Խարդախ սխեմաներ Ֆինանսական Ապահովություն

ՖԻՆԵԴՈՒ

საქართველოს ეროვნული ბანკი
National Bank of Georgia

BTU BUSINESS & TECHNOLOGY UNIVERSITY

საქართველოს პრეზიდენტის სარეზერვო ფონდი

մարտ **2024**

Հավանաբար լսել եք խարդախ սխեմաների մասին, որոնք մարդկանց ֆինանսական կորուստներ են պատճառում: Այս գրքույկի նպատակն է ձեզ տեղեկատվություն տրամադրել ֆինանսական խարդախության ամենատարածված ձևերի մասին և գործնական խորհուրդներ տալ, որոնք կօգնեն ձեզ խուսափել խարդախությունից:

Ինտերնետային Խարդախություն

Քանի որ բնակչության ճնշող մեծամասնությունը ակտիվորեն օգտվում է ինտերնետից, այսօր հենց ինտերնետի օգտատերերն են խարդախների համար ամենահեշտ հասանելի և գրավիչ թիրախը: Համացանցի ակտիվ տարածումն ու օգտագործումը, ինչպես նաև տեխնոլոգիական զարգացումները նոր տեսակի ռիսկեր են ստեղծել խարդախության առումով:

Ինտերնետում խարդախության ամենատարածված ձևերից մեկը ֆիշինգն է: «Ֆիշինգ» (phishing) տերմինը ծագել է անգլերեն «fishing» բառից, որը նշանակում է ձկնորսություն:

Ֆիշինգի շրջանակներում, խարդախների կողմից օգուտ ստանալու նպատակով տեղի է ունենում ինտերնետի օգտատերերի մասին այնպիսի տեղեկությունների ձեռքբերում, ինչպիսիք են անձնական համարը, ինտերնետ բանկինգի գաղտնաբառը, քարտի կամ բանկային հաշվի համարը, քարտի հետևի կողմում նշվող CVV կոդը՝ անվտանգության երեք թվերը (օրինակ՝ VISA և Mastercard քարտեր) կամ չորս թվերը (օր. American Express տեսակի քարտեր) ծածկագիրը և այլ գաղտնի տեղեկատվություն: Ունենալով այս տվյալները՝ խարդախները կարող են առանց ձեր թույլտվության իրականացնել տարբեր չարտոնված գործողություններ (օրինակ՝ ձեր անունից պարտք վերցնել) և յուրացնել ձեր գումարը:

Ֆիշինգը սովորաբար կատարվում է էլեկտրոնային նամակներ (e-mail) ուղարկելու միջոցով:

Նման նամակն առաջին հայացքից նման է վստահելի աղբյուրի հաղորդագրության, ինչպիսին է բանկի, ապահովագրական ընկերության, վճարային ծառայություններ մատուցողի և այլ կազմակերպությունների, որոնց հետ պոտենցիալ զոհը կարող է հարաբերություններ ունենալ:

Խարդախ հաղորդագրությունը հաճախ պարունակում է հղում դեպի կայք, որի հասցեն գրեթե չի տարբերվում իրական էջի հասցեից: Սակայն կեղծ կայք մտնելիս օգտատիրոջ մուտքագրած տեղեկատվությունը՝ անուն և ազգանուն, ինտերնետ բանկինգի օգտանուն և գաղտնաբառ, բանկային քարտ կամ հաշվի համար, անվտանգության կոդ և այլն, ավտոմատ կերպով անցնում է այսպես կոչված՝ «Ֆիշերի» ձեռքը: Խարդախ էլեկտրոնային նամակը կարող է նաև պարունակել ֆայլ, որի բացման դեպքում հնարավոր է դառնում մուտք գործել ձեր համակարգիչ: Կան ֆիշինգի այլ տարածված մեթոդներ:

Այդպիսի մեթոդներից մեկը սոցցանցերում կեղծ առաջարկներ տարածելն է: Այս դեպքում սոցիալական ցանցի օգտատերը կարող է բախվել գովազդի կամ առաջարկի հետ, որի հետևը կանգնած է կեղծ կազմակերպություն կամ անձ (անձանց խումբ), որի նպատակն է ստանալ օգտատիրոջ անձնական և գաղտնի տվյալները: Ուստի պետք է ուշադիր լինել սոցիալական ցանցերից ստացվող առաջարկների հանդեպ, և ավելի լավ է հնարավորինս սահմանափակել անձնական տեղեկատվության փոխանակումը սոցիալական ցանցերի միջոցով:

Ֆիշինգը կարող է իրականացվել նաև առանց ինտերնետի: «Սմիշինգը»/smishing՝ SMS-ֆիշինգը ֆիշինգի տեսակ է, որն իրականացվում է կարճ տեքստային հաղորդագրություն ուղարկելու միջոցով, որտեղ նամակ ուղարկողը բանկի կամ այլ կազմակերպության անունն է, և որի բովանդակությունը պարունակում է հղում դեպի խարդախ կայք: Իսկ վիշինգը / vishing հեռախոսային խարդախության ձև է, որն օգտագործվում է խարդախների կողմից՝ գաղտնի տեղեկատվություն ստանալու համար: Օրինակ, խարդախները կարող են զանգահարել հաճախորդներին բանկի անունից և խնդրել նրանց փոխանցել քարտի տվյալները և PIN-ը: Ուստի օգտատերը պետք է զգույշ լինի նաև հեռախոսային զրույցների ժամանակ:

Հիշեք, որ ֆիշինգ/կեղծ նամակները հաճախ հայտնվում են «սպամի» տեսքով: Առանց ստացողի համաձայնության և առանց նրա ցանկության էլեկտրոնային նամակներ ուղարկելու գործընթացը կոչվում է «Սպամինգ»/ spamming: Սովորաբար, նման էլ. նամակները գովազդային տեսք ունեն, թեև հաքերները հաճախ օգտագործում են «սպամինգը» նաև խարդախ սխեմաների համար և տարբեր բովանդակության հաղորդագրություններ են ուղարկում պոտենցիալ զոհերին, օրինակ՝ դրամական պարգև պահանջելը, խարդախության նպատակով ծանոթանալու խնդրանքը, գումարի վերադարձի կամ փոխհատուցման պահանջը և այլն: Ուստի զգուշացեք առաջարկներից, որոնք գալիս են «սպամի» տեսքով՝ առանց ձեր ցանկության:

Անձնական և ֆինանսական տեղեկատվության գողությունը միակ սպառնալիքը չէ, որի առջև կարող է կանգնել ֆիշինգի զոհ օգտատերը: Ֆիշինգական/խարդախ վեբ կայքը կարող է նաև պարունակել վնասակար կամ լրտեսող ծրագրեր: Այսպիսով, եթե դուք չունեք բանկային հաշիվ, որը կարող է հետաքրքրել խարդախներին, դա չի նշանակում, որ դուք լիովին ապահով եք: Խարդախը կարող է գողանալ ձեր էլ. փոստի տվյալները, որպեսզի օգտագործի այն սպամ և վիրուսներ տարածելու համար այլ օգտատերերի շրջանում:

Ամփոփելով, կարևոր է զգույշ լինել ձեր անձնական տեղեկատվության հետ: Հնարավորինս ձեռնպահ մնացեք անձնական/անձնագրի համարները,

ինչպես նաև բանկային քարտի և հաշվի մանրամասները, ներառյալ քարտի համարը, փին կոդը, քարտի գործողության ժամկետը և քարտի հետևի 3 կամ 4 նիշանոց անվտանգության կոդը հայտնելուց: Եթե վստահ չեք, որ իսկապես խոսում եք ձեր բանկի հետ՝ լինի դա էլ. փոստով, SMS, հեռախոսով կամ սոցիալական ցանցով, անպայման կապվեք բանկի հետ պաշտոնական հեռախոսահամարով և խնդրեք պարզաբանել իրավիճակը: Հիշեք, որ ֆիշինգային խարդախությունների հաջողությունը մեծապես կախված է օգտատերերի անտեղյակությունից և անզգուշությունից:

Ինտերնետային խարդախությունից խուսափելու համար ավելի լավ է ինտերնետային տիրույթում չօգտագործել ձեր հիմնական քարտը, որի վրա ունեք աշխատավարձ, կամ որի վրա ունեք մեծ գումար, որպեսզի խուսափեք ինտերնետային խարդախությունից;

Տարբեր ապրանքներ և ծառայություններ առցանց գնելու համար ցանկալի է ունենալ առանձին հաշիվ և քարտ, որտեղ կպահեք ճիշտ այնքան գումար, որքան որ անհրաժեշտ է առցանց գնումներ կատարելու համար: Այնուամենայնիվ, լրացուցիչ, թեկուզ ոչ կատարյալ, բայց անվտանգության մեխանիզմ է ինտերնետ-գործարքների իրականացումը անվտանգ կայքերում: Անվտանգ է համարվում այն վեբ հասցեն, որը սկսվում է https: // կամ shttp: // և ոչ թե http: //-ով: Կայքի անվտանգությունը մատնանշվում է նաև կողպված կանաչ կողպեքի խորհրդանիշով, որը հայտնվում է կայքի հասցեի դաշտում և որի վրա սեղմելով՝ կարող եք դիտել կայքի վստահելիությունն ու անվտանգությունը հաստատող վկայականը:

Բացի այդ, նախընտրելի է առցանց վճարում կատարել այնպիսի կայքից, որն ունի 3D անվտանգության տեխնոլոգիա, և ավելի լավ է, որ ձեր քարտի վրա ակտիվացված լինի 3D պաշտպանության մեխանիզմը:

Նաև, ձեր բջջային և ինտերնետ-բանկինգ մուտք գործելու համար ավելի լավ է օգտագործել բարդ գաղտնաբառ և ակտիվացնել երկմակարդակ նույնականացման ֆունկցիան, որն ի նկատի ունի գաղտնաբառից բացի անվտանգության լրացուցիչ միջոցների օգտագործում, օրինակ՝ SMS-ի, էլ. փոստի կամ հատուկ սարքի միջոցով՝ թոքենի (այսպես կոչված «դիջիփաս/անցակող», որը ստեղծում է մեկանգամյա օգտագործման կոդը) ստացումն ու համակարգ մուտք գործելը: Ինտերնետ-բանկինգի կամ մոբայլ բանկինգի միջոցով գործարքներ իրականացնելիս խորհուրդ է տրվում նաև օգտագործել երկաստիճան նույնականացում, որի դեպքում յուրաքանչյուր գործարքի համար կստանաք եզակի ծածկագիր SMS-ի, էլ. փոստի կամ թոքենի միջոցով: Ինչ վերաբերում է գաղտնաբառին, ապա ցանկալի է, որ այն բաղկացած լինի առնվազն տասներկու նիշից և պարունակի ինչպես մեծատառ, այնպես էլ փոքրատառ տառեր, թվեր և այլ նշաններ (օրինակ՝ կետ, գծիկ, բացականչական նշան):

Մի պահեք քարտի տվյալները, ինտերնետ-բանկինգի օգտանունը և գաղտնաբառը ձեր համակարգչում, բջջային հեռախոսում և այլ էլեկտրոնային սարքերում:
Հանրային WiFi-ից (անլար ինտերնետ) օգտվելիս մի՛ օգտվեք ինտերնետ բանկինգից և մի՛ մուտքագրեք քարտի տվյալները համակարգ: Ձեր էլեկտրոնային սարքերը, ներառյալ սմարթֆոնները, պլանշետները և նոութբուքերը, հաքերային հարձակումներից պաշտպանելու համար խորհուրդ ենք տալիս ժամանակին թարմացնել ձեր ծրագրերը և համոզվել, որ օգտագործում եք հակավիրուսային ծրագրի վերջին տարբերակները:

Ի վերջո, այս կամ այն կայքի իսկությունն ու ծագումը որոշելու համար կարող եք օգտվել WHOIS ծառայությունից (արձանագրությունը), որն առաջարկում են բազմաթիվ կայքեր: Բավական է մուտքագրել կասկածելի կայքի (դոմենի) հասցեն (օրինակ՝ www.whois.net, www.whois.com, և այլն), WHOIS-ը կփնտրի հանրային տվյալների բազաներում և ձեզ տեղեկատվություն կտրամադրի կայքի մասին, ինչպիսիք են գրանցումը և վավերականությունը, կայքի ներկայիս սեփականատերը և այլն: Սա կօգնի ձեզ պարզել կայքի իսկությունը: Օրինակ, եթե դուք գիտեք, որ ձեզ ծանոթ ընկերության կայքը երկար ժամանակ գոյություն ունի, իսկ կասկածելի կայքի գրանցման ամսաթիվը համեմատաբար նոր է, դուք հավանաբար գործ ունեք խարդախության հետ:
Խարդախություն բանկային վճարային քարտի, բանկոմատի և POS-տերմինալի միջոցով

Եթե ուշադրություն չդարձնեք, խարդախները կարող են նույնիսկ գողանալ ձեր կրեդիտ քարտի տվյալները, երբ դուք օգտվում եք բանկոմատից կամ փոս-տերմինալից:
Զգույշ եղեք բանկոմատից օգտվելիս. թույլ մի տվեք, որ այլ մարդիկ շատ մոտ կանգնեն ձեզ և տեսնեն, թե ինչ PIN կոդ եք հավաքում: Օգտագործելիս մյուս ձեռքով փակեք բանկոմատի ստեղնաշարը, լավ նայեք բանկոմատին և համոզվեք, որ բանկոմատում կամ մերձակայքում չկա որևէ տեսախցիկ կամ սարք, որը չի պատկանում բանկին, և կարող է գրանցել ձեր քարտի տվյալները:
Ի վերջո, համոզվեք, որ չեք թողնում ձեր քարտը և գումարը բանկոմատում:

Մի պահեք քարտի տվյալները, ինտերնետ-բանկինգի օգտանունը և գաղտնաբառը ձեր համակարգչում, բջջային հեռախոսում և այլ էլեկտրոնային սարքերում:
Հաճախորդները հաճախ իրենց քարտը թողնում են առանց հսկողության, ինչը ձեռնտու է խարդախների համար: Քարտը և ֆինանսական փաստաթղթերը մի թողեք գրասեղանի վրա աշխատավայրում կամ համալսարանում, մեքենայում կամ հասարակական վայրերում, որտեղ այլ անձ կարող է տեսնել դրանք: Քարտի վրա մի գրեք PIN կոդը և դրամապանակում մի դրեք քարտն ու թղթի վրա գրված PIN կոդը միասին: Նույնպես, ինչպես արդեն նշեցինք, չուղարկեք քարտի տվյալները՝ համարը, վավերականության ժամկետը, անվտանգության կոդը հեռախոսով կամ էլեկտրոնային փոստով և մի տրամադրեք այս տվյալները նույնիսկ ձեր ընկերներին և ընտանիքի անդամներին:

Կարևոր է խոսել նաև սկիմինգի մասին, որը ֆինանսական խարդախության ամենաընշանավոր ձևերից մեկն է: Skimming-ի ժամանակ բանկոմատի կամ POS տերմինալի վրա տեղադրվում է հատուկ սարք՝ սքիմեր / skimmer, որի նպատակն է գողանալ քարտի տվյալները (PIN կոդը, քարտի համարը, վավերականության ժամկետը, անվտանգության ծածկագիրը), որը խարդախն օգտագործում է՝ փողերը յուրացնելու համար:
Որպեսզի ձեզ պաշտպանեք սքիմինգից, բանկոմատ օգտագործելիս, հատկապես արտերկրկում, համոզվեք, որ այն լավ լուսավորված վայրում է (իսկ գիշերը ցանկալի է պաշտպանված միջավայրում (օրինակ՝ բանկի շուրջօրյա սպասարկման կենտրոնում) գտնվող բանկոմատներից օգտվել), չի նկատվում որևէ վնասվածք, և որ կասկածելի սարքեր տեղադրված չեն անմիջապես բանկոմատի վրա: Օրինակ, եթե բանկոմատի ստեղնաշարի վրա, որի միջոցով հաճախորդը մուտքագրում է իր քարտի PIN կոդը, կպցրած է որևէ սարք կամ թափանցիկ ռետինե/պլաստիկե թափանցիկ թաղանթ, ապա վճարային քարտը մի տեղադրեք բանկոմատում և մի հավաքեք PIN կոդը այդ բանկոմատում: Նաև, բանկոմատից օգտվելուց առաջ համոզվեք, որ բանկի պաշտոնական գրությունը բանկոմատիէկրանին է:

Եթե վստահ չեք, որ բանկոմատից օգտվելն անվտանգ է, ապա ավելի լավ է ձեռնպահ մնաք այն օգտագործելուց և խնդրի առկայության դեպքում անմիջապես տեղեկացնեք բանկին: Դուք նաև պետք է պահպանեք անվտանգության նախազգուշական միջոցները POS-տերմինալից օգտվելիս. համոզվեք, որ այն վնասված չէ: Նաև պահանջեք, որ գործարքն իրականացվի ձեր ներկայությամբ և երբեք քարտը մի տվեք սպասարկող անձնակազմին (ներառյալ բենզալցակայաններում, ռեստորաններում և այլ վայրերում), քանի որ այդ պահին կա ձեր քարտի տվյալները գողանալու վտանգ: Նկատի ունեցեք, որ տվյալների գողությունը կարելի է անել ոչ միայն հատուկ սարքերի միջոցով, այլ նաև շատ հեշտությամբ՝ լուսանկարելով կամ նույնիսկ պատճենելով տվյալները: Ուստի թույլ մի տվեք, որը քարտը դուրս գա ձեր տեսադաշտից:

Ֆինանսական խարդախություններից պաշտպանվելու համար լավ է օգտվել բանկի SMS ծառայությունից, որը թույլ կտա ակնթարթորեն ստանալ տեղեկատվություն քարտով կատարված գործարքների մասին: Բանկային քաղվածքների պարբերական ստուգումը լավ միջոց է քարտով գործարքները վերահսկելու համար:

Այսպիսով, դուք հեշտությամբ կնկատեք այն կասկածելի գործարքները, որոնք հնարավոր է, որ դուք չեք կատարել: Եթե ձեր վճարային քարտը կորել կամ գողացվել է, անմիջապես դիմեք քարտը թողարկած ֆինանսական հաստատությանը և խնդրեք, որ քարտն արգելափակվի: Շատ դեպքերում քարտը կարող եք արգելափակել նաև առցանց և մոբայլ բանկինգի միջոցով: Եթե դուք չեք արգելափակում քարտը, խարդախները, ովքեր գողացել կամ գտել են ձեր քարտը, կարող են ակնթարթորեն կեղծ գործարքներ իրականացնել:

Խարդախություն կեղծ փողերի օգտագործմամբ

Կեղծ փողերով ևս հնարավոր է խարդախություն իրականացնել: Մեզանից յուրաքանչյուրը կարող է դառնալ նման խարդախ սխեմայի զոհ: Ուշադիր եղեք կանխիկ գումար ստանալու ժամանակ, նայեք ձեզ տրամադրված թղթադրամին և ստուգեք անվտանգության առանձնահատկությունները, որոնք տարբերում են իրական փողը կեղծ փողից: Կեղծ թղթադրամ հայտնաբերելու դեպքում դուք պետք է դիմեք ձեր ծառայություններ մատուցողին կամ Վրաստանի Ազգային բանկին ու իրավապահ մարմիններին:

Ֆինանսական բուրգեր

Ժամանակակից աշխարհում ֆինանսական խարդախության ամենատարածված ձևերից են այսպես կոչված Ֆինանսական բուրգերը, որոնց մասին տեղեկատվության տիրապետումը կօգնի ձեզ խուսափել կասկածելի գործարքներում ակամա ներգրավվելուց:

Ֆինանսական բուրգը գործունեության մի ձև է, որի ժամանակ տեղի է ունենում բնակչությունից փողերի հավաքում և դրա դիմաց, որպես կանոն, առաջարկում են շուկայական տոկոսադրույքների համեմատ շատ ավելի բարձր եկամուտներ:

Ֆինանսական բուրգը, մեծ մասամբ, շահութաբեր ներդրում չի կատարում, և հաճախորդին խոստացված օգուտների դիմաց վճարման միակ աղբյուրը նոր և (կամ) գործող անդամներից լրացուցիչ միջոցներ ներգրավելն է:Անկախ նրանից, թե որքան հաջողակ է թվում նման ընկերությունը ժամանակի ինչ-որ պահի, նոր անդամներ և/կամ լրացուցիչ միջոցներ ներգրավելը կարևոր է սխեմայի գործարկման համար: Հետևաբար, երբ անհնար է դառնում նոր անդամներ և/կամ լրացուցիչ միջոցներ ներգրավելը, ընկերությունն այլևս չի կարողանում կատարել իր պարտավորությունները անդամների հանդեպ, և ֆինանսական բուրգն անխուսափելիորեն փլուզվում է, Ֆինանսական բուրգի և դրա ճանաչելի նշանների մասին լրացուցիչ տեղեկություններ կարող եք նաև կարող եք դիտել ստորև ներկայացված տեսանյութները.

- www.finedu.gov.ge
- www.youtube.com/@FineduGeorgia

Ուշադիր եղեք Ձեր խնայողությունները որևէ կազմակերպությանը վստահելիս, տեղեկացեքկազմակերպության գործունեության և ֆինանսական վիճակի մասին և համոզվեք, որ գործ չունեք խարդախ սխեմաների հետ: Հիշեք, որ հիմնականում խոստացված բարձր եկամուտը կապված է բարձր ռիսկի հետ: Ի վերջո, ոչ ոք ապահովագրված չէ ֆինանսական խարդախություններից: Հետևաբար, խոհեմությունն ու զգուշությունը, ինչպես նաև սեփական իրավունքների և պարտականությունների և ֆինանսական խարդախության ամենատարածված ձևերի իմացությունը կօգնեն ձեզ պաշտպանվել խարդախ սխեմաներից և ժամանակին արձագանքել խարդախության դեպքում:

Մաղթում ենք ձեզ
ֆինանսական անվտանգություն: