

ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

Քարտային զեղծարարության արդյունքում ստացված միջոցների լվացման միտումների վերաբերյալ

Քարտային զեղծարարությունը¹ ենթադրում է այլ անձին պատկանող բանկային քարտի համ դրան համարժեք գործիքի տվյալների ապօրինի ձեռքբերում՝ հաշվին առկա դրամական միջոցները տնօրինելու նպատակով: Քարտային զեղծարարության դեպքերը կարող են դրսևորվել ինչպես հաճախորդին մոլորեցնելու և գործարքների կատարման համար նրա համաձայնությունը ստանալու, այնպես էլ հաճախորդի հաշվով առանց նրա իմացության և հաստատման գործարքներ կատարելու եղանակով:

2021 թվականի հոկտեմբերին Եվրոպական կենտրոնական բանկի կողմից հրապարակված տվյալների համաձայն քարտային զեղծարարության արդյունքում կորուստների մասնաբաժինն ընդհանուր գործարքների ծավալում կազմում է 3.6 տոկոս, ընդ որում, քարտային զեղծարարությունների ծավալի կեսից ավելին կապված է **անդրսահմանային գործարքների** հետ:²

Անվտանգ գործարքների եվրոպական ասոցիացիայի 2022 թվականի ուսումնասիրության արդյունքները ցույց են տալիս, որ քարտային զեղծարարությունների թվում մեծ մաս են կազմում **տեխնոլոգիական միջոցների օգտագործմամբ** կատարված դեպքերը:³ Իրավախախտները ֆիշինգային հարձակումների կամ այլ հնարքների օգտագործմամբ հասանելիություն են ստանում հաճախորդի բանկային քարտի տվյալներին և կատարում իրենց կողմից կառավարվող հաշիվներին փոխանցումներ կամ առցանց հարթակներում վճարումներ:

Հայաստանում բացահայտված քարտային զեղծարարության դեպքերի ուսումնասիրությունը ցույց է տալիս, որ հատկապես տարածված են այն դեպքերը, երբ հանցագործները, տուժողների հաշիվներին հասանելիություն ստանալու նպատակով, **հեռախոսազանգով կամ առցանց հարթակներում ներկայանում են** որպես ֆինանսական հաստատության աշխատակից կամ պետական մարմնի ներկայացուցիչ: Հանցագործը խոստանում է որոշակի ֆինանսական շահ (այդ թվում՝ պետության կողմից տրամադրվող ֆինանսական աջակցություն կամ վարկ), որի համար պահանջում և ստանում է հասանելիություն անձի բանկային քարտի տվյալներին, էլեկտրոնային դրամապանակի մուտքանվանը և գաղտնաբառին, գործարքը հաստատելու համար ստացված կարճ

¹ Քարտային զեղծարարությունը կարող է դրսևորվել համակարգչային հափշտակության, խարդախության կամ այլ հանցակազմերի տեսքով:

² European Central Bank, “Seventh report on card fraud” (2021), առցանց հասանելի է www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html#toc6 հղմամբ:

³ EAST, “Fraud Update 1-2022” March 2022, առցանց հասանելի է www.association-secure-transactions.eu/east-publishes-fraud-update-1-2022/ հղմամբ. EAST, “Fraud Update 2-2022” July 2022, առցանց հասանելի է www.association-secure-transactions.eu/east-publishes-fraud-update-2-2022/ հղմամբ:

հաղորդագրությունների բովանդակությանը և այլ տեղեկությունների:⁴ Ստեղծված իրավիճակում տուժողները սեփական կամքով հանցագործներին հասանելիություն են տալիս իրենց անձնական տվյալներին՝ դրանով իսկ հնարավորություն ընձեռելով հափշտակել գումարներ իրենց բանկային հաշիվներից և էլեկտրոնային դրամապանակներից: Որոշ դեպքերում հանցագործները, օգտագործելով էլեկտրոնային դրամապանակներին ստացած հասանելիությունը, տուժող անձանց անունից դիմում և ստանում են վարկեր ու հափշտակում տրամադրված գումարները:

Քրեական գործերի շրջանակներում բացահայտվել է նաև անձանց տվյալներին հասանելիություն ստանալու նպատակով **օրինական գործունեություն իրականացնող կազմակերպության կեղծ կայքէջի ստեղծման** դեպք:⁵ Այսպիսի սխեմաներում հանցագործները ստեղծում են, օրինակ, առցանց ինտերնետ շահումով խաղերի հարթակի նմանությամբ կայքէջ, որն արտաքին տեսքով չի տարբերվում կազմակերպության պաշտոնական կայքէջից: Նշված կեղծ կայքէջում իրենց իրական մուտքանունը և գաղտնաբառը մուտքագրած անձինք դրանք հասանելի են դարձնում հանցագործներին: Վերջինները ստացված տվյալների օգտագործմամբ մուտք են գործում տուժողների իրական անձնական հաշիվներ, որոնց կցված վճարման միջոցներից (օրինակ՝ բանկային քարտերից) կատարում են փոխանցումներ իրենց անձնական հաշիվներին կամ առցանց հարթակներում գնումներ:

ՀՀ կենտրոնական բանկի ֆինանսական դիտարկումների կենտրոնի կողմից իրականացված կասկածելի գործարքի կամ գործարար հարաբերության վերաբերյալ հաշվետվությունների վերլուծությունները ցույց են տալիս, որ բանկային քարտերի կամ դրանց համարժեք գործիքների տվյալներին ապօրինի կերպով հասանելիություն ստացած անձինք հանցավոր գումարների օրինականացման նպատակով չարաշահում են նաև **առևտրի և սպասարկման կետերի կողմից օգտագործվող անկանխիկ վճարման համակարգերը**: Այսպես, տեխնոլոգիական արագ զարգացումները և հատկապես առցանց առևտրի ընդլայնված հնարավորությունները նպաստել են վիրտուալ ՊՈՍ տերմինալների օգտագործման ծավալների աճին:⁶ Այս զարգացումների համատեքստում զեղծարարները,

⁴ «Համակարգչային հափշտակություն և փողերի լվացում կատարելու գործը դադարանում է», 07.09.2022թ., առցանց հասանելի է www.investigative.am/news/view/hamakargchayin-hapshtakutyun-poxeri-lvacum.html հղմամբ: «Համակարգչային տեխնիկայի օգտագործմամբ տարբեր չափերի գումարներ հափշտակելու գործից անջատված մասի նախաքննությունն ավարտվել է» (տեսանյութ), 05.01.2022թ., առցանց հասանելի է www.investigative.am/news/view/hamakargchi-mijocov-hapshtakutyun1.html հղմամբ: «Ավարտվել է երկու տասնյակից ավել անձանցից և ֆինանսական կազմակերպություններից կատարված համակարգչային հափշտակության վարույթի նախաքննությունը», 14.10.2022թ., առցանց հասանելի է www.investigative.am/news/view/hapshtakutyun-erku-tasnyakic-avel-andzancic-avart.html հղմամբ:

⁵ «Ավարտվել է համակարգչային տեխնիկայի օգտագործմամբ հափշտակություն կատարելու, համակարգչային տեղեկատվությանն ապօրինի տիրանալու գործի նախաքննությունը», 04.07.2022թ., առցանց հասանելի է www.investigative.am/news/view/hapshtakutyun-hamakargchayin-texnikayigorcadrmamb.html հղմամբ:

⁶ ՊՈՍ տերմինալները սարքեր են, որոնք օգտագործվում են վճարողի կետերում անկանխիկ վճարումներ ընդունելու համար: Վիրտուալ ՊՈՍ տերմինալներն էլեկտրոնային լուծումներ են, որոնք տեղադրվում են վճարողի կայքէջում և ընձեռում են տվյալ վճարողից առցանց գնումներ կատարելու հնարավորություն:

առանց ձեռնարկատիրական գործություն իրականացնելու նպատակի, ստեղծում են իրավաբանական անձինք կամ հաշվառվում են որպես անհատ ձեռնարկատեր միայն վիրտուալ ՊՈՍ տերմինալ ձեռք բերելու նպատակով: Վերջինը թույլ է տալիս այլ անձանց բանկային քարտերի կամ դրանց համարժեք գործիքների տվյալների ապօրինի օգտագործմամբ հափշտակված միջոցները ներկայացնել որպես ձեռնարկատիրական գործունեությունից ստացված եկամուտներ: Այսպիսով, հափշտակված գումարները ֆինանսական համակարգում երևում են որպես հաճախորդների կողմից բիզնեսին կատարված վճարումներ և առաջին հայացքից կասկածներ չեն առաջացնում:

Ստորև ներկայացվում են այն ազդեցիկները, որոնք կարող են վկայել բանկային քարտերի կամ դրանց համարժեք գործիքների տվյալների ապօրինի օգտագործմամբ գումարների հափշտակության կամ հափշտակված գումարների օրինականացման փորձի մասին.

- Էլեկտրոնային դրամապանակ նոր սարքից մուտք գործելուց կարճ ժամանակ հետո հաճախորդը կատարում է իր կողմից սովորաբար կատարվող գործարքների գումարների չափն էականորեն գերազանցող գումարով գործարքներ և/կամ ներկայացնում վարկի ստացման հայտ: Դրամապանակի համալրումից կարճ ժամանակ հետո գումարները կանխիկացվում են կամ փոխանցվում այլ դրամապանակների/ բանկային հաշիվների:
- Ինտերնետ շահումով խաղերի կայքէջում անձնական էջ նոր սարքից մուտք գործելուց հետո հաշիվը համալրվում է հաճախորդի խաղային վարքագծին ոչ բնորոշ մեծ գումարի չափով: Անձնական խաղային հաշվի համալրումից կարճ ժամանակ հետո գումարները փոխանցվում են այլ խաղային հաշվի կամ կանխիկացվում են կամ փոխանցվում այլ դրամապանակների/ բանկային հաշիվների:
- Հաճախորդի բանկային հաշիվներին մեծ թվով արտասահմանյան քարտերից մուտքագրվում են գումարներ, գործարքների բնույթը չի համապատասխանում հաճախորդի գործարար բնութագրին: Հաճախորդը ստացված միջոցները կարճ ժամանակ հետո կանխիկացնում է կամ փոխանցում այլ դրամապանակների/ բանկային հաշիվների:
- Հաճախորդի բանկային հաշիվներին արտասահմանյան քարտերից ստացված փոխանցումները հաճախ չեղարկվում են գործարքը կատարողի կողմից:
- Հաճախորդի բանկային հաշիվներին փոխանցումները ստացվում են քարտերից, որոնց մասով առկա են տեղեկություններ կորցված կամ գողացված լինելու մասին: