**ფინანსური თაღლითობა და ფინანსური უსაფრთხოება**

**გაკვეთილის მიზნები:**

* მოსწავლეები ეცნობიან ფინანსური თაღლითობის გავრცელებულ სქემებს (ფიშინგი, ფინანსური პირამიდა, მავნე პროგრამები, კერძო გარიგებებთან დაკავშირებული თაღლითობები და სხვ.) და მათ ამომცნობ ნიშნებს;
* მოსწავლეები ეცნობიან ფინანსური თაღლითობის თავიდან არიდების გზებსა და ფინანსური უსაფრთხოების ზომებს;

**სასურველი შედეგები:**

* მოსწავლეებს შეუძლიათ თაღლითობის შემთხვევების ამოცნობა და მისგან თავის დაცვა;
* მოსწავლეები აცნობიერებენ, რომ პერსონალური და ფინანსური ინფორმაციის მოფრთხილება დაეხმარებათ თავი დაიცვან კიბერთაღლითობისგან;
* მოსწავლეები აცნობიერებენ, რომ მაღალი სარგებელი დაკავშირებულია მაღალ რისკთან;

**ძირითადი ცნებები:**

ფიშინგი, მავნე პროგრამა, ფინანსური პირამიდა, ავთენტიფიკაცია, პერსონალური ინფორმაცია

**რა გზებით ცდილობენ თაღლითები ჩვენი თანხის მითვისებას?**

თაღლითები ჩვენი თანხების მისათვისებლად სოციალურ ინჟინერიას იყენებენ, ანუ დარწმუნებისა და მანიპულირების ხელოვნებას. ისინი სანდო ორგანიზაციებად წარმოაჩენენ თავს და დამაჯერებელ ისტორიებს თხზავენ, რამაც შეიძლება ადამიანს ინტერნეტში რისკიანი ქმედებისკენ უბიძგოს. მაგალითად, დააჭიროს ყალბ ბმულებს, გაუგზავნოს ფული უცნობ ადამიანს, გაამჟღავნოს თავისი პერსონალური ინფორმაცია და ა.შ.

ტექნოლოგიების განვითარებასთან ერთად თაღლითობის მეთოდებიც იცვლება, ამიტომ მნიშვნელოვანია, არ მოვადუნოთ ყურადღება და ვიყოთ მუდამ სკეპტიკური. განსაკუთრებით მაშინ, როცა საქმე მარტივად ფულის შოვნას და მომგებიან დაპირებებს ეხება. რადგან ხშირად, რაც არარეალურად კარგად ჟღერს, მართლაც არარეალური აღმოჩნდება ხოლმე.

თაღლითები ჩვენი თანხის მითვისებას, პირველ რიგში, ჩვენი პერსონალური და ფინანსური მონაცემების მოპარვით ცდილობენ. პერსონალური მონაცემი არის ნებისმიერი სახის ინფორმაცია, რომლითაც შეიძლება პირის იდენტიფიცირება. მაგალითად, სახელი, გვარი, პირადი ნომერი, ტელეფონის ნომერი და ა.შ. ფინანსურ, სენსიტიურ ინფორმაციას კი შეიძლება მივაკუთვნოთ საბანკო ბარათის მფლობელის სახელი და გვარი, ბარათის ნომერი, უსაფრთხოების კოდი, ტელეფონის ნომერზე მოსული ერთჯერადი კოდი, რომლითაც გადახდას ვადასტურებთ, ინტერნეტბანკის მომხმარებლის სახელი და პაროლი და ა.შ. რაში იყენებს თაღლითი მოპარულ მონაცემებს? სენსიტიური ინფორმაციის ცოდნა თაღლითს თქვენს ბარათზე და ინტერნეტბანკზე წვდომის საშუალებას აძლევს, ანუ მას თავისუფლად შეუძლია თქვენი საბანკო ანგარიშიდან თანხის განკარგვა.

გარდა პერსონალური მონაცემების ქურდობისა, თაღლითები ჩვენი თანხის მითვისებას ფინანსურ პირამიდებში ჩვენი გაწევრიანებით ცდილობენ. ანუ გვთავაზობენ ჩვენი ფული ერთი შეხედვით ძალიან მომგებიან საქმეში დავაბანდოთ, მაგრამ ასეთი სქემები, ადრე თუ გვიან, ყოველთვის იშლება და მისი მონაწილეები ვეღარ ახერხებენ არათუ მოგების, არამედ დაბანდებული თანხის უკან დაბრუნებასაც.

**როგორ ამოვიცნოთ ფინანსური თაღლითობა?**

მოდი, ცალ-ცალკე განვიხილოთ თაღლითობის რამდენიმე ფორმა და როგორ შეიძლება, ჩვენ მომხმარებლებმა, ამოვიცნოთ თაღლითობის ნიშნები?

***ფიშინგი***

ფიშინგის დროს თაღლითი ცდილობს მოტყუებით გადაგიყვანოთ ბმულზე, რომელზეც ყალბი ვებგვერდია და თქვენი პერსონალური ინფორმაციის შეყვანა მოითხოვება. ყალბი ვებგვერდი ვიზუალურად ძ ამა თუ იმ ორგანიზაციის ვებგვერდს, ან რომელიმე ბანკის ინტერნეტბანკს და მომხმარებელი ფიქრობს, რომ თავისი პერსონალური ინფორმაცია ნამდვილ ვებგვერდზე შეჰყავს. ყალბ გვერდზე შეყვანილი ნებისმიერი ინფორმაცია კი თაღლითთან ხვდება და მას თქვენს ანგარიშზე წვდომის საშუალებას მისცემს.

იმისთვის, რომ მომხმარებელი ყალბ ვებგვერდზე გადაიყვანონ, თაღლითები მისთვის ცნობილი კომპანიის, ან ხშირად ბანკის სახელით აგზავნიან ელექტრონულ წერილს, შეტყობინებას ტელეფონით ან სოციალური ქსელით, შეიძლება სოციალურ ქსელში განათავსონ პოსტი ან რეკლამა, ან სულაც ტელეფონით დაუკავშირდნენ მომხმარებელს. ტექსტი კი რამე სასწრაფო ქმედების განხორციელებისკენ, თანხის მიღებისკენ, ან რამეს მოგებისკენ, გათამაშებაში მონაწილეობისკენ მოუწოდებს, მაგალითად:

„თქვენი ინტერნეტბანკი დაიბლოკა, იმისთვის, რომ შეუფერხებლად ისარგებლოთ საბანკო სერვისებით, გთხოვთ, სასწრაფოდ გადახვიდეთ წერილში მოცემულ ბმულზე და შეხვიდეთ თქვენს ინტერნეტბანკში“.

„თქვენ გაქვთ ფულადი გზავნილი, თქვენს ანგარიშზე ჩაირიცხა თანხა - თანხის მისაღებად გადადით ბმულზე და შეიყვანეთ ბარათის/ინტერნეტბანკის მონაცემები“.

„მიიღეთ მონაწილეობა გათამაშებაში და მოიგეთ პრიზები - გადადით ბმულზე და შეიყვანეთ თქვენი ინფორმაცია“.

„თქვენ მოიგეთ უფასო მეგაბაიტები, გასააქტიურებლად გადადით ბმულზე და შეიყვანეთ თქვენი ბარათის მონაცემები“.

„თქვენი გასაყიდი ნივთის საფასური გადახდილია, თანხის მისაღებად, გთხოვთ, გადახვიდეთ ბმულზე და შეავსოთ ფორმა“

ეს ტექსტები შეიძლება დროთა განმავლობაში შეიცვალოს, თუმცა სქემა ერთნაირია - მსგავსი მაცდური შემოთავაზებებით, ან სასწრაფოდ გასაკეთებელი ქმედებებით თაღლითი გიბიძგებთ თავის მიერ გამოგზავნილ ბმულზე გადახვიდეთ, სადაც უკვე თქვენი პერსონალური და სენსიტიური ინფორმაციის შეყვანა მოითხოვება.

***როგორ ამოვიცნოთ ფიშინგი?***

* **დააკვირდით შეტყობინების გამომგზავნს ან შეთავაზების ავტორს**

ფიშინგ შეტყობინების ავტორის, ელექტრონული ფოსტის, ან სოციალურ ქსელში გვერდის დასახელება მიმსგავსებულია რეალური ორგანიზაციისას, მაგრამ თუ კარგად დააკვირდებით, აღმოაჩენთ, რომ რამდენიმე სიმბოლო განსხვავებულია დასახელებაში ან გვერდის მისამართში.

* **დააკვირდით შეტყობინების შინაარსს**

ფიშინგ შეტყობინებაში, ან შეთავაზებაში მოცემულია ბმული, მიმაგრებული ფაილი, ან შესავსები ფორმა, სადაც თქვენი საბანკო მონაცემების შეყვანა მოითხოვება. შეტყობინება გიბიძგებთ სასწრაფო ქმედების განხორციელებისკენ, რამეს მოგებისკენ და ა.შ. ასეთი შეტყობინებები ხშირად შეიცავს გრამატიკულ ან ორთოგრაფიულ შეცდომებს, ტექსტი გაუმართავია, ან სულაც, ავტომატურად ნათარგმნს ჰგავს.

* **დააკვირდით წერილში მოცემულ ბმულს/ვებგვერდის მისამართს**

წერილში მოცემულ ბმულზე მაუსის გადატარებით და არა დაწკაპუნებით, გამოჩნდება ვებგვერდის რეალური მისამართი. დააკვირდით, ის ძალიან მიმსგავსებულია და რამდენიმე სიმბოლოთი განსხვავდება ნამდვილი ვებგვერდის მისამართისგან. ამასთან, დაცული ვებგვერდის მისამართი უნდა იწყებოდეს https://-ით და მისამართის ველში ჩანდეს ბოქლომის სიმბოლო.

***მავნე პროგრამები***

თქვენი ფინანსური ინფორმაცია შეიძლება თაღლითმა მავნე პროგრამებითაც მოიპოვოს, ამიტომ დაიცავით თქვენი მოწყობილობების - კომპიუტერის, ლეპტოპის, სმარტფონის უსაფრთხოება. მავნე პროგრამის მიზანი, კომპიუტერული მოწყობილობისთვის ზიანის მიყენება ან ინფორმაციის მოპარვაა, ამ ინფორმაციაში კი თავისუფლად შეიძლება, თქვენი ბარათის, ან ინტერნეტბანკის მონაცემებიც მოხვდეს.

***რა გზით შეიძლება აღმოჩნდეს მავნე პროგრამა თქვენს მოწყობილობაში?***

* **ფიშინგის შედეგად** - მაგალითად, ყალბი ვებგვერდიდან ან ელექტრონული წერილიდან მიმაგრებული ფაილის ჩამოტვირთვით.
* **ინფორმაციის მატარებელი მოწყობილობებიდან** - მაგალითად, მეხსიერების ბარათი, USB, სადაც ბოროტმოქმედები სხვადასხვა მავნე პროგრამას ტვირთავენ და მსხვერპლისთვის თვალსაჩინო ადგილას ათავსებენ.
* **მონაცემების გაცვლისა და გადმოწერის პლატფორმებიდან** - გადმოსაწერ ან გასაზიარებელ ფაილებზე შესაძლებელია თანდართული იყოს სხვადასხვა მავნე კოდი.
* **არალიცენზირებული**, **ე.წ. „დაკრეკილი“ პროგრამული უზრუნველყოფის ჩამოტვირთვით.**

***გარიგებებთან დაკავშირებული თაღლითობები***

ხშირად, თაღლითობა მაშინაც შეიძლება მოხდეს, როდესაც კერძო პირებთან ვაწარმოებთ გარიგებებს ინტერნეტით, მაგალითად, ვყიდულობთ ან ვყიდით ნივთს, ვსესხულობთ თანხას და ა.შ.

თუ მომხმარებელს ინტერნეტში განთავსებული აქვს გასაყიდი ნივთი, თაღლითებმა შესაძლოა თავი პოტენციურ მყიდველებად გაასაღონ და ნივთის მფლობელის პერსონალური მონაცემების მოპარვა სცადონ. მაგალითად, შესთავაზონ, რომ ნივთის ფოსტით გაგზავნის ხარჯებს თავად გადაიხდიან და საფოსტო მომსახურების, ან გადახდის ფორმა გამოაგზავნონ შესავსებად, სადაც, თითქოსდა თანხის ჩარიცხვის მიზნით, ბარათის მონაცემების შეყვანა მოითხოვება. სინამდვილეში კი, თქვენს ანგარიშზე თანხის ჩასარიცხად საჭიროა ანგარიშის ნომერი, და არა თქვენს ბარათზე დატანილი ინფორმაცია. ბარათის მონაცემების გამჟღავნებით, პირიქით, თქვენი ანგარიშიდან თანხის ჩამოჭრის საშუალებას მისცემთ თაღლითს.

ინტერნეტით ასევე შეიძლება შეგხვდეთ ორგანიზაციის, ან კერძო პირის შეთავაზება თანხის მარტივად გასესხების შესახებ, თანაც მომხმარებლის გადახდისუნარიანობისა და საკრედიტო ისტორიის შემოწმების გარეშე. ეს ნიშნავს, რომ გამსესხებლისთვის არ არის მნიშვნელოვანი, რამდენად შეძლებს მსესხებელი აღებული თანხის უკან დაბრუნებას, ან რამდენად დროულად ფარავდა ის წარსულში აღებულ სესხებს. ასეთი შემოთავაზებების უკან, დიდი შანსია, თაღლითობა იდგეს და ვითომ სესხის გამცემმა, სესხის ჩარიცხვამდე წინასწარ საკომისიოს გადარიცხვა მოითხოვოს მომხმარებლისგან. საბოლოოდ, კი, მიღებული საკომისიოს თანხა მიითვისოს და არავითარი სესხი არ გასცეს. ასევე, შესაძლოა, თითქოსდა სესხის ჩარიცხვის მიზნით, მომხმარებელს ბარათის მონაცემების გაგზავნა სთხოვოს, რაც უკვე იცით, რომ თაღლითს ბარათზე წვდომისა და თანხის მითვისების საშუალებას აძლევს.

***როგორ ამოვიცნოთ გარიგებებთან დაკავშირებული თაღლითობები?***

* ნივთის გაყიდვის შემთხვევაში მყიდველი თავად გიგზავნით გადახდის, ან საფოსტო მომსახურების შესავსებ ფორმას;
* მყიდველი თავად გთავაზობთ თანხის გადახდის მეთოდს და არ თანხმდება თქვენ მიერ შეთავაზებულს, მაგალითად, თანხის ჩარიცხვას საბანკო ანგარიშის ნომერზე;
* მყიდველი თქვენგან ითხოვს ბარათის ინფორმაციის გამჟღავნებას.
* სესხის გაცემის შემთხვევაში ორგანიზაცია არ ინტერესდება თქვენი საკრედიტო ისტორიითა და გადახდისუნარიანობით;
* ორგანიზაცია არ არის საქართველოს ეროვნული ბანკის ზედამხედველობის ქვეშ;
* ორგანიზაცია ითხოვს საკომისიოს წინასწარ გადარიცხვას.

***ფინანსური პირამიდა***

როგორც დასაწყისში ვახსენე, თაღლითები ჩვენი თანხის მითვისებას ფინანსურ პირამიდებში ჩვენი გაწევრიანებითაც ცდილობენ. ამ სქემის მთავარი ხიბლი, ფულის მარტივად და სწრაფად შოვნის დაპირებაა. ამ დროს თაღლითები მომხმარებელს სთავაზობენ თანხის დაბანდებას, მაგალითად, რამე საქმეში, აქტივში და ა.შ. და სანაცვლოდ, გარკვეულ სარგებელს პირდებიან. ეს სქემები, შეიძლება სხვადასხვანაირად იყოს შეფუთული, მაგალითად, კომპანია სთავაზობდეს მომხმარებელს თავისი დანაზოგის შენახვას და სანაცვლოდ, მაღალი საპროცენტო სარგებლის დარიცხვას, რაც მნიშვნელოვნად აღემატება ბაზარზე არსებულ საპროცენტო განაკვეთებს. შეიძლება კომპანიამ მომხმარებელს გარკვეული პროდუქტის, ან მომსახურების ყიდვა შესთავაზოს, მაგალითად, სხვადასხვა აქსესუარი, ტურისტული საგზური, კოსმეტიკური საშუალება და ა.შ, თუმცა მათი ფასი, საბაზროსთან შედარებით მაღალია და ამ დროს, ასევე მოითხოვება სხვა ადამიანების გაწევრიანებაც ამ პროდუქტების მათზე გაყიდვის გზით. ბოლო ხანებში ასევე გავრცელდა ვირტუალური აქტივების ყიდვის შეთავაზებაც, სადაც თანხის მისაღებად, მომხმარებლისგან მარტივი ქმედებები, მაგალითად, სპორტული აქტივობა, ან ვიდეოს ყურება და ა.შ. მოითხოვება.

მიუხედავად იმისა, რომ ასეთი სქემები სხვადასხვანაირად არის შეფუთული და ერთი შეხედვით, მომგებიან ბიზნეს საქმიანობას ჰგავს, არსი ერთია: არ ჩანს კომპანიის ბიზნესმოდელი, ანუ ბუნდოვანია, რეალურად რაში აბანდებთ თქვენს თანხას და როგორ უნდა მოიტანოს ამან მოგება. ასეთი კომპანიები არ ახორციელებენ რეალურ ინვესტიციას და მომხმარებლის შემოსავალი მხოლოდ ამ სქემაში სხვა ადამიანების გაწევრიანებაზეა დამოკიდებული - ანუ კომპანია დაპირებულ სარგებელს ან მოგებას ბიზნესსაქმიანობიდან კი არ გიხდით, არამედ თანხის გადახდის ერთადერთი წყარო ახალი ან არსებული წევრებისგან დამატებითი თანხების მოზიდვაა. ასეთი სქემები კი, ადრე თუ გვიან, ყოველთვის იშლება: მაშინ როდესაც ახალი წევრების მოძიება და მაშასადამე, მათგან თანხების მიღება შეუძლებელი ხდება და არსებული წევრები ვეღარ იღებენ შემოსავალს.

***როგორ ამოვიცნოთ ფინანსური პირამიდა?***

* კომპანია ფულის შოვნას მარტივად გპირდებათ;
* კომპანია ბაზარზე არსებულთან შედარებით გაცილებით მაღალ საპროცენტო სარგებელს ან შემოსავალს გპირდებათ;
* კომპანია შემოსავლის მისაღებად გთხოვთ ახალი წევრების მიყვანას ან გარკვეული პროდუქციის საბაზროსთან შედარებით მაღალ ფასად შეძენას, ან ახალი წევრების შესვლა თქვენგან დამოუკიდებლადაა საჭირო;
* კომპანიის მიერ მოზიდული თანხების დაბანდების მექანიზმები ბუნდოვანია, ან არ არსებობს კომპანიის მიერ ეკონომიკური საქმიანობის წარმოების ნიშნები;
* კომპანია როგორც წესი, აწარმოებს მასშტაბურ სარეკლამო კამპანიებს, მათ შორის სოციალურ ქსელითა და ცნობილი ადამიანების მონაწილეობით

**როგორ დავიცვათ თავი ფინანსური თაღლითობისგან?**

მნიშვნელოვანია, ყოველთვის ყურადღებით მოვეკიდოთ ნებისმიერ შემოთავაზებას და გვახსოვდეს, რომ რაც უფრო მაღალია დაპირებული სარგებელი, მით მაღალია ფინანსურ შემოთავაზებასთან დაკავშირებული რისკიც.

ჩვენი პერსონალური და ფინანსური მონაცემების გაფრთხილება, ჩვენი ანგარიშების, ელექტრონული ფოსტისა თუ კომპიუტერული მოწყობილობების დაცვა კი ფინანსური უსაფრთხოების შენარჩუნებაში დაგვეხმარება.

დასასრულს, რამდენიმე რჩევას გაგიზიარებთ, რაც დაგეხმარებათ თავი დაიცვათ ფინანსური თაღლითობისგან:

* გამოიჩინეთ სიფრთხილე ყველა მიღებულ უცნობ ან მოულოდნელ შეტყობინებასთან, თუნდაც სანდო წყაროდან მიღებულს ჰგავდეს.
* არ დაუჯეროთ შემოთავაზებებს, რომლებიც რაიმეს მოგებას გპირდებათ და ამისთვის, ბმულზე გადასვლას და ფინანსური ინფორმაციის გამჟღავნებას ითხოვს.
* არასდროს გადახვიდეთ ინტერნეტბანკში შეტყობინებაში მოცემული ბმულიდან - დაიმახსოვრეთ თქვენი ინტერნეტბანკის მისამართი და ყოველთვის თქვენით აკრიფეთ ის ინტერნეტბრაუზერის მისამართის ველში.
* არ გახსნათ და ჩამოტვირთოთ უცნობი გამომგზავნისგან მიღებულ წერილში მიმაგრებული ფაილი.
* არავის გაუზიაროთ ინტერნეტბანკის მომხმარებლის სახელი და პაროლი, ტელეფონით მიღებული ერთჯერადი კოდი, ბარათის ნომერი, მოქმედების ვადა და უსაფრთხოების კოდი - არც პირადად, არც სატელეფონო ზარით, ელექტრონული ფოსტითა თუ სოციალური ქსელით.
* გადაამოწმეთ ინფორმაცია იმ ორგანიზაციასთან, ვისგანაც მიიღეთ შეტყობინება, ან ვისი სახელითაც ვრცელდება შეთავაზება ოფიციალურ საკონტაქტო ნომერზე.
* გამოიყენეთ რთული პაროლები, რომლებიც შედგება მინიმუმ 10-12 სიმბოლოსგან, რომელიც მოიცავს დიდ და პატარა ასოებს, რიცხვებსა და სიმბოლოებს. სხვადასხვა ანგარიშისთვის, გქონდეთ სხვადასხვა პაროლი. სადაც შესაძლებელია, გაააქტიურეთ 2 ფაქტორიანი ავთენტიფიკაცია, ანუ პაროლის გარდა, გამოიყენეთ იდენტიფიკაციის მეორე საფეხური, მაგალითად, ერთჯერადი კოდი, ან ბიომეტრიული მონაცემებით იდენტიფიკაცია.
* ისარგებლეთ ლიცენზირებული პროგრამული უზრუნველყოფებით კომპიუტერსა თუ სმარტფორნში, პერიოდულად განაახლეთ პროგრამული უზრუნველყოფა. აპლიკაციები ჩამოტვირთეთ მხოლოდ ოფიციალური მაღაზიებიდან და დაყენებისას დააკვირდით, რა წვდომებს ითხოვს თქვენს სმარტფონში.
* დანაზოგის განთავსების ან თანხის სესხების შემთხვევაში, გადაამოწმეთ, რამდენად არის ორგანიზაცია ეროვნული ბანკის ზედამხედველობის ქვეშ.
* გამოიჩინეთ სიფრთხილე თანხის დაბანდებისას, სანამ რომელიმე ორგანიზაციაში დააბანდებდეთ თქვენს სახსრებს, მოიძიეთ ინფორმაცია ამ კომპანიის საქმიანობის შესახებ და დარწმუნდით, რომ საქმე არ გაქვთ თაღლითურ სქემასთან. ყოველთვის მოითხოვეთ ხელშეკრულება, კარგად გაეცანით და დარწმუნდით, რომ პირობები თქვენთვის მისაღებია.
* დაფიქრდით, როდესაც საეჭვოდ მაღალ სარგებელს გთავაზობენ, რადგან როგორც ვთქვით, სხვა თანაბარ პირობებში, მაღალ სარგებელს, მაღალი რისკიც უკავშირდება და თუ რამე არარეალურად კარგად გვეჩვენება, დიდი ალბათობით, მართლაც არარეალური აღმოჩნდება ხოლმე.