

ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

Ձանգվածային մարքեթինգի մոդելով խարդախության սխեմաների էության, տեսակների և բնութագրիչների վերաբերյալ

ՀՀ տարածքում գործող ֆինանսական և ոչ ֆինանսական հաստատություններին, ինչպես նաև հանրության լայն շերտերին զանգվածային մարքեթինգի մոդելով խարդախության (այսուհետ՝ ՋՄՄԽ) սխեմաների վերաբերյալ իրազեկելու նպատակով հայաստանյան և միջազգային փորձի հիման վրա կատարվել է վերլուծություն, որում նկարագրվում են նշված երևույթի էությունը, տեսակները, ինչպես նաև դրա կիրառությամբ գործարկվող սխեմաների հայտնաբերման բնութագրիչները:

1. ՋՄՄԽ-ի էությունը

ՋՄՄԽ-ի սխեմաներում կապի ժամանակակից միջոցները, այդ թվում՝ հեռախոսը, ինտերնետը, էլեկտրոնային փոստը, հեռուստատեսությունը, ռադիոն, իսկ երբեմն էլ անձնական շփումները օգտագործվում են մեկ կամ մի քանի երկրում խարդախության բազմաթիվ պոտենցիալ զոհերի գտնելու, նրանց հետ կապի մեջ մտնելու և խաբեությամբ, համոզելու կամ պահանջելու միջոցով դրամական միջոցների կամ այլ արժեքների տիրանալու նպատակով:

ՋՄՄԽ-ի առաջին դեպքերն արձանագրվել են տասնամյակներ առաջ՝ սակավաթիվ երկրներում: Ներկայում սա դարձել է գլոբալ խնդիր, և տարբեր երկրների պատկան մարմինները պետք է համակարգված ջանքեր գործադրեն այս տեսակի հանցավոր գործունեության դեմ պայքարի համար: ՋՄՄԽ-ի սխեմաները սովորաբար գործարկվում են արտերկրում գործող հանցավոր խմբավորումների կողմից՝ կապի ժամանակակից միջոցներով: Խարդախության արդյունքում ստացված միջոցները փոխանցվում են տարբեր ուղղություններով՝ դրանց ստացման աղբյուրը քողարկելու համար: Հանցավոր խմբավորումները տարբեր երկրներում հավաքագրում են «աշխատակիցների»՝ սխեմաները գործարկելու և հանցավոր միջոցների շարժն ապահովելու նպատակով:

Խարդախները գործարկված սխեմաների պոտենցիալ զոհերին ընտրում են տարբեր աշխարհամասերի բազմաթիվ երկրներից՝ օգտվելով այն հանգամանքից, որ միջազգային սահմանները իրավապահ մարմինների համար որոշակի դժվարություններ են ստեղծում նման սխեմաների գործունեությունն արգելելու հարցում: Սխեմաները կարող են գործարկվել աշխարհի ցանկացած անկյունից, ինչը բարդացնում և ժամանակատար է դարձնում խարդախների հայտնաբերումը:

Այս հանցագործությունների զոհերի մոտ հաճախ դրսևորվող մեղքի, ամոթի ու շփոթվածության զգացումը հոգեբանական արգելք է ստեղծում դրանց բացահայտման ճանապարհին: ԶՄՄԽ-ի զոհերի վնասներն արտահայտվում են խնայողությունների կամ ունեցվածքի կորստի, ֆիզիկական ռիսկերի կամ բռնության սպառնալիքների, ընկճվածության կամ առողջական խնդիրների, մինչև անգամ ինքնասպանության մասին մտքերի, փորձերի կամ կատարված փաստերի տեսքով:

2. ԶՄՄԽ-ի տեսակները

ԶՄՄԽ-ն իրականացվում է բազմապիսի սխեմաներով, որոնց նպատակը մարդկանց և կազմակերպությունների ունեցվածքին, դրամական միջոցներին, ծառայություններին կամ տեղեկատվությանը տիրանալն է: Աշխարհում լայն տարածում են գտել ԶՄՄԽ-ի սխեմաների հետևյալ տեսակները.

1) Կանխավճարի ստացման խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին հսկայական հարստության անիրական խոստումներով գայթակղելով՝ համոզում են ինչ-ինչ հարկերի և միջնորդավճարների համար կանխավճարներ կատարել:

Օրինակ. Ա անձը ստանում է էլեկտրոնային նամակ հետևյալ բովանդակությամբ՝ «Ես Բ երկրի նախկին նախագահի որդին եմ: Իմ հայրը զոհվելուց հետո ինձ թողել է հսկայական հարստություն, սակայն գործող կառավարության օրոք այդ միջոցների մի մասը սառեցվել է, իսկ ինքս գտնվում եմ քաղաքական հալածյալի կարգավիճակում: Այս հանգամանքներում նպատակահարմար չէ միջոցները պահել մեր ընտանիքի անդամներից որևէ մեկի անունով: Եթե հնարավոր է, կուզենայի այդ միջոցները ժամանակավորապես փոխանցել ձեր հաշվին: Դրա դիմաց Դուք կստանաք միջոցների 5%-ը: Խնդրում եմ հետաքրքրված լինելու դեպքում պատասխանել այս նամակին»:

Հետագա շփումների ընթացքում պարզվում է, որ այս հսկայական միջոցների «սեփականատերը» ինչ-ինչ «հիմնավոր» պատճառաբանություններով գումար չունի բանկային փոխանցումներ կամ անհրաժեշտ փաստաթղթային ձևակերպումներ կատարելու համար, և Ա անձից խնդրում է կանխավճար՝ հետագա հատուցման պայմանով: Որոշակի ժամանակ Ա անձի վստահությունը չարաշահելով գումարներ կորզելուց հետո խարդախը խզում է նամակագրական կապը:

Ընդ որում, որոշ դեպքերում Ա-ի հաշվեհամարը և անձնական տվյալները կարող են օգտագործվել Ա-ի գումարները խարդախությամբ քարտից կորզելու կամ վերջինի հաշիվը փողերի լվացման սխեմաներում որպես տարանցիկ հաշիվ օգտագործելու համար:

2) Առցանց սակարկությունների միջոցով իրականացվող գնումների խարդախ սխեմաները, որոնց դեպքում կազմակերպիչներն օգտվում են գնորդների ու վաճառողների անտեղյակությունից և ինտերնետի ընձեռած հնարավորություններից՝ իրենց ինքնությունն ու գտնվելու փաստացի վայրը թաքցնելու նպատակով: Այս սխեմաներում կիրառվող հանցավոր մեթոդների թվին են պատկանում գերավճարների գանձումը, գնված ապրանքների ուշ մատակարարումը կամ չմատակարարումը, ապրանքի իրական վիճակի վերաբերյալ սխալ տեղեկությունների տրամադրումը:

Օրինակ. Ա անձը, ով փնտրում է հազվագյուտ տեսակի հին մետաղադրամ, առցանց աճուրդով զբաղվող քիչ հայտնի ինտերնետային կայքից տեղեկանում է դրա աճուրդային վաճառքի մասին՝ մեկնարկային ցածր գնով: Աճուրդում «հաղթելով» և մետաղադրամը սպասվածից ցածր գնով գնելով՝ Ա-ն տեղեկացվում է, որ գումարի կեսը պետք է վճարի այդ պահին, իսկ մյուս կեսը՝ ապրանքը ստանուց հետո: Համապատասխան փոխանցումը կատարելուց հետո Ա-ն այդպես էլ չի ստանում իր «գնած» մետաղադրամը: Ընդ որում, նմանատիպ սխեմաներում փոխանցումները կատարվում են կա՛մ դրամական փոխանցումներ իրականացնող տարբեր համակարգերով՝, կա՛մ ինտերնետ վճարումների համակարգերով, կա՛մ Ա-ի երկրում գտնվող միջնորդի միջոցով՝ ամեն կերպ խուսափելով ուղիղ բանկային փոխանցումից, որի դեպքում Ա-ն կկարողանար իմանալ խարդախի նույնականացնող տվյալները, երկիրը և բանկային հաշվեհամարը:

3) Բարեգործության խարդախ սխեմաները, որոնց դեպքում հավաքագրված միջոցների ընդամենը մի փոքր մասն է ուղղվում սկզբնապես հայտարարված նպատակներին, կամ այդ միջոցներն ընդհանրապես չեն ուղղվում հիշյալ նպատակներին: Խարդախներն այս դեպքում շահարկում են կարեկցանք առաջացնող պատճառներ, օրինական գործող բարեգործական կազմակերպությունների անուններ, հումանիտար կամ բնապահպանական աղետներին դիմակայելու հիմնավորումներ և այլն:

Օրինակ. Ա երկրում ավերիչ փոթորկի հետևանքներից տուժած մարդկանց օգնություն ցուցաբերելու համար ստեղծվում է Բ բարեգործական հիմնադրամը, որը օրինական ձևով միջոցներ է հավաքում քաղաքացիներից և կազմակերպություններից: Այդ նույն ժամանակ Գ անձը, որևէ կապ չունենալով Բ հիմնադրամի հետ, ներկայանում է որպես Բ-ի լիազոր անձ և սկսում է վերջինի անունից բազմաթիվ մարդկանց զանգվածային էլեկտրոնային նամակներ ուղարկել՝ խնդրելով գումարներ փոխանցել իբրև թե փոթորկից տուժածներին օգնելու

¹ Օրինակ՝ Moneygram, Sigue Money Transfer և այլն

նպատակով բացված, սակայն իրականում իր կողմից տնօրինվող հաշվեհամարին: Այս հաշվեհամարին հավաքագրված գումարները հետագայում Գ-ի կողմից տնօրինվում են սեփական հայեցողությամբ՝ բնականաբար չուղղվելով փոթորկից տուժածներին օժանդակությանը:

4) Կեղծ չեքերի օգտագործմամբ խարդախության սխեմաները, որոնց դեպքում ներգրավված անձից պահանջվում է ուղարկված կեղծ չեքը բանկերի միջոցով իրացնելուց հետո ստացված միջոցների մեծ մասը փոխանցել ուղարկողին/ սխեմայի կազմակերպչին: Հաճախ է պատահում, որ չեքն իրացնելուց շաբաթներ անց բանկը բացահայտում է տվյալ վճարային գործիքի կեղծ լինելը, ինչի համար պատասխանատվության է ենթարկվում դրա ներկայացնողը:

Օրինակ. Ա կազմակերպությունը վաճառում է թանկարժեք ապրանքներ: Գնորդ Բ-ն, պատճառաբանելով գումարի մեծությունը, Ա-ի հետ պայմանավորվում է, որ գնված ապրանքի դիմաց վճարումը կատարելու է չեքի օգնությամբ: Ա-ն վճարումն ընդունում է չեքով և տրամադրում գնված ապրանքը, իսկ մի քանի օր անց չեքը կանխիկացնելու նպատակով բանկ ներկայացնելիս պարզվում է, որ այն կեղծ է:

Ընդ որում, նկարագրված դեպքում Բ-ն կարող է լինել ինչպես կեղծ չեքերի պատրաստողը, այնպես էլ միջնորդ, ով որոշակի (միջնորդա)վճարի դիմաց կազմակերպում է անձամբ կամ փոստի միջոցով ստացված կեղծ չեքերի իրացումը:

5) Շտապ օգնության խարդախ սխեմաները, որոնց դեպքում մարդկանցից անհապաղ ֆինանսական օժանդակություն են խնդրում գրավի դիմաց կալանքից ազատման կամ անհետաձգելի բժշկական ծախսեր հոգալու համար: Այս դեպքում խարդախը ներկայանում է որպես մեկը, ում ընտանիքի անդամին կամ մոտ ընկերոջը (հաճախ՝ արտերկրում սովորող ուսանողին) կալանքից ազատելու կամ շտապ բուժօգնություն ցուցաբերելու համար միջոցներ են հարկավոր:

Օրինակ. Ա անձը սոցիալական շփման կայքերի միջոցով, ինչ-ինչ ընդհանուր հետաքրքրություններից ելնելով ծանոթանում է Բ-ի հետ: Որոշ ժամանակ շփումից հետո Բ-ն հայտնում է Ա-ին, որ իր կինը վթարի է ենթարկվել, և անհրաժեշտ է շտապ վիրահատական միջամտություն: Վիրահատության դիմաց վճարելու հրատապությունը և տվյալ պահին իր ծանր ֆինանսական վիճակը հաշվի առնելով՝ Բ-ն խնդրում է (հետագայում վերադարձնելու պայմանով) փոխանցում կատարել իր կողմից մատնանշած հաշվեհամարին: Ընդ որում, այս սխեմայում հնարավոր է կիրառել թե՛ զանգվածային հաղորդագրությունների տեխնիկան, թե՛ ավելի հասցեական մոտեցումներ՝ սոցիալական ցանցերի միջոցով նախապես ճշտելով պոտենցիալ զոհի անձնական տվյալները, ընտանիքի անդամներին, նրանց կարգավիճակը և այլն:

6) Աշխատանք կամ բիզնես առաջարկող խարդախ սխեմաները, որոնց դեպքում կազմակերպիչները երաշխավորում են նվազագույն ջանքերով և առանց բավարար աշխատանքային փորձի կամ դրա բացակայության պարագայում հեշտությամբ գումարներ վաստակելը: Սրանց թվին են պատկանում բրգաձև սխեմաները, տանը աշխատանքի, հսկիչ գնումների և փոստային վերաառաքման առաջարկները, արտասահմանում աշխատանքի գրավիչ առաջարկները և այլն: Այս սխեմաների մասնակիցներից հաճախ պահանջվում է սկզբից ևեթ գնել թանկարժեք պարագաներ կամ ուսուցողական նյութեր, իսկ արդեն մասնակցության շրջանակներում կարող է առաջարկվել կեղծ ֆինանսական գործիքներ իրացնել:

Օրինակ. Ինտերնետային կայքը, որը զբաղվում է յուրահատուկ, հանրային սպասարկման վայրերում և վաճառակետերում ոչ հասանելի ժամացույցների վաճառքով, գնորդներին խրախուսելու համար առաջարկում է որոշակի խմբաքանակի գնման դեպքում դառնալ իրենց գործակալը և գումար աշխատել՝ նոր հաճախորդներ ներգրավելով: Սակայն, ինչպես պարզվում է հետագայում, վաճառվող ապրանքի գինն էականորեն գերազանցատված է, իսկ գործակալ դառնալու համար անհրաժեշտ ապրանքի խմբաքանակը չափազանց մեծ՝ ողջամիտ ժամկետում վերավաճառելու համար:

7) Արտասահմանյան վիճակախաղերի կամ շահումով խաղերի խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին համոզում են գոյություն չունեցող դրամական շահումների ստացման նպատակով ինչ-ինչ հարկերի և միջնորդավճարների համար կանխավճարներ կատարել:

Օրինակ. Ա անձը որոշակի ինտերնետային կայք է մուտք գործում, որտեղ հայտնվում է մի պատուհան՝ տեղեկացնելով, որ Ա-ն այդ կայքի 100 հազարերորդ այցելուն է, ինչի կապակցությամբ ստանալու է խոշոր մրցանակ: Ընդ որում, մրցանակը ստանալու համար պետք է զանգահարել ինչ-որ հեռախոսահամարով: Զանգահարելուց հետո պարզվում է, որ մրցանակը ստանալու համար անհրաժեշտ է նախապես մուծել եկամտահարկը: «Եկամտահարկը» մուծելուց հետո մրցանակը, բնականաբար, չի հաջողվում ստանալ (քանի որ հեռախոսազանգերին դադարում են պատասխանել, ներկայացնում են նոր պահանջներ և այլն):

8) Ներդրումային խարդախ սխեմաները, որոնց դեպքում մասնակիցներին երաշխավորվում են մեծ եկամուտներ արժեթղթերի, անշարժ գույքի, նավթարդյունահանման ձեռնարկությունների, հուշադրամների, թանկարժեք քարերի և այլ բիզնեսներում ներդրումների դիմաց: Սրանք հայտնի են նաև որպես «կաթսայատնային գործարքների» խարդախ սխեմաներ: Այս սխեմաների գործողության սկզբունքը փոքր ներդրումների դիմաց մեծ եկամուտներ խոստանալն է:

Օրինակ. Ա երկրի Բ քաղաքացուն զանգահարում է Գ-ն, ով ներկայանալով որպես Դ երկրի ֆոնդային բորսայում գրանցված Ե «հեղինակավոր» կազմակերպության լիազոր անձ, առաջարկում է նրան Ե-ի բաժնետոմսեր սովորականից 30% զեղչված գնով: Գ-ն ներկայացնում է Ե-ի զարգացման մեծ հեռանկարները և խոստանում տարեկան 100% զուտ եկամուտ ներդրված գումարի համեմատ, ինչը կապահովվի թե բաժնետոմսերի գնի աճի, թե շահաբաժինների վճարման միջոցով: Ընդ որում, այս առաջարկին վերջնական պատասխան պետք է տրվի հաշված ժամերի ընթացքում, քանի որ թողարկված բաժնետոմսերը տեղաբաշխվում են մեծ արագությամբ:

Բ անձը ստուգում է Ե կազմակերպության վերաբերյալ ինտերնետում հասանելի տեղեկատվությունը (ինչը սովորաբար սահմանափակվում է հենց Ե-ի կողմից ներկայացվող տվյալներով) և, առաջարկը գրավիչ համարելով, ներդնում է 7000 ԱՄՆ դոլար: 1 ամիս անց Բ-ն ստանում է բավականին մեծ շահաբաժին և պարզում, որ կազմակերպության բաժնետոմսերի գինը աճել է 30%-ով:

Գ-ն դարձյալ զանգահարում է Բ-ին՝ հայտնելով, որ ընկերության բաժնետերերից մեկը վաճառում է իր բաժնետոմսերը խիստ շահավետ պայմաններով և թույլտվություն է տալիս Բ-ն պետք է կատարի 100,000 ԱՄՆ դոլարի ներդրում:

Ներդրումը կատարելուց որոշ ժամանակ անց պարզվում է, որ Ե կազմակերպության բաժնետոմսերը արժեզրկվել են, և քանի որ այն գրանցված է Դ երկրում, Ա երկրի քաղաքացին որևէ իրական հնարավորություն չունի իմաստավոր քայլեր ձեռնարկելու՝ իր ներդրումները վերադարձնելու համար:

9) Վարկերի, վարկային քարտերի և դրամաշնորհների խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին առաջարկվում են գոյություն չունեցող վարկեր, վարկային քարտեր և դրամաշնորհներ՝ նախապես ինչ-ինչ վարչական ծախսերի կամ միջնորդավճարների փոխհատուցման պայմանով: Խարդախների հիմնական թիրախը սովորաբար անհատներն ու փոքր ձեռնարկություններն են:

Օրինակ. Ա անձը ստանում է էլեկտրոնային նամակ, որտեղ Բ-ն, ներկայանալով որպես Գ հեղինակավոր միջազգային կազմակերպության լիազոր անձ, տեղեկացնում է Ա-ին, որ նա ընտրվել է որպես Գ-ի կողմից տրամադրվող ամենամյա դրամաշնորհի հաղթող: Ա-ն պետք է ուղարկի իր անձնական տվյալները և ստանա գումարը, որը պետք է ծախսվի կրթական, գործարար կամ հասարակական նպատակներով: Ա-ն ներկայացված ձևաթերթում լրացնում է իր անձնական տվյալները և ուղարկում Բ-ին: Հաջորդ նամակով Բ-ն տեղեկացնում է, որ Ա-ի անունով 1 միլիոն ԱՄՆ դոլարի չեք է դուրս գրվել, որը նրան կուղարկվի

փոստային առաքման (50 ԱՄՆ դոլար) և ապահովագրության (400 ԱՄՆ դոլար) վճարումները կատարելուց անմիջապես հետո: Ա-ն կատարում է այս վճարումները, ինչպես նաև հետագայում այլ պատճառաբանություններով պահանջվող լրացուցիչ վճարումներ, սակայն այդպես էլ չի ստանում ցանկալի «դրամաշնորհը»:

10) Բիզնեսներին առաջարկվող խարդախ սխեմաները, որոնց դեպքում կեղծված վճարային փաստաթղթերի, գոյություն չունեցող գործարար տեղեկատվություն կամ կեղծ ինտերնետային կայքերում զեղչված գներով ապրանքների վաճառքի պատրվակով գումարներ են շորթվում գործող բիզնեսներից:

Օրինակ. Ա կազմակերպությունը, որ օգտվում է Բ գործարար տեղեկատվի ծառայություններից, իբրև թե Բ-ից, սակայն իրականում՝ խարդախ սխեմայի կազմակերպիչներից ստանում է էլեկտրոնային նամակ, որով հայտնվում է, որ Բ-ի տեղեկատվական ռեսուրսներում Ա-ի կոնտակտներն ու գովազդը պահելու համար անհրաժեշտ է շտապ կատարել վճարում: Կից ներկայացվում է հաշիվ-ապրանքագիրը, որով, նախ, իրականում նախատեսվում է գանձել ավելի մեծ գումար, քան սովորաբար վճարում է Ա կազմակերպությունը, և երկրորդ՝ որպես վճարման շահառու նշված է լինում այլ, խարդախների կողմից վերահսկվող հաշվեհամար: Ա-ի աշխատակիցը, ուշադիր չուսումնասիրելով նամակը և հաշիվ-ապրանքագիրը կամ իր մոտ առաջացած կասկածները փարատելով Բ-ի «ներկայացուցիչների» հետ լրացուցիչ շփման միջոցով, կատարում է վճարումը:

11) Գործարքի առարկայի հատկանիշների սխալ ներկայացմամբ խարդախ սխեմաները, որոնց դեպքում առաջարկվում են տարբեր ապրանքներ և ծառայություններ, այդ թվում՝ վարկերի ապահովագրության ու վերավարկավորման ծրագրեր, արձակուրդի անցկացման, գույքի ժամանակավոր օգտագործման հնարավորություններ, որևէ երկրում բնակության իրավունքի ստացման միջնորդության, առողջապահական և այլ ծառայություններ: Այս սխեմաները, որոնց բնույթը, շրջանակը և իրականացման եղանակները խիստ բազմազան են, ունեն մի ընդհանրություն՝ դրանց զոհերը որպես կանոն չեն ստանում խոստացված ապրանքները կամ ծառայությունները, կամ ստանում են խոստացվածից էապես ցածր արժեքով ապրանքներ կամ ծառայություններ:

Օրինակ. Ա անձը ստանում է էլեկտրոնային նամակ, որտեղ գովազդվում է մի դեղամիջոց, որի միջոցով այն օգտագործողն առանց դիետայի կարողանում է նիհարել 15 կգ ընդամենը 3 շաբաթում: Միջնորդ Բ-ին վճարելով ապրանքի դիմաց՝ Ա-ն ստանում է այդ դեղամիջոցը. սակայն դրա կիրառությունը, ի լրումն խոստացված արդյունքը չապահովելուն, չվերականգնվող վնասներ է հասցնում Ա-ի առողջությանը: Հետագայում պարզվում է, որ դեղամիջոցը չի արտոնագրվել Գ

երկրի առողջապահության նախարարության կողմից՝ դրա ունեցած կողմնակի ազդեցությունների պատճառով:

12) Հատուցման խարդախ սխեմաները, որոնց դեպքում նախկինում խարդախության սխեմաների զոհ դարձած անձանց առաջարկվում է ինչ-ինչ վարչական և այլ ծախսերի համար որոշակի կանխավճարի դիմաց վերականգնել կորցրած գումարը: Այս սխեմաների դեպքում խարդախները հաճախ ներկայանում են որպես փաստաբան, իրավապահ մարմինների աշխատակից կամ պետական պաշտոնյա:

Օրինակ. Ա անձը, ով դարձել է տարատեսակ խարդախ սխեմաներից մեկի զոհը, ստանում է նամակ Բ-ից, ով ներկայանում է որպես Գ երկրի (որտեղից էլ կատարվել է խարդախությունը) ոստիկանության աշխատակից: Նա հայտնում է, որ քննում է Ա-ի գործը՝ նրա կրած վնասի հատուցման համար, և պահանջում է որոշակի գումար՝ հետաքննության ծախսերը հոգալու նպատակով: Այս հարցի շուրջ բանակցելու ընթացքում հնարավոր է նաև, որ Ա-ից պահանջեն տրամադրել իր հաշվի վերաբերյալ տվյալներ՝ հատուցման գումարը ստանալու համար: Իրականում, սակայն, Բ-ն նախկինում կատարված խարդախության մասնակից է, իսկ Ա-ին կրած վնասի փոխհատուցման խոստումները, ինչպես նաև նրա հաշվի տվյալներն օգտագործվում են խարդախությամբ լրացուցիչ գումարներ կորզելու համար:

13) Ռոմանտիկ հարաբերությունների խարդախ սխեմաները, որոնց դեպքում խարդախների թիրախը ինտերնետային ժամադրությունների և սոցիալական ցանցերի՝ ռոմանտիկ հարաբերություններ փնտրող օգտատերերն են: Պարբերական ինտիմ զրույցների և փոքրարժեք նվերների միջոցով պոտենցիալ զոհերի վստահությունն ու համակրանքը շահելուց հետո խարդախները նրանցից շորթում են դրամական միջոցներ կամ արժեքավոր իրեր: Այս սխեմաների զոհերի հավաստմամբ, խարդախները գումարներ են կորզում ճանապարհորդական փաստաթղթերի ու օդանավի տոմսի ձեռք բերման, դեղամիջոցների ու բուժման ծախսերի կատարման, բարեգործական ծրագրերի իրականացման, ֆինանսական դժվարությունների հաղթահարման պատճառաբանություններով:

Օրինակ. Ա-ն սոցիալական շփման կայքի միջոցով ծանոթանում է Բ-ի հետ: Պարբերական և երկարատև ռոմանտիկ շփման արդյունքում Բ-ին հաջողվում է շահել Ա-ի համակրանքը և վստահությունը: Նրանք հետագա հարաբերությունների, համատեղ կյանքի, հնարավոր է նաև՝ համատեղ բիզնեսի պլաններ են մշակում: Այնուհետև Բ-ն սկսում է տարբեր պատրվակներով պարբերաբար ֆինանսական օժանդակություն խնդրել և ստանալ Ա-ից: Երբ ստացված գումարները հասնում են պատկառելի չափերի, կամ երբ Ա-ի մոտ Բ-ի իրական նպատակների հետ կապված կասկածներ են առաջանում, Բ-ն խզում է նամակագրական կապը:

14) Արևմտա-աֆրիկյան ավանդական խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին գայթակղում են հսկայական հարստության արագ ստացման խոստումներով: Խարդախների ներկայացմամբ, պոտենցիալ զոհերի ֆինանսական օգնությունը հարկավոր է լինում արտասահմանյան որևէ երկրից կամ ընկերությունից հաճախ միլիոնավոր դոլարների հասնող գումարներ օրինական ճանապարհով ստանալու կամ հափշտակելու համար, ինչի դիմաց նրանք խոստանում են ստացված կամ հափշտակված միջոցների որոշակի բաժինը: Արևմտա-աֆրիկյան ավանդական խարդախ սխեմաները հաճախ կոչվում են «419-ի խարդախություններ»՝ ըստ Նիգերիայի քրեական օրենսգրքում այդ հանցագործությունը նախատեսող հոդվածի համարի: Նմանատիպ խարդախ սխեմաների թվին են պատկանում.

14.1) Սևացված թղթադրամների խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին համոզում են գնել հատուկ լուծույթներ՝ այս կամ այն պատճառով սևացված ու օգտագործման համար անպիտան դարձած թղթադրամների գումավորումը հեռացնելու (մեկ այլ դեպքում՝ սովորական սև թղթի կտորներն իրական թղթադրամների վերածելու համար):

Օրինակ. Ա-ն ուղարկում է նամակ հազարավոր օգտատերերի՝ ներկայացնելով, որ ինքը հաջողացրել է ինչ-ինչ ձևերով Բ երկիր ներմուծել 1 միլիոն ԱՄՆ դոլար՝ սև ներկով թաքցնելով դրանց օրինակելի վճարամիջոց լինելու հանգամանքը: Սև գույնն անվտանգ հեռացնելու համար գոյություն ունի լուծույթ, որը կարողանում է թղթադրամներին վերադարձնել դրանց իրական գույնը և տեսքը: Ա-ն տեղեկացնում է, որ ինքն անվճար տրամադրում է լուծույթը, սակայն պետք է ստանա մաքրված թղթադրամների 30%-ի չափ գումար: Գ օգտատերը փորձում է ստուգել և պատվիրում 1.000 ԱՄՆ դոլարի սև թղթադրամ և լուծույթը: Փորձը հաջող է անցնում և, հրապուրվելով հեշտ գումար աշխատելու հնարավորությունից, Գ-ն այս անգամ պատվիրում է 100.000 ԱՄՆ դոլարին համարժեք սև թղթադրամ՝ վճարելով 30.000 ԱՄՆ դոլար: Սակայն այս անգամ պարզվում է, որ դրանք պարզապես սև թղթեր են:

14.2) Ժառանգության խարդախ սխեմաները, որոնց դեպքում պոտենցիալ զոհերին համոզում են ինչ-ինչ հարկերի և միջնորդավճարների համար կանխավճարներ կատարել՝ նախկինում նրանց անհայտ և ներկայում մահացած բարեկամների թողած ժառանգությունը ստանալու նպատակով

Օրինակ. Ա-ն էլեկտրոնային նամակ է ստանում Բ-ից, որով վերջինս հայտնում է, որ ինքը մի քանի ամիս առաջ մահացած մեծահարուստ Գ-ի անձնական փաստաթանն է: Ընդ որում Գ-ի և Ա-ի ազգանունները համընկնում են: Բ-ն հայտնում է, որ Գ-ն մահանալով թողել է հսկայական ժառանգություն և չունի որևէ

ժառանգորդ. հետևաբար այդ հսկայական կարողությունը պետք է դառնա պետական սեփականություն: Բ-ն հանձն է առնում որոշակի միջնորդավճարի դիմաց այնպես կազմակերպել իրավական գործընթացները, որ Ա-ն համարվի Գ-ի միակ ժառանգորդը՝ ստանալով Գ-ի հսկայական կարողությունը: Հետագա շփումների ընթացքում Բ-ն իրավաբանական ձևակերպումների, հարկային ծախսերի փոխհատուցման և այլ պատճառաբանություններով Ա-ից ստանում է որոշակի գումարներ և յուրացնում դրանք:

15) Թաքցված էական պայմաններով պայմանագրային առաջարկի խարդախ սխեմաները, որոնց դեպքում կազմակերպիչները, պոտենցիալ զոհերի վերաբերյալ տվյալներ հայթայթելով, համացանցի կամ փոստային ծառայության միջոցով զանազան պայմանագրեր են ուղարկում նրանց՝ այդ պայմանագրերի կարևորագույն պայմանները շարադրելով առաջին հայացքից աննկատելի եղանակով, օրինակ՝ շատ մանր տառատեսակով, փաստաթղթի վերջում կամ ծանոթագրությունների մասում: Այս սխեմայի նպատակն է, որ պայմանագրի արտաքուստ գրավիչ պայմաններով հետաքրքրված զոհերը, առանց պայմանագիրը մանրակրկիտ ուսումնասիրելու, ստորագրեն և հետ ուղարկեն այն, ինչից հետո նրանք պարտավորված կլինեն ըստ պայմանագրի կատարել համապատասխան վճարումները:

Օրինակ. Ա անձը փոստային ծառայության միջոցով ստանում է պայմանագիր, որով Բ-ն առաջարկում է Ա-ին հանդես գալ որպես նախատեսվող առևտրային միջոցառման, օրինակ՝ ցուցահանդեսի կազմակերպման պատասխանատու (նախկինում Ա-ն մասնակցած է եղել նմանատիպ միջոցառումների, որտեղից էլ Բ-ն վերցրել է Ա-ի տվյալները): Ա-ից պահանջվում է ընդամենը ստուգել իր տվյալների ճշտությունը, ստորագրել և հետ ուղակել կազմակերպիչներին:

Պայմանագրի սկզբում աչքի ընկնող տեղում և ձևով նշվում է, որ Ա-ի թեկնածության առաջադրումը լիովին անվճար է, սակայն պայմանագրի մեջ որևէ աննկատ տեղում և ձևով նշվում է, որ ցուցահանդեսի կազմակերպման պատասխանատուն պարտավորվում է Բ-ին միջնորդության համար 3 տարի շարունակ տարեկան 1.000 ԱՄՆ դոլար վճարել, անգամ եթե միջոցառման իրականացումը հետաձգվում կամ չեղյալ է հայտարարվում:

Ա-ն ստորագրում է և հետ է ուղարկում առաջին հայացքից ոչինչ չպարտավորեցնող պայմանագիրը և որոշ ժամանակ անց Բ-ից ստանում է վճարման պահանջ՝ ըստ պայմանագրով սահմանվածի: Խարդախության սխեմայի զոհերը հաճախ կատարում են պահանջվող վճարումը՝ իրենց համարելով իրավաբանական տեսանկյունից անելանելի վիճակում:

16) Իրավասու մարմինների անունից կատարվող զանգերի խարդախ սխեմաները, որոնց դեպքում կազմակերպիչները, հիմնելով զանգերի իրականացման կենտրոն, կատարում են զանգվածային զանգեր տարբեր երկրներ՝ ներկայանալով որպես որևիցե իրավասու մարմնի աշխատակից և տեղեկացնելով պոտենցիալ զոհերին, իբր թե նրանք, անկախ իրենց կամքից, ներգրավվել են փողերի լվացման կամ այլ հանցավոր գործունեության մեջ և պատասխանատվության չենթարկվելու համար պետք է որոշակի գումար փոխանցեն նշված հաշվեհամարին:

Օրինակ. Բ անձը Գ երկրից զանգահարում է Ա-ին (Ա-ի մասին որոշակի տվյալներ հավաքագրելուց հետո) և ներկայանում որպես փողերի լվացման և ահաբեկչության դեմ պայքարի միջազգային կառույցի աշխատակից: Բ-ն հայտնում և հավաստիացնում է Ա-ին, որ իբր թե Ա-ն, իր կամքից անկախ, ներգրավվել է թմրամիջոցների ապօրինի շրջանառությանն առնչվող գործարքների մեջ և քրեական պատասխանատվությունից խուսափելու համար պետք է որոշակի գումար փոխանցի նշված հաշվեհամարին: Խարդախության սխեմայի կազմակերպիչները որպես զոհ հաճախ ընտրում են մարդկանց, ովքեր ինչ-ինչ պատճառներով հակված չեն լինի պաշտպանության համար դիմել իրավապահ մարմիններին:

17) Ցանցահեռների կողմից գործարար հարաբերություններին միջամտելու խարդախ սխեմաները, որոնց դեպքում ցանցահեռները, գործարար հարաբերությունների մեջ գտնվող անձանց նամակագրությանը հասանելիություն ստանալով, իրենք են սկսում մեկի անունից մյուսին նամակներ ուղարկել՝ նպատակ ունենալով խաբեությամբ գումարներ կորզել բնականոն գործարար հարաբերությունների շրջանակում կատարվող վճարումները իրենց կողմից վերահսկվող հաշիվներին ուղղելու միջոցով:

Օրինակ. Ա կազմակերպությունը էլեկտրոնային նամակագրություն է վարում իր արտասահմանյան գործընկեր Բ կազմակերպության հետ՝ շուրջ 30,000 ԱՄՆ դոլար արժեքով ապրանքի հերթական խմբաքանակ պատվիրելու համար: Նամակագրության որոշակի պահից սկսած Գ անձը կարողանում է Բ-ից ծածուկ և Ա-ի համար աննկատ կերպով միջամտել նամակագրությանը և այնպես անել, որ դրանից հետո ինքը ստանա Ա-ի ու Բ-ի միջև նամակագրությունը: Այնուհետև Գ-ն Բ-ի անունից շարունակում է նամակագրությունը Ա-ի հետ և վճարումը կատարվելուց առաջ հայտնում իր հաշվեհամարի փոփոխության մասին՝ առաջարկելով 30,000 ԱՄՆ դոլարը փոխանցել իր նշած նոր հաշվեհամարին: Ա-ն, չկասկածելով հնարավոր խարդախության մասին և չփորձելով այլընտրանքային եղանակով կապվել Բ-ի հետ, փոխանցում է գումարը, որը Գ-ն շատ արագ կանխիկացնում է ու փակում հաշվեհամարը:

18) Շուկայականից ակնհայտ ցածր գնով ապրանքների «վաճառքի» խարդախ սխեմաները, որոնց դեպքում հանցագործները մատչելի գնով ապրանքների (բջջային հեռախոս, ավտոմեքենա, բնակարան և այլն) վաճառքի հայտարարություններ են տեղադրում տարբեր կայքերում, իսկ այդ ապրանքները գնել ցանկացող պոտենցիալ զոհերից պահանջում են համապատասխան դրամական միջոցների առկայությունը հավաստելու նպատակով արագ դրամական փոխանցումների համակարգով «ձևական» փոխանցում իրականացնել, և փոխանցումը հաստատող փաստաթուղթն ուղարկել իրենց՝ առանց նշելու փոխանցումը ստանալու համար անհրաժեշտ եզակի հղման համարը: Փոխանցման վերաբերյալ տեղեկատվությունը ստանալուց հետո հանցագործները կարողանում են փոխանցման եզակի հղման համարը չունենալու պարագայում ինչ-ինչ զարտուղի ճանապարհներով այլ երկրում ստանալ փոխանցված միջոցները:

Օրինակ. Ա անձը հայաստանյան հայտարարությունների կայքերից մեկում տեսնում է շուկայականից էականորեն ցածր գնով ավտոմեքենայի վաճառքի հայտարարություն, որտեղ վաճառողի տվյալներում նշված է արտասահմանյան հեռախոսահամար: Խարդախ վաճառող Բ անձի հետ կապ հաստատելով՝ Ա-ն տեղեկացում է, իբր Բ-ն որոշ ժամանակ ապրել է Հայաստանում, որտեղ ունի ավտոմեքենա, որը ցանկանում է վաճառել: Միաժամանակ Բ-ն նշում է, որ մոտ ժամանակներում ընդամենը մի քանի օրով գալու է Հայաստան և այդ ժամանակ էլ ցանկանում է արագ ձևակերպել ավտոմեքենայի վաճառքի գործարքը: Ավտոմեքենայի վաճառքի պայմանների վերաբերյալ Ա-ի հետ համաձայնության գալով՝ Բ-ն նշում է, որ որպեսզի այլ գնորդների հետ այլևս չբանակցի, իրեն անհրաժեշտ է հավաստիանալ, որ տվյալ պահին Ա-ն ունի ավտոմեքենայի վաճառքի գնի չափով գումար: Այդ նպատակով Բ-ն հրահանգում է Ա-ին արագ դրամական փոխանցումների համակարգով ² գնորդի համար վստահելի անձի անունով «ձևական» փոխանցում կատարել և փոխանցումը հաստատող փաստաթղթի նկարը էլեկտրոնային եղանակով ուղարկել իրեն՝ նախօրոք նկարի մեջ փակելով փոխանցումը ստանալու համար անհրաժեշտ եզակի հղման համարը: Բ-ն նաև Ա-ին տեղեկացնում է, որ փոխանցումը կատարելուց որոշ ժամանակ անց Ա-ն կարող է չեղարկել փոխանցումը և հետ ստանալ գումարը:

Ըստ այդմ՝ Ա-ն կատարում է փոխանցումը իր հարազատներից մեկի՝ Գ-ի անունով, նկարում է փոխանցումը հաստատող փաստաթուղթը և ուղարկում Բ-ին: Փոխանցման վերաբերյալ տեղեկատվությունը ստանալով Բ-ն, ով ունի հայկական անձնագրի նմուշ և դրա հիման վրա Գ-ի անունով կեղծ անձնագիր է պատրաստում, իրեն հայտնի ճանապարհով (օրինակ՝ ցանցահեռության միջոցով) իմանում է

² Օրինակ՝ Moneygram, Sigue Money Transfer և այլն

փոխանցման եզակի հղման համարը և վերոնշյալ կեղծ անձնագրով արտերկրից ստանում է գումարը:

Վերը նկարագրված ՋՄՄԽ-ի սխեմաները հաճախ կիրառվում են որոշակի համակցությամբ: Օրինակ, վիճակախաղերի խարդախ սխեմաներում երբեմն օգտագործվում են կեղծ չեքերով խարդախ սխեմաների տարրեր, բրգաձև սխեմաները հաճախ գործարկվում են ներդրումային սխեմաների տեսքով, ռոմանտիկ հարաբերությունների սխեմաները ներառում են ինչ-ինչ պատճառաբանություններով կանխավճարների ստացման խարդախ սխեմաների տարրեր և այլն:

ՋՄՄԽ-ի սխեմաների գործարկումը հաճախ զուգորդվում է նույնականացնող տվյալների գողությամբ, հատկապես ինտերնետի միջոցով: Հանցագործներն ապօրինաբար տիրանում են այնպիսի տեղեկատվության, ինչպիսիք են մարդու անուն ազգանունը, վարկային քարտի համարը, բանկային հաշվեհամարը կամ այլ անձնական նույնականացնող տվյալներ: Գողացված տեղեկատվությունն առանց դրա տիրոջ գիտության օգտագործվում է այնպիսի վիրտուալ տիրույթներում, որոնց մասին խարդախության զոհը կարող է անգամ տեղյակ չլինել (օրինակ՝ որոշակի կայքեր, բլոգեր, էլեկտրոնային հարթակներ և այլն):

Խարդախները փոխհամաձայնեցված գործողությունների միջոցով ՋՄՄԽ-ի սխեմաներ գործարկում և հանցավոր եկամուտներ ստանում են՝ գտնվելով տարբեր երկրներում և անգամ տարբեր մայրցամաքներում: Օրինակ, աֆրիկյան որևէ երկրում խարդախը սրճարանից ինտերնետով կարող է շտապ օգնության խարդախ սխեմայով գումարներ կորզել ԱՄՆ-ի քաղաքացուց՝ նրան հրահանգելով փոխանցում կատարել Ասիայում գտնվող իր համագործակից խարդախի հաշվին, ով իր հասանելիք միջնորդավճարը պահելուց հետո ստացված միջոցները փոխանցում է Եվրոպայում գտնվող «գլխավոր» խարդախին: Խարդախ սխեմաները կազմակերպվում են այնպես, որ թույլ տան հնարավորինս արագ ու հեշտ եկամուտներ ստանալ:

3. ՋՄՄԽ-ի բնութագրիչները

ՋՄՄԽ-ի հետևյալ բնութագրիչների իմացությունը կարող է օգտակար լինել դրա հնարավոր սխեմաները ճանաչելու և բացահայտելու գործում.

- Հաճախակի և կրկնվող մուտքային-ելքային գործարքներ,
- Մեծածավալ կանխիկ մուտքեր և փոխանցումներ,
- Արտասահմանյան (մեծածավալ) փոխանցումների անմիջապես կանխիկացում,

- Երրորդ անձանց կողմից կանխիկ մուտքեր,
- «Կանխիկ դրամի սուրհանդակների»³ միջոցով գումարների տեղաշարժ,
- Բազմաթիվ փոխկապակցված տրոհված գործարքներ,
- Կլոր գումարով գործարքներ,
- Առանց առերես շփման գործարքներ (այդ թվում՝ կանխիկ դրամի ընդունման մեքենաների միջոցով),
- Միմյանց հետ որևէ կապ կամ հարաբերություն չունեցող անձանց միջև փոխանցումներ,
- Փողերի լվացման առումով բարձր ռիսկային երկրներ կամ այդ երկրներից փոխանցումներ, որոնք որևէ ակնհայտ գործարար նպատակ չեն հետապնդում,
- Կեղծված վճարային փաստաթղթերի օգտագործմամբ փոխանցումներ,
- Կեղծված չեքերի օգտագործմամբ գործարքներ,
- Բնակչության խոցելի խմբերի (օրինակ՝ միայնակ ծերերի) կողմից արագ փոխանցման համակարգերի միջոցով արտասահմանյան փոխանցումներ՝ առանց հստակ նպատակի,
- Կատարվող փոխանցումների վերաբերյալ հարցեր տալու դեպքում փոխանցողի «պաշտպանական» վարքագիծ,
- Հաճախորդի գործարար բնութագրին անհամապատասխան խոշոր գործարքներ,
- Անձնական հաշիվների օգտագործում բիզնես նպատակներով կատարվող գործարքների համար,
- Նույն աշխարհագրական տարածքում արագ փոխանցման բազմաթիվ համակարգերի միջոցով գործարքներ,
- Վարկային քարտերով ինտերնետային գործարքներ,
- Ինտերնետային վճարման համարգերի միջոցով գործարքներ,
- Կարճ ժամանակահատվածում նույն շահառուին բազմաթիվ անձանց կողմից կատարվող փոխանցումներ,
- Նույն ֆինանսական հաստատությունում հաճախորդի կողմից բացված բազմաթիվ հաշիվներ:

Վերը ներկայացված բնութագրիչներից մեկի կամ մի քանիսի առկայությունից հնարավոր չէ միանշանակ եզրահանգման գալ որևէ խարդախ սխեմայի գոհի կամ կազմակերպչի հետ գործ ունենալու մասին: Զոհերը հաճախ չունեն սեփական միջոցներ, և կազմակերպիչների հրահանգով ապահովում են վերջինների հափշտակած միջոցների տեղաշարժը՝ որոշակի միջնորդավճարի դիմաց: Այդպիսով

³ Կանխիկ դրամը երկրների մաքսային սահմանով ֆիզիկապես տեղափոխող անձինք

զոհն ինքը դառնում է հանցավոր շղթայի մասնակից: Նրան այդ քայլին դրդելու համար կազմակերպիչը կարող է համոզել կամ սպառնալ՝ օգտվելով նրա անօգնական կամ խոցելի վիճակից: Արդյունքում գործարկված ապօրինի գործողությունների շղթան հաճախ շատ դժվար է բացահայտել:

Միջոցների փոխանցումը կատարվում է տարատեսակ գործարքների միջոցով: Գումարները կարող են մուտքագրվել և ելքագրվել մեկ կամ մի քանի հաշվից, կանխիկ կամ փոխանցումների միջոցով, հաշիվները կարող են բացված լինել կեղծ փաստաթղթերի հիման վրա, փոխանցումները կարող են կատարվել արագ փոխանցման համակարգերով՝ առանց հաշիվ բացելու, հափշտակված գումարները կարող են արտերկիր տեղափոխվել նախքան դրանց ծագման վերաբերյալ կասկածներ առաջանալը և/կամ հաշվետվականության պահանջների ենթակա դառնալը, հաշիվներ բացելու կամ փոխանցումներ կատարելու համար խարդախները կարող են օգտվել գողացված նույնականացնող տվյալներից և այլն:

Այդուհանդերձ, վերը նկարագրված բնութագրիչները համակցության մեջ, ինչպես նաև ՋՄՄԽ-ի տեսակների վերաբերյալ պատկերացում ունենալու պարագայում կարող են կարևոր ուղղորդիչ նշանակություն ունենալ դրանցից բխող սպառնալիքներին հակազդելու հարցում: