თალლითური სქემები და ფინანსური უსაფრთხოება

ფინედუ

საქართველოს ეროვნული ბანკი
National Bank of Georgia

BTU BUSINESS & TECHNOLOGY UNIVERSITY

საქართველოს პრეზიდენტის სარეზერვო ფონდი

მარტი **2024**

ალბათ, გსმენიათ თაღლითური სქემების შესახებ, რომელთა გამოც ადამიანები ფინანსურად ზარალდებიან. ამ ბროშურის მიზანია, გაგაცნოთ ინფორმაცია ფინანსური თაღლითობის ყველაზე გავრცელებული ფორმებისა და იმ პრაქტიკული რჩევების შესახებ, რომლებიც თაღლითობის თავიდან არიდებაში დაგეხმარებათ.

ინტერნეტ თაღლითობა

ფდღევანდელ დღეს, რამდენადაც მოსახლეობის უდიდესი ნაწილი აქტიურად იყენებს ინტერნეტს, სწორედ ინტერნეტ მომხმარებლები წარმოადგენენ თაღლითებისთვის ყველაზე ადვილად ხელმისაწვდომ და მიმზიდველ სამიზნეს. ინტერნეტის აქტიურმა გავრცელებამ და მოხმარებამ და, ასევე, ტექნოლოგიურმა განვითარებამ თაღლითობის თვალსაზრისით ახალი სახის რისკები წარმოქმნა.

ინტერნეტ თაღლითობის ერთ-ერთი ყველაზე გავრცელებული ფორმაა ფიშინგი. ტერმინი ფიშინგი (phishing) ინგლისური სიტყვიდან - fishing - მოდის, რაც თევზაობას ნიშნავს. ფიშინგის ფარგლებში, თაღლითების მხრიდან პირადი სარგებლის მიღების მიზნით ხდება ინტერნეტ მომხმარებლის შესახებ ისეთი ინფორმაციის მოპოვება, როგორიცაა პირადი ნომერი, ინტერნეტ ბანკის პაროლი, ბარათის ან საბანკო ანგარიშის ნომერი, ბარათის უკანა მხარეს დატანილი უსაფრთხოების 3-ნიშნა (მაგ.: VISA და Mastercard ტიპის ბარათებზე) ან 4-ნიშნა (მაგ.: American Express-ის ტიპის ბარათებზე) კოდი, და სხვა კონფიდენციალური ინფორმაცია. ამ მონაცემების ხელში ჩაგდების გზით, თაღლითებს თქვენი ნებართვის გარეშე სხვადასხვა არასანქცირებული ოპერაციის განხორციელება (მაგალითად, თქვენი სახელით სესხის აღება) და თქვენი თანხის მითვისება შეუძლიათ. ფიშინგი, როგორც წესი, ელექტრონული წერილების (e-mail) დაგზავნით ხორციელდება. ასეთი წერილი, ერთი შეხედვით, ისეთი სანდო წყაროსგან მიღებულ შეტყობინებას ჰგავს, როგორიცაა ბანკი, სადაზღვევო კომპანია, საგადახდო მომსახურების პროვაიდერი და სხვა ორგანიზაცია, რომელთანაც პოტენციურ მსხვერპლს შეიძლება ჰქონდეს ურთიერთობა. თაღლითურ გზავნილში ხშირად მოცემულია ვებგვერდის ბმული, რომლის მისამართი თითქმის არ განსხვავდება ნამდვილი გვერდის მისამართისგან. თუმცა, გაყალბებულ ვებგვერდზე გადასვლისას, მომხმარებლის მიერ შეყვანილი ინფორმაცია - სახელი და გვარი, ინტერნეტ-ბანკის მომხმარებლის სახელი და პაროლი, საბანკო ბარათის ან ანგარიშის ნომერი, უსაფრთხოების კოდი, და ა.შ.
- ავტომატურად ხვდება ე.წ. „ფიშერის“ ხელში. თაღლითურ ელექტრონულ წერილზე შეიძლება ასევე მიმაგრებული იყოს ფაილი, რომლის გახსნის შედეგადაც შესაძლებელი ხდება თქვენს კომპიუტერში შეღწევა.

არსებობს ფიშინგის სხვა გავრცელებული მეთოდებიც. ერთ-ერთ ასეთ მეთოდს სოციალურ ქსელში ყალბი შემოთავაზებების გავრცელება წარმოადგენს. ამ შემთხვევაში, სოციალური ქსელის მომხმარებელს შეიძლება შეხვდეს რეკლამა ან შეთავაზება, რომლის უკანაც ყალბი ორგანიზაცია ან ისეთი პიროვნება (პიროვნებათა ჯგუფი) დგას, რომლის მიზანსაც მომხმარებლის პირადი და კონფიდენციალური მონაცემების მოპოვება წარმოადგენს. შესაბამისად, ყურადღება გმართებთ სოციალურ ქსელებში მიღებულ შეთავაზებებთან დაკავშირებით და უმჯობესია, მაქსიმალურად შეზღუდოთ სოციალური ქსელით პირადი ინფორმაციის გაზიარება. ფიშინგი ინტერნეტის გარეშეც შეიძლება განხორციელდეს.

„სმიშინგი“ / smishing – SMS-ფიშინგი - ფიშინგის ერთ-ერთი ნაირსახეობაა, რომელიც მოკლე ტექსტური შეტყობინების გაგზავნის გზით ხორციელდება, სადაც წერილის გამომგზავნად ბანკის ან სხვა ორგანიზაციის სახელია მითითებული და რომლის შიგთავსიც თაღლითურ ვებმისამართზე გადასასვლელ ბმულს შეიცავს. ვიშინგი / vishing კი სატელეფონო თაღლითობის სახეობა, რომელსაც თაღლითები კონფიდენციალური ინფორმაციის მიღების მიზნით იყენებენ. მაგალითად, თაღლითები შესაძლოა, მომხმარებელს ბანკის სახელით ტელეფონით დაუკავშირდნენ და ბარათის რეკვიზიტებისა და პინ-კოდის გაზიარება სთხოვონ. შესაბამისად, მომხმარებელმა სატელეფონო კომუნიკაციის დროსაც უნდა გამოიჩინოს სიფრთხილე.

გაითვალისწინეთ, რომ ფიშინგური/ყალბი ელექტრონული წერილები ხშირად „სპამის“ სახით მოდის. „სპამინგი“ / spamming ელექტრონული წერილების მიმღების დაუკითხავად და მისი სურვილის გარეშე დაგზავნის პროცესს ეწოდება. როგორც წესი, მსგავსი წერილები სარეკლამო ხასიათისაა, თუმცა ჰაკერები „სპამინგს“ ხშირად თაღლითური სქემებისთვისაც იყენებენ და პოტენციურ მსხვერპლთან სხვადასხვა შინაარსის შეტყობინებებს აგზავნიან, როგორიცაა თანხის გადარიცხვის მოთხოვნა მოგებული პრიზის მისაღებად, გაცნობის მოთხოვნა თაღლითობის მიზნით, არასწორად ჩარიცხული თანხის უკან დაბრუნების მოთხოვნა, მედიკამენტების ან სხვა ნაწარმის შესყიდვის შეთავაზება და სხვა. ამიტომ, უფრთხილდით თქვენი სურვილის გარეშე, „სპამის“ სახით მოსულ შემოთავაზებებს. პირადი და ფინანსური ინფორმაციის მოპარვა არ არის ერთადერთი საფრთხე, რომლის წინაშეც ფიშინგის მსხვერპლი მომხმარებელი შეიძლება დადგეს. ფიშინგური/ყალბი ვებგვერდი შეიძლება მავნე ან ჯაშუშურ პროგრამასაც შეიცავდეს. ამრიგად, თუ თქვენ არ გაქვთ საბანკო ანგარიში, რომლითაც შეიძლება თაღლითები დაინტერესდნენ, ეს იმას არ ნიშნავს, რომ სრულიად უსაფრთხოდ ხართ. თაღლითს შეუძლია თქვენი ელექტრონული ფოსტის მონაცემების მოპარვა, რათა ის სხვა მომხმარებლებში „სპამისა“ და ვირუსების გასავრცელებლად

გამოიყენოს.
რომ შევაჯამოთ, აუცილებელია, გაუფრთხილდეთ თქვენს პირად ინფორმაციას. მაქსიმალურად შეიკავეთ თავი პირადი/პასპორტის ნომრის, ასევე, საბანკო ბარათის და ანგარიშის მონაცემების, მათ შორის, ბარათის ნომრის, პინ-კოდის, ბარათის მოქმედების ვადისა და ბარათის უკანა მხარეს მოცემული 3- ან 4-ნიშნა უსაფრთხოების კოდის გაზიარებისაგან. თუ არ ხართ დარწმუნებული, რომ ნამდვილად თქვენს მომსახურე ბანკს ესაუბრებით - იქნება ეს ელ-ფოსტით, SMS-ით, ტელეფონით თუ სოციალური ქსელებით - აუცილებლად დაუკავშირდით ბანკს ოფიციალურ ტელეფონის ნომერზე და სთხოვეთ სიტუაციაში გარკვევა.
დაიმახსოვრეთ, რომ ფიშინგური/ თაღლითური შეტევების წარმატება დიდწილად დამოკიდებულია მომხმარებელთა გაუთვითცნობიერებლობასა და უყურადღებობაზე!
ინტერნეტ თაღლითობის თავიდან აცილების მიზნით ინტერნეტით „შოპინგის“ მოყვარულებმა უმჯობესია არ გამოიყენოთ თქვენი ძირითადი ბარათი, რომელზეც ხელფასი გერიცხებათ, ან რომელზეც დიდი ოდენობის თანხა გაქვთ განთავსებული; სხვადასხვა ნივთისა და მომსახურების ონლაინ-სივრცეში შესაძენად სასურველია, იქონიოთ ცალკე ანგარიში და ბარათი, სადაც თანხის ზუსტად იმ ოდენობას შეინახავთ, რაც ინტერნეტ-შესყიდვის შესასრულებლად არის საჭირო.
ამასთან, უსაფრთხოების დამატებითი, თუმცა არასრულყოფილი მექანიზმია ინტერნეტ ტრანზაქციების დაცულ ვებგვერდებზე განხორციელება, სადაც ვებგვერდის მისამართი იწყება https://-ით ან shttp:// და არა http://-ით. ვებგვერდის დაცულობაზე ასევე მიუთითებს ჩაკეტილი მწვანე ბოქლომის სიმბოლო, რომელიც ვებგვერდის მისამართის ველში ჩანს და რომელზე დაჭერითაც შეგიძლიათ ვებგვერდის სანდოობისა და უსაფრთხოების დამადასტურებელი სერტიფიკატის ნახვა.

დამატებით, სასურველია, ინტერნეტ გადახდა განხორციელდეს ისეთი ვებგვერდიდან, რომელსაც 3D უსაფრთხოების ტექნოლოგია აქვს, ხოლო თქვენს ბარათზე გააქტიურებული იყოს 3D დაცვის მექანიზმი.

ამასთან, თქვენს მობაილ და ინტერნეტბანკში შესასვლელად უმჯობესია, გამოიყენოთ რთული პაროლი და გააქტიუროთ ორდონიანი ავტორიზაციის ფუნქცია, რომელიც გულისხმობს პაროლის მითითებასთან ერთად დამატებითი უსაფრთხოების საშუალებების გამოყენებას, როგორიცაა სისტემაში შესვლის დამადასტურებელი ერთჯერადი კოდის SMS-ით, ელ-ფოსტით ან სპეციალური მოწყობილობით - თოქენით (ე.წ. „დიჯიპასით“, რომელიც აგენერირებს ერთჯერადი სარგებლობის კოდს) მიღებასა და სისტემაში შეყვანას.
ორდონიანი ავტორიზაციის გამოყენება მიზანშეწონილია ინტერნეტბანკით ან მობაილბანკით ტრანზაქციების განხორციელების დროსაც, რა შემთხვევაშიც, თითოეული ტრანზაქციის

განსახორციელებლად SMS-ით, ელ-ფოსტით ან თოქენით მიიღებთ უნიკალურ კოდს. რაც ეხება პაროლს, სასურველია, რომ ის არანაკლებ რვა სიმბოლოსგან შედგებოდეს და შეიცავდეს როგორც დიდ, ისე პატარა ასოებს, ციფრებსა და სხვა სიმბოლოებს (მაგ. წერტილს, დეფისს, ძახილის ნიშანს).
ბარათის რეკვიზიტები, ინტერნეტბანკის მომხმარებლის სახელი და პაროლი არ შეინახოთ კომპიუტერში, მობილურში და სხვა ელექტრონულ მოწყობილობებში.
საჯარო WiFi-ით (უსადენო ინტერნეტით) სარგებლობისას, არ ისარგებლოთ ინტერნეტბანკით და სისტემაში არ შეიყვანოთ ბარათის მონაცემები. თქვენი ელექტრონული მოწყობილობების - მათ შორის, სმარტფონების, პლანშეტების და ლეპტოპების - ჰაკერული შეტევებისგან დასაცავად, გირჩევთ დროულად განაახლოთ პროგრამული უზრუნველყოფა და დარწმუნდეთ, რომ ანტივირუსული პროგრამების უახლეს ვერსიებს იყენებთ.
დაბოლოს, იმისთვის, რომ დაადგინოთ ამა თუ იმ ვებსაიტის ნამდვილობა და წარმომავლობა, შეგიძლიათ WHOIS მომსახურება (პროტოკოლი) გამოიყენოთ, რომელსაც არაერთი ვებგვერდი გვთავაზობს. ამისათვის, საკმარისია მიუთითოთ საეჭვო ვებმისამართის (დომენის) დასახელება, WHOIS კი საჯარო მონაცემთა ბაზებში მოიძიებს და მოგაწვდით აღნიშნული ვებმისამართის შესახებ ისეთ ინფორმაციას, როგორიცაა მისი რეგისტრაციისა და მოქმედების ვადა, დომენის ამჟამინდელი მფლობელი და სხვა.

ეს კი დაგეხმარებათ ვებგვერდის ნამდვილობის დადგენაში. მაგალითად, თუ იცით, რომ თქვენთვის ნაცნობი კომპანიის ვებგვერდი დიდი ხანია არსებობს, საეჭვო ვებგვერდის რეგისტრაციის თარიღი კი შედარებით ახალია - სავარაუდოდ, თაღლითობასთან გაქვთ საქმე.

თაღლითობა საბანკო საგადახდო ბარათის, ბანკომატისა და პოს-ტერმინალის გამოყენებით

თუ არ გამოიჩენთ ყურადღებას, თაღლითებმა თქვენი საგადახდო ბარათის მონაცემები შესაძლოა, მაშინაც მიითვისონ, როდესაც ბანკომატით ან პოს-ტერმინალით სარგებლობთ.
ბანკომატით სარგებლობისას გამოიჩინეთ სიფრთხილე: არ დაუშვათ, რომ სხვა ადამიანი თქვენთან ზედმეტად ახლოს იდგეს და ხედავდეს, თუ რა კოდს კრეფთ; დაფარეთ ბანკომატის კლავიატურა, როდესაც მას იყენებთ, კარგად დაათვალიერეთ ბანკომატი და დარწმუნდით, რომ ბანკომატზე ან მის მიმდებარე ტერიტორიაზე არ არის დაყენებული ისეთი კამერა ან მოწყობილობა, რომელიც ბანკს არ ეკუთვნის და რომელმაც შესაძლოა თქვენი ბარათის მონაცემები

დააფიქსიროს. დაბოლოს, მიაქციეთ ყურადღება, რომ ბარათი და ფული, ბანკომატში არ დაგრჩეთ.

მომხმარებლები საკუთარ ბარათს, ხშირად, უყურადღებოდ ტოვებენ, რაც ხელსაყრელია თაღლითებისთვის. არ დატოვოთ ბარათი და ფინანსური დოკუმენტები მაგიდაზე სამსახურში ან უნივერსიტეტში, მანქანაში ან საზოგადოებრივი თავშეყრის ადგილებში, სადაც მასზე ხელი სხვა ადამიანს მიუწვდება. არ დააწეროთ პინ-კოდი თქვენს ბარათს და ბარათი და ფურცელზე ამოწერილი პინ-კოდი საფულეში ერთად არ განათავსოთ. ამასთან, როგორც უკვე ვისაუბრეთ, არ გაგზავნოთ ბარათის მონაცემები - ნომერი, მოქმედების ვადა, უსაფრთხოების კოდი - ტელეფონით ან ელ. ფოსტის საშუალებით და არ გაუზიაროთ ეს მონაცემები თქვენს მეგობრებსა და ოჯახის წევრებსაც კი. მნიშვნელოვანია, ვისაუბროთ სკიმინგზეც, რომელიც ფინანსური თაღლითობის ერთ-ერთი საყურადღებო ფორმაა. სკიმინგის დროს, ბანკომატზე ან პოს ტერმინალზე სპეციალური მოწყობილობა - სკიმერი მონტაჟდება, რომელიც მიზნად ისახავს ბარათის მონაცემების (პინ-კოდი, ბარათის ნომერი, მოქმედების ვადა, უსაფრთხოების კოდი) მოპარვას, რომლებსაც თაღლითი თანხის მისათვისებელად იყენებს. სკიმინგისგან თავის დაცვის მიზნით, ბანკომატის გამოყენებისას - განსაკუთრებით, საზღვარგარეთ მოგზაურობისას - დარწმუნდით, რომ ის განათებულ ადგილასაა განთავსებული (ღამის საათებში კი უმჯობესია, თუ დაცულ გარემოში (მაგ. ბანკის თვითმომსახურების 24-საათიან სერვის ცენტრებში) არსებულ ბანკომატებს გამოიყენებთ), არ ემჩნევა დაზიანებები და რომ უშუალოდ ბანკომატზე არ არის დამონტაჟებული საეჭვო მოწყობილობები. მაგალითად, თუ ბანკომატის კლავიატურაზე, რომლის მეშვეობითაც მომხმარებელს შეჰყავს საკუთარი ბარათის პინ-კოდი, გადაკრულია რაიმე მოწყობილობა ან რეზინის/ პლასტმასის გამჭვირვალე გარსი, არ განათავსოთ საგადახდო ბარათი ბანკომატში და არ აკრიფოთ პინ-კოდი მოცემულ ბანკომატზე. ამასთან, ბანკომატის გამოყენებამდე დარწმუნდით, რომ მის ეკრანზე ბანკის ოფიციალური წარწერა არის განთავსებული.
თუ არ ხართ დარწმუნებული, რომ ბანკომატის გამოყენება უსაფრთხოა, მაშინ აჯობებს, თავი შეიკავოთ მისი გამოყენებისგან, პრობლემის არსებობის შესახებ კი დაუყოვნებლივ აცნობოთ ბანკს.
პოს–ტერმინალით სარგებლობის დროსაც უნდა დაიცვათ უსაფრთხოების ზომები: დარწმუნდით, რომ მას არ ემჩნევა დაზიანებები. ამასთან, მოითხოვეთ ტრანზაქცია თქვენი თანდასწრებით ჩატარდეს და არასდროს გაატანოთ ბარათი მომსახურე პერსონალს (მათ შორის ბენზინგასამართ სადგურებზე, რესტორნებსა და სხვა ადგილებში), რამდენადაც ამ დროს ჩნდება რისკი, რომ თქვენი ბარათის მონაცემები მოიპარონ. გაითვალისწინეთ, რომ მონაცემების მოპარვა არა მხოლოდ სპეციალური მოწყობილობებით, არამედ ძალიან მარტივად, ფოტოს

გადაღებით ან მონაცემების გადაწერითაც კი შეიძლება მოხდეს. ამიტომ, არ დაუშვათ, რომ ბარათმა თქვენი მხედველობის არეალი დატოვოს.

ფინანსური თაღლითობისგან თავის დაცვის მიზნით, კარგი იდეაა ბანკის SMS-მომსახურებით სარგებლობა, რაც საშუალებას მოგცემთ, მომენტალურად მიიღოთ ინფორმაცია თქვენი ბარათით განხორციელებული ოპერაციების შესახებ მობილურ ტელეფონზე. ამასთან, ბარათით განხორციელებული ოპერაციების გაკონტროლების კარგი საშუალებაა საბანკო ამონაწერის რეგულარული შემოწმება. ამ გზით, მარტივად შეამჩნევთ იმ საეჭვო ტრანზაქციებს, რომლებიც, შესაძლოა, თქვენ არ შეგისრულებიათ. საგადახდო ბარათის დაკარგვის ან მოპარვის შემთხვევაში, დაუყოვნებლივ დაუკავშირდით იმ საფინანსო ორგანიზაციას, რომელმაც გადმოგცათ ბარათი და მოითხოვეთ ბარათის დაბლოკვა. ხშირ შემთხვევაში, ბარათის დაბლოკვა ინტერნეტ და მობაილ ბანკითაც შეგიძლიათ. თუ ბარათს არ დაბლოკავთ, თაღლითებმა, რომლებმაც მოიპარეს ან იპოვეს თქვენი ბარათი, შესაძლოა მყისიერად განახორციელონ თაღლითური ოპერაციები.

თაღლითობა გაყალბებული ფულის გამოყენებით

თაღლითობის განხორციელება გაყალბებული ფულის საშუალებითაც არის შესაძლებელი. ამგვარი თაღლითური სქემის მსხვერპლი კი ნებისმიერი ჩვენგანი შეიძლება აღმოჩნდეს. გამოიჩინეთ ყურადღება ნაღდი ფულის მიღებისას, დააკვირდით თქვენთვის გადმოცემულ ბანკნოტს და შეამოწმეთ ის დამცავი ნიშნები, რომლებიც ნამდვილ ფულს ყალბი ფულისგან განასხვავებს. გაყალბებული ბანკნოტის აღმოჩენის შემთხვევაში აუცილებლად უნდა მიმართოთ თქვენს მომსახურე ან საქართველოს ეროვნულ ბანკს და სამართალდამცავ ორგანოებს.

ფინანსური პირამიდები

თანამედროვე სამყაროში ფინანსური თაღლითობის ერთ-ერთი გავრცელებული ფორმა ე.წ. ფინანსური პირამიდაა, რომლის შესახებაც ინფორმაციის ფლობა დაგეხმარებათ თავი დაიცვათ საეჭვო გარიგებებში უნებლიედ ჩართვისგან. ფინანსური პირამიდა საქმიანობის ისეთი ფორმაა, რომლის ფარგლებშიც მოსახლეობისგან ხდება თანხების მოზიდვა და სანაცვლოდ, როგორც წესი, ბაზარზე არსებულ საპროცენტო განაკვეთებთან შედარებით გაცილებით მაღალი სარგებლის შეთავაზება.

ფინანსური პირამიდა, უმეტესწილად, არ ახორციელებს მომგებიან ინვესტიციას და მომხმარებლისთვის დაპირებული სარგებლის გადახდის ერთადერთი წყარო ახალი და/ან არსებული წევრებისგან დამატებითი სახსრების მოზიდვაა.
მიუხედავად იმისა, თუ რამდენად წარმატებული ჩანს ასეთი კომპანია დროის რომელიმე მომენტში, სქემის ფუნქციონირებისთვის აუცილებელია ახალი წევრების და/ან დამატებითი თანხის მოზიდვა. შესაბამისად, როდესაც შეუძლებელი გახდება ახალი წევრების და/ან დამატებითი თანხის მოზიდვა, კომპანია ვეღარ გაისტუმრებს წევრების მიმართ არსებულ ვალდებულებებს და ფინანსური პირამიდა აუცილებლად დაიშლება, მისი წევრები კი დაკარგავენ დაბანდებულ ფულს.
ფინანსური პირამიდისა და მისი ამომცნობი ნიშნების შესახებ დამატებითი ინფორმაცია შეგიძლიათ მიიღოთ საქართველოს ეროვნული ბანკის მიერ მომზადებულ მასალებში:

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

ყურადღება გამოიჩინეთ თქვენი დანაზოგის რომელიმე ორგანიზაციისთვის მინდობისას - მოიძიეთ ინფორმაცია ამ ორგანიზაციის საქმიანობის და ფინანსური მდგომარეობის შესახებ, და დარწმუნდით, რომ საქმე არ გაქვთ თაღლითურ სქემებთან.
დაიმახსოვრეთ, რომ სხვა თანაბარ პირობებში, მაღალ დაპირებულ სარგებელს მაღალი რისკიც უკავშირდება. დაბოლოს, არავინაა დაზღვეული ფინანსური თაღლითობისგან. შესაბამისად, წინდახედულობა და სიფრთხილე, ასევე, საკუთარი უფლებებისა და პასუხისმგებლობებისა და ფინანსური თაღლითობის ყველაზე გავრცელებული ფორმების ცოდნა დაგეხმარებათ თავი დაიცვათ თაღლითური სქემებისგან და დროულად მოახდინოთ რეაგირება თაღლითობის ფაქტის დადგომის შემთხვევაში.

გისურვებთ ფინანსურ უსაფრთხოებას!