

Ֆինանսական զեղծարարություններից խուսափելու նպատակով ՀՀ կենտրոնական բանկը հորդորում է

1. Զգոն եղեք անձնական տվյալների տրամադրման ժամանակ.

Երբեք այլ անձանց մի տրամադրեք մոբայլ/օնլայն բանկինգի մուտքանունները և գաղտնաբառերը, բանկային քարտի երեսին կամ հակառակ կողմում նշված եռանիշ/քառանիշ թվերը (CVV), բանկային քարտի վավերականության ժամկետները, հեռախոսահամարին (SMS-ով) կամ էլեկտրոնային փոստի հասցեին (email-ով) ստացված հաստատման կոդերը/գաղտնաբառերը: Բանկերի և/կամ պետական կառույցների աշխատակիցները երբեք չեն պահանջում նման տեղեկություններ:

Երբեք մի տրամադրեք ձեր անձնագրային տվյալները կասկածելի անձանց, կայքերին կամ կազմակերպություններին:

Բանկերը և պետական մարմինները կարող են պահանջել անձնագրային տվյալներ միայն իրենց պաշտոնական գործառույթների շրջանակում, սակայն նրանք երբեք չեն խնդրի դրանք հաղորդել էլեկտրոնային փոստով, սոցիալական ցանցերի միջոցով կամ հաղորդագրությունների տարբեր հարթակների միջոցով (WhatsApp, Viber, Telegram և այլն):

Մի հրապարակեք ձեր անձնական տվյալները սոցիալական ցանցերում, ֆորումներում կամ այլ կայքերում: Բացի այդ, բանկային քարտերի տվյալները, PIN-կոդերը, բանկային մուտքանուններն ու գաղտնաբառերը մի պահեք համակարգչում կամ հեռախոսի մեջ:

2. Զգուշացեք կասկածելի զանգերից.

Եթե զանգահարում են անձանոթ համարից և ներկայանում որպես ՀՀ կենտրոնական բանկի, իրավապահ մարմինների, պետական կազմակերպությունների կամ բանկերի անունից և առաջարկում կասկածելի գործարքներ (օրինակ՝ հայտնում են ձեր անունից վարկի ձևակերպման փորձի, կասկածելի գործարքի մասին և ուղղորդում մուտք գործել մոբայլ բանկինգ, տրամադրել հաստատման կոդեր, չեղարկել գործարքներ), անմիջապես ընդհատեք զանգը:

Եթե կասկածում եք, որ ձեզ զանգահարողը զեղծարար է, ինքներդ զանգահարեք ձեր բանկի հեռախոսահամարով, որը նշված է բանկային քարտի հակառակ կողմում կամ բանկի պաշտոնական կայքում:

3. Մի կատարեք ֆինանսական գործարքներ անհայտ անձանց պահանջով.

Եթե զանգահարում են կամ սոցիալական ցանցերի միջոցով կապ են հաստատում և ներկայանում ՀՀ կենտրոնական բանկի անունից և խնդրում են կամ պարտադրում գումար փոխանցել «պաշտպանված» կամ «հատուկ» հաշիվներին կամ առաջարկում

վարկ ձևակերպել՝ մի կատարեք ոչ մի գործողություն: ՀՀ կենտրոնական բանկը չի իրականացնում ֆիզիկական անձանց բանկային սպասարկում (չի բացում հաշիվներ և չի տրամադրում վարկեր):

4. Ապահովեք ձեր էլեկտրոնային սարքավորումների անվտանգությունը.

Հետևեք, որ ձեր համակարգիչներում և բջջային հեռախոսներում մշտապես առկա լինեն հակավիրուսային ծրագրեր և պարբերաբար թարմացրեք դրանք: Թույլ մի տվեք, որպեսզի երրորդ անձը հասանելիություն ստանա այդ սարքավորումներին: Մի տրամադրեք այդ սարքավորումների մուտքի գաղտնաբառերը ոչ ոքի՝ նույնիսկ ձեր հարազատներին:

5. Նախքան գնումներ կատարելը՝ ուսումնասիրեք կայքէջը.

Միշտ ունեցեք առանձին բանկային քարտ առցանց գնումներ կատարելու համար: Այդ քարտը համալրեք միայն գնումից առաջ և այդ պահին անհրաժեշտ գումարի չափով: Նախքան գնումներ կատարելը՝ ուսումնասիրեք կայքէջը, ծանոթացեք էջի իսկությանը, ուշադրություն դարձրեք, որ կայքի հասցեի կողքին լինի անվտանգ կապի նշան (օրինակ՝ կայքի հասցեն պետք է սկսվի <https://>-ով և/կամ հասցեի կողքին պետք է առկա լինի փականի նշան՝ ): Մի լրացրեք ձեր անձնական, բանկային տվյալները կասկածելի կայքերում:

6. Մուտք մի գործեք անհայտ, անծանոթ հղումներով և մի մուտքագրեք անձնական տվյալներ.

Մի անցեք կասկածելի նամակներում նշված հղումներով, որոնք առաջարկում են ստանալ ծանրոցներ, մասնակցել հարցումների կամ խոստանում արագ և հեշտ եկամուտներ, խոշոր շահումներ: Զգուշացեք այն նամակներից, որոնք շտապ արձագանքի պահանջ են ներկայացնում, պահանջում են անձնական տեղեկություններ, պարունակում են քողարկված սպառնալիքներ կամ ճնշումներ:

7. Զգոն եղեք առցանց առևտրի կամ վարձակալության էջերից օգտվելիս.

Նախապես համոզվեք գնորդի, վարձակալի կամ վարձատուի ինքնության մեջ: Նման գործարքների ժամանակ երբեք մի անցեք ստացված հղումներով: Հիշեք, որ գումար ստանալու համար կարիք չկա մուտք գործելու մոբայլ բանկինգ կամ որևէ այլ կայքէջ և պետք չէ լրացնել ձեր անձնական, բանկային տվյալները (նույնիսկ արագ դրամական փոխանցումներ ստանալու նախապայմանով):

Հաղորդագրությունից օգտվելու դեպքում հղումը սկզբնաղբյուրին պարտադիր է:

ԿԲ հասարակայնության հեղինակների ծառայություն

հեռ. (010) 592592-0702

էլ-փոստ. mcba@cba.am

www.cba.am