1ა.

ბანკომატთან დაკავშირებული თაღლითობა **სკიმინგის** გზით ხორციელდება. ამ დროს თაღლითი ბანკომატზე ამონტაჟებს სპეციალურ მოწყობილობას - **სკიმერს.** როდესაც თანხა ბანკომატიდან გამოგაქვს, თაღლითს შეუძლია, სკიმერის საშუალებით მოიპაროს შენი ბარათის მონაცემები: ბარათის ნომერი, მოქმედების ვადა, უსაფრთხოების კოდი, პინ-კოდი. ამ მონაცემებს კი თაღლითი შენი თანხის მისათვისებლად გამოიყენებს, მაგალითად, ინტერნეტით შესყიდვებისთვის.

1ბ.

შენ შეგიძლია თავი დაიცვა **სკიმინგისგან.** ამისთვის კი, ბანკომატის გამოყენებისას, სიფრთხილე უნდა გამოიჩინო: დააკვირდი ბანკომატს, ხომ არ ემჩნევა დაზიანებები? ხომ არ არის გადაკრული ბანკომატის კლავიატურაზე რაიმე მოწყობილობა? ხომ არ არის ჩამონტაჟებული ბარათის წამკითხველში თაღლითური მოწყობილობა? ასეთ დროს ბარათის წამკითხველი ხშირად გამოწეულია, მოძრაობს, მყარად არ არის დამაგრებული. ზოგჯერ ბანკომატზე ან მის მიმდებარე ტერიტორიაზე შეიძლება დამონტაჟებული იყოს კამერა, რომელიც ბანკს არ ეკუთვნის და რომელსაც ბარათის მონაცემების დაფიქსირება შეუძლია. თუ არ ხარ დარწმუნებული, რომ ბანკომატის გამოყენება უსაფრთხოა, მაშინ არ გამოიყენო ის! პრობლემის არსებობის შესახებ კი ბანკს უნდა აცნობო.

2ა.

ფიშინგი ინტერნეტთაღლითობაა, რომელიც მომხმარებელს მოტყუებით უბიძგებს, შეიყვანოს საკუთარი პერსონალური მონაცემები ყალბ ვებგვერდზე.

2ბ.

ფიშინგის დროს ელექტრონული ფოსტით, ან სოციალური ქსელით მოდის წერილი, რომელიც ნამდვილი ორგანიზაციისგან გამოგზავნილს ჰგავს. თაღლითები მოტყუებით ცდილობენ, გადაგიყვანონ წერილში მოცემულ ბმულზე, რომელიც ყალბ ვებგვერდზე გადადის. თაღლითის მიერ შექმნილი ვებგვერდი ვიზუალურად ძალიან ჰგავს ნამდვილი ორგანიზაციის ვებგვერდს (მაგალითად, ინტერნეტბანკის ან გადახდის გვერდს), თუმცა მასზე შეყვანილი ნებისმიერი ინფორმაცია (მაგალითად, ბარათისა და ინტერნეტბანკის მონაცემები) თაღლითის ხელში ხვდება. ეს კი მათ საშუალებას აძლევს, შენი თანხა მიითვისონ.

2გ.

ფიშინგისგან თავის დასაცავად, სიფრთხილე უნდა გამოიჩინო უცნობ და მოულოდნელ ელექტრონულ წერილებთან, თუნდაც ის ერთი შეხედვით, სანდო წყაროსგან იყოს. არ გადახვიდე ელექტრონულ წერილში მოცემულ ვებგვერდზე და არ შეიყვანო პერსონალური მონაცემები, როგორიცაა, მაგალითად, ბარათის მონაცემები, ინტერნეტბანკის სახელი და პაროლი.

2დ.

ზოგჯერ შეიძლება სოციალურ ქსელში შეგხვდეს რეკლამა, რომელიც რაიმეს მოგებას გპირდება, თუ კი შენი ინტერნეტბანკის, ან ბარათის მონაცემებს შეიყვან. არასდროს შეიყვანო ასეთ ვებგვერდებზე შენი პერსონალური ინფორმაცია, რათა არ გახდე **ფიშინგის** მსხვერპლი! ყოველთვის გადაამოწმე ინფორმაცია იმ ბანკთან, რომლის სახელითაც ვრცელდება რეკლამა, ან რომლის სახელითაც მიიღე წერილი.

3ა.

ბოლო წლებში გავრცელდა ე.წ. „ფორექს“ (FOREX) კომპანიები, რომლებიც მომხმარებლებს სთავაზობენ, საკუთარი დანაზოგი დააბანდონ მაღალრისკიან **ინვესტიციებში**, ელექტრონული პლატფორმის საშუალებით. აღსანიშნავია, რომ „ფორექს“ პლატფორმაზე საშუამავლო საქმიანობა ეროვნული ბანკის ზედამხედველობის ქვეშ მოექცა და მისი განხორციელების უფლება მხოლოდ ლიცენზირებულ საბროკერო კომპანიებს აქვთ.

3ბ.

ამის მიუხედავად, ბაზარზე მაინც გვხვდება არალიცენზირებული კომპანიები, რომლებიც მომხმარებლებს სთავაზობენ დააბანდონ დანაზოგი ე.წ. ფორექს პლატფორმაზე, ან ივაჭრონ უცხოური ვალუტით, რაც **ინვესტირებული** თანხის სრულად დაკარგვის მაღალ რისკებს უკავშირდება. ასეთი კომპანიები, მომხმარებლების შეცდომაში შეყვანის მიზნით, დასახელებაში ხშირად იყენებენ ისეთ ტერმინებს, როგორიცაა „საბროკერო“, „საინვესტიციო“ და ა.შ., თუმცა ეს არ ნიშნავს, რომ ასეთ კომპანიებს ლიცენზია აქვთ გავლილი ეროვნულ ბანკში.

3გ.

მომხმარებლების მოსაზიდად, ასეთი კომპანიები ხშირად მათ ბონუსებს, უფასო სწავლებას და გარანტირებულად დიდ მოგებას ჰპირდებიან. იმავდროულად ისინი სავაჭროდ იყენებენ გაურკვეველი/არასანდო წარმომავლობის პლატფორმებს, სადაც ხშირად არაკეთილსინდისიერი გზით ხდება კლიენტების სავაჭრო გარიგებებში ხელოვნურად ჩარევა და მათ მიერ **„ინვესტირებული“** თანხის წაგება. ეს წაგებული თანხა კი ფსევდო „ბროკერის“ შემოსავლად რჩება.

კომპანია, რომლებიც გთავაზობს უამრავ ბონუსს, დიდ მოგებას და გპირდება, რომ ორკვირიანი სწავლების შემდეგ საუკეთესო „ტრეიდერი“ (ანუ, ფასიანი ქაღალდებით მოვაჭრე) გახდები, დიდი ალბათობით, არაკეთილსინდისიერად და დანაშაულებრივად მოქმედებს!

3დ.

მანამ, სანამ FOREX-ში **ინვესტირებას** გადაწყვეტ, აუცილებლად მოიძიე ინფორმაცია იმ კომპანიის შესახებ, ვისაც უნდა ანდო შენი თანხა. პირველ რიგში, დარწმუნდი, რომ კომპანიას გააჩნია ეროვნული ბანკის ლიცენზია. აუცილებლად გაეცანი მის ბიზნეს მოდელს (ანუ როგორ ფუნქციონირებს კომპანია, რა პროდუქტს ქმნის, ვინ არის მომხმარებელი, საიდან იღებს მოგებას და ა.შ). ლიცენზირებული საბროკერო კომპანია ვალდებულია, გაგიმჟღავნოს, თუ რა ბიზნეს მოდელს იყენებს. ასევე, მან უნდა გაჩვენოს, თუ სად განხორციელდა თქვენ მიერ დადებული გარიგება. სრულიად წაიკითხე რისკების შესახებ გაფრთხილება, მოიძიე ინფორმაცია იმ ფინანსური ინსტრუმენტების შესახებ, რომლითაც უნდა ივაჭრო და მხოლოდ ყოველივე ამის შემდეგ გადაწყვიტე, გიღირს თუ არა ფულის დაბანდება ამ საქმიანობაში.

3ე.

გაითვალისწინე, რომ ლიცენზირებული FOREX კომპანიის შემთხვევაშიც არსებობს იმის მაღალი შანსი, რომ **ინვესტირებული** თანხა მთლიანად დაკარგო. ლიცენზირებულ კომპანიაში ფულის დაბანდება ამცირებს თაღლითობის რისკს, თუმცა ვერანაირად ვერ დაგიცავს ბაზარზე ფასების მოულოდნელი ცვლილებებისგან, რა შემთხვევაშიც, ფასების შემცირების გამო შესაძლებელია, დაკარგო თანხა. FOREX-ზე არსებული ფინანსური ინსტრუმენტებით ვაჭრობა მაღალრისკიანია და მოითხოვს სპეციფიურ ცოდნასა და მრავალწლიან გამოცდილებას!

1ა.

ბარათზე მნიშვნელოვანი ინფორმაციაა დატანილი: ბარათის ნომერი, მოქმედების ვადა, უკანა მხარეს კი უსაფრთხოების კოდი. ამ მონაცემების მოპოვებით, თაღლითს ბარათის ფიზიკურად მოპარვის გარეშეც შეუძლია შენს ბარათზე არსებული თანხის მითვისება. მაგალითად, ინტერნეტით რაიმეს ყიდვა შენი თანხით.

1ბ.

ბარათის მონაცემების მოპარვა კი შესაძლებელია ბარათისთვის სურათის გადაღებით, ბარათის მონაცემების ჩაწერით ან მარტივად, მონაცემების დამახსოვრებით. ეს მაშინ შეიძლება მოხდეს, თუ ბარათს კარგად არ ინახავ და ნებისმიერს შეუძლია მისი აღება. ასევე მაშინ, როცა, მაგალითად, მაღაზიაში ან კვების ობიექტში საფასურს ბარათით იხდი. ამიტომ, ძალიან მნიშვნელოვანია ამ დროს არ გადასცე ბარათი პერსონალს, არამედ ითხოვო პოსტერმინალის მოტანა და თავად გადაიხადო.

1გ.

ბარათის მონაცემების მოპარვა ფიშინგის გზითაც არის შესაძლებელი. ფიშინგის დროს, თაღლითი ნამდვილი ორგანიზაციის ვებგვერდის ყალბ ასლს ქმნის. ასეთ ყალბ ვებგვერდზე შეყვანილი ბარათის მონაცემები კი თაღლითის ხელში ხვდება. ამიტომ აუცილებელია დარწმუნდე, რომ ვებგვერდი ნამდვილად სანდოა. დააკვირდი ვებგვერდის მისამართის ველსაც: ის უნდა იწყებოდეს https://-ით და ველში უნდა ჩანდეს მწვანე ჩაკეტილი ბოქლომის სიმბოლო.

1დ.

მიუხედავად იმისა, რომ თაღლითობის რისკი არსებობს, შენ შეგიძლია მისგან თავის დაცვა. არავის ათხოვო **ბარათი** და არავის გაანდო ბარათზე დატანილი მონაცემები, ასევე ბარათის პინ-კოდი და ბარათით გადარიცხვისას ტელეფონზე მოსული ერთჯერადი კოდი.

თუ ვერ პოულობ ბარათს, ან ეჭვი გაქვს, რომ ბარათის მონაცემები მოპარულია, აუცილებლად დაუკავშირდი ბანკს და დაბლოკე ბარათი, რადგან თაღლითი მანამ შეძლებს მოპარული ბარათით სარგებლობას, სანამ მას არ დაბლოკავ. ბარათის დაბლოკვა ხშირად ინტერნეტბანკითაც არის შესაძლებელი.

1ე.

ბარათებთან დაკავშირებულ თაღლითობასთან საბრძოლველად ერთ–ერთი პრაქტიკული იდეაა სმს–მომსახურების გააქტიურება: ამ გზით, ყოველ ჯერზე, როდესაც შენი ანგარიშიდან რაიმე ოპერაცია განხორციელდება, აუცილებლად მიიღებ ტექსტურ შეტყობინებას და უკეთ შეძლებ როგორც საკუთარი ფინანსების კონტროლს, ისე თაღლითობისგან თავის დაცვას.

2ა.

პერსონალურ მონაცემებთან დაკავშირებული თაღლითობის შემთხვევაში, თაღლითი არამხოლოდ ბარათის ან ინტერნეტბანკის მონაცემების მოპოვებას ცდილობს, არამედ, ის მოქმედებს მსხვერპლის სახელით: თუ თაღლითმა საჭირო პერსონალური ინფორმაცია მოიპოვა (მაგალითად, სახელი, გვარი, პირადი ნომერი, ინტერნეტბანკის პაროლი და სხვა), მან შეიძლება მომხმარებლის სახელით განახორციელოს საბანკო ოპერაციები, მაგალითად, აიღოს სესხი ან საკრედიტო ბარათი, გახსნას ახალი ანგარიში, გადარიცხოს და მიითვისოს თანხა.

2ბ.

მომხმარებლის **პერსონალური ინფორმაცია** თაღლითებმა შეიძლება მოიპოვონ როგორც ფიზიკურად, მაგალითად, ჩვეულებრივი ფოსტიდან პერსონალური მონაცემების შემცველი წერილების მოპარვით, ან სანაგვე ურნაში გადაყრილი საბანკო ინფორმაციის შემცველი დოკუმენტებიდან; ასევე ონლაინ - ფიშინგისა თუ ჯაშუშური პროგრამების გამოყენებით. თაღლითებისთვის პერსონალური მონაცემების შეგროვების ერთ -ერთი საშუალება ასევე სოციალური ქსელია, სადაც მომხმარებლები ყოველდღიურად აზიარებენ პირად ინფორმაციას.

2გ.

თაღლითობისგან თავის დასაცავად ყოველთვის გაუფრთხილდი **პერსონალურ მონაცემებს!** არ გააზიარო შენი პირადი ნომერი, ბარათის მონაცემები და სხვადასხვა ანგარიშის პაროლები (მაგ., ინტერნეტბანკის, ფეისბუქის, ელ.ფოსტის და ა.შ.); არავის ათხოვო შენი საბანკო საგადახდო ბარათი და პირადობის დამადასტურებელი მოწმობა; მოერიდე საეჭვო ვებგვერდებზე ბარათის მონაცემების შეყვანას. ამასთან, მნიშვნელოვანია, აკონტროლო შენს ანგარიშზე თანხების მოძრაობა.

3ა.

ე.წ. **„ფინანსური პირამიდა“** ერთ–ერთი გავრცელებული თაღლითური სქემაა, რომლის ფარგლებშიც, ორგანიზაცია იზიდავს თანხას მომხმარებლებისგან და სანაცვლოდ მათ მაღალ სარგებელს (საპროცენტო განაკვეთს) ჰპირდება. ხშირად ის სარგებელი, რომელსაც ფინანსური პირამიდა გვთავაზობს, გაცილებით უფრო მაღალია, ვიდრე საპროცენტო განაკვეთები, რომლებიც ბაზარზეა გავრცელებული (მაგ., რომლებსაც ბანკები გვთავაზობენ).

3ბ.

ფინანსური პირამიდა რეალურ ბიზნესს არ აწარმოებს. ერთადერთი გზა იმისთვის, რომ პირამიდამ მიიღოს შემოსავალი და შესაბამისად, საკუთარ წევრებს გადაუხადოს დაპირებული სარგებელი, არის ახალი ან უკვე არსებული წევრებისაგან დამატებითი თანხის მოზიდვა. სწორედ ახალი და/ან არსებული წევრებისგან მოზიდულ თანხებს ანაწილებს ფინანსური პირამიდა ძველ მონაწილეებზე. ამიტომ, ადრე თუ გვიან, როდესაც ახალი წევრების და შესაბამისად, ახალი თანხების მოძიება შეუძლებელი ხდება, ფინანსური პირამიდა აუცილებლად იშლება, ხოლო მისი მონაწილეები ზარალდებიან.

3გ.

ხშირად, **ფინანსური პირამიდის** შემთხვევაში, სარგებლის მისაღებად შეიძლება, შემოგთავაზონ რაიმე ნივთის ან მომსახურების, მაგალითად, აქსესუარის, კოსმეტიკური საშუალებების, ტურისტული საგზურების და ა.შ., ყიდვა ან გაყიდვა. თუმცა, მათი ფასი საბაზროზე გაცილებით მაღალია. ამგვარი სქემის მიზანია, წევრმა დამატებით გაყიდოს აღნიშნული ნივთი ან მომსახურება და ამ გზით სხვებიც "გააწევრიანოს" სქემაში.

3დ.

სანამ რომელიმე კომპანიაში დააბანდებდეთ ფულს, კარგად გაეცანით ამ ბიზნესის საქმიანობას. ასევე, დასვით კითხვები და მოიძიეთ ინფორმაცია შემდეგ საკითხებზე: ვინ დაიცავს თქვენს უფლებებს, თუ ფულს ამ კომპანიას მიანდობთ? რომელიმე სახელმწიფო ორგანიზაცია ზედამხედველობს ამ კომპანიის საქმიანობას? რა გსმენიათ ამ კომპანიის შესახებ ახალ ამბებში? ხომ არ გთხოვთ ეს კომპანია სხვა წევრების მიყვანას იმის სანაცვლოდ, რომ მიიღოთ თქვენი სარგებელი? ხომ არ გთხოვთ ეს კომპანია რაიმე ნივთის ან მომსახურების არაგონივრულად მაღალ ფასში შეძენას?

დაიმახსოვრეთ, რომ მცირე დროში გამორჩეულად მაღალი საპროცენტო სარგებლის მიღების დაპირება კარგი მანიშანებელია იმისა, რომ სარისკო, შესაძლოა, არაკეთილსინდისიერ ბიზნესთანაც კი გქონდეთ საქმე!