարագիտության տեսակ, որի ժամանակ կիրառվում է SMS կամ տեքստային հաղորդագրություններ:

Denial of Service, Distributed Denial of Service - ծառայության անջատումը (Denial of Service) կիբերհարձակման տեսակներից է, երբ հարձակվողը ծանրաբեռնում է ցանցը կամ համակարգչային ծրագիրը, այնպես որ այն չի կարող պատասխանել օրինական պահանջներին: Հասանելի ծառայության մերժման (DDOS) հարձակումը ևս ծառայում է նույն նպատակին, սակայն նման դեպքում հարձակումը չի իրականացվում մեկ, այլ համակարգչային ցանցի միջոցով (բազմաթիվ տարբեր համակարգիչների ներգրավմամբ):

Man-in-the-middle - հարձակումը հայտնի է որպես հաքերի կողմից երկու սուբյեկտների միջև հաղորդակցության խափանում, ինչը թույլ է տալիս հարձակվողին (հաքերին) կարդալ և ստանալ կողմերի միջև փոխանակված տեղեկատվությունը:

Կիբեր հիգիենա - կրկնվող և ընդհանուր պրակտիկա, որոնք կօգնեն Ձեզ առցանց լինել անվտանգ:

Խոցելիություն - բացթողում տեղեկատվական համակարգում, համակարգի անվտանգության ընթացակարգերում, ներքին հսկողության կարգերում, որոնք կարող են առաջանալ կամ շահագործվել երրորդ կողմի կողմից (threat source):

Ծրագրային փաթչ (patch) - ծրագրային ապահովման բաղադրիչ, որն ինստալացիայի ժամանակ ուղղակիորեն փոխում է ֆայլերը կամ սարքի կարգավորումները, որը կապված է մեկ այլ ծրագրային ապահովման բաղադրիչի հետ՝ առանց համարի կամ համապատասխան ծրագրային բաղադրիչի թողարկման մանրամասների փոփոխության:

Բազմագործոն նույնականացում - կույնականացման գործընթաց՝ կիրառելով երկու կամ ավելի գործոն: Գործոնները ներառում են. (i) այն, ինչ գիտեք (օրինակ՝ գաղտնաբառը/անձնական նույնականացման համարը (PIN)); (ii) այն, ինչ ունեք (օրինակ՝ ծածկագրային նույնականացման սարք, թոքեն); կամ (iii) ինչ-որ բան, որը պատկանում է անձին (օրինակ՝ կենսաչափական տվյալներ):

Կոդավորում - տվյալների ծածկագրային փոխակերպում այսպես կոչված «պարզ տեքստից» այսպես կոչված «գաղտնագրված տեքստում», որը թաքցնում է տվյալների սկզբնական նշանակությունը՝ դրանց բացահայտումը կամ կիրառումը կանխելու համար: Եթե փոխակերպումը շրջելի է, ապա համապատասխան հակադարձման գործընթացը կոչվում է «գաղտնազերծում», որը վերափոխում է և գաղտնագրված տվյալները վերականգնում է իր սկզբնական վիճակին:

Պահեստային պատճեններ - անհրաժեշտության դեպքում վերականգնումը պարզեցնելու համար ստեղծված ֆայլերի և ծրագրերի պատճեն:

Ռոութեր - հաղորդակցման սարք, որը հաղորդագրություններ է փոխանցում երկու ցանցերի միջև:

1. Կիբերանվտանգության ընդհանուր սկզբունքներ

1.1. Ի՞նչ է կիբերանվտանգությունը

Կիբերանվտանգությունը ցանցերի, սարքերի և տվյալների պաշտպանությունն է անօրինական գործողությունից, հասանելիությունից կամ հանցավոր օգտագործումից, որն առաջանում է տեղեկատվության գաղտնիության, ամբողջականության և մատչելիության ապահովման գործընթացի միջոցով: Ձեր անձնական տվյալների մեծ մասը պահվում է Ձեր համակարգչում, սմարթֆոնում կամ փլանշետում: Կարևոր է իմանալը, թե ինչպես պաշտպանել Ձեր տեղեկատվությունը՝ ոչ միայն անհատների, այլ նաև կազմակերպությունների համար: Ամեն անգամ, երբ Դուք օգտագործվում եք համացանցից, հայտնվում եք անվտանգության ընտրության առջև: Ձեր և պետության անվտանգությունը կախված է առցանց տարածքում պատասխանատու որոշումներ ընդպլնելուց: Անվտանգ համացանց ունենալու համար անհրաժեշտ է, որ բոլորս գիտակցենք մեր կիբեր պատասխանատվությունը:

Ինչպես նշված է սահմանման մեջ, կիբերանվտանգության նպատակը տեղեկատվության գաղտնիության, ամբողջականության և մատչելիության ապահովումն է:

- **Գաղտնիություն** - ապահովում է տվյալների հասանելիությունը միայն այն մարդկանց համար, որոնց այդ տեղեկատվությունն անհրաժեշտ է: Օրինակ, եթե Դուք համացանցում տեղեկատվություն տեղադրեք, ապա այն ընդմիշտ գոյություն կունենա:
- **Ամբողջականություն** - ապահովում է տվյալների ճշգրտությունն ու ամբողջականությունը: Օրինակ՝ փոփոխված/խեղաթյուրված տվյալներն արժեք չունեն նրանց համար, որոնց անհրաժեշտ է այդ տեղեկատվությունը:
- **Մատչելիություն** - ցանկացած պահին ապահովում է տեղեկատվության հասանելիություն բոլորի համար,

որոնց անհրաժեշտ է այդ տեղեկատվությունը: Օրինակ, արագ և հուսալի կապն օգնում է համակարգչային ծրագրերին ավելի արդյունավետ աշխատել:

1.2. Վտանգներ

1.2.1. Վնասակար կոդ

Վնասակար կոդը (Malware) սահմանվում է որպես վնասակար ծրագիր, որը ներառում է լրտեսային ծրագիր (Spyware), թալանող ծրագիր (Ransomware), վիրուսներ (Virus) և (Worm) ճիճուներ: Վնասակար ծրագիրը կարող է գործարկվել այն ժամանակ, երբ օգտատերը կտտացնում է վնասակար էլ. փոստի կցորդը կամ հղումը, ինչը հանգեցնում է օգտատիրոջ համակարգչային ծրագրում վնասակար ծրագրի իստալացիային: Որոշ վնասակար ծրագրեր կարող են.

- Սահմանափակել մուտքը համակարգչային ցանցի կարևոր բաղադրիչներին՝ փրկագին ստանալու նպատակով (ransomware)
- Ապահովել նոր, լրացուցիչ վնասակար ծրագրերի իստալացումը

- Հաստատակամ սկավառակից գաղտնի տեղեկատվություն ստանալ (լրտեսային ծրագիր՝ spyware)
- Ոչնչացնել և անօգտագործելի դարձնել համակարգչային ծրագրի առանձին բաղադրիչներ:

1.2.2. Անձի առևանգում և խարդախություններ

Անձի առևանգումը (identity theft) և խարդախություններըը հանցագործություններ են, որոնց զոհ կարող են դառնալ նույնիսկ նրանք, որոնք երբեք չեն օգտվել համակարգչից: Կան բազմաթիվ ուղիներ, որոնցով հանցագործները կարող են հասանելիություն ձեռք բերել Ձեր տվյալների նկատմամբ, գողանալ Ձեր էլեկտրոնային դրամապանակը, գաղտնալսել Ձեր հեռախոսազանգերը, վերցնել Ձեր փաստաթուղթը, որի վրա նշված է Ձեր հաշվեհամարը:

1.2.3. Denial of Service

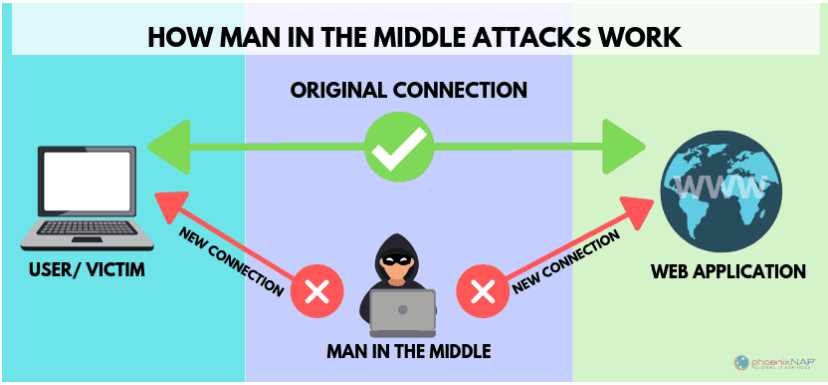
Ծառայության անջատումը (Denial of Service) կիբերհարձակման տեսակներից է, երբ հարձակվողը ծանրաբեռնում է ցանցը կամ համակարգչային ծրագիրը,

այնպես որ այն չի կարող պատասխանել օրինական պահանջներին: Հասանելի ծառայության մերժման (DDOS) հարձակումը ևս ծառայում է նույն նպատակին, սակայն նման դեպքում հարձակումը չի իրականացվում մեկ, այլ համակարգչային ցանցի միջոցով (բազմաթիվ տարբեր համակարգիչների ներգրավմամբ): Նման հարձակումները կարող են ծառայել նաև մեկ այլ նպատակի. կիբերհարձակվողը կարող է արդյունավետորեն կիրառել ժամանակը քանի ցանցն անկառավարելի է և սկսել հերթական հարձակումները:

Սրա հետ մեկտեղ, հարկ է նշել, որ գոյություն ունի բոթնեթ (botnet), որը DDoS հարձակման տեսակ է: Նման պահերին հարձակվողները (հաքերները) կարող են օգտագործել միլիոնավոր կոտրված (վտանգված) սարքեր: Բոթնեթները հաճախ հիշատակվում են նաև որպես զոմբի համակարգեր, որոնք հարձակվում են թիրախային համակարգերի վրա և փորձում են ծանրաբեռնել դրանց հնարավորությունները: Բոթնեթը կարող է տեղադրվել աշխարհի ցանկացած վայրում, ինչըն էլ դրա կառավարումն էլ ավելի է բարդացնում:

1.2.4. Man in the Middle

Man-in-the-middle հարձակումը հայտնի է որպես հաքերի կողմից երկու սուբյեկտների միջև հաղորդակցության խափանում, ինչը թույլ է տալիս հարձակվողին (հաքերին) կարդալ և ստանալ կողմերի միջև փոխանակված տեղեկատվությունը: MITM հարձակումները հաճախակի են լինում այն ժամանակ, երբ այցելուները միանում են անապահով (չկոդավորված) հանրային Wi-Fi ցանցին:



1.2.5. Phishing

Ֆիշինգ է կոչվում վստահելի սուբյեկտ դառնալու նպատակով էլ. փոստի, SMS տեքստային հաղորդագրության կամ հեռախոսի միջոցով հուզական տեղեկատվություն, այդ թվում՝ սպառողի անուններ, գաղտնաբառեր և վարկային քարտի մանրամասներ, ստանալու փորձի գործընթացը:

Ֆիշինգայինի հարձակման ժամանակ հարձակվողը հրատապության, հետաքրքրասիրության կամ վախի զգացում է առաջացնում: Ֆիշինգային հաղորդագրությունները ստիպում են զոհերին տրամադրել հուզական տեղեկատվություն, սեղմել վնասակար կայքերի հղումներին կամ բացել քաղվածքները, որոնք պարունակում են վնասակար ծրագրեր:

1.2.6. Գաղտնաբառի կոտրում (Password Cracking)

Կիբերհարձակվողը հեշտությամբ կարող է ստանալ բազմաթիվ տեղեկություններ, եթե ձեռք է բերում օգտատիրոջ գաղտնաբառը: Գաղտնաբառը կոտրելու տարբեր եղանակներ գոյություն ունեն.

- **Ուրակավորում (brute force attack)** - հաքերը պարզապես կռահում է օգտատիրոջ գաղտնաբառը՝ հիմնվելով համապատասխան հուշումների վրա (օրինակ՝ ծննդյան օր, շան անուն և այլն), սակայն ուրակավորված հարձակումը կարող է լինել ավելի խիստ մտածված ու բարդ: Օրինակ, շատ մարդիկ օգտագործում են նույն գաղտնաբառը տարբեր

համակարգերի համար: Որոշ գաղտնաբառեր կարող են առցանց հասանելի լինել կոտրված (բացահայտված) կայքերի տվյալների բազաներում, և այդպիսով հաքերը կարող է օգտագործել Ձեր բացահայտված գաղտնաբառը այլ համակարգեր կոտրելու համար:

- **Բառարանային հարձակում (Dictionary attack)** - բառարանային հարձակումը որակավորված հարձակումից (brute force attack) մի փոքր ավելի ձևավորված օրինակն է: Այն օգտագործում է ավտոմատացված գործընթաց, երբ հարձակվողը փորձում է գուշակել Ձեր գաղտնաբառը՝ հիմնվելով հաճախ օգտագործվող գաղտնաբառերի և արտահայտությունների ցանկի վրա (օրինակ՝ շատ օգտատերեր օգտագործում են հետևյալ գաղտնաբառերը՝ 123456, qwerty, password, etc.): Բառարանների մեծ մասը բաղկացած է ամենատարածված գաղտնաբառերից և բառակապակցություններից: Մարդիկ հաճախ որպես գաղտնաբառ օգտագործում են հիշվող արտահայտություններ, որոնք սովորաբար

ներկայացված են որպես բառեր: Հիմնականում սա է պատճառը, որ համակարգերը խրախուսում են մարդկանց օգտագործել բազմանիշ գաղտնաբառեր:

1.3. Պաշտպանության մեխանիզմներ՝ կիբեր հիգիենա

1.3.1. Կիբեր հիգիենան դարձրեք Ձեր առօրյայի մի մասը

Ձեր կիբերանվտանգության կանոնավոր մոնիթորինգը նվազեցնում է կիբեր սպառնալիքների իրացման ռիսկերը: Ինչպես ցանկացած սովորություն, կիբեր հիգիենան ևս պահանջում է ռեժիմ և կրկնություն:

Կիբեր հիգիենայի գործընթացը սկսեք այսպես կոչված «հիշեցման» (Reminder) սահմանմամբ կամ նշեք ամսաթվերն օրացույցում, որպեսզի Ձեր սարքի հետ կապված մի շարք առաջադրանքներ կատարելու համար սկանավորեք հակավիրուսային ծրագիրը, թարմացնեք Ձեր բոլոր սարքերի օպերացիոն համակարգերը, ստուգեք անվտանգության փաթչերը, ջնջեք Ձեր կոշտ սկավառակը և փոխեք Ձեր գաղտնաբառերը:

1.3.2. Կիբեր հիգիենայի համար հիմնական քայլեր

Կիբեր հիգիենան դա ընդհանուր պրակտիկա է, որը կօգնեն Ձեզ առցանց լինել անվտանգ: Սույն փաստաթղթում ներկայացված է կիբեր հիգիենայի լավագույն փորձի օրինակ, որը ներառում է ինը կարևոր քայլ:

Քայլ 1՝ Ապահովեք վստահելի հակավիրուսային ծրագրի ինստալացիան

Առաջին և, հավանաբար, ամենակարևոր քայլը հակավիրուսային ծրագիր ներբեռնելն է: Ինչի՞ համար է այն ստեղծված: Հակավիրուսային ծրագիրը ծրագիր կամ ծրագրերի միություն է, որը սկանավորում և գտնում է համակարգչային վիրուսներ կամ այլ վնասակար ծրագրեր: Մասնավորապես, հակավիրուսային ծրագիրն ապահովում է.

- Գտնել այն թղթապանակները, որոնք պարունակում են վնասակար կոդ (ծրագիր)
- Ավտոմատ կերպով սկանավորման պլանավորում և իրագործում
- Մեկ կոնկրետ թղթապանակի, Ձեր ամբողջ համակարգչի կամ ֆրեշ դրայվի սկանավորում՝ ելնելով Ձեր կոնկրետ անհրաժեշտությունից

- Վնասակար և ծրագրային ապահովման ջննջում:

Քայլ 2՝ Կիրառեք «Ֆաերվոլ» ցանցը

Firewall-ի կիրառումը ևս մեկ գլխավոր քայլ է կիբեր հիգիենան պաշտպանելու համար: Firewalls դա պաշտպանության առաջին հնարքն է ցանցի անվտանգության առումով, ինչը խոչընդոտում է որակավորում չունեցող օգտատիրոջ հասանելիությունը Ձեր վեբ-կայքերի, էլ. հասցեի սերվերների և տեղեկատվական այլ աղբյուրների նկատմամբ, որոնց նկատմամբ հասանլիություն կարելի է ձեռք բերել հենց համացանցում:

Քայլ 3՝ Պարբերաբար թարմացրեք ծրագրային ապահովությունը

Պարբերաբար թարմացրեք Ձեր հավելվածները, վեբ բրաուզերները և օպերացիոն համակարգերը՝ համոզվելու համար, որ Դուք աշխատում եք ամենավերջին ծրագրերով, որոնք կանխում կամ շտկում են անվտանգության բացթողումները (խոցելիությունները): Այս թարմացումները հատկապես կարևոր են, քանի որ դրանք հաճախ պարունակում են ծրագրային ապահովման փաթչեր (patch):

Ծրագրային ապահովման մշակողները (հավելված ստեղծող ընկերությունները) թողարկում /հրապարակում են անվտանգության փաթեչեր այն ժամանակ, երբ հայտնաբերում են ծրագրային ապահովման բացթողումներ, որոնք հարձակվող հաքերներն օգտագործում են համակարգեր ներթափանցելու համար:

Քայլ 4՝ Օգտագործեք բարդ գաղտնաբառեր

Ձեր բոլոր սարքերի համար բարդ գաղտնաբառեր սահմանելը կարևոր է: Ձեր գաղտնաբառը պետք է լինի եզակի և բարդ, պարունակի առնվազն 12 նիշ, ներառյալ թվեր, նշաններ և մեծ ու փոքր տառեր: Ձեր գաղտնաբառը կանոնավոր կերպով փոխելը (և չկիսվել կամ կրկին օգտագործել) պաշտպանում է Ձեզ հաքերներից:

Քայլ 5՝ Օգտագործեք բազմագործոն նույնականացումը

Երկգործոն կամ բազմագործոն նույնականացումը լավագույն փորձն է, որն առաջարկում է պաշտպանության հավելյալ միջոց: Երկգործոն նույնականացումը սովորաբար պահանջում է, որ Դուք տրամադրեք Ձեր գաղտնաբառը և

օգտանունը եզակի կոդով, որն ուղարկվում է Ձեր բջջային հեռախոսին: Բազմագործոն նույնականացումը, օգտագործելով կենսաչափական տվյալները, ավելացնում է անվտանգության լրացուցիչ շերտեր, ինչպիսիք են դեմքի կամ մատնահետքի ճանաչում, որպեսզի հաքերների համար դժվարացնի մուտքը Ձեր սարք և անձնական տվյալներ:

Քայլ 6՝ Օգտագործեք սարքի կոդավորումը

Չնայած այն բանին, որ շատ ընկերություններ ունեն ավտոմատ կերպով տվյալների կոդավորման գործառույթ, կարող է անհրաժեշտ լինի Ձեր սարքերի և այլ կրիչների (օրինակ՝ USB, flash drive) կոդավորում, որոնք պարունակում են հուզական տվյալներ՝ այդ թվում՝ նոութբուքեր, փլանշեթներ, սմարթֆոններ, կրիչներ, պահեստային թղթապանակներ և cloud: Հաճախ շատ սարքեր օգտագործում են կոդավորումը՝ որպես սմարթֆոններում պահվող տվյալների լռելյայն հատկություն: Որոշ հավելվածներ օգտագործում են ամբողջական կոդավորում, մինչդեռ այլ ծառայություններ կոդավորում են Ձեր սարքերի տվյալները և պահեստավորում դրանք cloud-ի մեջ: Հավելյալ տարբերակ է

նաև կոդավորված USB հիշողության քարտի կիրառումը՝ հուզական տվյալները պաշտպանելու համար:

Քայլ 7՝ Պարբերաբար ստեղծեք պահեստային պատճեններ

Կարևոր է, որ Ձեր արժեքավոր թղթապանակները պահեստավորել օֆլայն, արտաքին կոշտ սկավառակի վրա կամ քլաուդի մեջ: Սա կօգնի Ձեզ պաշտպանել Ձեր կարևոր թղթապանակները տարբեր տեսակի տվյալների կորստի ռիսկերից, հատկապես, եթե հաքերները հասանելիություն ձեռք բերեն Ձեր սարքերից որևէ մեկի նկատմամբ:

Քայլ 8՝ Մաքրեք կոշտ սկավառակը

Եթե Դուք վաճառում եք Ձեր սեփական նոութբուքը, փլանշեթը կամ սմարթֆոնը, ապա կարևոր է անվտանգության միջոցներ ձեռնարկել՝ կանխելու Ձեր մասին անձնական կամ հուզական տեղեկությունները գնորդի ձեռքն ընկնելու համար: Եթե կոտրեն Ձեր սարքը, մաքուր կոշտ սկավառակը նշանակում է ավելի քիչ տեղեկատվություն հարձակվողների համար: Սակայն, հնարավոր է, որ միայն թղթապանակների կամ տվյալների հեռացումը բավարար չլինել: Լավ կիբեր

հիգիենայի համար անհրաժեշտ է ֆորմատավորել սկավառակը և մաքրել (wipe out): Օրինակ, եթե ցանկանում եք վաճառել ձեր համակարգիչը, որն օգտագործում էիք առցանց բանկային ծառայության համար, պետք է հաշվի առնեք սկավառակը մաքրելու մասին՝ Ձեր կոշտ սկավառակից հեռացնելու բոլոր ծրագրերն ու տվյալները:

Քայլ 9՝ Պաշտպանեք Ձեր րոութերը

Չմոռանաք պաշտպանել Ձեր անլար ցանցը: Դա անելու համար անհրաժեշտ է փոխել հիշատակված անունը և գաղտնաբառը, որը րոութերի վրա նշված է արտադրողի կողմից: Ինչպես նաև տեղադրելուց հետո անհրաժեշտ է անջատել հեռակառավարման գործառույթը: Բացի այդ, համոզվեք, որ Ձեր րոութերն առաջարկում է WPA2 կամ WPA3 կոդավորում՝ ցանցով ուղարկվող տեղեկատվության գաղտնիության ամենաբարձր մակարդակը պահպանելու համար:

1.4. Կիբերանվտանգությունը փոքր և միջին կազմակերպությունների համար

Այս դասագրքում տրված են հինգ արագ և հեշտ քայլեր, որոնք կօգնեն Ձեզ խնայել ժամանակ, գումար և պաշտպանել Ձեր կազմակերպության հեղինակությունը: Դասագիրքը չի երաշխավորում պաշտպանություն բոլոր տեսակի կիբերհարձակումներից, սակայն ստորև բերված քայլերը զգալիորեն կնվազեցնեն Ձեր բիզնեսի/կազմակերպության կիբերհանցագործության զոհ դառնալու ռիսկը:

1.4.1. Քայլ 1՝ Ձեր տվյալների պահեստային պատճենի ստեղծում

Մտածեք, թե որքանով է Ձեր կազմակերպությունը կախված այնպիսի կարևոր տվյալներից, ինչպիսիք են հաճախորդի/քաղաքացու տվյալները, պատվերները և վճարման մանրամասները: Հիմա պատկերացրեք, թե որքան ժամանակ կարող եք աշխատել առանց դրանց:

Յուրաքանչյուր ձեռնարկություն կամ կազմակերպություն, անկախ չափից, պետք է մշակի կարևոր տեղեկատվության

պահեստավորման պատճենները և պետք է վստահ լինի, որ այդ պահեստային պատճենները վերջնականն են (up-to-date) և անհրաժեշտության դեպքում կարելի է վերականգնել: Սրանով Դուք վստահ կապացուցվեք, որ Ձեր կազմակերպությունը կարող է շարունակել գործել նույնիսկ այնպիսի իրադարձություններից հետո, ինչպիսիք են ջրհեղեղները, հրդեհները, ֆիզիկական վնասը կամ գողությունը: Բացի այդ, եթե Դուք ունեք տվյալների պահեստային պատճեններ, որոնք կարող եք արագ վերականգնել, Ձեր կազմակերպությունն ավելի քիչ խոցելի է փրկագինների հարձակումների նկատմամբ (ransomware attacks):

Ներկայացված գլուխները տալիս են հինգ խորհուրդ, որոնք պետք է հիշել պահեստային պատճեններ կազմելիս:

Խորհուրդ 1՝ Սահմանեք անհրաժեշտ պահեստային պատճենները

Առաջին քայլը Ձեզ համար կարևոր նշանակություն ունեցող տվյալները բացահայտելն է: Այսինքն՝ տեղեկատվություն, առանց որի Ձեր բիզնեսը չի կարող գործել: Սովորաբար, դա

ներառում է փաստաթղթեր, լուսանկարներ, էլ. հասցե, կոնտակտներ և օրացույցներ, որոնց մեծ մասը պահվում է Ձեր համակարգչի, հեռախոսի, փլանշետի կամ ցանցի մի քանի սովորական թղթապանակներում:

Խորհուրդ 2՝ Պահեք պահեստային պատճենները համակարգից առանձին

Դա կլինի USB կրիչ, առանձին սկավառակ թե ուրիշ համակարգիչ, տվյալների պահեստային պատճենների նկատմամբ հասանալիությունը պետք է սահմանափակվի այնպես, որ դրանք.

- ¬ Հասանելի չլինեն անձնակազմի համար
- ¬ Ոչ միշտ են միացված (ֆիզիկապես կամ տեղանքային ցանցին) սարքին, որն ունի բնօրինակ
- ¬ Ransomware (և այլ վնասակար ծրագիր) հաճախ այն կարող է ավտոմատ կերպով տեղափոխվել կցված պահեստ, ինչը նշանակում է, որ ցանկացած նման պահեստավորված պատճեն կարող է նաև վիրուսոտվել և հնարավոր չլինի վերականգնել պահեստավորված պատճենը: Ավելի խելացի գտնվելու համար, Դուք պետք է

մտածեք Ձեր պահեստավորված պատճեններն մեկ այլ տեղ պահելու մասին: Այդ կերպ հրդեհը կամ գողությունը չեն հանգեցնի երկու օրինակների կորստի: Դրան հասնելու համար քլաուդային պահեստավորման լուծումները (տես ստորև) տնտեսական և արդյունավետ միջոց են:

Խորհուրդ 3՝ Հաշվի առեք քլաուդ պահեստը

Հավանաբար, Դուք արդեն օգտագործում եք այսպես կոչված քլաուդային պահեստավորումը Ձեր առօրյա աշխատանքում և անձնական կյանքում՝ առանց նույնիսկ դրա մասին իմանալու: Ինչպես կարգն է, եթե Դուք չունեք Ձեր էլ.հասցեի սերվերը, Ձեր էլ.հասցեն արդեն պահվում է այսպես կոչված քլաուդի մեջ:

Քլաուդային պահեստի օգտագործումը (որտեղ ծառայություններ մատուցողը պահում է Ձեր տվյալներն իր ենթակառուցվածքում) նշանակում է, որ Ձեր տվյալները ֆիզիկապես առանձնացված են Ձեր գտնվելու վայրից: Նման դեպքում Դուք նույնպես կշահեք մատչելիության բարձր աստիճանից: Ծառայությունների փրովայդերները կարող են

Ձեր կազմակերպությանը տրամադրել տվյալներ և վեբ ծառայություններ՝ առանց նախապես թանկարժեք սարքավորումներում ներդրումներ կատարելու: Փրովայդերներից շատերն առաջարկում են սահմանափակ քանակությամբ անվճար պահեստային տարածք (օրինակ՝ Google Drive-ն առաջարկում է մինչև 15 ԳԲ անվճար տարածք) և փոքր բիզնեսի համար ավելի մեծ պահեստային հզորություններ՝ նվազագույն ծախսերով:

Խորհուրդ 4՝ Կարդացեք քլաուդային անվտանգության հրահանգը

Ոչ բոլոր ծառայությունների փրովայդերներն են նույնը, սակայն շուկան բավականին հասուն է, և փրովայդերների մեծամասնությունը ճիշտ ներկառուցված անվտանգության լավ փորձ ունի: Ձեր IT ծառայությունների կարևոր մասերը փրովայդերներին փոխանցելով՝ Դուք կարող եք օգտվել մասնագիտացված փորձից, որը հաճախ հասանելի չէ փոքր և միջին կազմակերպությունների համար: Սակայն, նախքան փրովայդերների հետ կապ հաստատելը, խորհուրդ ենք տալիս ծանոթանալ քլաուդային անվտանգության միջազգային փորձին:

Խորհուրդ 5՝ Պահեստային պատճենի ստեղծումը դարձրեք Ձեր առօրյա բիզնեսի մասը

Կազմակերպությունների համար պահեստային պատճենների ստեղծումն այնքան էլ հետաքրքիր գործընթաց չէ (և միշտ կլինեն ավելի կարևոր առաջադրանքներ, որոնք, ըստ Ձեզ, պետք է առաջնահերթ լինեն), սակայն ցանցային կամ քլաուդային պահեստավորման լուծումների մեծ մասն այժմ թույլ է տալիս ավտոմատ կերպով ստեղծել պահեստային պատճեններ: Օրինակ, երբ որոշ տեսակի նոր ֆայլեր պահվում են նշված թղթապանակներում: Ավտոմատ պահեստային պատճենների օգտագործումը ոչ միայն խնայում է Ձեր ժամանակը, այլ նաև ապահովում է Ձեր ֆայլերի վերջին տարբերակը, որպեսզի անհրաժեշտության դեպքում այն դրանք կիրառեք:

Պահուստային շատ լուծումներ (back-up solution) պարզ և մատչելի են՝ հաշվի առնելով բիզնեսի համար կարևոր անվտանգության վերահսկումները: Լուծում (ծրագրային ապահովում) ընտրելիս պետք է նաև հաշվի առնել, թե որքան տվյալների պահեստավորված պատճեններ պետք է ստեղծեք

և որքան արագ պետք է կարողանաք մուտք գործել տվյալներ ցանկացած միջադեպից հետո:

1.4.2. Քայլ 2՝ Ձեր կազմակերպության պաշտպանումը վնասակար ծրագրերից

Վնասակար ծրագրի ապահովումը (ինչպես նաև հայտնի է որպես «վնասակար ծրագիր») դա ծրագրային ապահովում կամ վեբ բովանդակություն է, որը կարող է վնասել Ձեր կազմակերպությանը: Վնասակար ծրագրերի ամենահայտնի ձևը վիրուսներն են, ինքնապատճենվող ծրագրերը, որոնք վարակում են օրինական ծրագրերը:

Հետևյալ գլուխները պարունակում են հինգ անվճար և հեշտ իրագործելի խորհուրդներ, որոնք կօգնեն կանխել վնասակար ծրագրերը Ձեր կազմակերպությանը վնասելուց:

Խորհուրդ 1՝ Ինստալացրեք և/կամ միացրեք հակավիրուսային ծրագիր

Հակավիրուսային ծրագիրը, որը հաճախ անվճար ներառված է հանրաճանաչ օպերացիոն համակարգերում, պետք է

օգտագործվի բոլոր համակարգիչների և լեփթոփի վրա: Ձեր գրասենյակային սարքավորումների համար կարող եք սեղմել «Միացնել», որով ծրագիրը կակտիվացվի:

Խորհուրդ 2՝ Սահմանափակեք անձնակազմին արգելված հավելվածների ներբեռնումը

Բջջային հեռախոսների և փլանշեթների համար հավելվածները պետք է ներբեռնեք միայն արտադրողի կողմից հաստատված, այսպես կոչված «մարքեթփլեյսներից» (օրինակ՝ Google Play-ից կամ Apple App Store-ից): Հավելվածներն այստեղ փորձարկվում են վնասակար ծրագրերից պաշտպանվածության որոշակի մակարդակ ապահովելու համար: Դուք պետք է սահմանափակեք անձնակազմին անհայտ վաճառողներից անվստահելի (երրորդ կողմի) հավելվածներ ներբեռնելը:

Կազմակերպության անձնակազմի հաշիվները պետք է ունենան բավարար հասանելիություն, որն անհրաժեշտ է իրենց դերը կատարելու համար, և լրացուցիչ թույլտվություններ (օրինակ՝ ադմինիստրատորի իրավունքները) պետք է տրվեն միայն նրանց, ովքեր դրանց

կարիքն ունեն: Երբ ստեղծվում են ադմինիստրատիվ հաշիվներ (accounts), դրանք պետք է օգտագործվեն միայն այս հատուկ առաջադրանքի (կառավարման) համար, իսկ սովորական օգտատերերի հաշիվները պետք է օգտագործվեն ընդհանուր աշխատանքի համար:

Խորհուրդ 3՝ Նորացրեք Ձեր ողջ IT ենթակառուցվածքը (փաթչինգը)

Համոզվեք, որ Ձեր IT ենթակառուցվածքը (օրինակ՝ թաբլեթներ, սմարթֆոններ, նոութբուքեր և համակարգիչներ) համահունչ է մշակողների, սարքավորումների մատակարարների և վաճառողների վերջին տարբերակների հետ: Այս թարմացումների կիրառումը (գործընթաց, որը հայտնի է որպես փաթչինգ) ամենակարևոր բաներից մեկն է, որ կարող եք անել՝ բարելավելու Ձեր անվտանգությունը: Օպերացիոն համակարգերը, ծրագրերը, հեռախոսները և հավելվածները պետք է հասանելի լինեն «ավտոմատ թարմացման» համար:

Հատկանշական է, որ ինչ-որ պահի թարմացումներն այլևս հասանելի չեն լինի (քանի որ բոլոր ապրանքներն ունեն

աջակցության ծառայության կյանքի ցիկլ), որի ժամանակ դուք պետք է մտածեք այն փոխարինելու ժամանակակից այլընտրանքով:

Խորհուրդ 4՝ Վերահսկեք USB կրիչներն ու հիշողության քարտերի կիրառումը

Բոլորս գիտենք, թե որքան կարևոր է օգտագործել USB կրիչներ կամ հիշողության քարտեր՝ կազմակերպությունների և մարդկանց միջև թղթապանակներ փոխանցելու համար: Սակայն մեկ օգտատիրոջ կողմից վարակված USB ֆլեշ հիշողության քարտի օգտագործումը բավական է ամբողջ կազմակերպության տեղեկատվությունը ոչնչացնելու համար:

Երբ կրիչներն ու ֆլեշ հիշողության քարտերը բաց են կիսվում, դժվար է հետևել, թե ինչ կա դրանց վրա կամ ով է օգտագործել դրանք: Դուք կարող եք նվազեցնել վարակի (վիրուսների) հավանականությունը հետևյալ եղանակներով.

- Օգտատերերի մեծամասնության համար ֆիզիկական մուտքն արգելափակելու միջոցով
- Հակավիրուսային միջոցների կիրառմամբ
- Օգտագործել միայն հաստատված կրիչներ և քարտեր Ձեր կազմակերպության ներսում, և ոչ այլուր:

Այս հրահանգները դարձրեք Ձեր կազմակերպության/ընկերության քաղաքականության մի մասը, որպեսզի կարողանաք խուսափել Ձեր կազմակերպության համար անցանկալի ռիսկերից: Կարող եք նաև խնդրել անձնակազմին թղթապանակները փոխանցել այլընտրանքային միջոցներով (ինչպիսին են էլ. հասցեն կամ քլաուդային ծառայությունները), այլ ոչ թե USB ֆլեշ հիշողության քարտ օգտագործելու:

Խորհուրդ 5՝ Միացրեք Ձեր firewall

Firewall-ները ստեղծում են «բուֆերային գոտի» Ձեր սեփական ցանցի և արտաքին ցանցերի (օրինակ՝ համացանցի) միջև: Ամենահայտնի օպերացիոն համակարգերն այժմ ներառում են firewall:

1.4.3. Քայլ 3՝ Ձեր սմարթֆոնների և թաբլեթների անվտանգության պաշտպանություն

Բջջային տեխնոլոգիան այժմ ժամանակակից կազմակերպության/բիզնեսի էական մասն է: Մեր տվյալների մեծ մասը պահվում է փլանշեթներում և սմարթֆոններում:

Ավելին, այս սարքերն այժմ նույնքան հզոր են, որքան ավանդական համակարգիչները, և քանի որ դրանք հաճախ հեռանում են գրասենյակի և տան անվտանգությունից, նրանք ավելի շատ պաշտպանության կարիք ունեն, քան «սղեքստոփային» սարքավորումները:

Հաշվի առնելով դա՝ հաջորդ գլուխներում կգտնեք 5 խորհուրդներ, որոնք կօգնեն Ձեզ անվտանգ պահել Ձեր բջջային սարքերը և դրանցում պահվող տեղեկատվությունը:

Խորհուրդ 1՝ Ակտիվացրեք գաղտնաբառով պաշտպանությունը

Համապատասխան բարդ PIN-ը կամ գաղտնաբառը (ոչ այն, որը կարելի է գուշակել կամ նույնականացնել Ձեր սոցիալական մեդիայի էջերից) թույլ չի տա միջին մակարդակի հանցագործին մուտք գործել Ձեր հեռախոս: Այսօր շատ սարքեր ունեն մատնահետքի ճանաչում՝ Ձեր սարքն առանց գաղտնաբառ պահանջելու փակելու համար: Սակայն, այս գործառույթները միշտ չէ, որ ակտիվացված են, այնպես որ ստուգեք, արդյոք դրանք ակտիվացված են:

Խորհուրդ 2՝ Վստահ եղեք, որ հնարավոր է կորսված կամ գողացված սարքերին հետևելը, արգելափակելը կան ջնջելը

Աշխատակիցների փլանշեթները կամ հեռախոսները կարող են կորսվել կամ գողանալ: Բարեբախտաբար, սարքերից շատերն ունեն անվճար վեբ գործիքներ, որոնք սարքի կորցնելու պարագայում դառնում են անգնահատելի: Դուք կարող եք կիրառել դրանք, որպեսզի

- Վերահսկեք սարքի գտնվելու վայրը
- Հեռավար կարգով անջատեք սարքի նկատմամբ հասանելիությունը
- Հեռավար կարգով ջնջեք սարքում պահված տվյալները
- Ստանաք սարքում պահված տվյալների պահեստային պատճենը

Ի սկզբանե այս գործիքների տեղադրումը Ձեր կազմակերպության բոլոր սարքերում կարող է բարդ թվալ, սակայն օգտագործելով շարժական սարքերի կառավարման ծրագիրը, Դուք կարող եք մեկ սեղմումով Ձեր սարքերը դնել ստանդարտ կազմաձևման:

Խորհուրդ 3՝ Նորացրեք Ձեր սարքը

Կարևոր չէ, թե որ հեռախոսը կամ փլանշետն է օգտագործում Ձեր կազմակերպությունը, կարևոր է դրանք նորացնել: Բոլոր արտադրողները (օրինակ՝ Windows, Android, iOS) հայտարարում են կանոնավոր նորացված տարբերակների մասին, որոնք պարունակում են անվտանգության կարևոր առանձնահատկություններ՝ սարքը պաշտպանելու համար: Գործընթացը բավականին արագ, պարզ և անվճար է: Նման պարագաներում խորհուրդ է տրվում սարքը միացնել ավտոմատ նորացման ռեժիմին: Համոզված եղեք, որ Ձեր աշխատակիցները գիտեն, թե որքան կարևոր են այդ նորացումները և, անհրաժեշտության դեպքում, բացատրեք, թե ինչպես նորացնել սարքը: Որոշակի ժամանակահատվածից հետո նորացումներն այլևս հասանելի չեն լինի (քանի որ սարքը մոտենում է շահագործման ավարտին՝ end of life), այդ ժամանակ անհրաժեշտ է հին սարքը փոխարինել ժամանակակից այլընտրանքով:

Խորհուրդ 4՝ Նորացրեք Ձեր հավելվածները

Ճիշտ այնպես, ինչպես Ձեր կազմակերպության սարքերի օպերացիոն համակարգերը, ինստալացված բոլոր

հավելվածները նույնպես պետք է պարբերաբար նորացվեն ծրագրային ապահովման մատակարարի փաթչերով: Այս նորացումները ոչ միայն կավելացնեն նոր հնարավորություններ, այլև կշտկեն անվտանգության հետ կապված ցանկացած խոչընդոտ: Համոզվեք, որ անձնակազմը գիտի, թե ինչպես և երբ նորացնել սարքերը:

Խորհուրդ 5՝ Չմիանաք անհայտ Wi-Fi Hotspot-երին

Երբ օգտագործում եք Wi-Fi (օրինակ՝ հյուրանոցում կամ ռեստորանում), գոյություն չունի հեշտ ճանապարհ պարզելու համար թե ով է վերահսկում համացանցը: Եթե Դուք միանաք ցանցին, ապա շահագրգիր կողմը կարող է հասնաելիություն ձեռք բերել.

- Ինչ եք անում ցանցին միանալու ժամանակ
- Ձեր օգտատիրոջ անուն-ազգանունը, որը նշված է մի շարք տարբեր հավելվածներում և վեբ-ծառայություններում

Անվտանգության ամենապարզ միջոցը ոչ թե համացանցին միանալն է անհայտ Wi-Fi-ի միջոցով, այլ օգտագործել Ձեր բջջային 3G կամ 4G բջջային ցանցը, որը կունենա ներկառուցված անվտանգություն: Սա նշանակում է, որ Դուք կարող եք նաև օգտագործել „tethering“-ը (որտեղ Ձեր մյուս

սարքերը կիսում են 3G/4G կապը) կամ Ձեր բջջային ցանցի կողմից տրամադրվող անլար „dongle“ կապը (օրինակ՝ անլար MiFi modem): Ինչպես նաև կարող եք օգտագործել վիրտուալ մասնավոր ցանցեր (VPN), որոնք կոդավորում են Ձեր տվյալները՝ նախքան դրանք համացանցով ուղարկելը: Եթե դուք օգտագործում եք երրորդ կողմի VPN-ներ, Դուք պետք է ստուգեք, թե որքանով է հուսալի փրովայդերը և ինքներդ կարգավորեք այն:

1.4.4. Քայլ 4՝ Գաղտնաբառերի կիրառումը Ձեր տվյալների պաշտպանության համար

Նոութբուքները, համակարգիչները, փլանշեթները և սմարթֆոնները պարունակում են բազմաթիվ տվյալներ, որոնք կարևոր են Ձեր բիզնեսի համար՝ հաճախորդների անձնական տվյալներ, ինչպես նաև մանրամասներ այն առցանց հաշիվների մասին, որոնց մուտք եք գործում: Կարևոր է, որ այս տվյալները հասանելի լինեն Ձեզ, սակայն ոչ որակավորում չունեցող օգտատերերի համար:

Գաղտնաբառերը, ճիշտ կիրառելու դեպքում, անվճար, հեշտ և արդյունավետ միջոց են՝ կանխելու որակավորում չունեցող

օգտատերերի մուտքը Ձեր սարքեր: Հետևյալ գլուխներում ներկայացված են 5 խորհուրդներ, որոնք պետք է հիշել գաղտնաբառեր օգտագործելիս.

Խորհուրդ 1՝ Վստահ եղեք որ միացրել եք գաղտնաբառով պաշտպանությունը

Սահմանեք էկրանի կողպման գաղտնաբառ, PIN կամ նույնականացման այլ եղանակ (օրինակ՝ մատնահետք կամ դեմքով ապակողպում): Եթե Դուք հիմնականում օգտագործում եք մատնահետք կամ դեմքով ապակողպում, ապա ավելի հազվադեպ կմուտքագրեք Ձեր գաղտնաբառը, ուստի մտածեք երկար գաղտնաբառ սահմանելու մասին, որը դժվար կլինի կռահել:

Գաղտնաբառերի պաշտպանությունը միայն սմարթֆոնների և փլանշեթների համար չէ: Համոզվեք, որ Ձեր գրասենյակային սարքավորումները (ինչպես նաև լեփթոփները և համակարգիչները) օգտագործում են կոդավորման գործիքներ (օրինակ՝ BitLocker Windows-ի համար), վստահելի հարթակի մոդուլ (TPM) կամ FileVault-ի միջոցով macOS-ում: Ժամանակակից սարքերից շատերն ունեն հզոր կառուցված կոդավորում, սակայն կոդավորման համար նախ պետք է միացնել և կարգավորել:

Խորհուրդ 2՝ Օգտագործեք երկքայլ հաստատում «կարևոր» հաշիվների համար

Կարևոր է երկքայլ հաստատման կիրառումը (հայտնի է որպես 2 քայլ հաստատում – 2SV) Ձեր ցանկացած հաշվի համար, որտեղ այս գործառույթը հասանելի է: Նշվածը զգալիորեն բարելավում է Ձեր անվտանգությունը՝ առանց ավելորդ ջանքերի: 2SV-ն պահանջում է երկու տարբեր մեթոդներ Ձեր ինքնությունը «ապացուցելու» համար: Հետևաբար, նախքան ցանկալի համակարգ մուտք գործելը, որպես կանոն, Դուք պետք է մուտքագրեք գաղտնաբառ և մեկ այլ տվյալ: Դա կարող է լինել Ձեր սմարթֆոնին ուղարկված կոդը (կամ բանկային քարտի ընթերցողից ստացված կոդը), որը Դուք պետք է մուտքագրեք ձեր գաղտնաբառի հետ:

Խորհուրդ 3՝ Խուսափեք կանխատեսելի գաղտնաբառեր օգտագործելուց

Եթե Դուք պատասխանատու եք Ձեր կազմակերպության IT քաղաքականության համար, համոզվեք, որ գաղտնաբառի մասին տեղեկությունները տրամադրվում են անձնակազմին այնպիսի ձևով, որը նրանց համար հեշտ է գիտակցել և

հասկանալ:

Գաղտնաբառերը պետք է հեշտ հիշվի, սակայն ուրիշների համար՝ դժվար գուշակելի: Այս առումով կա մի լավ կանոն. «Համոզվեք, որ Ձեզ լավ ճանաչող մեկը չի կարող կռահել Ձեր գաղտնաբառը 20 փորձից»: Աշխատակիցները պետք է նաև խուսափեն օգտագործել ամենատարածված գաղտնաբառերը, որոնք հանցագործները կարող են գուշակել:

Հիշեք, որ Ձեր IT համակարգերը չպետք է պահանջեն անձնակազմից կիսվել հաշիվներով կամ գաղտնաբառերով՝ աշխատանքն ավարտելու համար: Համոզվեք, որ յուրաքանչյուր օգտատեր անձնական մուտք ունի նախապես սահմանված համակարգեր, և որ տրամադրված մուտքի մակարդակը միշտ ամենացածրն է (least privilege approach), որն անհրաժեշտ է իր աշխատանքը կատարելու համար: Նվազեցրեք անհարկի մուտքը համակարգեր, որոնց կարիքը Ձեր աշխատակիցները չունեն:

Խորհուրդ 4՝ Օգնեք ձեր անձնակազմին զբաղվել «գաղտնաբառի վերակայմամբ»

Եթե Դուք պատասխանատու եք Ձեր կազմակերպությունում գաղտնաբառերի օգտագործման համար, կան մի քանի լուծումներ, որոնք կարող են բարելավել Ձեր կազմակերպության անվտանգությունը: Ամենակարևորն այն է, որ Ձեր աշխատակիցները հիշելու համար տասնյակ ոչ աշխատանքային գաղտնաբառեր չեն ունենա: Անհրաժեշտ չէ կանոնավոր կերպով փոխել գաղտնաբառերն այն ծառայությունների համար, որոնք օգտատերը չի օգտագործում: Փոխեք գաղտնաբառերն այն համակարգերում, որոնք օգտատերերն ակտիվորեն օգտագործում են: Ինչպես նաև հաշվի առեք, որ Ձեր գաղտնաբառը փոխելը կարևոր է, եթե կասկածում եք, որ Ձեր գաղտնաբառը խափանվել է:

Դուք նաև պետք է ներդնեք գաղտնաբառերի մենեջեր (գաղտնաբառերի պահեստ), որպեսզի աշխատակիցները կարողանան ապահով կերպով պահել կարևոր հաշիվների գաղտնաբառերը (օրինակ՝ էլ.փոստը և բանկային ծառայությունները): Աշխատակիցները հաճախ մոռանում են իրենց գաղտնաբառերը, այնպես որ համոզվեք, որ նրանք

կարող են հեշտությամբ փոխել իրենց գաղտնաբառերը:

Խորհուրդ 5՝ Փոխեք բոլոր կանխադրված գաղտնաբառերը

Ամենատարածված սխալներից մեկն արտադրողների լռելյայն գաղտնաբառերի (default passwords) օգտագործումն է, որոնցով թողարկվում են սմարթֆոններ, նոութբուքեր և այլ տեսակի սարքավորումներ: Փոխեք բոլոր կանխադրված գաղտնաբառերը՝ նախքան սարքերն անձնակազմին հանձնելը: Դուք նաև պետք է պարբերաբար ստուգեք սարքերը (և ծրագրային ապահովումը) անփոփոխ լռելյայն գաղտնաբառերի համար:

1.4.5. Քայլ 5՝ Ֆիշինգի հարձակման կանխում

Ինչպես կարգն է, ֆիշինգային հարձակման ժամանակ խաբեբաները կեղծ նամակներ են ուղարկում հազարավոր մարդկանց և խնդրում նրանց տրամադրել հուզական տեղեկատվություն (ինչպիսին բանկային տվյալներն են) կամ սեղմել վնասակար հղումների վրա: Հարձակվողը կարող է

փորձել խաբել Ձեզ՝ գումար ուղարկելու կամ Ձեր հաշիվների (accounts) տվյալները ստանալու համար: Հարձակվողը կարող է նաև քաղաքական կամ գաղափարական դրդապատճառ ունենալ կազմակերպության մասին տեղեկատվություններ ստանալու համար:

Ֆիշինգի էլեկտոնային նամակների հայտնաբերումը գնալով ավելի է բարդանում: Անկախ նրանից, թե որն է Ձեր կազմակերպությունը/բիզնեսը, ինչ-որ պահի Դուք կդառնաք ֆիշինգային հարձակման զոհ: Այս գլուխը պարունակում է մի քանի պարզ քայլեր, որոնք կօգնեն Ձեզ բացահայտել ամենատարածված ֆիշինգային հարձակումները:

Խորհուրդ 1՝ Կարգավորեք հաշիվները՝ նվազագույնի հասցնելու հաջող հարձակումների ազդեցությունը

Դուք պետք է նախապես կազմաձևեք Ձեր անձնակազմի հաշիվները՝ օգտագործելով «նվազագույն արտոնություն» սկզբունքը: Դա նշանակում է, որ անձնակազմին պետք է տրվի օգտատերերի իրավունքների ամենացածր մակարդակը, որը բավարար է իրենց աշխատանքը կատարելու համար:

Հետևաբար, նույնիսկ եթե նրանք դառնում են ֆիշինգի հարձակման զոհ, հնարավոր վնասը նվազագույնի է հասցվում: Վնասակար ծրագրի պատճառած վնասը կամ հաշվի մուտքի մանրամասների կորուստը հետագայում նվազեցնելու համար համոզվեք, որ Ձեր աշխատակիցները մուտք չունենան համացանց կամ չստուգեն նամակներն ադմինիստրատորի իրավունքներ ունեցող հաշվից: Ադմինիստրատորի հաշիվն օգտատիրոջ հաշիվ է, որը թույլ է տալիս կատարել փոփոխություններ, որոնք ազդում են այլ օգտատերերի վրա: Ադմինիստրատորները կարող են փոխել անվտանգության կարգավորումները, ինստալացնել ծրագրային ապահովումը և սարքն ու հասանելիություն ձեռք բերեն համակարգչի բոլոր թղթապանակների նկատմամբ: Այսպիսով, ադմինիստրատորի հաշվի նկատմամբ չարտոնված մուտք ունեցող հարձակվողը կարող է շատ ավելի մեծ վնաս հասցնել, քան սովորական օգտատիրոջ հաշիվ մուտք ունեցող հարձակվողը:

Օգտագործեք երկգործոն նույնականացումը (2FA) այնպիսի կարևոր հաշիվների համար, որոնցից է էլեկտրոնային հասցեն: Օգտագործելով այդ մեթոդը, նույնիսկ եթե

հարձակվողը գիտի Ձեր գաղտնաբառը, նա չի կարողանա մուտք գործել Ձեր հաշիվ:

Խորհուրդ 2՝ Մտածեք այն մասին, թե ինչպես եք աշխատում

Մտածեք այն մասին, թե ինչպես կարող է ինչ-որ մեկը թիրախավորել Ձեր կազմակերպությունը և համոզվեք, որ աշխատակիցները հասկանում են աշխատանքի նորմալ ձևերը (հատկապես այլ կազմակերպությունների հետ համագործակցելիս), որպեսզի նրանք ավելի լավ պատրաստված լինեն բացառիկ/անկանոն պահանջները բավարարելու համար:

Ընդհանուր մեթոդները ներառում է այն ծառայության հաշիվ-ապրանքագիր ուղարկում, որը չեք օգտագործել և այդ կերպ, երբ կցորդը բացվում է, վնասակար ծրագիրն ավտոմատ կերպով տեղադրվում է Ձեր համակարգչում: Երկրորդը՝ աշխատակիցներին խաբելն է էլեկտրոնային նամակների միջոցով՝ գումար փոխանցելու կամ կազմակերպության մասին տեղեկատվություն ստանալու նպատակով: Մտածեք Ձեր սովորական աշխատանքային պրակտիկայի մասին և

ինչպես կարող եք ճանաչել վերը նշված հնարքները: Օրինակ՝

- Աշխատակիցները գիտե՞ն, թե ինչ անել էլ. հասցեին ստացված հարցումների հետ և որտեղից օգնություն ստանալ
- Հարցրեք ինքներդ Ձեզ, արդյոք մենեջերը պետք է ներգրավվի էլ. հասցեի հարցումը հաստատելու համար
- Լա՞վ եք հասկանում Ձեր կանոնավոր գործնական հարաբերությունները: Խաբեբաները հաճախ ֆիշինգային նամակներ են ուղարկում խոշոր կազմակերպություններից (օրինակ՝ բանկերից)՝ հույս ունենալով, որ էլ. հասցեի որոշ օգտատերեր կապ կունենան այդ ընկերության հետ: Եթե նամակ եք ստանում մի կազմակերպությունից, որի հետ գործնական հարաբերություններ չունեք, անպայման ստուգեք այն:
- Մտածեք, թե ինչպես կարող եք խրախուսել և աջակցել Ձեր աշխատակիցներին, որպեսզի հարցեր առաջանա կասկածելի կամ պարզապես անսովոր հարցումների վերաբերյալ, նույնիսկ եթե դրանք ստանում են կարևոր մարդկանցից (օրինակ՝ ընկերության հիմնադիրից կամ կազմակերպության ղեկավարից):

Խորհուրդ 3. Ստուգեք ֆիշինգի ակնհայտ նշանները

Ակնկալել, որ աշխատակիցները կկարողանան նույնականացնել և ջնջել բոլոր ֆիշինգի էլեկտրոնային նամակները, անհնար է և մեծ բացասական ազդեցություն կունենա կազմակերպչական/բիզնեսի արտադրողականության վրա: Սակայն, ֆիշինգային շատ փորձեր դեռևս համապատասխանում են ավանդական հարձակման ձևին, ուստի փնտրեք հետևյալ նախազգուշական նշանները.

- ¬ Ֆիշինգի բազմաթիվ խարդախություններ ծագում են արտասահմանում և հաճախ ունեն վատ ուղղագրություն, քերականություն և կետադրություն: Երբեմն հարձակվողները փորձում են ստեղծել պաշտոնական տեսք ունեցող նամակներ՝ այդ թվում լոգոները և գրաֆիկան: Հետևաբար, ուշադիր ստուգեք, թե արդյոք համապատասխան են ուղարկված նամակի ձևավորումը և ուղղագրությունը
- ¬ Եթե Ձեզ անունով չեն դիմում և օգտագործում են ստանդարտ հասցե՝ «Հարգելի հաճախորդ», «Ընկեր» կամ «Գործընկեր»: Սա կարող է նշան լինել, որ ուղարկողն

իրականում չի ճանաչում Ձեզ, ինչը նույնպես ֆիշինգի խարդախության մի մասն է

- ¬ Ուշադրություն դարձրեք, թե արդյոք էլ. նամակը պարունակում է արտահայտություններ, որոնք պահանջում են Ձեր անմիջական գործողությունը: Հաճախ օգտագործվում են ֆիշինգային արտահայտություններ, ինչպիսիք են «ուղարկեք այս տվյալները 24 ժամվա ընթացքում» կամ «Դուք հանցագործության զոհ եք դարձել, անմիջապես սեղմեք այստեղ»
- ¬ Ուշադիր հետևել էլ. նամակին, որը, ինչպես երևում է, ստացել եք Ձեր կազմակերպության բարձրաստիճան անձից և վճարում է կատարվում կոնկրետ բանկային հաշվեհամարին: Նայեք ուղարկողի անվանը: Արդյո՞ք դա օրինական է հնչում, թե՞ փորձում է անձնավորել ինչ-որ մեկին
- ¬ Եթե նամակը չափազանց լավ է հնչում: Օրինակ, դժվար թե ինչ-որ մեկը ցանկանա Ձեզ փող տալ առանց պատճառի:

Էլեկտրոնային հասցեի զտման ծառայությունները փորձում են ֆիշինգային նամակներ ուղարկել սպամի

թղթապանակներին, սակայն ֆիլտրումը սահմանող կանոնները պետք է հարմարեցվեն Ձեր կազմակերպության կարիքներին: Եթե կանոնները չափազանց բաց են և կասկածելի, նամակը չի ուղարկվի սպամ/աղբային թղթապանակներին: Նման դեպքում օգտատերերը ստիպված կլինեն կառավարել մեծ թվով էլեկտրոնային նամակներ, ինչը նրանց կողմից որոշակի էներգիա կպահանջի: Եվ, եթե կանոնները չափազանց խիստ են, որոշ օրինական նամակներ կարող են անհետանալ: Հետևաբար, ժամանակի ընթացքում Ձեզ հարկավոր է փոխել կանոնները՝ փոխզիջում ապահովելու համար:

Խորհուրդ 4. Տեղեկացրեք բոլոր հարձակումների մասին

Համոզվեք, որ Ձեր աշխատակիցները խրախուսվում են պոտենցիալ հարձակման մասին հայտնել համապատասխան կազմակերպչական միավորին կամ պատասխանատու անձին: Նման պարագայում կարևոր է քայլեր ձեռնարկել՝ հնարավորինս շուտ վնասակար ծրագրեր փնտրելու և գաղտնաբառերը փոխելու համար:

Մի պատժեք աշխատակիցներին, եթե նրանք սեղմում են ֆիշինգի էլ. հասցեին: Սա կհուսահատեցնի մարդկանց ապագայում հաշվետվություններ ներկայացնելու և կարող է այնքան վախեցնել նրանց, որ չափազանց շատ ժամանակ և էներգիա ծախսեն յուրաքանչյուր էլ. նամակն ուսումնասիրելու համար: Այս երկու բաները երկարաժամկետ հեռանկարում ավելի շատ կվնասեն Ձեր բիզնեսը:

Խորհուրդ 5. Ստուգեք Ձեր թվային հետքը

Հարձակվողներն օգտագործում են Ձեր կազմակերպության և անձնակազմի մասին հանրությանը հասանելի տեղեկատվություն, որպեսզի իրենց ֆիշինգային հաղորդագրություններն ավելի վստահելի դարձնեն: Նրանք նշված տեղեկատվությունը ստանում են կազմակերպության վեբ-կայքից և սոցիալական ցանցերի հաշիվներից (տեղեկատվություն, որը հայտնի է ինչպես «թվային հետք»):

- Իմացեք Ձեր կազմակերպության վեբ-կայքում և սոցիալական մեդիայի էջերում տարածվող տեղեկատվության ազդեցության մասին: Ի՞նչ պետք է

իմանան Ձեր վեբ-կայքի այցելուները, և ի՞նչ մանրամասներ են ավելորդ (սակայն կարող են օգտակար լինել հարձակվողների համար):

- Իմացեք, թե Ձեր գործընկերները, կապալառուները և մատակարարները կազմակերպության մասին առցանց կերպով ինչ տեղեկատվություն են փոխանակում:
- Օգնեք Ձեր աշխատակիցներին հասկանալ, թե ինչպես կարող է անձնական տեղեկատվության փոխանակումն ազդել իրենց և Ձեր կազմակերպության վրա: Սա չի նշանակում, որ մարդիկ պետք է համացանցից հեռացնեն իրենց բոլոր հետքերը: Կարևոր է աջակցել նրանց, երբ նրանք կառավարում են իրենց թվային հետքը՝ ստեղծելով պրոֆիլ, որն աշխատում է նրանց և կազմակերպության համար:

2. Թեմատիկ օրինակներ

2.1. Անձնական տվյալների պաշտպանություն. Ինչ պետք է իմանանք

2.1.1. Ի՞նչ է իրենից ներկայացնում իմ անձնական տվյալը

Վրաստանի «Անձնական տվյալների պաշտպանության մասին» օրենքը սահմանում է, որ անձնական տվյալները ցանկացած տեսակի տեղեկատվություն են, որոնք կարող են օգտագործվել անձի նույնականացման համար: Օրինակ՝ Ձեր անունը, ազգանունը, անձնական համարը, լուսանկարը, տեսագրությունը, էլ. փոստի հասցեն, բանկային հաշվեհամարը, սոցիալական ցանցի հաշիվը, անձնական նամակագրությունը: Անձնական տվյալները ներառում են նաև տեղեկություններ Ձեր աշխատավայրի, եկամտի, ընտանեկան կարգավիճակի և այլնի մասին:

Ինչպես նաև գոյություն ունեն անձնական տվյալների հատուկ կատեգորիաներ: Այս կատեգորիան ներառում է տեղեկություններ՝ կապված անձի ռասայական կամ էթնիկ

պատկանելության, քաղաքական հայացքների, կրոնական կամ փիլիսոփայական համոզմունքների, մասնագիտական միության անդամակցության, առողջական վիճակի, սեռական կյանքի, դատվածությունների, վարչական կալանքի, խափանման միջոցների, միջնորդության համաձայնագրերի, դիվերսիայի, զոհ ճանաչվելու հետ: Բացի այդ, հատուկ կատեգորիան ներառում է կենսաչափական և գենետիկական տվյալներ, որոնք ֆիզիկական անձին թույլ են տալիս նույնականացնել վերը նշված հատկանիշներով:

Վրաստանի գործող օրենսդրությունը սահմանում է անձնական տվյալների հատուկ կատեգորիաների պաշտպանության ավելի բարձր չափանիշ, ինչպես նաև կանոնների խախտման դեպքում պատժամիջոցների մեխանիզմներն ավելի խիստ են, քան ստանդարտ անձնական տվյալների դեպքում:

2.1.2. Ի՞նչ է նշանակում անձնական տվյալների ապօրինի մշակում

Ըստ Վրաստանի «Անձնական տվյալների պաշտպանության մասին» օրենքի՝ տվյալների մշակումը ցանկացած

գործողություն է, որը կատարվում է անձնական տվյալների վրա՝ հավաքագրում, գրանցում, պահպանում, օգտագործում, բացահայտում, լուսանկարում, փոխանցում երրորդ կողմին, տարածում, ջնջում, ոչնչացում և այլն:

Քաղաքացու անձնական տվյալները կարող են մշակվել ցանկացած պետական կամ մասնավոր կազմակերպության կողմից, որի հետ քաղաքացին հարաբերություններ ունի: Օրինակ՝

- Սուպերմարկետների ցանցը մշակում է քաղաքացու անձնական տվյալները, երբ քաղաքացին գրանցում է հավատարմության քարտը
- Կլինիկան մշակում է քաղաքացու անձնական տվյալները՝ ախտորոշումներ, հետազոտություններ կատարելիս, հիվանդության պատմություն կազմելիս
- Սոցիալական ցանցը մշակում է քաղաքացու (օգտատիրոջ) անձնական տվյալները, երբ նա հրապարակում է իր լուսանկարը կամ գրանցման նպատակով համապատասխան դաշտում մուտքագրում է իր էլ. փոստի հասցեն և գաղտնաբառը
- Ուսումնական հաստատությունը մշակում է ուսանողի

անձնական տվյալները, երբ ուսանողը գրանցվում է ուսումնական դասընթացին, որի համար նշում է իր անձնական համարը, անունն ու ազգանունը:

Բոլոր կազմակերպությունները, որոնք առընչվում են քաղաքացու անձնական տվյալների հետ, հանդիսանում են տվյալներ մշակողներ, իսկ քաղաքացին տվյալների սուբյեկտ է:

Հաշվի առնելով անձնական տվյալների հուզականությունը՝ Վրաստանի գործող օրենսդրությունը սահմանում է կանոններ, սկզբունքներ, հիմքեր և անվտանգության միջոցներ, որոնց մշակողը պետք է հետևի տվյալների մշակման ժամանակ: Այս կանոնների խախտմամբ տվյալների հավաքագրումը, պահպանումը, օգտագործումը և տարածումն անօրինական է:

2.1.3. Տվյալների մշակման հիմունքներ

Տվյալների մշակումը թույլատրելի է, եթե

• **Գոյություն ունեն տվյալների սուբյեկտի համաձայնությունը.** անձի կամավոր, տեղեկացված և հստակ արտահայտված

համաձայնությունն իր անձնական տվյալների մշակմանը: Օրինակ՝

- ¬ Կայքում գրանցվելիս կամ հավելվածը ներբեռնելիս. համաձայնություն վեբ-կայքում տեղադրված գաղտնիության քաղաքականությանը
- ¬ Բժշկական հարցաթերթ կամ հավատարմության քարտ բացելիս. պայմանագիր կնքելիս

• **Տվյալների մշակումը նախատեսված է օրենքով**. որոշ դեպքերում տարբեր օրենսդրական ակտերով նախատեսված է քաղաքացիների անձնական տվյալների մշակման անհրաժեշտությունը

• **Տվյալների մշակումը պահանջվում է տվյալների մշակողի կողմից՝ օրենքով իրեն վերապահված պարտականությունները կատարելու համար,** օրինակ՝ տվյալները որոշակի ժամկետով հարկային նպատակներով պահելու համար

• **Տվյալների մշակումն անհրաժեշտ է տվյալների սուբյեկտի կենսական շահերը պաշտպանելու համար,** օրինակ՝ եթե մարդու կյանքին վտանգ է սպառնում արտակարգ իրավիճակի ժամանակ, և անհրաժեշտ է

որոշել գտնվելու վայրը՝ նրան փրկելու համար

- **Տվյալների մշակումն անհրաժեշտ է տվյալների մշակողի կամ երրորդ կողմի օրինական շահերը պաշտպանելու համար,** բացի այն պարագայից, երբ գոյություն չունի տվյալների սուբյեկտի իրավունքների և ազատության պաշտպանության գերակա շահ
- Տվյալները հանրությանը հասանելի են կամ սուբյեկտը տվյալները հասանելի է դարձրել: Օրինակ՝
  - ¬ Սոցիալական ցացնում բոլորին հասանելի կերպով տեղադրված լուսանկար
  - ¬ Առցանց վաճառքի հարթակում բոլորին հասանելի կերպով տեղադրված կոնտակտային տվյալներ
- **Տվյալների մշակումն անհրաժեշտ է օրենքով սահմանված կարգով հանրային կարեւոր շահերի պաշտպանության համար,** օրինակ՝ հանցագործության կանխարգելումը, սեփականության կամ անչափահասների պաշտպանությունը վնասակար հետևանքներից
- **Տվյալների մշակումն անհրաժեշտ է տվյալների սուբյեկտի դիմումը դիտարկելու կամ նրան**

ծառայություններ մատուցելու համար:

Հատուկ կատեգորիայի տվյալների մշակումը թույլատրվում է միայն տվյալների սուբյեկտի գրավոր համաձայնությամբ կամ այն դեպքերում, երբ

- Դատվածության և առողջական վիճակի հետ կապված տվյալների մշակումն անհրաժեշտ է՝ կախված աշխատանքային պարտավորությունների և հարաբերությունների բնույթից, այդ թվում՝ աշխատանքի վերաբերյալ որոշում կայացնելու համար
- Տվյալների մշակումն անհրաժեշտ է տվյալների սուբյեկտի կամ երրորդ կողմի կենսական շահերը պաշտպանելու համար, և տվյալների սուբյեկտը ֆիզիկապես կամ իրավաբանորեն ի վիճակի չէ համաձայնություն տալ տվյալների մշակմանը
- Տվյալները մշակվում են հանրային առողջության պաշտպանության, առողջության պահպանման կամ հաստատության (աշխատողի) կողմից՝ անհատի առողջության պահպանման նպատակով, ինչպես նաև,

եթե դա անհրաժեշտ է առողջության պահպանման համակարգի կառավարման կամ գործունեության համար

• Տվյալների սուբյեկտը հրապարակել է իր մասին տվյալները՝ առանց դրանց օգտագործման հստակ արգելքի

• Տվյալները մշակվում են քաղաքական, փիլիսոփայական, կրոնական կամ մասնագիտական ասոցիացիայի կամ շահույթ չհետապնդող կազմակերպության կողմից օրինական գործունեության ընթացքում: Նման դեպքում տվյալների մշակումը կարող է առնչվել միայն այս ասոցիացիայի/կազմակերպության անդամներին կամ այս ասոցիացիայի/կազմակերպության հետ մշտական կապ ունեցող անձանց հետ

• Տվյալների մշակումն իրականացվում է մեղադրյալների/դատապարտյալների անձնական գործերն ու ռեգիստրները կազմելու նպատակով՝ հաշվի առնելով պատիժը կրելու անհատական պլանավորման և/կամ դատապարտյալին պատժի կրումից պայմանական ազատելու և պատժի չկրած մասի ավելի թեթև պատժաչափով փոխարինելու հետ կապված խնդիրները

• Տվյալները մշակվում են «Ազատազրկման հետ չկապված պատիժների կատարման կանոնների և պրոբացիայի մասին» Վրաստանի օրենքի 2-րդ հոդվածով նախատեսված իրավական ակտերի կատարման նպատակով

• Տվյալները մշակվում են «Միջազգային պաշտպանության մասին» Վրաստանի օրենքով ուղղակիորեն նախատեսված դեպքերում

• Տվյալները մշակվում են միգրացիոն տվյալների միասնական վերլուծական համակարգի գործարկման համար

• Տվյալները մշակվում են կրթության առանձնահատուկ պայմանների կարիք ունեցող անձանց կրթության իրավունքն իրացնելու նպատակով։

2.1.4. Տվյալների մշակման սկզբունքներ

Անձնական տվյալները մշակելիս անհրաժեշտ է հաշվի առնել հետևյալ սկզբունքները.

• **Արդարություն ու օրինականություն.** անձնական տվյալները պետք է մշակվեն արդար և օրինական՝ առանց անձի արժանապատվությունը ոտնահարելու

• **Հստակ սահմանված իրավական նպատակի առկայություն.** անհրաժեշտ է ունենալ կոնկրետ նպատակ, որի համար մշակվում են տվյալները: Տվյալների օգտագործումն այլ նպատակներով չի թույլատրվում

• **Համաչափություն ու համարժեքություն.** տվյալները պետք է մշակվեն նվազագույն չափով, որն անհրաժեշտ է տվյալների մշակման հատուկ նպատակին հասնելու համար: Տվյալներն ինքնին նույնպես պետք է համապատասխան լինեն այս նպատակին

• **Ճշմարտություն ու ճշգրտություն.** տվյալները պետք է լինեն ճշմարիտ և ճշգրիտ, անհրաժեշտության դեպքում՝ թարմացվեն, ինչպես նաև ստուգվեն տեղեկատվության աղբյուրի հավաստիությունը, շտկվեն կեղծ և ոչ ճշգրիտ տվյալները

• **Պահպանման ժամկետ.** անձնական տվյալները պետք է պահպանվեն օրենքով սահմանված ժամկետում կամ նպատակին հասնելու համար

անհրաժեշտ ժամանակահատվածում: Նպատակին հասնելուց հետո դրանք պետք է ջնջվեն կամ պահվեն ոչ անձնապես ճանաչելի ձևով:

Եթե կարծում եք, որ կազմակերպությունը չունի Ձեր տվյալների մշակման իրավական հիմք կամ խախտում է օրենքով սահմանված որևէ սկզբունք, կարող եք դիմել անձնական տվյալների պաշտպանության ծառայություն կամ դատարան:

Խախտման դեպքում «Անձնական տվյալների պաշտպանության մասին» օրենքը սահմանում է վարչական պատասխանատվություն՝ նախազգուշացման կամ տուգանքի տեսքով:

2.1.5. Ինչպե՞ս պահանջել ինձ մասին տեղեկատվություն

- Դուք կարող եք անձնական տվյալների մշակման մասին տեղեկատվություն պահանջել ինչպես բանավոր, այնպես էլ գրավոր
- Դուք իրավունք ունեք հանրային հաստատությունում ծանոթանալու Ձեր մասին անձնական տվյալներին և

անվճար ստանալու այդ տվյալների պատճենները, բացառությամբ այն տվյալների, որոնց համար Վրաստանի օրենսդրությամբ վճար է նախատեսված

- Կարևոր է իմանալ, որ Դուք իրավունք ունեք պահանջել տեղեկատվություն միայն Ձեր անձնական տվյալների մասին: Այլ անձի տվյալների մշակման մասին տեղեկատվություն պահանջելու համար անհրաժեշտ է հաստատել հատուկ լիազորություն կամ ներկայացուցչություն, օրինակ՝ ծնողի, երեխայի կամ փաստաբանի կողմից հաճախորդի տվյալների վերաբերյալ տեղեկություններ ստանալու հարցում:

2.1.6. Անձնական տվյալների շտկում, ջնջում և թարմացում

Եթե սուբյեկտի անձնական տվյալները թերի են, ոչ ճշգրիտ, չթարմացված կամ եթե դրանց հավաքագրումն ու մշակումն իրականացվել է օրենքի պահանջների խախտմամբ, սուբյեկտն իրավունք ունի պահանջելու դրանց ուղղումը, թարմացումը, լրացումը, արգելափակումը (տվյալների ժամանակավոր կասեցում), ջնջումը կամ ոչնչացումը:

Սուբյեկտն ընտրում է խնդրանքի ցանկալի ձևը: Դա կարելի է անել ինչպես բանավոր, այնպես էլ գրավոր: Տվյալները մշակողը պարտավոր է բավարարել հարցումն այն ստանալուց հետո 15 օրվա ընթացքում կամ սուբյեկտին հայտնել հարցումը բավարարելու մերժման պատճառը:

2.1.7. Ուղիղ մարքեթինգի նպատակով անձնական տվյալների մշակում

Ուղիղ մարքեթինգը սպառողներին ապրանքների, ծառայությունների կամ աշխատանքի առաջարկն է տեքստային հաղորդագրությունների, փոստի, հեռախոսազանգերի, էլ.հասցեի կամ ուղիղ հաղորդակցության միջոցով:

Տվյալները կարող են մշակվել ուղիղ մարքեթինգային նպատակներով, եթե

- Քաղաքացին տվել է գրավոր համաձայնություն
- Տեղեկատվությունը հասանելի է բոլորի համար կամ կազմակերպությունը ձեռք է բերել այն օրինական կերպով:

Հաճախ օգտատերերն իրենք են համաձայնում անձնական տվյալների, այդ թվում՝ կոնտակտային տվյալների օգտագործմանը: Օրինակ՝ կրեդիտ քարտը լրացնելիս մենք խանութին թույլ ենք տալիս մեզ հաղորդագրություններ ուղարկել, բջջային օպերատորին թույլ ենք տալիս օգտագործել մեր հեռախոսահամարը՝ գործընկեր ընկերությունների մարքեթինգային նպատակներով, մենք դառնում ենք բանկի հաճախորդ, համաձայնում ենք ուղարկել տեղեկատվական և գովազդային հաղորդագրություններ և այլն:

Ընկերությունները կարող են օգտագործել մեր կոնտակտային տվյալներն ուղիղ մարքեթինգային նպատակներով, նույնիսկ եթե այդ տեղեկատվությունը հասանելի է հանրությանը: Օրինակ, եթե Դուք հրապարակում եք հեռախոսահամար առք ու վաճառքի կայքում, հրապարակայնորեն նշեք էլ. փոստի հասցեն ֆեյսբուքյան էջում և այլն:

Սակայն անկախ այն բանից, թե Դուք համաձայնել եք, որ կազմակերպությունն օգտագործի Ձեր տվյալներն ուղիղ մարքեթինգային նպատակներով, Դուք պետք է կարողանաք հրաժարվել՝ նույն ձևով, որով առաջարկն արվել է կամ այլ

մատչելի և համարժեք միջոցներով:

Օրինակ՝ գովազդային հաղորդագրությանն անպայման պետք է կցված լինի հրաժարման մեխանիզմը և հստակ ցուցումը, թե ինչպես կարող է քաղաքացին դադարեցնել գովազդային հաղորդագրություն ստանալը՝ այսպես կոչված SMS OFF, էլեկտրոնային փոստի դեպքում նամակին պետք է կցվի այսպես կոչված Unsubscribe մեխանիզմ:

Դուք իրավունք ունեք ցանկացած պահի և ցանկացած ձևով (բանավոր, գրավոր) պահանջելու տվյալների մշակողին դադարեցնել Ձեր տվյալներն ուղիղ մարքեթինգային նպատակներով օգտագործելը: Ընկերությունը պետք է դադարեցնի Ձեր տվյալների կիրառումն ուղիղ մարքեթինգային նպատակներով Ձեր հարցումից հետո 10 աշխատանքային օրվա ընթացքում:

Դուք իրավունք ունեք իմանալու, թե ինչ տվյալներ են մշակվում Ձեր մասին և ցանկացած պահի պահանջել դրանց ուղղում, թարմացում, ավելացում, արգելափակում, ջնջում կամ ոչնչացում: Ինչպես նաև Դուք իրավունք ունեք իմանալու, թե ով է ծավալում մարքեթինգային գործունեություն, ինչ

աղբյուրից և ինչ հիմքով են ստացել Ձեր տվյալները:

2.2. Ֆիշինգ և էլեկտրոնային փոստի անվտանգություն

2.2.1. Ի՞նչ է սոցիալական ճարտարագիտությունը

Սոցիալական ճարտարագիտությունը զոհին մանիպուլյացիայի ենթարկելու, ազդելու կամ խաբելու մարտավարություն է, որպեսզի հարձակվողը կարողանա վերահսկողություն հաստատել համակարգչային ծրագրի վրա, գողանալ անձնական կամ ֆինանսական տեղեկատվություն: Սոցիալական ճարտարագիտությունը կիրառում է հոգեբանական մանիպուլյացիա, որպեսզի հարձակվողը կարողանա հուզական տեղեկատվության հասանելիություն ձեռք բերել կամ ստիպել զոհին խախտել անվտանգության կանոնները/նորմերը:

Սոցիալական ճարտարագիտական հարձակումները տեղի են ունենում մեկ կամ մի քանի փուլերով: Սկզբում կիբերհանցագործը ընդհանուր տեղեկատվություն է հավաքում զոհի մասին, որը կօգնի նրան բացահայտել ներխուժման հնարավոր ուղիները և անվտանգության թույլ կողմերը: Հաջորդ քայլում հարձակվողն օգտագործում է

պատրվակի ձև, ինչպիսին է նմանակումը (impersonation), որպեսզի շահի զոհի վստահությունը: Նշված վստահության հիման վրա զոհը հրապարակում է հուզական տեղեկատվություն և/կամ թույլ է տալիս հարձակվողին մուտք գործել թիրախային համակարգ:

Սոցիալական ճարտարագիտության հարձակման տեսակներ

Սոցիալական ճարտարագիտական հարձակումների շատ տարբեր ձևեր կան, որոնք կարող են իրականացվել ցանկացած վայրում, որտեղ մարդը գտնվում է: Ստորև ներկայացված են սոցիալական ճարտարագիտական հարձակումների տարածված ձևերը:

Ի՞նչ է ֆիշինգը

Ֆիշինգ է կոչվում վստահելի սուբյեկտ դառնալու նպատակով էլ. փոստի, SMS տեքստային հաղորդագրության կամ հեռախոսի միջոցով հուզական տեղեկատվություն, այդ թվում՝ սպառողի անուններ, գաղտնաբառեր և վարկային քարտի մանրամասներ ստանալու փորձի գործընթացը: Ֆիշինգային հարձակման ժամանակ հարձակվողը հրատապության, հետաքրքրասիրության կամ վախի զգացում է առաջացնում: Ֆիշինգային հաղորդագրությունը զոհին հուշում է

տրամադրել հուզական տեղեկատվություն, սեղմել վնասակար վեբ-կայքի հղման վրա կամ բացել վնասակար ծրագրեր պարունակող հավելվածները:

Ի՞նչ է Վիշինգը

Vishing-ը սոցիալական ճարտարագիտության տեսակ է, որի ժամանակ կիրառվում է ձայնային հաղորդակցություն: Այս տեխնիկան կարող է զուգակցվել սոցիալական ճարտարագիտության այլ տեսակների հետ, որոնք ստիպում են զոհին զանգահարել կոնկրետ հեռախոսահամարին և բացահայտել հուզական տեղեկատվություն: Ֆիշինգային հարձակումները կարող են իրականացվել ամբողջությամբ ձայնային հաղորդակցության միջոցով՝ օգտագործելով այսպես կոչված Voice over Internet Protocol (VoIP) լուծումներ և հեռարձակման ծառայություններ: VoIP-ը հեշտությամբ թույլ է տալիս զանգահարողի նույնականացման (ID) կեղծումը, որից հարձակվողը կարող է օգտվել հանրության կողմից վստահված անձին նմանակելու համար: Օրինակ՝ զոհը կարող է ստանալ հեռախոսազանգ և իրեն ներկայացնել որպես պետական կամ մասնավոր հաստատություն, բայց իրականում դա հարձակվողի զանգ լինի:

Ի՞նչ է սմիշինգը

Smishing-ը դա սոցիալական ճարտարագիտության տեսակ է, որի ժամանակ կիրառվում է SMS կամ տեքստային հաղորդագրություններ: Տեքստային հաղորդագրությունները կարող են պարունակել հղումներ, ինչպիսիք են վեբ-կայքերը, էլ.փոստի հասցեները կամ հեռախոսահամարները, որոնց վրա սեղմելով հնարավոր է ավտոմատ կերպով բացվի բրաուզերի պատուհանը, էլեկտրոնային նամակը կամ հավաքի համարը: Էլեկտրոնային փոստի, ձայնի, տեքստային հաղորդագրությունների և բրաուզերի գործառույթների ինտեգրումը մեծացնում է հավանականությունը, որ օգտատերը կդառնա վնասակար գործունեության զոհ:

Ի՞նչ է բեյթինգը (Baiting)

Բեյթինգը (խաբեցուցիչ) դա սոցիալական ճարտարագիտության տեսակ է, երբ խարդախն օգտագործում է կեղծ խոստում զոհին թակարդի մեջ պահելու համար, ինչը կարող է հանգեցնել անձնական և/կամ ֆինանսական տեղեկատվության արտահոսքի՝ վնասակար ծրագրերի խարդախ ակտիվացման միջոցով: Որպես կանոն, բեյթինգի ժամանակ կիրառվում է վնասակար կոդ, որն ունի գրավիչ անուն:

Բեյթինգի ամենատարածված ձևն օգտագործում է ֆիզիկական կրիչ (օրինակ՝ USB flash drive)՝ վնասակար ծրագրեր տարածելու համար: Օրինակ՝ հարձակվողը վնասակար ծրագրով (խաբեցուցիչ) վարակված ֆլեշ հիշողության քարտ է թողնում նշանավոր վայրում, որտեղ պոտենցիալ զոհն անպայման կտեսնի այն: Երբ զոհն օգտագործում է ֆլեշ կրիչն աշխատանքային կամ տնային համակարգչում, վնասակար ծրագիրն ավտոմատ կերպով ինստալացիա է լինում համակարգում:

Ի՞նչ է հետապնդումը (Tailgating)

Հետապնդումը (tailgating, ինչպես նաև հայտնի է որպես "piggybacking") դա ֆիզիկական հարձակման տեսակ է, երբ չլիազորված անձը սոցիալական ճարտարագիտության միջոցով մուտք կունենա պաշտպանված տարածք (օրինակ՝ նախասրահ, գրասենյակ, պաշտպանված սենյակ և այլն): Օրինակ, հարձակվողը կարող է ձևանալ որպես վարորդ, կուրիեր, գրասենյակի աշխատակից, մաքրուհի, էլեկտրիկ կամ այլք: Հարձակվողը կարող է սպասել դռան մոտ, և երբ աշխատակիցը/բնակիչը կբացի դուռը, հարձակվողը խնդրում է աշխատակցին/բնակիչին պահել դուռը՝ այդպիսով մուտք ունենալով դեպի տարածք:

Ի՞նչ է վախեցնելը (Scareware)

Scareware-ը դա սոցիալական ճարտարագիտության տեսակներից է, որը ներառում է զոհերին վախեցնել կեղծ ահազանգերով և սպառնալիքներով: Հարձակվողը վախեցնում է զոհին, որ նրա համակարգը վարակված է վնասակար ծրագրերով, ինչի համար նա առաջարկում է ծրագրային նոր ապահովում իստալացնել: Փաստորեն, վերոհիշյալ ծրագրի ինստալացումը հանցագործին տալիս է տուժողի համակարգչի հեռահար մուտք:

2.2.2. Ի՞նչ պետք է իմանանք ֆիշինգի մասին

Ֆիշինգային հարձակումները կարող են լինել տարբեր տեսակի կազմակերպություններից, ինչպիսիք են բարեգործական կազմակերպությունները, հագուստի խանութները, սուպերմարկետների ցանցերը և այլն: Ինչպես նաև, հարձակվողները հաճախ օգտվում են ընթացիկ իրադարձություններից և տարվա որոշակի ժամանակներից: Օրինակ, ֆիշինգային հարձակումները կարող են ներառել.

- Բնական աղետներ (օրինակ՝ Կատրինա փոթորիկ, ինդոնեզական ցունամի)

- Համավարակներ և առողջապահական սպառնալիքներ (օրինակ՝ H1N1, COVID-19)
- Տնտեսական խնդիրներ
- Քաղաքական գլխավոր իրադարձություններ (ընտրություններ)
- Տոներ (Ամանոր, Սուրբ Ծնունդ, Զատիկ և այլն):

2.2.3. Ինչպե՞ս բացահայտենք ֆիշինգը

Ուղարկողի կասկածելի հասցե – ուղարկողի հասցեն կարող է լինել լեգիտիմ բիզնեսի իմիտացիա: Կիբերհանցագործները հաճախ օգտագործում են էլ.փոստի հասցե, որը շատ նման է հեղինակավոր ընկերության հասցեին՝ մի քանի նիշ փոխված կամ բաց թողնված (օրինակ՝ www.microsoft.com –ի փոխարեն www.microsofttt.com):

Ընդհանուր ողջույններ և ստորագրություն - ֆիշինգի կարևոր ցուցիչներից են այնպիսի ընդհանուր ողջույնները, ինչպիսիք են «Հարգելի հաճախորդ» կամ «Պարոն/Տիկին», ինչպես նաև ստորագրության մասում կոնտակտային տեղեկատվության բացակայությունը: Համեմատության համար, վստահելի

կազմակերպությունը սովորաբար դիմում է Ձեզ անունով և տրամադրում է Ձեզ իր կոնտակտային տվյալները:

Կեղծված հիպերհղումներ և վեբ-կայքեր - եթե սեղմում եք նամակի տեքստի հղումներից որևէ մեկի վրա, և հղումները չեն համընկնում տեքստի հետ, որը տեսնում եք, ապա հղումը կարող է կեղծ լինել: Վնասակար կայքերը կարող են նման լինել օրինական կայքին, սակայն URL-ը կարող է օգտագործել տիրույթի այլ տարբերակ (օրինակ՝ .com՝ .net-ի փոխարեն): Հարկ է նշել, որ կիբերհանցագործները կարող են օգտագործել URL-ի կրճատման ծառայություն՝ հղումի իրական նպատակակետը թաքցնելու համար:

Ուղղագրություն և դասակարգում - ֆիշինգի հնարավոր փորձի ցուցիչներ են քերականության և նախադասության վատ կառուցվածքը, ուղղագրական սխալները և անհամապատասխան ձևաչափումը: Համեմատության համար, հեղինակավոր հաստատություններն ունեն անձնակազմ, որը կազմում, ստուգում և ուղղում է հաճախորդների նամակագրությունները:

Կասկածելի բաղվածքներ - վնասակար ծրագրերի տարածման տարածված մեխանիզմներից մեկն

էլեկտրոնային նամակների օգտագործումն է, որոնք օգտատիրոջը հուշում են ներբեռնել և բացել քաղվածքի տեսքով կցված թղթապանակը: Հարձակվողը կարող է ստեղծել հրատապության պատրանք/սցենար՝ համոզելու օգտվողին ներբեռնել կամ բացել թղթապանակը, որը կցված է որպես հավելված՝ առանց նախապես ստուգելու:

2.2.4. Ինչպե՞ս կանխել ֆիշինգը

- Զգույշ եղեք հեռախոսազանգերից, SMS-ից կամ էլ.փոստի հաղորդագրություններից, որոնք Ձեզ խնդրում են տրամադրել տարբեր հուզական տեղեկատվություն: Եթե անհայտ անձը պնդում է, որ հանդիսանում է օրինական կազմակերպության ներկայացուցիչ, փորձեք ստուգել նրա ինքնությունն անմիջապես ընկերության հետ
- Մի տրամադրեք անձնական տեղեկատվություն կամ տեղեկատվություն Ձեր կազմակերպության, այդ թվում՝ նրա կառուցվածքի կամ ցանցերի մասին, եթե վստահ չեք անձի հեղինակության և ինքնության մեջ
- Մի բացահայտեք անձնական կամ ֆինանսական տեղեկատվությունն էլեկտրոնային փոստով և մի

պատասխանեք նման տեղեկատվության հարցումներին էլ. փոստի միջոցով

- Մի ուղարկեք հուզական տեղեկատվություն համացանցով, քանի դեռ չեք ստուգել վեբ-կայքի անվտանգությունը
  - Ուշադրություն դարձրեք վեբ-կայքի Uniform Resource Locator (URL)-ին: «https»-ով սկսվող URL-ները ցույց են տալիս, որ կայքն ապահով է, մինչդեռ «http»-ը՝ ոչ
  - Փնտրեք այսպես կոչված Փակ կողպեքի պատկերակ (icon)՝ նշանը, որ ցանցի միջոցով փոխանցման ժամանակ Ձեր տեղեկատվությունը կգաղտնագրի:
- Եթե վստահ չեք, թե արդյոք էլեկտրոնային փոստի հարցումն օրինական է, փորձեք ստուգել այն՝ ուղղակիորեն կապվելով ընկերության հետ: Սակայն մի օգտագործեք էլ.փոստով ստացված կոնտակտային տվյալները: Փոխարենը ստուգեք ընկերության կոնտակտային տվյալները տարբեր այլընտրանքային աղբյուրների միջոցով (որոնողական համակարգեր, սոցիալական ցանցերում գրառումներ ու խմբեր և այլն)
- Տեղադրեք և օգտագործեք հակավիրուսային ծրագրեր, firewalls և էլ.փոստի զտիչներ

- Օգտվեք Ձեր էլ.փոստի հաճախորդի և վեբ բրաուզերի կողմից տրամադրված հակաֆիշինգի հնարավորությունից
- Օգտագործեք բազմագործոն նույնականացում (MFA):

Ի՞նչ եք անում երբ կարծում եք, որ զոհ եք

- Եթե կարծում եք, որ Դուք բացահայտել եք Ձեր կազմակերպության վերաբերյալ հուզական տեղեկատվություն, անպայման տեղեկացրեք կազմակերպության համապատասխան աշխատակիցներին (տեղեկատվական անվտանգության վարչություն, IT վարչություն)
- Եթե կարծում եք, որ Ձեր բանկային հաշիվները կարող են վտանգված լինել, անմիջապես դիմեք Ձեր ֆինանսական հաստատությանը (բանկին) և փակեք ցանկացած վտանգված հաշիվ: Վերահսկեք Ձեր հաշիվը ցանկացած անբացատրելի գործարքների համար
- Անմիջապես փոխեք բոլոր գաղտնաբառերը, որոնք կարող են հայտնի լինել հարձակվողին: Եթե Դուք օգտագործում եք նույն գաղտնաբառը տարբեր ռեսուրսների համար, համոզվեք, որ այն փոխում եք

յուրաքանչյուր հաշվի համար և այլևս չօգտագործեք այդ գաղտնաբառն ապագայում

¬ Կապ հաստատեք ոստիկանության հետ և տեղեկացրեք կիբերհարձակման մասին:

2.3. Ապատեղեկատվությունն առցանց տիրույթում. Նույնականացում և վերահսկման կանխարգելիչ մեխանիզմներ

Եվրոպական խորհրդի պարզաբանմամբ՝ քարոզչությունը, ապատեղեկատվությունը և կեղծ լուրերը կարող են նպաստել հասարակական կարծիքի բևեռացմանը, բռնի ծայրահեղականությանը և ատելության խոսքին և, ի վերջո, քայքայել ժողովրդավարությունները և նվազեցնել վստահությունը նրանց նկատմամբ:

«Քարոզչություն», «ապատեղեկատվություն» և «կեղծ լուրեր» եզրույթները հաճախ օգտագործվում են փոխադարձաբար: Դրանք օգտագործվում են հղում կատարելու տարբեր եղանակներով, որոնց միջոցով տեղեկատվության

փոխանակումը դիտավորյալ կամ ակամա վնաս է պատճառում, սովորաբար՝ կապված որոշակի բարոյական կամ քաղաքական գործի կամ տեսակետի առաջմղման հետ:

Կարող ենք առանձնացնել տեղեկատվության երեք հստակորեն տարբեր օգտագործում, որոնք պատկանում են MDM կատեգորիային.

- **Mis-information (ոչ ճիշտ տեղեկատվություն)** - կեղծ տեղեկատվություն, որը տարածվել է առանց վնաս պատճառելու մտադրության
- **Dis-information (ապատեղեկատվություն)** - կեղծ տեղեկատվություն, որը տարածվել է վնաս պատճառելու մտադրությամբ
- **Mal-information (վնասակար տեղեկատվություն)** - ստույգ տեղեկատվություն, որը տարածվել է վնաս պատճառելու մտադրությամբ:

Թեև այս երևույթներից և ոչ մեկը արտասովոր չէ, դրանք վերջերս նոր նշանակություն են ձեռք բերել տեղեկատվական և հաղորդակցական տեխնոլոգիաների (ICT) բարդ ձևերի լայն տարածումով: Օրինակ՝ տեքստի, լուսանկարների, տեսանյութերի կամ հղումների առցանց փոխանակումը թույլ

է տալիս տեղեկատվությունը մի քանի ժամվա ընթացքում դառնալ վիրուսային:

2.3.1. Ինչպես բացահայտենք MDM

Քննադատորեն գնահատեք տեղեկատվական լանդշաֆտը և ժամանակ տրամադրեք աղբյուրներն ու հաղորդագրությունները վերանայելու համար:

Ցանկացած ձևով բովանդակությանը ծանոթանալիս ինքներդ Ձեզ տվեք հետևյալ հարցերը.

- Արդյո՞ք դա հուզական արձագանք է առաջացնում
- Արդյո՞ք համարձակ հայտարարություն է անում վիճահարույց հարցի վերաբերյալ
- Արդյո՞ք սա անսովոր պնդում է
- Արդյո՞ք այն պարունակում է clickbait
- Արդյո՞ք այն պարունակում է համապատասխան տեղեկատվություն, որը համապատասխանում է համատեքստին
- Արդյո՞ք այն չափազանցնում կամ խեղաթյուրում է փոքր քանակությամբ տեղեկատվություն

- Արդյո՞ք այն վիրուսային է դարձել չստուգված կամ քիչ ստուգված հարթակներում:

Սրանք մի քանի ուղղորդող հարցեր են, որոնք կօգնեն Ձեզ բացահայտել MDM-ը: Եթե նույնիսկ հարցերից մեկը վերաբերում է աղբյուրին, դա ինքնաբերաբար չի վարկաբեկում տեղեկատվությունը: Դա նման է այն բանին, որ Ձեր հետազոտությունն անեք նախքան դրան վստահելը:

2.3.2. Ինչպե՞ս կարող են կազմակերպությունները միջոցներ ձեռնարկել MDM-ի դեմ

Կազմակերպությունները կարող են պաշտպանվել MDM սպառնալիքներից՝ օգտագործելով հետևյալ ռազմավարությունները և վերահսկողությունը.

- Ստեղծեք սոցիալական մեդիայի և վեբ մոնիթորինգի համակարգ, ինչպես նաև ահազանգման ծառայություններ՝ Ձեր ապրանքանիշի և կազմակերպությունների հետ կապված կեղծ լուրերը բացահայտելու և հետևելու համար: Այս ծառայությունները հաճախ թույլ են տալիս վերահսկել ոչ

միայն Ձեր սեփական սոցիալական մեդիայի պրոֆիլները, այլև հանրային գրառումները, վեբ ֆորումները, վեբ-կայքերը, ակնարկները, հիշատակումները և այլն

- Օգտագործեք որոնման համակարգի օպտիմալացում (SEO)՝ թափանցիկ, բարձրորակ բովանդակությամբ ցանկացած վեբ-կայքում: SEO-ն օգտագործվում է Ձեր կայքը և սոցիալական մեդիան որոնման համակարգերի (օրինակ՝ Google-ը) օպտիմալացնելու համար և կարող է տարբերություն դնել վեբ-կայքի դիրքի ցուցադրման միջև (Ձըր կազմակերպությանն ուղղված MDM-ից վեր կամ ներքև)
- Օգտագործեք Answer Engine Optimization-ը (AEO), որը կենտրոնանում է ձայնային ասիստենտների վրա, ինչպիսիք են Google Home-ը, Amazon Alexa-ն կամ Siri-ն՝ օպտիմալացնելու այս սարքերի պատասխանները՝ Ձեր կազմակերպության մասին փաստերը նշելու համար, այլ ոչ թե կեղծ տեղեկատվություն
- Օգտագործեք հզորացման ցանցեր՝ Ձեր բովանդակության հասանելիությունն ու տեսանելիությունը բարձրացնելու համար, միաժամանակ կանխելով կեղծ տեղեկատվության

տարածումը: Հզորացնդող ցանցերը հանդես են գալիս որպես «ճշմարտության խոսողներ» և կարող են ներառել կազմակերպության գործընկերներին, ապրանքանիշի դեսպաններին և առկա հաճախորդներին

- Խրախուսեք ներգրավվածությունը Ձեր հաճախորդների և օգտատերերի հետ՝ վստահության ձևավորման և պահպանման համար: Օրինակ, որոնման համակարգերն օգտագործում են օգտատերերին և նրանց ակնարկները՝ ապրանքանիշի վստահելիությունն ավելի լավ գնահատելու համար
- Ստեղծեք արձագանքման թիմ՝ անուղղակիորեն հակազդելու MDM ցանկացած քարոզարշավին՝ ապահովելով սեղմ ժամկետներում օգտատերերին պատասխանների տրամադրումը
- MDM-ի հետ ուղիղ կապի մեջ մի մտեք: Պատասխանները պետք է կրեն պասիվ բնույթ և չպետք է տեղադրվեն այն գրառման տակ, որտեղ նշվում է MDM: Փոխարենը՝ պատասխանը կարող եք տեղադրել Ձեր վեբ-կայքում: Համոզվեք, որ MDM-ի պատասխանը ներառում է մանրամասն, թափանցիկ, փաստացի պատասխաններ: Արձագանքման մոտեցումները կարող են տարբեր լինել՝

կախված կազմակերպությունից:

2.3.3. Ինչպե՞ս կարող են օգտատերերը միջոցներ ձեռնարկել MDM-ի դեմ

Որպես տեղեկատվության սպառող՝ Դուք կարող եք ձեռնարկել հետևյալ գործողությունները՝ հետագայում բովանդակությունը հետաքննելու և MDM-ից պաշտպանվելու համար.

- ¬ Գտեք դիզայնի անտեղի տարրեր, ինչպիսիք են ոչ պրոֆեսիոնալ լոգոները, գույները, տարածությունները և անիմացիոն gif-երը
- ¬ Ստուգեք տիրույթի անունները՝ համոզվելու համար, որ դրանք համապատասխանում են կազմակերպությանը: Դոմենի անունը կարող է պարունակել սխալ կամ օգտագործել վերին մակարդակի տիրույթ (TLD), ինչպիսիք են .net կամ .org
- ¬ Ստուգեք, որ կազմակերպությունն ունի կոնտակտային տվյալներ, ֆիզիկական հասցե և «Մեր մասին» էջ
- ¬ Կատարեք WHOIS տիրույթի որոնում՝ տեսնելու, թե ում է պատկանում տիրույթը և հաստատեք, արդյոք այն

պատկանում է վստահելի կազմակերպությանը: WHOIS-ը դոմենի անունների տվյալների բազա է և պարունակում է տվյալներ տիրույթի սեփականատիրոջ, տիրույթի գրանցման և ժամկետի ավարտի մասին

- Կատարեք հակադարձ պատկերների որոնում (reverse image search), որպեսզի համոզվեք, որ պատկերները չեն պատճենվում օրինական վեբ-կայքից կամ կազմակերպությունից
- Օգտագործեք փաստերի ստուգման կայք, որպեսզի համոզվեք, որ Ձեր կարդացած տեղեկատվությունն արդեն իսկ ապացուցված չէ, որ կեղծ է
- Ինքնաբերաբար մի ենթադրեք, որ ստացված տեղեկատվությունը ճիշտ է, նույնիսկ եթե այն ստացել եք վստահելի աղբյուրից (օրինակ՝ ընկերոջից կամ ընտանիքի անդամից)
- Համոզվեք, որ տեղեկատվությունը հին չէ:

2.4. Մատակարարման շղթայի կիբերանվտանգություն

2.4.1. Ներածություն. Ի՞նչ է մատակարարման շղթան

ԵՄ-յան կիբերանվտանգության գործակալության սահմանման համաձայն՝ (The European Union Agency for Cybersecurity – ENISA) - «մատակարարման շղթան ներկայացնում է գործընթացների, մարդկանց, կազմակերպությունների և դիստրիբյուտորների էկոհամակարգ, որոնք մասնակցում են վերջնական լուծման կամ արտադրանքի ստեղծման և մատուցման գործընթացին: Կիբերանվտանգության մատակարարման շղթան ներառում է ռեսուրսների լայն շրջանակ (տեխնիկային և ծրագրային ապահովում)՝ պահեստավորում (քլաուդային կամ տեղային), բաշխման մեխանիզմներ (վեբ հավելվածներ, առցանց խանութներ) և կառավարման ծրագրային ապահովում»:

ENISA սահմանում է մատակարարման շղթայի չորս հիմնական տարրեր.

- **Մատակարար.** միավոր, որն ապրանք կամ ծառայություն է մատակարարում մեկ այլ կազմակերպության

- **Մատակարարի ակտիվներ.** արժեքավոր տարրեր, որոնք մատակարարն օգտագործում է ապրանք կամ ծառայություն արտադրելու համար
- **Օգտատեր.** սուբյեկտ, որը սպառում է մատակարարի կողմից արտադրված ապրանքը կամ ծառայությունը
- **Օգտատիրոջ ակտիվներ.** արժեքավոր տարրեր, որոնք պատկանում են թիրախին:

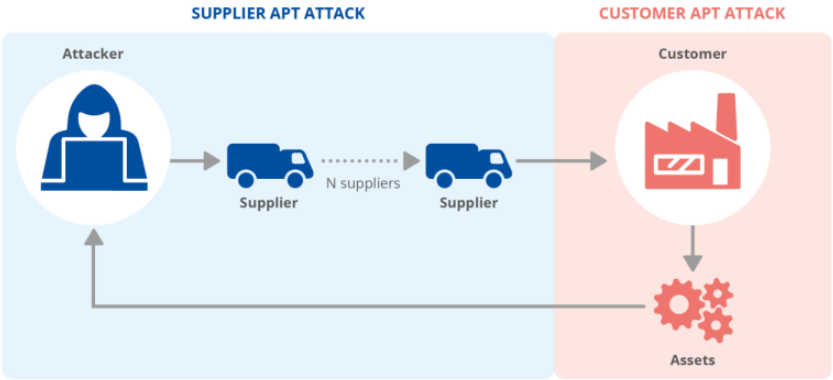
Միավորը կարող է լինել անհատ, անհատների խումբ կամ կազմակերպություն: Ակտիվները կարող են լինել մարդիկ, ծրագրեր, փաստաթղթեր, ֆինանսներ, սարքավորումներ կամ այլք:

2.4.2. Ինչպե՞ս են օգտագործում հարձակվողները

Ըստ ENISA-ի՝ մատակարարման շղթայի հարձակումը առնվազն երկու հարձակումների համակցություն է: Առաջին հարձակումը մատակարարի վրա է, որն այնուհետև օգտագործվում է թիրախի վրա հարձակվելու համար՝ ակտիվներին հասանելիություն ստանալու համար: Թիրախը կարող է լինել օգտատերը կամ այլ մատակարար: Հետևաբար, որպեսզի հարձակումը դասակարգվի որպես

մատակարարման շղթայի հարձակում, պետք է թիրախավորվեն և՛ մատակարարը, և՛ հաճախորդը:

Դիագրամը ցույց է տալիս «պարզ մեխանիզմը», թե ինչպես է մատակարարման շղթան հարձակվում հաքերային խմբերի կողմից (Advanced Persistent Threat - APT): Նախ, մատակարարը վտանգված է, որն այնուհետև վտանգում է օգտատիրոջը:

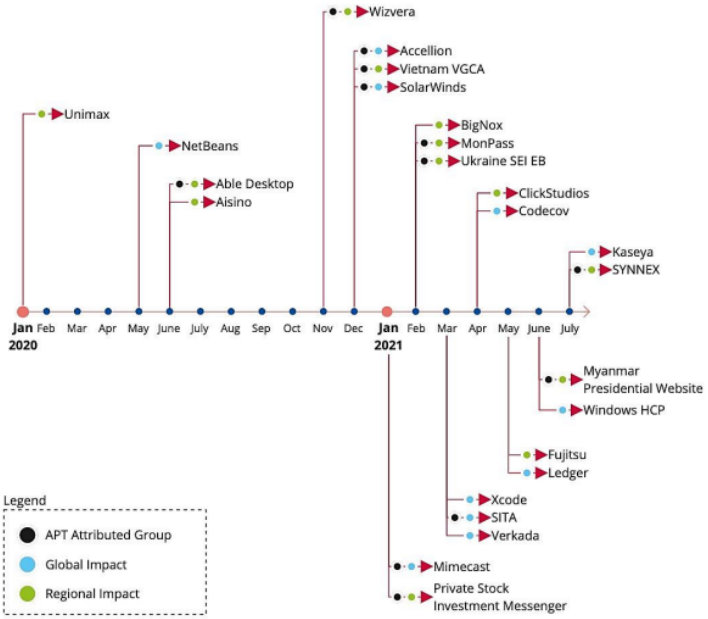


Դիագրամ #1 ՝ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

2.4.3. Ինչու՞ է կարևոր

2020-2021 թվականներին մենք տեսանք մատակարարման շղթայի մի շարք հարձակումներ՝ տարբեր երկրների պետական և մասնավոր կառույցների վրա: Դիագրամա #2-

ում ներկայացված տարբեր հարձակումների վերաբերյալ տեղեկություններից ուշագրավ է այն փաստը, որ հարձակումների հետևում հիմնականում կանգնած են պետության կողմից հովանավորվող APT խմբերը և այդ հարձակումներն ունեցել են ինչպես տարածաշրջանային, այնպես էլ համաշխարհային ազդեցություն:



Դիագրամ #2՝ ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

Վերոհիշյալ հարձակումների ամենահայտնի օրինակներից մեկը SolarWinds Orion-ի դեպքն է: Նշված հարձակումը վերագրվել է Ռուսաստանի Արտաքին հետախուզության ծառայության (Russian Foreign Intelligence Service (SVR)) հետ կապ ունեցող APT 29 խմբին:

2.4.4. Մատակարարման շղթայի տեսակներ

Մատակարարման շղթայի անվտանգության հարցը համակարգային է և կարևոր է ճիշտ մոտեցման ընտրությունը: Օրինակ, մենք կարող ենք դիտարկել մատակարարման շղթայի տարրերի հետևյալ կատեգորիաները.

2.4.5. Վնասակար ծրագրային ապահովման գնում

ICT մատակարարման շղթայի հետ կապված ռիսկերի առաջին օրինակներից է վնասակար ծրագրերի գնումը/օգտագործումը: Դասական իմաստով՝ ծրագրային ապահովում.

1. Կարող է պարունակել վնասակար կոդ, որը վնասում է օգտատիրոջը
2. Կարող է հավաքագրել օգտատիրոջ մասին հուզական տեղեկատվություն:

<u>Դիտարկենք վտանգ պարունակող ծրագրային ապահովման մի քանի դեպքեր</u>

I. **Kaspersky անվտանգության համակարգ** - տարիներ շարունակ Վրաստանում ամենատարածված անվտանգության համակարգերից մեկը Kaspersky հակավիրուսն էր: Ե՛վ մասնավոր, և՛ հասարակական կազմակերպություններն ակտիվորեն օգտագործում էին «լեգենդար» հակավիրուսը, որն, ինչպես ասում էին, «լավ էր բռնում ռուսական վիրուսները»: ԱՄՆ Հաղորդակցման դաշնային հանձնաժողովը (Federal

Communications Commission) Կասպերսկու արտադրանքը համարել է սպառնալիք ազգային անվտանգության համար և արգելել է դրանց օգտագործումը: Նմանապես, Մեծ Բրիտանիայի և Գերմանիայի կառավարությունները կոչ են արել սպառողներին զերծ մնալ վերը նշված ապրանքներից:

II. **Mail.Ru** - ռուսական փոստային ծառայություն, որն ակտիվորեն կիրառվում է հետխորհրդային տարածքի երկրներում: Օգտատիրոջ համար կարևոր է գիտակցել, որ նման ծառայությունից օգտվելիս ռուսական հատուկ ծառայությունները կարող են օգտագործել իրենց անձնական տվյալները, նամակագրությունը, շահերը և վարքագիծը:

III. **1C ERP** – 1C ռուսական ընկերություն է, որի արտադրանքը 1C ERP Վրաստանում լայնորեն տարածված է: Բացի այդ, տեղական շուկայում կան բազմաթիվ խորհրդատվական ընկերություններ, որոնք ապահովում են այս համակարգի զարգացումը և աջակցությունը: Որոշում կայացնելիս ընկերության ղեկավարների համար կարևոր է գիտակցել, որ կազմակերպության բիզնես գործընթացների

թվայնացման համար օգտագործվող ռուսական ծրագրային ապահովումը պարունակում է հետևյալ ռիսկերը. մատակարարման շղթայի հարձակման պարզությունը և ռուսական արտադրանքի վրա կախվածությունը (որը կարող է այլևս հասանելի չլինել՝ հաշվի առնելով աշխարհաքաղաքական իրավիճակը և պատժամիջոցները):

IV. **Yandex Taxi -** տաքսի ծառայություն, որն օգտագործում է ռուսական ծրագրային ապահովումը և հավաքագրում է օգտատիրոջ մասին տարբեր տեսակի անձնական և բանկային տվյալներ՝ անուն, ազգանուն, հասցե, հեռախոսահամար, տեղաշարժման երթուղիներ, բանկային քարտի տվյալներ և այլն: Տարբեր աղբյուրների համաձայն՝ Յանդեքսն ակտիվորեն համագործակցում է Ռուսաստանի Անվտանգության դաշնային ծառայության հետ և տեղեկատվություն է տրամադրում օգտատերերի մասին, ինչը պարտադրում է Ռուսաստանի օրենքը: Առանձին-առանձին մեկ օգտատիրոջ մասին տեղեկատվությունը կարող է կարևոր չլինել, սակայն ազգային մակարդակում մեծ քանակությամբ

անձնական տվյալների փոխանցումը թշնամական պետություն ստեղծում է ազգային անվտանգության նոր մարտահրավերներ:

Յուրաքանչյուր ամբողջական և սպառիչ չէ:

2.4.6. Վտանգ պարունակող սարքի գնում

Սարքավորումների ռիսկային գնումների ամենատարածված օրինակներից մեկը **չինական արտադրության հսկողության համակարգերի գնումն է**: Միջազգային լավագույն փորձը ցույց է տալիս, որ սարքավորումները կարող են օգտագործվել նաև մատակարարման շղթայի հարձակումներում: Հետևաբար, **զարգացած** երկրներն աշխատում են վտանգավոր սարքավորումներ արտադրողներին հայտնաբերելու և դրանք արգելելու ուղղությամբ: Օրինակ՝ **չինական Huawei, Dahua, Hikvision սարքավորումների օգտագործումը/գնումն ԱՄՆ պետական կառույցներում արգելված է** (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, https://www.acquisition.gov/far/4.2101).

2.4.7. Աջակցության ծառայություններին առընչվող ռիսկեր

Ծրագրային ապահովման և սարքավորման մատակարարման շղթայի ռիսկերը դիտարկելիս կարևոր է ճիշտ գնահատել աջակցության ծառայություններ մատուցողի հետ կապված ռիսկերը: Մասնավորապես, ցանկացած ծրագրային ապահովման կամ սարքավորման գնումը ենթակա է ուղեկցող երաշխիքային պայմաններին և աջակցության համապատասխան ծառայություններին: Ծրագրի սկզբնական փուլում որոշվում են կարիքները, ընտրվում, գնահատվում և ինտեգրվում է լիցենզիաների կամ տեխնիկականական լուծումների շրջանակը, որին հաջորդում են տարբեր տեսակի օժանդակ ծառայություններ (օրինակ՝ ա) 5 աշխատանքային օր, 9 աշխատանքային ժամ, բ) 7 օր, 24 ժամ և այլն):

Կարևոր է հաշվի առնել աջակցության ծառայություն մատուցող ընկերության տարածաշրջանը և ապահովել համագործակցությունը բարեկամ կամ չեզոք երկրի գրասենյակի ներկայացուցիչների հետ:

2.4.8. Խորհրդատվական ծառայությունների մատուցմանն առընչվող ռիսկեր

Ինչպես ծրագրային ապահովման և սարքավորումների գնումների դեպքում, **կարեւոր է կառավարել ծառայությունների մատակարարման շղթայի սպառնալիքները: Խորհրդատվական ծառայությունների հետ կապված ռիսկերը ներառում են.**

Խորհրդատուներ ընտրելիս կարևոր է հաշվի առնել նրանց նախապատմությունը և մասնագիտական հմտությունները: Խորհրդատվական ծառայություններ մատուցելիս խորհրդատուները հավաքագրում են տեղեկատվություն կազմակերպության ենթակառուցվածքի մասին, ուսումնասիրում են թույլ և ուժեղ կողմերը, հետևում են աշխատակիցների հմտություններին և կրիտիկական իրավիճակներում գործելու պատրաստակամությանը: Կարևոր է, որ կազմակերպությունը հասկանա վերը նշված ռիսկերը և ապահովի, որ կազմակերպության մասին կարևոր տեղեկատվության փոխանցումն առավելագույնս սահմանափակվի թշնամական երկրների ներկայացուցիչներով: Նման խորհրդատվական ծառայությունների օրինակներ են՝ ֆինանսական աուդիտ,

համապատասխանության աուդիտ, IT աուդիտ, կազմակերպչական աուդիտ, տեղեկատվական անվտանգության աուդիտ և խորհրդատվական ծառայություններ, IT գնահատում, IT ենթակառուցվածքային նախագծեր և այլն:

2.4.9. IT կադրերի միգրացիա

Ռուսաստանի Դաշնության դեմ կիրառվող պատժամիջոցներին զուգահեռ IT ոլորտի բազում ռուս մասնագետներ տեղափոխվել են Վրաստան՝ պատժամիջոցներից խուսափելու և եվրոպական ու միջազգային նախագծերի վրա աշխատանքը շարունակելու համար: Վրաստանը բավականին լավ հարկային օրենսդրություն ունի՝ ծրագրային ապահովման մշակողներին և ծրագրային ապահովման արտադրողներին ներգրավելու համար (եկամտահարկ մինչև 5 տոկոս):

Ներկա պահին անհնար է ճշգրիտ գնահատել վերը նշված միգրացիայի հնարավոր հետևանքները: Բացի այդ, որակյալ կադրերի հոսքը կարող է նպաստել պետական և մասնավոր ընկերությունների թվային վերափոխմանը, քանի որ

Վրաստանը IT ոլորտի որակյալ կադրերի պակաս ունի: Տեղական ընկերությունները, այդ թվում՝ երկրի կարևոր տեղեկատվական ենթակառուցվածքը, հնարավորություն ունեն լրացնել շուկայում առկա բացը նոր ի հայտ եկած հմուտ միգրանտներով և նրանց ընկերություններով այն ժամանակ, երբ գործնականում կան ռիսկերը փոխհատուցելու արդյունավետ վերահսկողության շատ քիչ մեխանիզմներ:

Երկրորդ հերթին, **արագացված թվային փոխակերպման գինը կարող է լինել կարեւոր տեղեկատվական ենթակառուցվածքը:** Հաշվի առնելով Ռուսաստանի հետ տարածաշրջանային հարաբերությունների համատեքստը՝ Վրաստանը բախվում է աճող սպառնալիքների՝ կապված մատակարարման շղթայի և այսպես կոչված ներքին սպառնալիքներով (insider threat): **Դասական սահմանմամբ՝ վերոհիշյալ ստարտափները չեն համապատասխանում մատակարարման շղթայի հարձակումների սահմանմանը, սակայն Ռուսաստանի հետախուզական ծառայությունները սովորաբար ռուսական ընկերություններից ուղղակի կամ անուղղակի մուտք են փնտրում հաճախորդների տվյալներին՝ ստեղծելով ինչպես մատակարարման շղթա, այնպես էլ ներքին սպառնալիքներ:**

Բացի այդ, Վրաստանի պետական սեկտորը քիչ կունենա կամ ընդհանրապես չի ունենա իրավական լծակներ՝ զտելու տեղական գրանցված IT ընկերություններին իր թենդերներից:

2.5. Սոցիալական ցանցերի անվտանգ կիրառում

Վերջին տասնամյակում սոցիալական ցանցերը մեծ ժողովրդականություն են վայելում: Սա հիանալի հնարավորություն է Ձեր ընկերների, ընտանիքի կամ բոլորովին անծանոթ մարդկանց հետ կայուն կապեր հաստատելու համար: Դրա միջոցով ժամանակակից մարդը ստանում է ծով տեղեկատվություն՝ ըստ կոնկրետ հետաքրքրությունների և ծանոթ շրջանակի: Ամեն օր միլիոնավոր մարդիկ օգտվում են տարբեր սոցիալական ցանցերից, և նրանց ընդհանուր թիվը հասնում է մի քանի միլիարդի: Դրանցից ամենահայտնիներն են Facebook-ը, TikTok-ը, Instagram-ը, WeChat-ը, PinTerest-ը, Linkedin-ը և այլն: Շատ հայտնի կազմակերպություններ և անհատներ ստեղծել են սոցիալական ցանցի հաշիվ և այն օգտագործում են որպես լայն լսարանի հետ կապ հաստատելու և շփվելու միջոց:

Առաջարկում ենք 10 խորհուրդ, որոնք պետք է հաշվի առնել սոցիալական ցանցերից անվտանգ օգտվելու համար.

2.5.1. Ստուգեք կարգավորումները

Սոցիալական ցանցի օգտագործումը սկսվում է դրանում գրանցվելուց՝ այսպես կոչված հաշիվ ստեղծելով: Արդեն այս փուլում Դուք կհանդիպեք քայլ առ քայլ հաղորդագրություններին և առաջարկություններին, թե ինչ անել գրանցման ժամանակ: Օրինակ՝ հեշտ հիշվող գաղտնաբառ մուտքագրելիս սոցիալական ցանցն ավտոմատ կերպով Ձեզ խորհուրդ կտա բարդ գաղտնաբառ դնել, և որպես տարբերակներից մեկը կառաջարկի նաև անվտանգության լրացուցիչ միջոց, օրինակ՝ Ձեր բջջային հեռախոսահամարին միանվագ կոդ ստանալով կանցնեք նույնականացում: Մի անտեսեք այս առաջարկությունները և հաշվի առեք անվտանգության պահանջները նույնիսկ սկզբնական փուլում:

Գրանցվելուց հետո լավ կլինի այցելել մենյուի անվտանգության և գաղտնիության բաժինները: Այստեղ Դուք կգտնեք բոլոր կարևոր կարգավորումները, որոնք կարող եք

կարգավորել՝ էապես նվազեցնելու ապագա միջադեպերի հավանականությունը, ինչպիսիք են՝

- Ձեր աքաունթի այսպես կոչված կոտրում/հաքերավորում, այսինքն՝ չարտոնված մուտք
- Ձեր կողմից կառավարվող էջերի կորուստ
- Ձեր անձնական նամակագրությունն ուրիշների ձեռքը գցել-հանրայնականացնել
- Անցանկալի անձանց կողմից անհանգստացնող նամակներ և
- Պոտենցիալ վտանգավոր հղումներ ստանալ և այլն:

Հիշեք, որ անվտանգության կարգավորումները կարգավորելու վրա ծախսված մի քանի րոպեն ապագայում Ձեզ շատ ժամանակ և նյարդեր կխնայի, ամենայն հավանականությամբ, կկանխի տհաճ միջադեպերը և կնվազեցնի կիբերանվտանգության ռիսկերը:

2.5.2. Ճանաչեք և կառավարեք Ձեր ընկերական շրջապատը

Այն բանից հետո, երբ գրանցվում եք սոցիալական ցանցում, սովորաբար առաջին քայլը դա ծանոթ-ընկերներին և հետաքրքիր անհատականություններին այսպես կոչված «ընկերներ»-ում ավելացնելն է: նրանց էջերին «հետևել/Following»-ը և նրանց հետ նամակագրություն ունենալն է:

Եղեք ուշադիր և ստուգեք, թե ում եք ավելացնում Ձեր ընկերների շրջանակում: Կիբերհանցագործները հաճախ ստեղծում են կեղծ հաշիվներ՝ Ձեր անձնական տվյալների հասանելիություն ստանալու կամ խարդախության միջոցով գումար կորզելու համար:

Ինչպես նաև մի մոռացեք, որ այս կամ այն մարդուն «ընկերներ»-ում ավելացնելուց հետո նա հնարավորություն կունենա տեսնելու այն լուսանկարը, տեսանյութը կամ տեքստային նյութը, որը Դուք հրապարակայնորեն չեք տեղադրում և տեղադրում եք միայն ընկերների շրջանակի համար:

Երկրորդ հերթին, կարևոր է հետևել, թե որ էջերն եք հավանում և հետևում, լինի դա կազմակերպություն, ընկերություն, թե հայտնի մարդ: Այս դեպքերում նույնպես հաճախ ստեղծվում են կեղծ և նմանատիպ էջեր, որոնք հաճախ ապատեղեկատվություն և ապակողմնորոշիչ ենթատեքստ (բովանդակություն) են տարածում:

2.5.3. Մեկ անգամ կիսվելը նշականում է ընդմիշտ կիսվել. ինչո՞վ եք կիսվում

Զգույշ եղեք Ձեր հեղինակության նկատմամբ, իմացեք, որ սոցիալական ցանցում մեկ անգամ «տեղադրված» տեղեկատվությունը կարող է ընդմիշտ մնալ այնտեղ, նույնիսկ եթե այն հեռացնեք կամ ջնջեք այն տեղադրելուց 2 րոպե անց: Նախքան որևէ տեսակի կոչ անելը, լուսանկար կամ տեսանյութ տարածելը, լավ մտածեք: Մտածեք սպասվող արդյունքների մասին: Ի՞նչ կարող է ստացվել դրանից: Շատ դեպքերում մարդիկ կարող են տարբեր մեկնաբանություններ տալ նույն իրադարձությանը, ուստի անվնաս մեկնաբանությունը, կարծիքը կամ լուսանկարը/տեսանյութը կարող են տարբեր կերպ ընկալվել մարդկանց տարբեր

խմբերի կողմից:

Մի քանի ուսումնասիրություններ են իրականացվել սոցիալական ցանցի ազդեցության կապակցությամբ, որը ցույց է տվել, որ, օրինակ, հարցված գործատուների ավելի քան 70%-ը հրաժարվել է աշխատանքի ընդունել թեկնածուներին՝ նախկինում նրանց կողմից սոցիալական ցանցում տեղեկատվություն հրապարակելու պատճառով:

Ինչպես նաև ամիսներ կամ տարիներ անց հաճախակի են լինում անախորժություններ, կոնֆլիկտներ, անհարմար իրավիճակներ՝ կապված որոշակի ժամանակահատվածում սոցիալական ցանցում իրականացված ակտիվության հետ:

2.5.4. Ուշադիր եղեք թե ում եք կիսվում

Հատկանշական է, որ վերը նշված ռիսկերը որոշ չափով կարող են նվազել այն մեխանիզմներով, որոնք ունի սոցիալական ցանցերի մեծ մասը, այսինքն՝ սահմանափակելով թիրախային լսարանը, մասնավորապես՝ կարող եք որոշել, թե ով կարող է.

- Տեսնել Ձեր կոնկրետ հրապարակումը, լուսանկարը կամ տեսանյութը
- Դրա առթիվ Ձեր մեկնաբանությունը
- Ձեզ ներքին կարգով նամակ գրելը և այլն:

Ինչպես նաև կարող եք սահամանել թե ինչքանով է Ձեր ցանկացած հրապարակումը հանրային, միայն ընկերների համար, միայն ընկերների փոքր շրջանակի համար, կամ պարզապես միայն Ձեզ համար, որպեսզի հետագայում հիշեք և հրապարակեք:

2.5.5. Իմացեք, թե ինչպես վարվել հատուկ իրավիճակներում

Գոյություն ունեն նախապես սահմանված ուղիներ, թե ինչպես վարվել հատուկ դեպքերում: Օրինակ, եթե ինչ-որ մեկը ենթարկում է բուլինգի, շանտաժի, նվաստացնում է և այլն: Դուք կարող եք գրել սոցիալական ցանցին համապատասխան հաղորդագրությունով և հայտնել դրա մասին, այսինքն՝ խնդրել վարչակազմին հետաքննել նշված դեպքերը և միջոցներ ձեռնարկել ընդդեմ կոնկրետ հաշվի:

Չնայած այն բանին, որ հաճախ է կեղծ հաշիվներով վերը նշված գործողությունների կարարումը, այնուամենայնիվ, կարևոր է հետևել կոնկրետ սոցիալական ցանցի կանոններին: Ամենապարզ դեպքում պարզապես ջնջել կամ արգելափակել «վիրավորող» հաշիվները:

Ինչպես նաև նախապես ծանոթացեք այն քայլերին և գործողություններին, որոնք պետք է ձեռնարկեք սոցիալական ցանցի հասանելիությունը կորցնելու դեպքում: Իմացեք, թե ինչ անել, եթե կիբերհանցագործները կոտրեն Ձեր հաշիվը, և Դուք կորցնեք դրա նկատմամբ հասանելիությունը: Ծանոթացեք պայմաններին ու կանոններին: Նախապես պատրաստեք այն փաստաթղթերը կամ տեղեկությունները, որոնք ձեզնից կպահանջեն սոցիալական ցանցի վարչությունը կամ իրավապահ մարմինների աշխատակիցները:

Գոյություն ունեն որոշ տեխնիկական խորհուրդներ, որոնք զգալիորեն կնվազեցնեն ձեր սոցիալական ցանց չարտոնված հասանելիության հավանականությունը՝ այդպիսով նվազեցնելով հաքերների ու կիբերհանցագործների զոհ դառնալու ռիսկը:

2.5.6. Կիրառեք բարդ գաղտնաբառեր

Անպայման կիրառեք բարդ գաղտնաբառեր: Մի օգտագործեք նույն գաղտնաբառերը տարբեր կայքերում, քանի որ եթե մեկ ուրիշ տեղ կոտրեն Ձեր հաշիվը և իմանան գաղտնաբառը, ապա նույն գառտնաբառով կկարողանան մուտք գործել նաև Ձեր սոցիալական ցանցային հաշիվ: Ձգտեք ունենալ եզակի գաղտնաբառ բոլոր սոցիալական ցանցերում:

2.5.7. Միացրեք բազմագործոն նույնականացումը

Հատկապես կարևոր է միացնել լրացուցիչ նույնականացումը, որը ներառում է գաղտնաբառի հետ մեկ այլ նույնականացնող գործոնի ներմուծում: Հիմնականում դա մեկանգամյա կոդ է, որն ուղարկվում է Ձեր բջջային հեռախոսահամարին կամ ամենալավ պարագայում՝ մեկանգամյա կոդերի գեներատոր հավելված:

Իսկ լավագույն դեպքում կարելի է ձեռք բերել այսպես կոչված Hardware Token (օրինակ՝ Yubico USB/NFC/Lightning), որի ֆիզիկական տիրապետումն անհրաժեշտ է ցանկացած սոցիալական ցանցում կամ այլ ծառայության մեջ նույնականացման համար: Նույնիսկ եթե ինչ-որ մեկը ստանա

Ձեր գաղտնաբառը և մեկանգամյա SMS կոդը, նա, համենայնդեպս, չի կարողանա մուտք գործել Ձեր հաշիվ: Այս վերջին մեթոդը պահանջում է որոշակի գիտելիքներ և հմտություններ, որոնք կարելի է գտնել արտադրողի վեբ-կայքում և համապատասխան հրահանգներում:

2.5.8. Մինչ քլիք անելը ֆիքսեք

Հղումները սոցիալական ցանցերում (Post, Tweet, Messages) կիբերհանցագործների համար Ձեզ մոլորեցնելու և հուզական տեղեկատվություն ստանալու հեշտ միջոց են: Զգույշ եղեք, նախքան որևէ հղում սեղմելը, ինչպես նաև զգույշ եղեք այդ հղումներից որևէ բան ներբեռնելիս:

Եթե հղումը Ձեզ խնդրում է մուտքագրել սոցիալական ցանցի այն հաշվի անունը և գաղտնաբառը, որով Դուք մուտք եք գործել, իմացեք, որ շատ հավանական է, որ դա կիբերհանցագործների կողմից ստեղծած ծուղակ է՝ կոտրելու Ձեր հաշիվը:

2.5.9. Ստուգեք աղբյուրները

Սոցիալական ցանցերից ստացված տեղեկատվությունը զգալի ազդեցություն ունի մեր առօրյայի, որոշ դեպքերում՝ փաստերի ընկալման վրա: Վերջերս այն ակտիվորեն օգտագործվում է

- Հասարակական կարծիքի ձևավորման համար
- Ընտրություններին միջամտելիս
- Տրամադրության ուսումնասիրման կամ ձևավորելու համար
- Մարքեթինգային գործունեություն պլանավորելու համար
- Հատուկ ծառայությունների առաջադրանքներ կատարելու համար և այլն:

Սովորություն դարձրեք ստուգել Ձեր ստացած ցանկացած տեղեկատվության աղբյուրը: Հնարավորինս ճշտեք և պարզեք, թե ով, երբ, ինչու և ինչ ձևով է տարածում համապատասխան տեղեկատվությունը:

Զգույշ եղեք, նախքան եզրակացություններ անելը և տեղեկատվությունը վստահելի համարելը:

2.5.10. Ծանոթացեք անվտանգության և գաղտնիության հանձնարարականներին

Չնայած այստեղ ներկայացված ընդհանուր խորհրդին, կան անվտանգության և գաղտնիության հատուկ հանձնարարականներ՝ հարմարեցված տարբեր սոցիալական ցանցերին: Շատ դեպքերում այդ ամենը ներկառուցված է նույն սոցիալական հարթակում և ընդունում է հեշտ հասկանալի տեսողական խորհրդատվության և պարզաբանման ձև:

Ինչպես նաև ստեղծվում են բազմաթիվ վիդեո ուղեցույցներ, հոդվածներ և բլոգեր սոցիալական մեդիայի անվտանգ օգտագործման մասին:

Սոցիալական ցանցերն ամեն օր թարմացվում ու փոխվում են, հաճախ ստեղծվում են նոր տեսակի վեբ-կայքեր: Փորձեք հետևել վերջին խորհուրդներին և հանձնարարականներին, թե ինչպես դրանք անվտանգ օգտագործել: Եղեք մի քայլ առաջ կիբերհանցագործներից:

2.6. Բջջային սարքերի վտանգներ և պաշտպանական ուղիներ

Ձեր սմարթֆոնը կամ փլանշետը պահում է արժեքավոր տեղեկատվություն Ձեր, Ձեր ընտանիքի, ընկերների և գործընկերների մասին:

Երբևէ մտածե՞լ եք, թե ինչ տեղեկատվություն կարող է ստանալ մեկ ուրիշը, եթե ձեռք բերի Ձեր բջջային սարքը.

- Ձեր անձնական պլաններն ու գրությունները (Notes)
- Ձեր ծանոթ-բարեկամների մասին կոնտակտային տվյալներ
- Հուզական լուսանկարներ և տեսանյութեր
- Ո՞ւմ և երբ եք զանգում, զանգում են Ձեզ, որքան ժամանակով
- Գաղտնի ծառայության թղթապանակներ
- Ոչ հրապարակային և զիջող նամակագրություն (մեսենջերներ, սոցիալական ցանցեր)
- Տարբեր կայքերի և ծառայությունների գաղտնաբառեր
- Ինչ բովանդակության կայքեր եք մուտք գործում և ինչ եք դիտում
- Տեղեկատվություն ֆինանսական և բանկային եկամուտների մասին

- Տեղեկություններ նախկինում այցելած վայրերի մասին (որտեղ եք ապրում, աշխատում և ինչ վայրեր եք այցելում)
- Տեղեկություններ ձեր առողջության մասին (հիվանդություններ, պատվաստումներ, ֆիթնես, հուզական և վերարտադրողական առողջություն, վազքուղիներ, ալերգիաներ, ընդունված դեղամիջոցների տեսակը և ինտենսիվությունը)
- և այլն:

Հավանաբար տեսել եք մարդկանց, որոնք հուսահատ վիճակում են, որոնք կորցրել են իրենց բջջային սարքը: Այս նյարդայնության պատճառը պոտենցիալ վնասն է, որը կարող է պատճառել հեռախոսի տեղեկատվությունը չարտոնված ձեռքերում ընկնելը: Այս դեպքում վնասը շատ ավելի մեծ է, քան դրամական կորուստը, որն այս սարքի ձեռքբերման արժեքն է:

Հաշվի առեք ստորև բերված խորհուրդները՝ նվազեցնելու շարժական սարքերի հետ կապված կիբերանվտանգության ռիսկերը, պաշտպանելով Ձեզ, Ձեր սիրելիներին և Ձեր բիզնեսը:

2.6.1. Փին, գաղտնաբառ, մատնահետք և դեմք

Ձեր սարքը մուտք գործելու համար օգտագործեք բարդ փին-կոդեր և գաղտնաբառեր: Եթե սարքը թույլ է տալիս, լրացուցիչ սահմանեք մատնահետքը կամ դեմքի ճանաչումը: Սա պաշտպանության առաջին գիծն է, եթե կորցնեք Ձեր սարքը:

Կարևոր է, որ փին-ը կամ գաղտնաբառը բարդ լինեն (ոչ-1234 կամ ծննդյան տարեթիվ, մականուն), իսկ դրանք մի քանի անգամ սխալ մուտքագրելուց հետո բջջային սարքը որոշ ժամանակով բլոկ դրվի:

2.6.2. Թարմացումներ ու կրկնին թարմացումներ

Որպեսզի Ձեր բջջային սարքի օպերացիոն համակարգը և հավելվածները մշտապես թարմացվեն, ակտիվացրեք ավտոմատ թարմացումների գործառույթը: Հաքերները մշտապես փնտրում են ծրագրային ապահովման նոր խոցելիություններ: Արտադրողներն իրենց հերթին թողարկում են համապատասխան թարմացումները՝ նշված մարտահրավերներին դիմակայելու համար: Մշտապես թարմացվող օպերացիոն համակարգերը և հավելվածները շատ ավելի դժվարացնում են Ձեր բջջային սարքի կոտրումը:

Եթե հավելվածի թարմացումն ավարտվում է մի քանի վայրկյանում, ապա, որպես կանոն, օպերացիոն համակարգի (iOS, Android, Windows) թարմացումները պահանջում են որոշակի ժամանակ (10-20 րոպե), որի ընթացքում բջջային սարքը ժամանակավորապես չի կարող օգտագործվել: Մի հետաձգեք կարևոր թարմացումները կամ մի փոխեք համապատասխան անվտանգության կարգավորումները:

2.6.3. Հետևել

Ներբեռնեք և տեղադրեք կամ գործարկեք հատուկ հավելված՝ Ձեր բջջային սարքը համացանցով հետևելու համար: Այսպիսով, Դուք կկարողանաք գտնել շարժական սարքը կորցնելուց կամ գողանալուց հետո, իսկ վատագույն դեպքում՝ ջնջել դրանում առկա ցանկացած տեսակի տեղեկություն:

2.6.4. Վստահելի հավելվածներ

Ներբեռնեք հավելվածները միայն վստահելի և պաշտոնական հարթակներից.

- iPad-ի և iPhone-ի համար սա նշանակում է հավելվածներ

- ներբեռնել պաշտոնական Apple App Store-ից
- Անդրոիդի հավելվածները պետք է ներբեռնվեն Google Play-ից
- Amazon փլանշեթների համար՝ Amazon App Store-ից
- և այլն՝ արտադրողի կողմից նշված վստահելի ռեսուրսներից:

Երբ ներբեռնում եք հավելվածներ արտասահմանյան և քիչ հայտնի կայքերից, մեծ է հավանականությունը, որ դրանք ստուգում չեն անցնում և վիրուս են պարունակում:

Ինչպես նաև նախքան հավելված ներբեռնելը, ստուգեք, որ այն ունի դրական կարծիքներ օգտատերերի կողմից և ակտիվ թարմացումներ արտադրողի կողմից:

Խուսափեք անհայտ հավելվածներից, որոնք ունեն քիչ վարկանիշներ և հազվադեպ են անցնում թարմացման գործընթաց:

Եվ վերջում, անկախ նրանից, թե որտեղից եք ներբեռնել հավելվածը, խորհուրդ ենք տալիս հեռացնել այն, եթե այլևս դրա կարիքը չունեք կամ ակտիվորեն չեք օգտագործում:

2.6.5. Գաղտնիություն

Երբ ներբեռնում եք նոր հավելված, համոզվեք, որ ստուգել եք դրա գաղտնիության ընտրանքները: Օրինակ՝

- Արդյո՞ք հավելվածին անհրաժեշտ է հասանելիություն Ձեր բոլոր ընկերների կոնտակտային տվյալների նկատմամբ
- Մենք նաև խորհուրդ ենք տալիս անջատել տեղորոշման ծառայությունը բոլոր այն հավելվածների համար, որոնք, կարծում եք, որ կարիք չունեն որոշել Ձեր գտնվելու վայրը գործելու համար
- Եթե Ձեզ չեն բավարարում Ձեր սարքի համար հավելվածի տարբեր թույլտվությունները, օգտագործեք Ձեզ համար ընդունելի մեկ այլ անալոգ
- Ինչպես նաև պարբերաբար ստուգեք, թե հավելվածն ինչ գործառույթների համար ունի թույլտվություններ և համոզվեք, որ դրանք չեն փոխվել:

Իմացեք, որ հավելվածների կառավարման սանձերը Ձեր ձեռքերում են, և Դուք կարող եք որոշել, թե դրանցից ում հասանելի կլինի Ձեր **լուսանկարները, հաղորդագրությունները, տեսախցիկը, խոսափողը կամ գտնվելու վայրը:**

2.6.6. Պահեստային պատճեններ

Միշտ ունեցեք Ձեր տվյալների պահեստային պատճենները: Բջջային սարքերի դեպքում հնարավոր է պատճենավորել կամ փոխանցել լեփթոփներին ու անհատական սարքերին այսպես կոչված backup կամ օգտագործելով ներկառուցված առցանց կրկնօրինակում (օրինակ՝ օգտագործելով iCloud կամ Google Drive): Այս դեպքում Ձեր տեղեկատվությունը կպահվի նույնիսկ եթե ջնջեք այն, կորցնեք Ձեր սարքը կամ ֆիզիկապես վնասեք այն:

Համեմատաբար հեշտ է իրականացնել ավտոմատ կերպով պահեստային պատճենավորումը, սակայն լավ ծանոթացեք պահեստային պատճենների ստեղծման տեխնիկական հատկանիշներին:

Համոզվելու համար փորձեք մի քանի անգամ վերականգնել պահեստային պատճենները և համոզվեք, որ դրանք պահված են (պահեստավորված) Ձեզ համար ընդունելի կանոնի համաձայն.

- Պարբերականություն
- Ծավալ
- Հաճախականություն
- Պահեստային թղթապանակների բովանդակություն
- Պահեստային տարածք
- Պահպանման ձև
- և այլն:

2.6.7. Աշխատանք և հեռավար աշխատանք

Աշխատավայրում գտնվելու ժամանակ հատկապես զգույշ եղեք, որպեսզի տեսանկարահանման և լուսանկարահանման ժամանակ պատահաբար չնկարահանեք հուզական տեղեկատվություն (որի վրա երևում են գրատախտակներ, համակարգչի էկրաններ և այլն):

Վերջին շրջանում, համավարակի և այլ սպառնալիքների հետևանքով, մենք հաճախ ստիպված ենք աշխատել բջջային սարքերից, աշխարհի տարբեր ծայրերից՝ լինի դա տուն, սրճարան, հյուրանոց թե տրանսպորտ: Այս

դեպքում Ձեր բջջային սարքերի վրա հարձակման հավանականությունը հատկապես մեծ է, քանի որ կիբերհանցագործները գիտակցում են, որ Ձեր պաշտպանության մակարդակը շատ ավելի ցածր կլինի, քան աշխատավայրում (գրասենյակում)՝ կորպորատիվ-կազմակերպչական մակարդակում:

Հիշեք, որ եթե Դուք զբաղված եք և աշխատում եք շարժական/հեռակառավարմամբ, Ձեր շարժական սարքի չարտոնված մուտքը ոչ միայն վտանգի տակ է դնում Ձեր անձնական տվյալները, այլև այն կազմակերպության հուզական տեղեկատվությունը, որտեղ Դուք աշխատում եք: Դրա կորստի/արտահոսքի դեպքում Ձեր նկատմամբ կարող են կիրառվել կարգապահական-վարչական միջոցներ և ենթարկել պատասխանատվության:

2.6.8. Նվիրատվություն, վաճառք, նետում

Եթե որոշել եք փոխել Ձեր բջջային սարքը, լավ մտածեք նախքան հինը փոխելը: Հիշեք, թե ինչ տեղեկատվություն է այն

պարունակում: Ամբողջովին (և ոչ միայն լուսանկարները) ջնջեք Ձեր բջջային սարքը, օգտագործեք այսպես կոչված Factory Reset, Format ֆունկցիաները, որոնք ապահովում են դրանում պարունակվող բոլոր տեղեկատվության ամբողջական ջնջումը և գործարանային վիճակի վերադարձը:

Այս դեպքում շատ ավելի քիչ հավանական է, որ նոր սեփականատերը հասանելիություն ստանա Ձեր հին ֆայլերի նկատմամբ:

2.6.9. WiFi համացանցի կիրառում

Բջջային սարքի առավելությունն իսկապես նրա շարժունակությունն է, ինչը նշանակում է աշխատել ցանկացած վայրից՝ առանց մալուխների միջոցով համացանցին ֆիզիկապես միանալու:

Այս դեպքում սրճարաններում կամ ընդհանուր տարածքներում անվճար և բաց WiFi ցանցերից օգտվելու գրավիչ գայթակղություն կա:

Հիշեք, որ նման ցանցերն ավելի քիչ ապահով են, և շատ դեպքերում դրանց օգտագործմամբ իրականացվող

գործունեությունը կարող է ռիսկային լինել: Եթե վստահ չեք նման ցանցերի անվտանգության մեջ, մի զբաղվեք այնպիսի գործունեությամբ, ինչպիսին է՝ կարևոր հաղորդակցություն, բանկային գործարքների իրականացում, գաղտնի թղթապանակների փոխանցում և այլն:

2.6.10. Ֆորս-մաժորային իրավիճակում գործելու կարգ

Հիշեք, որ ձեր շարժական սարքերն ունեն եզակի նույնացուցիչներ (ներառյալ՝ IMEI համարը, MAC հասցեն, Serial համարը): Նշեք այս թվերը և անհրաժեշտության դեպքում դիմեք համապատասխան գերատեսչություններին: Նրանց օգնությամբ հնարավոր է լինում գտնել Ձեր կորած իրն իրավապահների ու բջջային/համացանց պրովայդերների օգնությամբ:

Ժամանակակից շարժական սարքերը հնարավորություն ունեն ավտոմատ գործողություններ կատարելու աղետալի իրավիճակներում, մասնավորապես՝ ցանկացած նախապես ընտրված համադրություն մուտքագրելիս.

- Ավտոմատ կերպով ուղարկում է Ձեր գտնվելու վայրը շտապ օգնության ծառայություններին
- Ուղարկում է անհրաժեշտ SMS հաղորդագրություն նախապես նշված համարին
- Ստանում է լուսանկարու տեսանյութ և ուղարկում նշված հասցեատիրոջը
- Ներկառուցված մոդուլի միջոցով այն գրանցում է Ձեր ընկնելը կամ ցանկացած ֆիզիկական միջադեպ:

Ծանոթացեք վերը նշված կանոններին և հիշեք, որ երբեմն բջջային սարքը պարզապես թվային կապի միջոց չէ:

Վրաստանի ռազմավարության և զարգացման կենտրոն

www.gcsd.org.ge
gcsd@gcsd.org.ge
032 2 22 26 67
Մցխեթայի #48/50