ფინანსური უსაფრთხოების გაძლიერება: საბანკო ანგარიშზე არასანქცირებული ჭვდომის პრევენციული მეთოდებისა და საერთაშორისო პრაქტიკების მიმოხილვა

| ანა მიქაძე

2024

ფინანსური უსაფრთხოების გაძლიერება: საბანკო ანგარიშზე არასანქცირებული წვდომის პრევენციული მეთოდების და საერთაშორისო პრაქტიკების მიმოხილვა

აბსტრაქტი

ეპოქაში, სადაც დომინირებს ციფრული ინოვაციები, უმთავრესი გახდა ფინანსური უსაფრთხოების ზომების გაძლიერება არაავტორიზებული წვდომისგან პრევენციებისთვის. კვლევა ანალიზს უკეთებს ციფრული ბანკინგის რთულ ლანდშაფტს, განიხილავს განვითარებად ტექნოლოგიურ მიღწევებს და მათ ადაპტაციას ფინანსურ სისტემებში. ძირითადი აქცენტი კეთდება არასანქცირებული წვდომის აღკვეთის ღონისძიებების ეფექტურობაზე, კიბერკრიმინალების მიერ გამოყენებული მეთოდების იდენტიფიცირებასა და ორმხრივი ეფექტის მნიშვნელობის აღქმადობაზე, რაც გამოიხატება ფინანსური ორგანიზაციებისა და მომხმარებლების დაზარალების თანაბარი შესაძლებლობით. გლობალურ კონტექსტში, მარეგულირებელი ჩარჩოებისა და კიბერუსაფრთხოების სტრატეგიების საერთაშორისო გამოკვლევა ასახავს ფინანსური სისტემების მიერ შემუშავებული დამცველობით სისტემებისა და პრაქტიკების ეფექტურობის. გარდა ამისა, კვლევა ეხმაურება საერთაშორისო ორგანიზაციების რეპორტების, ყოველწლიური ანგარიშების შედეგებს და ტრენდების მზარდ კოეფიციენტებს, რაც ხაზს უსვას და გამოკვეთს კიბერკრიმინალური აქტივობების, კერძოდ არაავტორიზებული წვდომისა და სახსრების გადარიცხვის, პრობლემის ემპირიულობას საბანკო სექტორის კიბერუსაფრთხოების მედეგობაში. ამ კვლევის მიგნებები ხელს უწყობს ციფრულ ბანკში არაავტორიზებული წვდომის გამოწვევების უფრო ღრმა გაგებას და იძლევა რეკომენდაციებს კიბერუსაფრთხოების მდგრადობის გასაძლიერებლად. კიბერ-რისკების რთული ლანდშაფტის ნავიგაციით, კვლევა მიზნად ისახავს მარეგულირებელი ორგანოების, ფინანსური ინსტიტუტებისა და კიბერუსაფრთხოების ექსპერტების დასკვნების შედეგების ანალიზით ერთობლივი პრაქტიკის ტენდენციურობის გამოაშკარავებას, რაც საერთაშორისო დონეზე წარმოსახავს ერთგვარ სტანდარტიზებულ მიდგომას ფინანსური სექტორის კიბერუსაფრთხოების გაძლიერების და განვითარებისთვის.

სარჩევი

შესავალი

ონლაინ ფინანსური სერვისების თანამედროვე სტრუქტურული სისტემის მრავალფეროვნება, რომელიც მიუხედავად იმისა, რომ ხელს უწყობს ფინანსური რესურსების მართვას და მომხმარებელს უქმის კომფორტულ ფინანსურ გარემოს, ზრდის მათ წინააღმდეგ მიმართული კიბერთავდასხმების რისკს. 2020-დან 2022-მდე Vmware-ის რეპორტები[1] ასახავს ფინანსური ინსტიტუტების მიერ დაფიქსირებული კიბერ საფრთხეების ზრდის ტენდენციას, რომლის თანახმადაც სექტორში ყოველწლიურად კიბერშეტევების საერთო რაოდენობის ორნიშნა პროცენტული ზრდა შეიმჩნევა. საბანკო სექტორში არსებული გამოწვევის ერთ-ერთი მიზეზი ფიზიკური პირების საბანკო ანგარიშების დაუცველობაა, რის შედეგადაც კრიმინალები მარტივად ახერხებენ საბანკო ბარათებზე არასანქცირებული ონლაინ წვდომის შედეგად მათი ფულადი სახსრების და აქტივების გადარიცხვას.

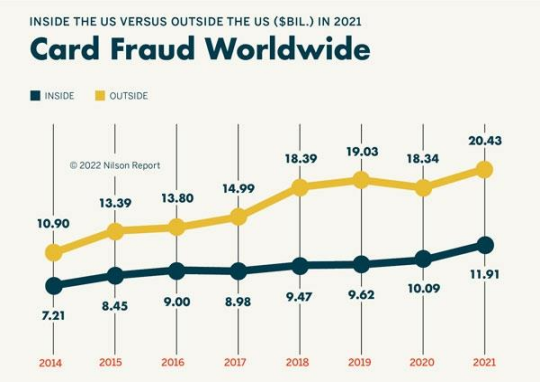
მსგავსი კიბერკრიმინალური ქმედების პოპულარიზება და ტენდენციურობა ფინანსური სექტორის მიერ კლიენტებისთვის შეთავაზებული პერსონალიზებული სერვისების გაციფრულებასთანაა დაკავშირებული. ფულადი ტრანზაქციები, რომლის განსახორციელებლად ბანკში მისვლა იყო საჭირო, ახლა გადის კიბერსივრცის უზარმაზარ ქსელში, რაც მსოფლიოს ფინანსურ სისტემებს უფრო ხელმისაწვდომს და ეფექტურს ხდის, ვიდრე ოდესმე ყოფილა. თუმცა სწორედ აქ ჩნდება მთავარი გამოწვევა და საფრთხე, რომელიც კიბერკრიმინალების მიერ მომხმარებელთა საბანკო პლასტიკური ბარათების რეკვიზიტების მოპარვითა და შემდგომში მათი პირადი მიზნებისთვის გამოყენებიდან გამომდინარეობს.

---

[1] კელერმანი, ტ., არფი, რ. (2020). *Modern Bank Heists 3.0: 25 CISOs from leading financial institutions reveal their thoughts on the 2020 attack landscape*, VMware Carbon Black.
Modern Bank Heists 3.0

კელერმანი, ტ., მაკელროი, რ. (2021). *Modern Bank Heists 4.0,* VMware Carbon Black.
Modern Bank Heists 4.0

კელერმანი, ტ. (2020). *Modern Bank Heists 5.0,* VMware Carbon Black.
Modern Bank Heists 5.0



ფიგურა 1: Nilson Report: Card Fraud Worldwide

Nilson Report[2]-ის მიხედვით, სავარაუდოა, რომ მსოფლიო მასშტაბით საკრედიტო ბარათების თაღლითობის შედეგად მიღებულმა ჯამურმა ზარალმა 43 მილიარდ დოლარს[3] გადააჭარბოს მომდევნო რამდენიმე წლის განმავლობაში. ეს მაჩვენებელი 2011 წლიდან 2021 წლამდე 9,84 მილიარდი დოლარიდან 32,4 მილიარდ დოლარამდე გაიზარდა, რაც მკაფიოდ წარმოაჩენს გაციფრულების შედეგების ნაკლოვანებას - ახალი გლობალური კიბერ რისკების წარმოშობასა და კიბერკრიმინალების ფინანსური სექტორით მეტად დაინტერესებას. თუმცა აუცილებელია აღინიშნოს, რომ ფინანსური საფრთხე არა მხოლოდ მომხმარებლებს, არამედ ფინანსურ ინსტიტუციებზეც ზემოქმედებს და ქმნის კლიენტების მხრიდან ერთგვარ უნდობლობის პრობლემას, რომელიც თავის მხრივ რეპუტაციას ულახავს საბანკო სექტორს.

შესაბამისად, ფინანსური სერვისების სწრაფმა დიგიტალიზაციამ, მოხერხებულობისა და ხელმისაწვდომობის გაზრდისას, უნებურად წარმოქმნა კიბერკრიმინალებისთვის მომხმარებელთა სენსიტიური ინფორმაციის უკანონოდ მოპარვის ახალი გზები, რასაც ხელს უწყობს ის ფაქტიც, რომ საზოგადოების ცნობიერება ამ სფეროში მწირია.

პრობლემის გადაჭრის აუცილებლობასა და აქტუალობას ხაზს უსვამს კიბერკრიმინალთა მუდმივად განვითარებადი სტრატეგიები, მეთოდები და უნარი გამოიყენონ ონლაინ საბანკო სისტემის უსაფრთხოების ხარვეზები, რაც პოტენციურად და გრძელვადიანი თვალსაწიერით გამოუსწორებელ ზიანს აყენებს მომხმარებლის ეკონომიკურ კეთილდღეობას და ეჭვის ქვეშ აგდებს საბანკო სექტორის ფუნქციონირებისთვის საჭირო ქვაკუთხედს - ნდობას.

კვლევა ცდილობს ნათელი მოჰფინოს თანამედროვე საბანკო სექტორში კიბერკრიმინალების მხრიდან მომხმარებლების სამიზნედ ამოღების შედეგად მათი საბარათე ანგარიშების რეკვიზიტების მოპარვის პრობლემას, რაც იწვევს არაავტორიზირებულ წვდომას

[2] შენიშვნა: ყველაზე სანდო გამოცემა, რომელიც აშუქებს ბარათების და მობილური გადახდის ინდისტრიის შესახებ ინფოს და ჟურნალებს, კვლევებს.

[3] Nilson Report. (2022). The Nilson Report.

და ფულადი სახსრებით ქურდობის ინციდენტების სიმრავლეს. კონკრეტულად, მიმოვიხილავთ კიბერდანაშაულებრივი ქსელის უკან მდგომ პირებს, მათ მოტივებსა და მეთოდებს, თუ როგორ ახერხებენ ისინი ისეთი ფსიქოლოგიური თუ ტექნიკური სქემების გამოყენებას მომხმარებელთა საბანკო მონაცემების მოსაპარავად და შემდგომში მსხვერპლთა პირადი ინტერნეტ ბანკინგის სივრცეში არაკანონიერი ტრანზაქციების განსახორციელებლად.

ბანკებისა და ფინანსური ინსტიტუტების კიბერუსაფრთხოების კონტექსტში აუცილებლობას წარმოადგენს ჰოლისტიკური მიდგომა, რაც გულისხმობს არა მხოლოდ ციფრული უსაფრთხოების ტექნიკური ასპექტების, ასევე ადამიანური ფაქტორების გათვალისწინებას, როგორიცაა მომხმარებლის ქცევა, ნდობა და ინფორმირებულობა. შესაბამისად, ბანკთა და ფინანსურ ინსტიტუტთა კიბერ რისკებისადმი მედეგობა შეიძლება დამოკიდებული იყოს არა მხოლოდ ციფრული სისტემების ძლიერი დაცვის პრაქტიკაზე, ასევე მისი კლიენტების ფსიქოლოგიურად ნდობასა და გულუბრყვილობისკენ მიდრეკილებაზეც. Deloitte-ის თანახმად[4], ბანკები თავიანთი ბიუჯეტის თითქმის 11%-ს ხარჯავენ კიბერუსაფრთხოების გაძლიერებაზე, შესაბამისად, კრიმინალებისთვის შედარებით მარტივი სამიზნე აღნიშნული ორიდან მომხმარებელი ხდება.

გამოყენებული მეთოდოლოგია არ გულისხმობს პირდაპირ თავდასხმებს ბანკის უსაფრთხოების ინფრასტრუქტურაზე. ნაცვლად ამისა, ის ეყრდნობა ფსიქოლოგიური გავლენისა და მანიპულაციის დახვეწილ, მაგრამ ძლიერ ინსტრუმენტებს, რომლებიც მიმართულია მომხმარებლებზე. ამ პროცესში, კიბერკრიმინალები მოქმედებენ ფინანსური ინსტიტუტისგან დამოუკიდებლად, შუამავლად იყენებენ ბანკთან უშუალო კონტაქტში მყოფ პირებს - მომხმარებლებს და განზრახ არიდებენ ბანკების უსაფრთხოების ქსელებზე აშკარა დარტყმის განხორციელებას თავს. შედეგად, რაიმე შესამჩნევი შეფერხებისა და მათი მხრიდან საეჭვო ქმედების აღმოჩენის გარეშე, დაწესებულების უსაფრთხოების გვერდის ავლით კრიმინალები ტოვებენ ნაკლებ მტკიცებულებასა და ამ გზით ამცირებენ მათი ვინაობის გამოაშკარავების რისკს. ეს ყოველივე ხაზს უსვამს კიბერდანაშაულის განვითარებად ბუნებას, სადაც თავდამსხმელები სულ უფრო მეტად ეყრდნობიან დახვეწილ და ფსიქოლოგიურ მიდგომებს, რათა გაარღვიონ ყველაზე უსაფრთხო ფინანსური სისტემებიც კი.

[4] Deloitte. (2021). Reshaping the cybersecurity landscape.
https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/risk/Cybersecurity.pdf

გარდა ამისა, კვლევა ჩაუღრმავდება მოწინავე საერთაშორისო საფინანსო სექტორის ორგანიზაციების პრევენციულ მეთოდოლოგიებს არაავტორიზებული ონლაინ წვდომისა და ფულადი ტრანზაქციების წინააღმდეგ, მათ პროაქტიულ ნავიგაციასა და რეგულაციებს კიბერკრიმინალის ციფრულ სისტემებში შემცირებასთან დაკავშირებით. შედარებითი ანალიზით და პრევენციული მეთოდების შესწავლით შესაძლებელი გახდება საუკეთესო პრაქტიკების იდენტიფიცირება, საქართველოს ფინანსური ლანდშაფტისთვის შედარება და მსგავსებებისა და განსხვავებების წარმოჩენა. ამ გზით ნათელი გახდება ბანკების და სხვა ფინანსური ორგანიზაციების როლი ბოლო წლებში პოპულარული კიბერკრიმინალური დანაშაულებრივი ქმედებების წინააღმდეგ ბრძოლაში, რაც საფინანსო სექტორს, მომხმარებელთა ციფრული მედეგობისა და მათი გაძლიერებული ავთენტიფიკაციის წინსვლას შეუწყობს ხელს.

ტექნოლოგიური განვითარება და მათი ადაპტირება ციფრულ საბანკო სისტემაში : შეთავაზებების ეფექტურობა კლიენტებისთვის

საბანკო სექტორი ერთ-ერთი პირველია, რომელმაც სტრუქტურულად დაიწყო ტექნოლოგიების ადაპტირება მომსახურების სფეროში, რამაც რევოლუციური ზეგავლენა მოახდინა არა მხოლოდ ფინანსური ბაზრის, არამედ სრულიად ახალი სექტორის ფინანსური ტექნოლოგიების, იგივე ფინტექის განვითარებაზე. ჯერ კიდევ მე-19 საუკუნის შუა ხანებში ბანკებმა დაიწყეს ტელეგრაფისა და საკომუნიკაციო ტექნოლოგიების ადაპტირება[5], რამაც გაუმჯობესა ფინანსურ ცენტრებს შორის ინფორმაციის სწრაფი გადაცემის დახმარებით ტრანზაქციების სიჩქარე. ბოლო ათწლეულების განმავლობაში გაზრდილმა მოთხოვნამ კი ციფრულ საბანკო სერვისებსა და პროდუქტებზე წარმოშო ბანკებისთვის იმპერატივი მორგებოდნენ ცვალებად გარემოსა და ტექნოლოგიური ინოვაციების დანერგვით შეექმნათ

[5] The Payments Association. (2020, 12 ოქტომბერი). Fintech: The History and Future of Financial Technology.
https://thepaymentsassociation.org/article/fintech-the-history-and-future-of-financial-technology/

ეფექტური, ხელმისაწვდომი და პერსონალიზებული სერვისის სისტემა, რომელიც მომხმარებელს საშუალებას მისცემდა განეხორციელებინათ სხვადასხვა ფინანსური ტრანზაქციები დისტანციურად, მოხერხებულად და უსაფრთხოდ. რა თქმა უნდა, ეს ასევე შედიოდა ბანკების, როგორც კომერციული ორგანიზაციების, პრეფერენციაშიც. ინდუსტრიული რევოლუციების განმავლობაში საფინანსო სექტორი ნელ-ნელა ტექნოლოგიების ადაპტირებით ახდენს ეფექტურ პოზიციონირებას ხარჯების შემცირების, ტრანზაქციების მოცულობის გაზრდის, ბაზრის სეგმენტის გაფართოებისა და საოპერაციო პროცესების ეფექტიანად მართვის მიმართულებით[6]. McKinsey-ის ანგარიშის მიხედვით[7], ფინანსური ინდუსტრია, რომელიც ამჟამად აკონტროლებს დაახლოებით 370 ტრილიონი აშშ დოლარის აქტივებს მთელ მსოფლიოში, მომდევნო ათწლეულის განმავლობაში $500 ტრილიონ-დან 550 ტრილიონ აშშ დოლარამდე გაიზრდება. დიგიტალიზაციის ტრანსფორმაციული გავლენა საბანკო ინდუსტრიაზე აშკარად ჩანს ციფრული ბანკებისა და ტრადიციული ბანკების განსხვავებულ ტრაექტორიებში, განსაკუთრებით წმინდა საპროცენტო შემოსავლის (NII) ზრდის კუთხით. ციფრული ბანკების უპირატესობა მდგომარეობს სტრატეგიულად ტექნოლოგიებზე ორიენტირებასა და გამარტივებულ ოპერაციულ მოდელში, რაც ხარჯების მინიმიზაციას ახდენს. ამაზე ასევე მიუთითებს ავტომატიზაციისა და ხელოვნური ინტელექტის მიერ ადამიანური რესურსის ჩანაცვლების ტენდენციურობა. McKinsey-ის მიერ სტატიაში გამოთქმული მოლოდინით რამდენიმე წელში ბანკის ფუნქციების 25%-ს[8] მანქანები შეასრულებენ, რაც საკმაოდ დაწევს საოპერაციო ხარჯებს. დიგიტალიზაციის კონკურენტული უპირატესობაა მომხმარებლებისთვის მუდმივი ციფრული სერვისების შეთავაზებაც, რაც ასევე გავლენას ახდენს მომხმარებელთა სეგმენტის გაფართოებისაზეც. statista-ს ანგარიშის მიხედვით, რომელიც მიმოიხილავს საბანკო სექტორის ტენდენციასა და უახლეს მაჩვენებლებს, შესაძლებელია ტექნოლოგიური ტრანსფორმაციის მომგებიანობის იდენტიფიცირება. საიტის მიერ მოწოდებული ინფორმაციით, ტრადიციული

[6] Chu, Y., Ye, S., Li, H., Strauss, J., & Zhao, C. (2023). Can digitalization foster sustainable financial inclusion? Opportunities for both banks and vulnerable groups. Sustainability, 15(8), 6727.

[7] ც ი მ ე რ ი , ბ ., დ ი ე ც , მ . (2022,20 დ ე კ ე მ ბ ე რ ი). *The future of banks: A $20 trillion breakup opportunity.* McKinseyhttps://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-banks-a-20-trillion-dollar-breakup-opportunity

[8] ც ი მ ე რ ი , ბ ., დ ი ე ც , მ . (2022,20 დ ე კ ე მ ბ ე რ ი). *The future of banks: A $20 trillion breakup opportunity.* McKinseyhttps://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-banks-a-20-trillion-dollar-breakup-opportunity

საბანკო სექტორის წმინდა საპროცენტო შემოსავალი 2023-დან 2028 წლამდე 2.95%-ით[9], ხოლო ციფრული საბანკო სექტორის 13.39%-ით[10] გაზრდაა მოსალოდნელი, რაც მეტ წილად ასოცირდება დიგიტალიზაციის დადებით გავლენაზე.

საბანკო სექტორში ტექნოლოგიური განვითარება უკავშირდება თითქმის ორას წლიან ისტორიასა და ტექნოლოგიურ რევოლუციებს, შესაბამისად მისი ადაპტირება სხვადასხვა ფაქტორიდან გამომდინარე განსხვავებულად პროცესი და მსოფლიოს მასშტაბით. საბანკო სექტორის მოდერნიზაცია გარკვეულ ქვეყნებში, როგორიცაა საქართველო, ხშირად განპირობებული იყო ტექნოლოგიური ინფრასტრუქტურის სწრაფი გაუმჯობესებით. თუმცა ტექნოლოგიური პროგრესი საბანკო პრაქტიკის დანერგვისა და ფუნდამენტური ცოდნის ერთდროულ განვითარებას უსწრებდა, რაც თავის მხრივ დამატებით პრობლემებს უქმნიდა მომხმარებელთა უსაფრთხოებას და სისტემის მედეგობას. აღსანიშნავია, ისიც რომ განვითარებად ქვეყნებში კიბერუსაფრთხოების საკითხი საბანკო სექტორში უფრო მკაფიო და პრობლემატურ გამოწვევად მიიჩნეოდა მომხმარებელთა ფინანსური განათლებისა და ინფორმირებულობის ნაკლებობის გამო. ქსელური კიბერუსაფრთხოების ინდექსი (NCSI), რომელიც ზომავს ქვეყნების ეროვნული კიბერუსაფრთხოების სიმწიფის დონეს და ეფუძნება 30 ინდიკატორს, საშუალებას იძლევა კონკრეტული დასკვნები გამოვიტანოთ განვითარებად და განვითარებულ ქვეყნებთან მიმართებით. NCSI 2023[11] წლის ინდექსის მიხედვით, კიბერუსაფრთხოების სიმწიფის თვალსაზრისით საუკეთესო ხუთეულია: ესტონეთი, ფინეთი, დანია, შვედეთი, ნორვეგია. ყველა ეს სახელმწიფო განვითარებულ ქვეყანას წარმოადგენს, როდესაც კიბერუსაფრთხოების სიმწიფის თვალსაზრისით ბოლო ხუთეული ქვეყანაა: იემენი, სომალი, ერიტრეა, ლიბია, ავღანეთი განვითარებადია.

ტრანსფორმაციული პროცესი, რომელიც ხასიათდებოდა ტექნოლოგიური მიღწევების ასიმილაციის შეფერხებით მათ განხორციელებასთან მიმართებაში, ხაზს უსვამდა გამოწვევებს საბანკო სექტორში ფინანსური ტექნოლოგიების სრული პოტენციალის გამოყენების კუთხით. უფრო უკეთესად რომ გავშალოთ ფინანსური ტექნოლოგიური პროდუქტების უპირატესობებისა და უარყოფითი გვერდითი მოვლების გავლენა დღევანდელ თანამედროვე

[9] Statista. (2023). *Banking - Traditional Banks - Worldwide.* https://www.statista.com/outlook/fmo/banking/traditional-banks/worldwide
[10] Statista. (2023). Banking - *Digital Banks - Worldwide.* https://www.statista.com/outlook/fmo/banking/digital-banks/worldwide:
[11] e-Governance Academy. (2023). *National Cyber Security Index:* https://ncsi.ega.ee/ncsi-index/

ბანკინგზე აუცილებელია გამოვყოთ ტექნოლოგიური განვითარებისა და მათი ციფრულ საბანკო სისტემაში ადაპტირების მნიშვნელოვანი ეტაპები:

- **1970-1980-იანი წლები: კომპიუტერებისა და ელექტრონული ტრანზაქციები** - მასიურად იწყება კომპიუტერების ინტეგრირება საბანკო სექტორში და შესაბამისად, იზრდება ელექტრონული ტრანზაქციების რაოდენობაც. ტექნოლოგიების პოპულარიზებამ საბანკო სექტორში კი იმ პერიოდისთვის პოტენციურად გაზარდა კიბერკრიმინალების სისტემაზე წვდომის შესაძლებლობები და რისკი. სწორედ ამიტომ ხდება საჭირო სავალუტო ტრანზაქციის ანგარიშების[12] (CTR)[13] შევსების ვალდებულებაც, რომელიც ოფიციალურად საბანკო საიდუმლოების შესახებ კანონით (BSA) 1970 წელს მარეგულირებელმა ორგანომ - ფინანსური დანაშაულის აღსრულების ქსელმა (FinCEN) შეერთებულ შტატებში, ფულის გათეთრების, ტერორიზმის დაფინანსებისა და სხვა ფინანსური დანაშაულების მონიტორინგსა და წინააღმდეგ ბრძოლისთვის აამოქმედა.
- **1990-იანი წლები: ონლაინ ბანკინგი** - ხდება ბანკების მხრიდან ინტერნეტთან ინტეგრირებული სერვისების შეთავაზება მომხმარებლებისთვის, რაც ციფრულ ტრანსფორმაციაზე მიგვანიშნებს და პირდაპირპროპორციულად კავშირშია ვირტუალურ სივრცეში საბანკო ტრანზაქციების ზრდასა და კიბერკრიმინალების ახალი ფინანსური სექტორის სისუსტეების ბოროტად გამოყენებასთან. ამ პერიოდს უკავშირდება საბანკო სერვისების პირველი ვებსაიტის შექმნა სტენფორდის საკრედიტო კავშირის (ინგ. Stanford Credit Union) მიერ 1994 წელს[14], რაც ციფრული ბანკინგის ისტორიაში მნიშვნელოვან მომენტად არის მიჩნეული.

[12] შენიშვნა: დოკუმენტი, რომლის შევსებაც ფინანსურ ინსტიტუტებსა და ბანკებს სთხოვენ ნაღდი ფულის ოპერაციების შესახებ ანგარიშგებისთვის, რომლებიც აღემატება გარკვეულ ზღვარს.

[13] Financial Crimes Enforcement Network. (2023r). Currency Transaction Reporting. https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf

[14] Forbes. (2023). *What Is Digital Banking?* https://www.forbes.com/advisor/banking/what-is-digital-banking/

- **2000-იანი წლები : მობილური ბანკინგი** - მობილური ბანკინგის გავრცელებამ ციფრული ფინანსების ახალი განზომილება შექმნა. მობილური აპლიკაციების მეშვეობით ფინანსების მართვის პოპულარიზებას თან ახლდა ახალი სახის კიბერ საფრთხეები. ამ ეტაპისას საბანკო მომსახურების პროცესიდან შესაძლებელი გახდა მომხმარებლისთვის პერსონალური ინტერფეისის შეთავაზება, რაც ზღუდავდა ბანკების გავლენას დაეცვათ კლიენტები პოტენციური კიბერკრიმინალებისგან ჩარევის გარეშე. შესაბამისად, მობილური ბანკინგის აპლიკაციები გახდა სხვადასხვა თავდასხმების სამიზნე. 2000-იანი წლების დასაწყისში გავრცელდა ფიშინგის შეტევები და იზრდება არაავტორიზებული წვდომა და ფულის ტრანსფერების ინციდენტების რაოდენობა. ამასთან დაკავშირებით საინტერესო სტატისტიკურ მონაცემებს ავრცელებს 2003 წელს დაარსებული არაკომერციული ორგანიზაცია APWG, რომელიც მუშაობს ფიშინგ შეტევებთან საბრძოლველად. ორგანიზაციის მიერ 2004 წელს გამოქვეყნებული ანგარიშები გვაძლევს ინფორმაციას ფიშინგის ყოველთვიური საშუალო 50%-იანი[15] ზრდის მაჩვენებელზე. ინციდენტების 75%[16] ფინანსურ სექტორში დაფიქსირდა, ცნობილ ფინანსურ ინსტიტუტებს შორის იყვნენ : Citibank, US Bank, Paypal და სხვა. აღსანიშნავია ის ფაქტიც, რომ წლების განმავლობაში ის ციფრი და დანაშაულის ტენდენციურობა საკმაოდ იზრდება. ჩნდება ახალი მავნე პროგრამა (ინგ. Malware) - ტროიანები, როგორიცაა: Zeus და SpyEye, რომლებიც სპეციალურად ფინანსური ინსტიტუტებში არალეგალურად შესაღწევად და არაავტორიზებული ტრანზაქციების დასაწყებად იქნა შექმნილი კიბერკრიმინალებს მიერ.
- **2010-დან დღემდე : ფინტექის ინოვაცია** - ამ პერიოდში ინოვაციებმა სრულიად გარდასახა ფინანსური სერვისების ლანდშაფტი. ბაზარზე ჩნდება: მობილური გადახდის აპლიკაციები, რობო მრჩევლები[17] ინვესტიციების მენეჯმენტისთვის,

[15] Anti-Phishing Working Group (APWG). (2004, ნოემბერი). APWG Phishing Activity Report. https://docs.apwg.org/reports/APWG_Phishing_Attack_Report-Jul2004.pdf

[16] Anti-Phishing Working Group (APWG). (2004, ივლისი). *APWG Phishing Attack Report*. https://docs.apwg.org/reports/APWG_Phishing_Attack_Report-Jul2004.pdf

[17] შენიშვნა: რობო მრჩეველი არის ალგორითმსა და პროგრამულ უზრუნველყოფაზე დაფუძნებული ფინანსური

ბლოკჩეინზე დაფუძნებული პლატფორმები, როგორიცაა კრიპტოვალუტები და ასე შემდეგ. FinTech ინოვაციის ძირითად კომპონენტებად იქცა, რამაც არა მხოლოდ შეცვალა ფიზიკური პირების ფინანსური ტრანზაქციების წარმართვა, არამედ გზა გაუხსნა ალტერნატიულ ფინანსურ სისტემებს. ბოლო წლების გამოწვევად იქცა კრიპტო თაღლითობა, რასაც მოწმობს ფედერალური სავაჭრო კომისიის (FTC) მონაცემები[18], რომლის მიხედვითაც 46 000-ზე მეტმა ადამიანმა დაკარგა 1 მილიარდ დოლარზე მეტი კრიპტო თაღლითობის შედეგად 2021 წლის იანვრიდან 2022 წლის ივნისამდე. შესაბამისად, ფინტექის განვითარებითა და ახალი პროდუქტების ფინანსურ სექტორში ასიმილაციით, არა მხოლოდ მომხმარებლებისა და ბანკებისთვის, არამედ კიბერკრიმინალებისთვისაც, იზრდება ციფრულ სამყაროში ფინანსური სისტემების გამჭვირვალობა, რაც მომხმარებელთა დიგიტალ ბანკინგის სივრცეს სრულიად ხილულისა და ადვილად შეღწევადს ხდის.

საბანკო ტექნოლოგიების სწრაფმა გამოჩენამ არა მხოლოდ საბანკო მომსახურებისადმი მოთხოვნა და სეგმენტის არეალი, არამედ კრიმინალის დონეც გაზარდა საფინანსო სექტორში. ახალი შესაძლებლობების ადაპტირებისთვის, რომელსაც ფინტექი ნელ-ნელა აცნობდა საბანკო სექტორს, აუცილებელი ხდება მარეგულირებელი ბერკეტების გამოყენება. ფაქტია, რომ ბოლო სამი ათწლეულის განმავლობაში, გლობალიზაციისა და ფინანსური სექტორის ლიბერალიზაციის ტენდენციებით, საბანკო ინდუსტრიამ მნიშვნელოვანი ზრდა განიცადა. ფინანსურმა ინსტიტუტებმა სწრაფად გააფართოვეს თავიანთი სერვისები. ონლაინ ბანკინგის დანერგვით მომხმარებლებს მოუწოდეს ჩართულიყვნენ ციფრულ ტრანზაქციებში, როგორიცაა ფულადი გადარიცხვები, ანგარიშის ინფორმაციაზე წვდომა და ყოველთვიური

პროდუქტი, რომელიც ავტომატურად მინიმალური ადამიანური ზედამხედველობის ფარგლებში უზრუნველყოფს საინვესტიციო რჩევისა და პორტფელის მართვის სერვისებს

[18] ფლეტჩერი, ე. (2022, 3 ივნისი). *Reports show scammers cashing in on crypto craze*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

ავტომატიზებული გადახდები. თუმცა, ონლაინ აქტივობების ზრდამ წინა პლანზე წამოწია კიბერუსაფრთხოების კომპონენტი, რაც საბანკო სისტემის სისუსტედ და გამოწვევად იქცა.

არაავტორიზებული წვდომისთვის კიბერკრიმინალების მიერ გამოყენებული მეთოდებისა და თაღლითობის სქემები

თანამედროვე კიბერდანაშაულებრივ სივრცეში საბანკო ანგარიშებზე არასანქცირებული წვდომის ფენომენი და თაღლითურად ფულადი სახსრების გადარიცხვები კომპლექსურ და მრავალმხრივ ხასიათს იძენს. ამას ადასტურებს ასევე ფინანსური და რისკების საკონსულტაციო ფირმა კროლი (ინგ: Kroll), რომელმაც გამოუშვა უახლესი რეპორტი[19] 2023 წლის პირველ კვარტალში ჩატარებული კვლევის შედეგების გასაშუქებლად, რაშიც მონაწილეობა 400-მა სხვადასხვა საფინანსო სექტორში მომუშავე პირმა მიიღო. შედეგებმა აჩვენა, რომ გამოკითხულთა 69% გლობალურად ელოდება ფინანსური დანაშაულის რისკის გაზრდას მომდევნო 12 თვის განმავლობაში განსაკუთრებით დღევანდელ სამყაროში, სადაც ტექნოლოგიური ინოვაციები ახალ გზებსა და საშუალებებს ქმნის ისეთი კიბერკრიმინალებისთვის, რომელთა მიზანიც სხვების კონფიდენციალურობის დარღვევასა და მათი ფინანსური ანგარიშებით ბოროტმოქმედად სარგებლობას მოიცავს.

აქტორები, რომლებიც პასუხისმგებლები არიან არაავტორიზებული წვდომისა და სახსრების თაღლითურ გადარიცხვებზე, ავლენენ სხვადასხვა მეთოდებს და საშუალებებს ისე როგორც ონლაინ, ასევე ოფლაინ სივრცეში პოტენციურ მსხვერპლთა საბანკო ბარათის რეკვიზიტების მისაღებად, რომლებიც წარმოადგენს ბარათის იდენტურობის დამადასტურებელ ინფორმაციას, ესენია: ბარათის ნომერი (PAN - ძირითადი ანგარიშის ნომერი), ბარათის მფლობელის სახელი, მოქმედების ვადა, ბარათის ვერიფიკაციის კოდი (CVV/CVC/CVV2), PIN (პერსონალური საიდენტიფიკაციო ნომერი), ონლაინ საბანკო სერტიფიკატები. მსგავსი კრიმინალური ქმედების ჩადენისას მათი ძირითადი მიზანი და

[19] Kroll. (2023). *Fraud and Financial Crime Report: Can technology stop the threat of economic, crypto, and ESG crimes.* (გვ. 7)
https://www.kroll.com/-/media/kroll-images/pdfs/2023-fraud-and-financial-crime-report.pdf

სტიმული ფინანსური მოგებაა, რისთვისაც იდენტიფიცირებულია მრავალი დივერსიფიცირებული მეთოდი.

ყველაზე გავრცელებული მეთოდი გახლავთ სოციალური ინჟინერია, რაც გულისხმობს ინდივიდების მანიპულირებას, რათა მათ გაამჟღავნონ სენსიტიური ინფორმაცია. მაგალითად, კიბერკრიმინალმა შეიძლება დაურეკოს მსხვერპლს, წარმოაჩინოს თავი, როგორც ბანკის წარმომადგენელი და დაარწმუნოს იგი, მიაწოდოს ანგარიშის დეტალები ან გადააყენოს პაროლი ყალბ ვებსაიტზე, რის შემდეგადაც თავდამსხმელებს შეუძლიათ შეიძინონ შესვლის სერტიფიკატები და დაზარალებულთა საბანკო რეკვიზიტებით სცადონ წვდომა მრავალ ონლაინ ანგარიშზე, მათ შორის საბანკო ანგარიშებზე, ავტომატური სკრიპტების მეშვეობით. ზემოთ ხსენებული მეთოდები: ხმოვანი კომუნიკაციის გამოყენება ცნობილია როგორც ვიშინგი (Vishing), ხოლო SMS ან ტექსტურ შეტყობინებებით ინფორმაციის შეგროვებას - სმიშინგი (Smishing). ასევე 2022 წლის სტატისტიკური მონაცემებით ერთ-ერთი ყველაზე და რეპორტებული კიბერშეტევის სახეს წარმოადგენს სოციალური ინჟინერიის ქვე-ტიპი ფიშინგი (phishing). ფიშინგით, ჰაკერები ცდილობენ მოიპარონ ღირებული ინფორმაცია საკუთარი თავის სანდო წყაროდ შენიღბვითა და იმიტაციით. ფიშინგის სქემები შეიძლება იყოს რამდენიმე განსხვავებული ფორმით წარმოდგენილი, მათ შორის სატელეფონო ზარები, ყალბი ვებსაიტები და გაყიდვების ელ.წერილები. მსგავსი სახის იდენტობის გაყალბებისა და პოტენციურ მსხვერპლთა სენსიტიური ინფორმაციის მოპარვის ფაქტები 47,2%-ით გაიზარდა 2022 წელს 2021 წელთან შედარებით, რასაც ადასტურებს კიბერუსაფრთხოების და ნულოვანი ნდობის ციფრული ტრანსფორმაციის სფეროში ლიდერი კომპანიის 2023 წლის რეპორტი[20]. ასევე მომრავლდა ჰაკერული ორგანიზაციები, რომლებიც სწორედ ამ მეთოდის კომპლექსურ სქემას აგებენ ადამიანების მოსატყუებლად. მაგალითად, ფიშინგური ელფოსტა არის მატყუარა შეტყობინება, რომლებიც, ერთი შეხედვით სანდო წყაროდანაა, როგორიცაა ბანკი ან ლეგიტიმური ორგანიზაცია. ეს ელფოსტა ხშირად შეიცავს გადაუდებელ მოთხოვნებს, ბმულზე გადასვლის ინსტრუქციებსა ან საინტერესო შეთავაზებებს, რომლებიც იზიდავს მიმღებებს და ხაფანგში აგებს მათ. კონკრეტული ხერხი შეგვიძლია მივაწეროთ კომბინირებულ მეთოდს, როდესაც ჰაკერი არა მხოლოდ ფიშინგით არამედ მავნე

[20] Zscaler ThreatLabz. (2023). *2023 Phishing Report*. (გვ .3-4)
https://www.zscaler.com/resources/industry-reports/2023-threatlabz-phishing-report.pdf

პროგრამები/ჯაშუშური პროგრამებიის გამოყენებით ახერხებს ფიზიკური პირის ინფორმაციის ხელში ჩაგდებას. უკეთესად რომ განვმარტოთ, პროგრამები/ჯაშუშური პროგრამები (Keyloggers და Ransomware) მსხვერპლის მიერ ჩამოტვირთვისას ჰაკერებს საშუალებას აძლევს ფიზიკური პირის კომპიუტერში, ტელეფონში თუ სხვა მოწყობილობაში შენახულ ინფორმაციაზე მიიღოს წვდომა, მათ შორის საკრედიტო ბარათის ინფორმაცია და სხვა დეტალები.

აღსანიშნავია ის ფაქტი, რომ მეთოდოლოგია თუ როგორ მოხდება მომხმარებლის საბანკო რეკვიზიტების ინფორმაციის გაჟონვა სრულიად დამოკიდებულია ჰაკერის ტექნიკასა და სურვილზე. კიბერკრიმინალებმა შეიძლება დაიწყონ სოციალური ინჟინერიით წინასწარი ინფორმაციის შეგროვება, შემდეგ გადავიდნენ ფიშინგზე თავდაპირველი წვდომის მოსაპოვებლად და ბოლოს მოტყუებით გადმოაწერინონ მავნე პროგრამა, რათა შეინარჩუნონ კონტროლი და მიიღონ პერსონალური მონაცემები დროთა განმავლობაში. აღნიშნული სამი მეთოდიდან მხოლოდ ერთის ან მათი კომბინირებული სქემების შემუშავება სრულიად რელევანტური და გავრცელებულია კიბერკრიმინალურ სამყაროში, სადაც მუდმივად ავითარებენ ახალ ტაქტიკას, რათა მაქსიმალურად გაზარდონ წარმატების შანსები. თუმცა ეს არ გამორიცხავს ინფორმაციის მხოლოდ ერთი მეთოდის გამოყენებით მიღებას, ვთქვათ მეილზე ან SMS შეტყობინებაზე ბმულებისა და მავნე პროგრამების გაგზავნას, რაც გულისხმობს იმას, რომ ეს მეთოდები შეიძლება სრულიად არ გამომდინარეობდეს ერთმანეთისგან და არ იყოს დაკავშირებული, ან პირიქით.

კიბერკრიმინალური აქტივობების გავლენა: ეფექტი მომხმარებლებზე და ფინანსურ ინსტიტუტებზე

ონლაინ ბანკინგის სფეროში კიბერდანაშაულებრივი ქმედების მთავარ მიზეზებად ხშირად ბანკების მობაილ აპლიკაციების ციფრული დაუცველობა, ფიშინგის დახვეწილი ტაქტიკები, მესამე მხარის სერვისის პროვაიდერის მონაცემთა ბაზების გარღვევა და მომხმარებლის ინფორმირებულობის ნაკლებობა სახელდება, თუმცა აუცილებელი და საინტერესოა სურათი დაზარალებულთა: მომხმარებლებისა და ბანკების მხრიდან. მსგავსი

არალეგალური დანაშაულებრივი აქტები იმაზე უფრო დიდ ზეგავლენას ახდენს და ზარალს აყენებს ფიზიკურ პირებსა და ფინანსურ ინსტიტუტებს, ვიდრე ეს ერთი დანახვით ჩანს.

ფიზიკური პირებისთვის ნეგატიური შედეგების სპექტრი მხოლოდ ფინანსური ზარალით არ შემოიფარგლება და მოიცავს ემოციურ დისტრესსა და ნდობის ეროზიას. მომხმარებლები ებრძვიან კიბერშეტევებით გამოწვეულ შოკს, ბრაზს და შფოთვას, კონფიდენციალურობის დარღვევისა და დაუცველობის შეგრძნებას, რაც ამძაფრებს უნდობლობას ფინანსური ინსტიტუტების, ონლაინ სერვისების და ციფრული სფეროსადმი. საბოლოოდ კი იმ შედეგამდე მივდივართ, რომ მსხვერპლები თავს იკავებენ და აღარ უჩნდებათ სურვილი, ჩაერთონ ონლაინ აქტივობებში და ტრანზაქციებში, რაც აფერხებს ციფრული ეკონომიკის ზრდას. ფიზიკური პირები შეიძლება გახდნენ კიბერდანაშაულებრივი ტაქტიკის მსხვერპლი სხვადასხვა ფაქტორების გამო, მათ შორის კიბერუსაფრთხოების საუკეთესო პრაქტიკის შეზღუდული ინფორმირებულობის, მათი ონლაინ უსაფრთხოების ზედმეტად ნდობისა და სოციალური ინჟინერიის მანიპულაციური ტექნიკისადმი გულუბრყვილობით.

რაც შეეხება ფინანსური ინსტიტუტებსა და ორგანიზაციებს, როგორც უკვე აღვნიშნეთ, ისინი კლიენტების აქტივების მეურვეების როლს თამაშობენ და წარმოადგენენ ერთ-ერთ მთავარ ქვაკუთხედს კიბერკრიმინალურ ქმედებაში. შესაბამისად ისინიც, ასევე როგორც ფიზიკური პირები, არ არიან იმუნური კიბერშეტევებისგან.

ხშირად ბანკებს მომხმარებლის უსაფრთხოების დაცვის უზრუნველყოფისას ეკისრებათ ფინანსური პასუხისმგებლობა არაავტორიზებული ტრანზაქციის ასანაზღაურებლად, რაც ასევე იწვევს მათი მხრიდან დამატებითი რესურსების დახარჯვის აუცილებლობას გამოძიების ჩასატარებლად და პოტენციური მარეგულირებელი ჯარიმების გადასახდელად. კონკრეტული გულისხმობს შესაძლო მარეგულირებელი ექსპერტიზის ჩატარების აუცილებლობას, რომელსაც აწერებს მარეგულირებელი ორგანოები კიბერ ინციდენტების საპასუხოდ ზედამხედველობის გაძლიერების მიზნით, რამაც შეიძლება გამოიწვიოს აუდიტის და მკაცრი შესაბამისობის მოთხოვნების შესრულების აუცილებლობა. Entrust, სანდო გლობალური ლიდერი იდენტურობის, გადახდებისა და მონაცემთა უსაფრთხოების გადაწყვეტილებებში, 2022 წლის კვლევის რეპორტით[21] აშუქებს

[21] Entrust. (2022). *The Great Payments Disruption.*

მომხმარებელთა თაღლითობის შემდეგ შეცვლილ დამოკიდებულებას ბანკების მიმართ. შედეგები იუწყება, რომ ბანკის კლიენტთა 67% თაღლითობის შემდეგ წყვეტს კავშირს კონკრეტულ ორგანიზაციასთან და მის მიმართ სრულიად კარგავს ლოიალობას, რაც ძალიან ასევე დიდ ზარალს აყენებს და ეფექტს ახდებს ფინანსური დაწესებულების რეპუტაციაზე,

ამ ინფორმაციაზე დაყრდნობით ხაზი ესმება კიბერუსაფრთხოების ზომების გაძლიერებისა და ციფრულ ეპოქაში კიბერდანაშაულთან ბრძოლის კოლექტიური ძალისხმევის ხელშეწყობის აუცილებლობას. კიბერდანაშაულებრივი ტაქტიკისადმი ინდივიდების მანიპულირებისა და გულუბრყვილობის სიხშირე კი საზოგადოებაში კიბერუსაფრთხოების განათლებისა და ინფორმირებულობის მნიშვნელობაზე მიუთითებს, როგორც კიბერუსაფრთხოების ყოვლისმომცველი სტრატეგიის სასიცოცხლო მნიშვნელობის კომპონენტს.

მარეგულირებელი ჩარჩოები და კიბერუსაფრთხოების სტრატეგიები: ფინანსური სისტემების დაცვა გლობალურ კონტექსტში

გლობალურმა ფინანსურმა ლანდშაფტმა განიცადა უპრეცედენტო ტრანსფორმაცია ბოლო რამდენიმე ათწლეულის განმავლობაში. მოწინავე ტექნოლოგიების ადაპტაციასთან ერთად, ფინანსური სექტორი სულ უფრო ციფრული ხდება, რაც ერთი მხრივ მომხმარებლებს სთავაზობს შეუდარებელ კომფორტსა და სწრაფ სერვისს, თუმცა მეორე მხრივ დიგიტალიზაციის ეპოქამ გამოიწვია კიბერ საფრთხეების ახალი ტალღა, რაც უპრეცედენტო გამოწვევებს უქმნის ფინანსური სისტემებისა და მონაცემების უსაფრთხოებას. ციფრული სივრცის მოწყვლადობამ კიბერკრიმინალებს საშუალება მისცა ახალი გზების შემუშავების მოეპოვებინათ და მიეღოთ მგრძნობიარე ფინანსური ინფორმაცია და განეხორციელებინათ არაავტორიზებული ტრანზაქციები. შესაბამისად, ტექნოლოგიების ადაპტირებასთან ერთად

https://images.go.entrust.com/Web/EntrustInc/%7Bd2213af8-998f-43cd-8e6c-f91ac7eba616%7D_Global-Future-of-Banking-Report.pdf

ციფრული ფინანსური სისტემებისთვის მონაცემთა დაცვა ერთ-ერთი უმნიშვნელოვანესი პრიორიტეტი ხდება 21-ე საუკუნეში.

მარეგულირებელი ჩარჩოები და კიბერუსაფრთხოების სტრატეგიები ცენტრალურ როლს თამაშობს ფინანსური სექტორის დაცვაში კიბერ საფრთხეებისგან. ეს სტრატეგიები აუცილებელია საბანკო და სხვა ფინანსური სერვისების მთლიანობის შესანარჩუნებლად, ტრანზაქციების უსაფრთხოების უზრუნველსაყოფად და კლიენტების კონფიდენციალური ინფორმაციის დასაცავად. მძლავრი მარეგულირებელი ჩარჩოებისა და კიბერუსაფრთხოების ეფექტური ზომების საჭიროება განსაკუთრებით გამოხატულია განვითარებად ქვეყნებში, სადაც ტექნოლოგიური პროგრესის ტემპი ხშირად აღემატება კიბერუსაფრთხოების ცნობიერებას.

ამ თავში განვიხილავ მარეგულირებელი ჩარჩოებისა და კიბერუსაფრთხოების სტრატეგიების კრიტიკულ კავშირს ფინანსური სისტემების გლობალურ კონტექსტში. ხაზი გაესმება განვითარებადი კიბერ საფრთხეების ლანდშაფტს, მარეგულირებელი ორგანოების როლს და ფინანსური ინსტიტუტების მიერ რისკების შესამცირებლად გამოყენებულ სტრატეგიებს. ეს თავი იკვლევს თუ როგორია გლობალური ფინანსური სექტორის მრავალმხრივი დინამიკა და ამ მექანიზმების მნიშვნელოვან როლს ჩვენი ფინანსური კეთილდღეობის დაცვაში, არამედ მხარს უჭერს გლობალურ თანამშრომლობას იმ ეპოქაში, სადაც კიბერ საფრთხეებს საზღვრები არ აქვთ.

ურთიერთდაკავშირებულ სამყაროში მარეგულირებელი სტანდარტების ჰარმონიზაცია უმნიშვნელოვანესია. საერთაშორისო ორგანიზაციები, როგორიცაა ფინანსური სამოქმედო სამუშაო ჯგუფი (FATF) და საბანკო ზედამხედველობის ბაზელის კომიტეტი გულმოდგინედ მუშაობენ გლობალური ნორმების დასამკვიდრებლად, რომლებიც ხელს უწყობენ ფინანსური სისტემის მთლიანობას.

გლობალური მარეგულირებელი ჩარჩოები:

ონლაინ ბანკინგის სერვისები, განსაკუთრებით ფინტექისა და არაავტორიზებული გადარიცხვების კონტექსტში, შეიძლება განსხვავდებოდეს ქვეყნისა და რეგიონის მიხედვით. თუმცა, შესაძლებელია განვიხილოთ რამდენიმე ძირითადი რეგულაცია და სტანდარტი, რომლებიც ჩვეულებრივ გამოიყენება ან დანერგილია გლობალურად არაავტორიზებული გადარიცხვებისგან დასაცავად:

- know your client (KYC) რეგულაციები: KYC მოთხოვნები უზრუნველყოფს, რომ ბანკები და ფინანსური ინსტიტუტები ამოწმებდნენ თავიანთი კლიენტების ვინაობას. ეს რეგულაციები გადამწყვეტია ანგარიშებზე არაავტორიზებული წვდომისა და თაღლითური ტრანზაქციების განხორციელების თავიდან ასაცილებლად. ან სტანდარტებით იმპლემენტირებული მომხმარებლის იდენტიფიკაციის პროგრამის (CIP), მომხმარებლის კომპლექსური შემოწმებასა (DD) და მუდმივი მონიტორინგის საფეხურები უზრუნველყოფს KYC ინფორმაციის განახლებას და სისტემას საშუალებას აძლევს რეგულარულად შეამოწმოს საეჭვო ტრანზაქციები.
- ფულის გათეთრების წინააღმდეგ (AML) კანონები: AML-ის რეგულაციები შექმნილია ფულის გათეთრების და სხვა ფინანსური დანაშაულების გამოვლენისა და თავიდან ასაცილებლად. ისინი ხშირად ითხოვენ ფინანსურ ინსტიტუტებს საეჭვო ტრანზაქციების მონიტორინგს და მოხსენებას.
- გადახდის სერვისების დირექტივა (PSD2) (ევროპაში): PSD2 არის ევროპული რეგულაცია, რომლის მიზანია ელექტრონული გადახდების უსაფრთხოების გაძლიერება. მას შემოაქვს მომხმარებელთა ძლიერ ავტორიზაციას (SCA) ონლაინ ტრანზაქციებზე, რაც კიბერკრიმინალებისთვის უფრო რთულს გახდის არაავტორიზებული გადარიცხვების შესრულებას.
- მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) (ევროპაში): GDPR ორიენტირებულია პერსონალური მონაცემების დაცვაზე. ონლაინ საბანკო სერვისები უნდა შეესაბამებოდეს GDPR-ს მომხმარებელთა მონაცემების დამუშავებისას, რაც სასიცოცხლოდ მნიშვნელოვანია კიბერდანაშაულისგან თავის დასაცავად.
- კიბერუსაფრთხოების რეგულაციები: სხვადასხვა ქვეყნებს აქვთ კიბერუსაფრთხოების სპეციფიკური რეგულაციები, რომლებიც ფინანსურ ინსტიტუტებს ავალდებულებენ უსაფრთხოების მკაცრი ზომების დაცვას, რათა დაიცვან კლიენტების მონაცემები და სახსრები კიბერთავდასხმებისგან.
- ელექტრონული ფულადი სახსრების გადარიცხვის აქტი (EFTA) (შეერთებულ შტატებში): EFTA უზრუნველყოფს მომხმარებლებს ელექტრონულ ფულადი სახსრების გადარიცხვასთან დაკავშირებულ დაცვას, როგორიცაა

არაავტორიზებული გადარიცხვები. ის ადგენს წესებს და პასუხისმგებლობებს ფინანსური ინსტიტუტებისა და მომხმარებლებისთვის.

- საერთაშორისო სტანდარტები: არსებობს საერთაშორისო სტანდარტები და საუკეთესო პრაქტიკა, როგორიცაა ISO 27001 ინფორმაციული უსაფრთხოების მართვის სისტემებისთვის, რომელსაც ბევრი ბანკი და ფინტექ კომპანია ნებაყოფლობით იღებს მონაცემთა უსაფრთხოების უზრუნველსაყოფად.
- მომხმარებელთა დაცვის კანონები: ბევრ ქვეყანას აქვს მომხმარებელთა დაცვის კანონები, რომლებიც მიმართავენ იმ პირებს, რომლებიც განიცდიან არასანქცირებულ გადარიცხვებს ან თაღლითობას.

საქართველოში კიბერდანაშაულთან ბრძოლის მარეგულირებელი ჩარჩოებისა და სტრატეგიების დანერგვა ციფრულ ეპოქაში ფინანსური სისტემების განვითარებადი საფრთხეებისგან დაცვის გლობალური ძალისხმევის სასიცოცხლო კომპონენტია. ქვეყნის მარეგულირებელი მიდგომა განვითარდა კიბერ საფრთხეების ცვალებად ლანდშაფტზე და ციფრულ ტექნოლოგიებზე მზარდი დამოკიდებულების საპასუხოდ.

ბოლო წლებში საქართველომ განიცადა კიბერდანაშაულის შემთხვევების საგანგაშო ზრდა, კიბერკრიმინალები ციფრულ სივრცეში არსებულ მოწყვლადობას იყენებენ. აღსანიშნავია, რომ საქართველოს გაზრდილმა დამოკიდებულებამ ელექტრონულ კომერციასა და ინტერნეტ ბანკინგზე კიბერკრიმინალებს ახალი შესაძლებლობები მისცა თავიანთი საქმიანობის განსახორციელებლად. ციფრული ტექნოლოგიების გავრცელებამ და ინტერნეტის გამოყენებამ 2018 წლის მონაცემებით[22] საქართველოს მოსახლეობის დაახლოებით 65% ინტერნეტის აქტიური მომხმარებელი გახადა. გარდა ამისა, კოვიდ 19 პერიოდამდე ქვეყანაში 7,6 მილიონი საბანკო ბარათის გამოშვება ასახავს ციფრული ფინანსური ტრანზაქციების მზარდ ტენდენციას. კიბერდანაშაულის აქტივობების ეს ზრდა შეიძლება მივაწეროთ როგორც ციფრულ ტექნოლოგიებზე მზარდ დამოკიდებულებას, ასევე საზოგადოების ინფორმირებულობის ზრდას კიბერუსაფრთხოების საკითხებთან დაკავშირებით. ზოგადად, კიბერუსაფრთხოება, როგორც სახელმწიფო პრიორიტეტი, 2008

[22] Financial Monitoring Service of Georgia (FMS). (2019, ოქტომბერი). *Money laundering and terrorism financing risk assessment of Georgia*.(გვ .26)
https://www.fms.gov.ge/Uploads/files/NRA_Georgia_English.pdf

წლის რუსეთ-საქართველოს ომის[23] შემდგომ გახდა აღქმადი, როდესაც ჰიბრიდული შეტევების სუსტი წერტილი საბანკო სექტორი გახდა.

საქართველომ პროაქტიულად უპასუხა კიბერდანაშაულის ზრდას სპეციალური ინსტიტუტების შექმნით და კიბერუსაფრთხოების ზომების განხორციელებით. აღსანიშნავია საქართველოს ეროვნული ბანკის ინიციატივები:

- კიბერუსაფრთხოების ჩარჩოს შემუშავება: ეს ჩარჩო ციფრულ ბანკებს მისცემს მითითებებს, თუ როგორ უნდა გამოავლინონ, შეაფასონ და მართონ კიბერუსაფრთხოების რისკები. ის ასევე მოიცავს ისეთ თემებს, როგორიცაა ინციდენტზე რეაგირება და ბიზნესის უწყვეტობის დაგეგმვა.
- მრავალფაქტორიანი ავთენტიფიკაციის (MFA) და ბიომეტრიული ავთენტიფიკაციის გამოყენება: საგარეო საქმეთა სამინისტრო მომხმარებლებს ავალდებულებს ავტორიზაციის ორ ან მეტ ფაქტორს, როგორიცაა პაროლი და ერთჯერადი კოდი, მათ ანგარიშში შესასვლელად. ბიომეტრიული ავთენტიფიკაცია იყენებს უნიკალურ ფიზიკურ მახასიათებლებს, როგორიცაა თითის ანაბეჭდები ან სახის ამოცნობა, მომხმარებლების იდენტიფიცირებისთვის.
- ეროვნული ბანკი ასევე მოუწოდებს ციფრულ ბანკებს გამოიყენონ ხელოვნური ინტელექტის (AI) და მანქანათმცოდნეობის (ML) ტექნოლოგიები არაავტორიზებული ტრანზაქციების აღმოსაჩენად და თავიდან ასაცილებლად. AI და ML შეიძლება გამოყენებულ იქნას მომხმარებლის ქცევის გასაანალიზებლად და ისეთი შაბლონების იდენტიფიცირებისთვის, რომლებიც შეიძლება მიუთითებდეს თაღლითურ საქმიანობაზე.

საქართველოს ეროვნული ბანკი, კონსტიტუციით უფლებამოსილი დაწესებულება, რომელიც ფუნქციონირებს საქართველოში არსებული საფინანსო სექტორის ფინანსური

[23] საქართველოს მთავრობა. (2021, 30 სექტემბერი). დადგენილება No482. *საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ.*
https://www.matsne.gov.ge/ka/document/view/5263611?publication=0

მდგრადობისა და გამჭვირვალობის ხელშეწყობისათვის, არაავტორიზებული ტრანზაქციების წინააღმდეგ საბრძოლველად სხვადასხვა ზომებს იყენებს, მათ შორის ითხოვს ციფრული ბანკებისგან თაღლითობის რისკის მართვის ჩარჩოს არსებობისა და ყველა საეჭვო არაავტორიზებული ტრანზაქცია შეტყობინების აუცილებლობას. იგი მუშაობს ციფრულ ბანკებთან თაღლითობის აღმოჩენისა და პრევენციის ახალი ტექნოლოგიების შემუშავებისა და დანერგვისთვის.

ამ ძალისხმევის შედეგად, საქართველომ მიაღწია საერთაშორისო აღიარებას კიბერუსაფრთხოების ზომებისთვის და 2017 წლის კიბერუსაფრთხოების ინდექსში[24] 165 ქვეყანას შორის მერვე ადგილი დაიკავა, ბოლო გამოცემის[25] მიხედვით კი ის მსოფლიოს ქვეყნებს შორის 81.06 ქულით 55-ეა. ეს ინდექსი აფასებს ქვეყნების მზაობას კიბერშეტევების თავიდან ასაცილებლად.

საქართველოს სტრატეგიული მიზნებიდან გამომდინარე რეგულაციებისა და სტანდარტების ასიმილაცია და ეროვნულ კანონებთან ადაპტაცია მნიშვნელოვან ტრანსფორმაციულ ნაბიჯს წარმოადგენს ქვეყნის კიბერუსაფრთხოებისა და მდგრადობის გაძლიერებაში, რისთვისაც აუცილებელია საბანკო სექტორის, საქართველოს ერთ-ერთი წამყვანი სფეროს, ამ პროცესში მუდმივი თანამშრომლობა. ამისთვის კი სებ-ი ბოლო წლებია აქტიურ ღონისძიებებს ატარებს. საქართველოს ძალისხმევა კიბერუსაფრთხოებისა და მდგრადობის გასაძლიერებლად არა მხოლოდ შიდა სახელმწიფოებრივი რეგულაციებითა და სტანდარტებით არის განპირობებული, არამედ ევროკავშირთან (European Union - EU) ასოცირების შეთანხმებისადმი[26] მისი ვალდებულებით. ასოცირების შეთანხმება ასახავს საქართველოსა და ევროკავშირს შორის თანამშრომლობისა და გათანაბრების ყოვლისმომცველ ჩარჩოს სხვადასხვა სფეროში, მათ შორის ფინანსურ მომსახურებასა და კიბერუსაფრთხოებაში. ეს ჰარმონიზაციის პროცესი გადამწყვეტია იმის უზრუნველსაყოფად, რომ საქართველოს კიბერუსაფრთხოების ზომები შეესაბამება ევროკავშირის ზომებს და განაპირობებდეს ციფრული საბანკო სექტორის უსაფრთხოდ მუშაობას. საერთაშორისო

[24] International Telecommunication Union (ITU). (2017). *Guidelines for the implementation of 2017.* .https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[25] International Telecommunication Union (ITU). (2020). *Guidelines for the implementation of 2020.*https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[26] European Union. (2023, 6 მარტი). *Agreement on an Association between the European Union and Georgia (as amended)*. Official Journal of the European Union, L 72, 1-274. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014A0830%2802%29-20230306

სტანდარტებისადმი წლების განმავლობაში მრავალი ნაბიჯი იქნა გადადგმული კიბერუსაფრთხოების სტრატეგიების, სხვადასხვა ციფრული საბანკო მიმართულებებისთვის რეგულაციების ჩარჩოს შექმნისა და ადაპტირების მიმართულებით, ხორციელდება ისეთ ორგანიზაციებთან აქტუალური თანამშრომლობა, როგორიცაა ENISA, რაც აძლიერებს საქართველოს კიბერმედეგობას.

იმის შემდეგ რაც 2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია, რომელიც ვრცელდება ევროკავშირში რეგისტრირებულ ნებისმიერ ორგანიზაციაზე, რომელიც საქმიანობის ფარგლებში ამუშავებს პერსონალურ მონაცემებს, დაიწყო აქტიური რეგულაციების გატარება კომერციული ბანკებისა და მათი ციფრული სამყაროს წვდომის დაცვის მექანიზმების შესამუშავებლად. ძალისხმევის რამდენიმე კონკრეტული მაგალითი ქართულ ციფრულ ბანკში კიბერუსაფრთხოების გასაძლიერებლად:

1. 2019 წელს კიბერუსაფრთხოებასთან დაკავშირებული მოთხოვნები განისაზღვრა. რეგულაცია (და დაკავშირებული მოთხოვნები) მეტწილად NIST (5 ძირითადი ფუნქცია) სტანდარტს დაეფუძნა.
2. 2020 წელს ეროვნულმა ბანკმა გამოსცა რეგულაცია: "მომხმარებლის ძლიერი ავთენტიფიკაციის წესის დამტკიცების შესახებ[27]", რომელიც ციფრულ ბანკებს ავალდებულებს ყველა მომხმარებლისთვის MFA-ს დანერგვას.
3. 202ი წლის 25 მაისს ძალაში შევიდა რეგულირების ლაბორატორიის - ეროვნული ბანკის მიერ ინოვაციური ფინანსური მომსახურების ან/და პროდუქტის სატესტო გარემოში გამოსაცდელად შექმნილი ჩარჩო, რომელიც დღემდე 15-ზე მეტი პროექტი აქვს დამტკიცებული.
4. 2023 წელს ეროვნული ბანკი მუშაობს ციფრულ ბანკებთან, რათა განავითაროს თაღლითობის გამოვლენის ახალი სისტემა, რომელიც იყენებს AI და ML.

სებ-ის ძალისხმევა ქართულ ციფრულ ბანკში კიბერუსაფრთხოების გასაძლიერებლად ეხმარება მომხმარებლების დაცვას არაავტორიზებული ტრანზაქციებისგან და ციფრული საბანკო სექტორის მიმართ ნდობის ჩამოყალიბებაში. ქართულ ციფრულ ბანკებს ასევე

---

[27] საქართველოს ეროვნული ბანკი. (2020, 2 სექტემბერი). *მომხმარებლის ძლიერი ავთენტიფიკაციის წესის და მტკიცების შესახებ.* https://nbg.gov.ge/fm/%E1%83%98%E1%83%9C%E1%83%93%E1%83%98%E1%83%95%E1%83%98

მოუწოდებენ დაიცვან გლობალური ციფრული საფინანსო ასოციაციის (GDF) მითითებები. GDF გაიდლაინები მოიცავს თემების ფართო სპექტრს, მათ შორის მომხმარებელთა დაცვას, მონაცემთა უსაფრთხოებას და ფულის გათეთრების წინააღმდეგ ბრძოლას. მიუხედავად, საქართველოში დანერგილი პრევენციული აქტებისა საყურადღებოა საქართველოს ეროვნული ბანკში 2023 წლის ყოველწლიური, ,ფინანსური სტაბილურობის ანგარიში[28]", რომელიც აღწერს ბოლო წლის კომერციული ბანკების ოპერაციული ზარალის (39.3 მილიონი ლარის) 30%-იან ზრდას, რის ერთ-ერთ მიზეზად ფიშინგისა და მომსახურების შეფერხების განაწილებული (DDoS) შეტევებს ასახელებს. ასევე სებ-ის 2021[29] და 2022[30] წლის წლიურ ანგარიშებში ასახულია საგრძნობლად გაზრდილი გარე თაღლითობის რისკის მაჩვენებელიც, რომელიც 17%-დან 26%-მდე ავიდა. ეს კიდევ ერთხელ, ხაზს უსვამს ფინანსურ ორგანიზაციებში ეფექტური პრაქტიკების დანერგვის აუცილებლობას.

გლობალური ფინანსური ინსტიტუტები: კლიენტების სახსრების არასანქცირებული გადარიცხვების პრევენციის მეთოდოლოგიების ეფექტურობა მომხმარებლებზე კიბერდანაშაულის ზემოქმედების შესამცირებლად

21-ე საუკუნეში ციფრული ფინანსური სერვისების გავრცელება გახდა თანამედროვე ბანკინგის ნაწილი. ონლაინ ბანკინგიდან დაწყებული მობილური გადახდის აპლიკაციებით და რობო მრჩევლებით დამთავრებული, ტექნოლოგიამ მოახდინა რევოლუცია მომხმარებლებსა და ბანკთა შორის ურთიერთობის სახესა და პროცესზე. ასევე ყოველდღიურობის სახე მიიღო ფინანსური ტრანზაქციებმა და მასთან თანმდევი

[28] საქართველოს ეროვნული ბანკი. (2023). *ფინანსური სტაბილურობის ანგარიში.*
[29] საქართველოს ეროვნული ბანკი. (2021). *ყოველწლიური ანგარიში.* https://nbg.gov.ge/fm/%E1%83%9E%E1%83%A3%E1%83%91%E1%83%9A%E1%83%98%E1%83%99
[30] საქართველოს ეროვნული ბანკი. (2022). *ყოველწლიური ანგარიში.* *https://nbg.gov.ge/fm/%E1%83%9E%E1%83%A3%E1%83%91%E1%83%9A%E1%83%98%E1%83%99*

არალეგალური ქმედების სიხშირემ. ამასთან დაკავშირებით ინფორმაციას იძლევა ფედერალური სავაჭრო კომისიის (ინგ: FTC) 2023 წლის ყოველწლიური ჟურნალი[31], რომლის თანახმადაც 2019-დან 2022 წლის სტატისტიკით საბანკო სექტორში თაღლითობის რეპორტების რაოდენობა თითქმის გაორმაგდა (47.7% გაიზარდა). ეს ხაზს უსვამს ინოვაციური ციფრული თაღლითობის პრევენციის სტრატეგიების აუცილებლობას. შესაბამისად, საბანკო ინდუსტრიაში თაღლითობის პრევენცია არის ერთგვარი თავდაცვის მექანიზმი ფინანსური ეკოსისტემის მთლიანობისა და სტაბილურობის დასაცავად რისთვისაც ბოლო სამი ათწლეულის განმავლობაში საერთაშორისო ბანკები სხვადასხვა მარეგულირებელ ინსტიტუტებთან და ფინტექ კომპანიებთან თანამშრომლობით ავითარებენ საუკეთესო პრაქტიკებსა და ნერგავდნენ გაუმჯობესებულ მეთოდებს არაავტორიზებული ტრანზაქციებისა და მასთან დაკავშირებული თაღლითობის შესამცირებლად.

როგორც უკვე აღინიშნა, თაღლითობის გავლენა როგორც ბანკებზე, ასევე მომხმარებლებზე ღრმაა, რაც იწვევს დამანგრეველ შედეგებს ფინანსური ზარალისა და რეპუტაციის დაზიანების თვალსაზრისით. ამაზე დაყრდნობით ამ თავის საფუძველი მდგომარეობს ბანკების მიერ გამოყენებული პრაქტიკების გაანალიზებაში, რათა ადვილი გასაგები გახდეს თუ როგორ ცდილობენ ისინი არასანქცირებული წვდომის თავიდან აცილებას და როგორ იცავენ თავიანთ კლიენტების სახსრებს.

Global Finance, ფინანსური ჟურნალი, რომელიც აქვეყნებს მსოფლიოს ყველაზე უსაფრთხო ბანკების, საუკეთესო ციფრული ბანკების და სხვა ფინანსური ინსტიტუტების რეიტინგებს 1993 წლიდან დღემდე, ინარჩუნებს პრესტიჟს ფინანსურ ინდუსტრიაში. 2023 წლის განცხადების შედეგად Global Finance-მა გამოავლინა წლევანდელი წლის საერთაშორისო მასშტაბზე ფუნქციონირებადი TOP 50 ბანკი, რომელთა შორისაც მოხვდნენ: KFW, Zürcher Kantonalbank, BNG Bank, Rentenbank და სხვა.

ტოპ ფინანსური ბანკები 2023 წელს დიდ ინვესტიციებს ახორციელებენ კიბერუსაფრთხოების ზომებში, რათა დაიცვან თავიანთი მომხმარებლები არაავტორიზებული წვდომისგან. Cybersecuritydive-ის[32] მიერ მოწოდებული რეპორტის თანახმად, რომელიც

[31] Federal Trade Commission. (2022). *Consumer Sentinel Data Book 2022.* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf

[32] Jones, D. (2021,15 ნოემბერი). *Banks Outpace Other Industries in Cyber Investments, Defense Strategies*. Cybersecurity Dive.

დაფუძნებულია 88 ბანკის გამოკითხვაზე მთელი მსოფლიოს მასშტაბით, აჩვენებს, რომ უფრო დიდი ბანკები უფრო დიდ ინვესტიციებს ახორციელებენ კიბერუსაფრთხოებაში, ვიდრე დანარჩენ ინდუსტრიაში, ხოლო ბანკების 95% იყენებს ძლიერ კიბერმმართველობის პრაქტიკას, როგორიცაა CISO-ს ან CSO-ს. ასეხე COVID 19-ის შემდეგ კიდევ უფრო აქტუალური გახდა ინვესტიციების გაკეთება შემდეგ სქემების ჩამოყალიბებისთვის::

- **მრავალფაქტორიანი ავთენტიფიკაცია (MFA)**: MFA მომხმარებლებს ავალდებულებს ავტორიზაციის ორ ან მეტ ფაქტორს, როგორიცაა პაროლი და ერთჯერადი კოდი ტელეფონიდან, თავიანთ ანგარიშებში შესვლისას. ეს არის ერთ-ერთი ყველაზე ეფექტური გზა არაავტორიზებული წვდომის თავიდან ასაცილებლად, რადგან იგი ართულებს თავდამსხმელებს ანგარიშებზე წვდომის მოპოვებას, მაშინაც კი, თუ მათ მოიპარეს მომხმარებლის პაროლი.
- **თაღლითობის აღმოჩენის სისტემები (FDS)**: FDS აკონტროლებს მომხმარებლის აქტივობას საეჭვო ნიმუშებზე, რომლებიც შეიძლება მიუთითებდეს თაღლითობაზე. მაგალითად, თუ მომხმარებელი მოულოდნელად ეცდება დიდი თანხის გადარიცხვას უცნობ ანგარიშზე, FDS-მა შესაძლოა ტრანზაქცია განსახილველად მონიშნოს.
- **მონაცემთა დაშიფვრა:** კონკრეტული შიფრავს მომხმარებლის მონაცემებს ისე, რომ მათზე წვდომა არ შეიძლება არაავტორიზებული პირებისთვის, თუნდაც მათ შეეძლოთ დაარღვიონ ბანკის სისტემები. ეს ხელს უწყობს ისეთი მგრძნობიარე მონაცემების დაცვას, როგორიცაა კლიენტების სახელები, მისამართები და სოციალური უსაფრთხოების ნომრები.
- **კიბერუსაფრთხოების ტრენინგი თანამშრომლებისთვის:** თანამშრომლები გადიან ტრენინგებს ფიშინგის თავდასხმების და სხვა კიბერ საფრთხეების იდენტიფიცირებისთვის და მოხსენებისთვის. ეს ხელს უწყობს თანამშრომლების სხვადასხვა სახის სოციალური ინჟინერიის თავდასხმების მსხვერპლთა რისკის შემცირებას.
- **ნულოვანი ნდობის უსაფრთხოება:** ნულოვანი ნდობის უსაფრთხოება არის უსაფრთხოების მიდგომა, რომელიც ვარაუდობს, რომ ნაგულისხმევად არც ერთი

https://www.cybersecuritydive.com/news/banks-cyber-security-investments/610045/#:~:text=The%20report%2C%20based%20on%20a,employing%20a%20CISO%20or%20CSO

მომხმარებლის ან მოწყობილობის ნდობა არ შეიძლება. სისტემებსა და მონაცემებზე ყველა წვდომა დამოწმებულია და ავტორიზებულია უსაფრთხოების მრავალი კონტროლის საშუალებით. ეს ხელს უშლის არაავტორიზებული მომხმარებლების წვდომას სენსიტიურ მონაცემებზე, მაშინაც კი, თუ მათ შეუძლიათ დაარღვიონ ბანკის პერიმეტრის უსაფრთხოება.

- **ხელოვნური ინტელექტი (AI) და მანქანათმცოდნეობა (ML):** AI და ML გამოიყენება არაავტორიზებული წვდომის პრევენციის შესაძლებლობების გასაუმჯობესებლად მრავალი გზით. მაგალითად, AI და ML შეიძლება გამოყენებულ იქნას კიბერ საფრთხეების იდენტიფიცირებისთვის და რეაგირებისთვის უფრო სწრაფად და ეფექტურად, ვიდრე ტრადიციული მეთოდები. გარდა ამისა, AI და ML შეიძლება გამოყენებულ იქნას თაღლითობის აღმოჩენის უფრო დახვეწილი მოდელების შესაქმნელად.
- **ქცევის ანალიტიკა:** ეს ტექნოლოგია გამოიყენება მომხმარებელთა ქცევის მონიტორინგისთვის, რომელიც შეიძლება მიუთითებდეს თაღლითობაზე ან სხვა საეჭვო აქტივობაზე.
- **ბიომეტრიული ავთენტიფიკაცია:** ბიომეტრიული ტექნოლოგიები, როგორიცაა თითის ანაბეჭდი ან სახის ამოცნობა, უზრუნველყოფს უსაფრთხოების დამატებით ფენას საბანკო თაღლითობის პრევენციაში. ეს მეთოდები ადასტურებს მომხმარებლის იდენტურობას უნიკალური ბიოლოგიური მახასიათებლებით, ამცირებს არაავტორიზებული წვდომისა და ანგარიშის აღების რისკს.

ახლა მინდა განვიხილო კონკრეტულად რამდენიმე საერთაშორისოდ წოდებული ტოპ 50 საუკეთესო და დაცული ბანკების ინდივიდუალური მიდგომები არასანქცირებული წვდომისა და მომხმარებლების აქტივების დაცვის მექანიზმები, რათა მესამე პირმა, კრიმინალმა, ვერ შეძლოს არალეგალურად მოპარული ფინანსური მონაცემების გამოყენება და კლიენტის ციფრულ საბანკო სივრცის დაუცველობით ბოროტმოქმედება.

- **JPMorgan Chase:** JPMorgan Chase იყენებს კიბერუსაფრთხოების მრავალფეროვან ზომებს, რათა დაიცვას თავისი მომხმარებლები არაავტორიზებული წვდომისგან, მათ შორის MFA-ს, FDS-ს, მონაცემთა დაშიფვრას, ნულოვანი ნდობის უსაფრთხოებასა და AI და

ML. ბანკს ასევე აქვს რამდენიმე უსაფრთხოების სერტიფიკატი, მათ შორის ISO 27001 და PCI DSS. ასევე იგი იცავს კიბერუსაფრთხოების გლობალურად აღიარებულ სტანდარტებს, რაც უზრუნველყოფს მსოფლიოს 150-ზე[33] მეტ მარეგულირებელთან შესაბამისობას.

- HSBC: HSBC იყენებს ნულოვანი ნდობის უსაფრთხოების მიდგომას, რათა დაიცვას თავისი მომხმარებლები არაავტორიზებული წვდომისგან. ბანკი ასევე იყენებს AI-ს და ML-ს, რათა მონიტორინგს გაუწიოს კლიენტების ქცევა ისეთი შაბლონებისთვის, რომლებიც შეიძლება მიუთითებდეს თაღლითობაზე ან სხვა საეჭვო აქტივობაზე. ზემოთ აღნიშნულის დანერგვამ 2021-დან 2022 წლამდე საეჭვო ტრანზაქციების იდენტიფიცირებისა და თაღლითობის შემცირებას 25%-ით შეუწყო ხელი. ასევე ბანკის სახელს ეკუთვნის თაღლითობისა და კიბერ ცნობიერების აპი[34], რომელიც დიდ ბრიტანეთში 2021 წლის მაისში ჩაეშვა და გაფართოვდა ახლო აღმოსავლეთისა და ჩრდილოეთ აფრიკის რვა ბაზარზე, როგორც საპილოტე ინიციატივა ფინანსური განათლების გასაუმჯობესებლად.
- კანადის სამეფო ბანკი: კანადის სამეფო ბანკი იყენებს ტრადიციულ და მოწინავე უსაფრთხოების ზომების კომბინაციას, რათა დაიცვას თავისი მომხმარებლები არაავტორიზებული წვდომისგან. ეს ზომები მოიცავს MFA, FDS, მონაცემთა დაშიფვრას, კიბერუსაფრთხოების ტრენინგს თანამშრომლებისთვის, უწყვეტი რისკის მონიტორინგს, ნულოვანი ნდობის უსაფრთხოებას და AI და ML.
- BNP Paribas: BNP Paribas იყენებს კიბერუსაფრთხოების მრავალფეროვან ზომებს, რათა დაიცვას თავისი მომხმარებლები არასანქცირებული წვდომისგან, მათ შორის MFA, FDS, მონაცემთა დაშიფვრა, კიბერუსაფრთხოების ტრენინგი თანამშრომლებისთვის, ნულოვანი ნდობის უსაფრთხოება და AI და ML. ბანკის 2022 წლის რეპორტში[35] აღნიშნულია, რომ MFA იყო მთავარი ფაქტორი კლიენტების ანგარიშებზე არაავტორიზებული წვდომის შესამცირებლად. ფაქტი რომ თაღლითური შესვლის

[33] JPMorgan Chase & Co. (2021). 2021 Environmental, Social & Governance Report.(გვ 3 .58) https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/documents/jpmc-esg-report-2021.pdf

[34] HSBC. (2023). *Environmental, social and governance review*. (გვ 3 . 54)

[35] BNP Paribas. (2023). *2022 integrated report*. (გვ 3 29)

მცდელობები კლიენტების ანგარიშებზე მისი განხორციელების დღიდან 90%-ით შემცირდა იმის მანიშნებელია, რომ ინვესტირება კიბერუსაფრთხოების კუთხით მომხმარებელსა და ბანკს შორის ნდობის ესკალაციას ახდენს.

- Deutsche Bank: Deutsche Bank იყენებს კიბერუსაფრთხოების სხვადასხვა ზომებს, რათა დაიცვას თავისი მომხმარებლები არაავტორიზებული წვდომისგან, მათ შორის MFA-ს, FDS-ს, მონაცემთა დაშიფვრასა და ნულოვანი ნდობის უსაფრთხოებას. აღსანიშნავია, რომ ბანკმა, 2022 წლის რეპორტის[36] თანახმად, მიუხედავად იმისა რომ ფინანსური დანაკარგის 4.5%-ით შემცირება შეძლო, გარე თაღლითობის ხარჯი 12 მილიონიდან 28 მილიონამდე გაეზარდა (133.3%). თუმცა, მას საკმაოდ კარგი სტრატეგია აქვს შემუშავებული კიბერუსაფრთხოების მიმართულებით. 2022 წლის დეკემბერში გამოცხადებული ინოვაციური პარტნიორობა NVIDIA-თან[37] ხელოვნური ინტელექტისა (AI) და მანქანათმცოდნეობის (ML) გამოყენების კუთხით სწორედ ამ სტრატეგიისკენ გადადგმული ნაბიჯია.

ეს არის მხოლოდ რამდენიმე მაგალითი იმ არასანქცირებული წვდომის პრევენციის პრაქტიკისა, რომელსაც იყენებენ ტოპ ფინანსური ბანკები მთელს მსოფლიოში 2023 წელს.

მიუხედავად ინვესტიციების, რეგულაციებისა და მომხმარებელთა ინფორმირებულობის განსხვავებებისა, შესამჩნევია, რომ არსებობს საერთო პრაქტიკის სტრუქტურა, რომელიც ეროვნულ თუ საერთაშორისო დონეზე მსგავს საფეხურებს მოითხოვს. აღსანიშნავია ის ფაქტიც, რომ Global Finance-ის თანახმად, ცენტრალური და აღმოსავლეთ ევროპის (CEE) რეგიონის მასშტაბით TBC გახდა ის ბანკი, რომელმაც მიიღო 2023 წლის ჯილდო "საუკეთესო ინფორმაციული უსაფრთხოებისა და თაღლითობის მართვისთვის"[38], რომელიც ეფუძნება მრავალ ფაქტორს, მათ შორის ბანკის ინვესტიციას უსაფრთხოების ტექნოლოგიებში, მისი ფოკუსირება თანამშრომლების ტრენინგზე და ინფორმირებულობაზე და თაღლითობის პრევენციისა და რეაგირების გამოცდილებაზე.

---

[36] Deutsche Bank. (2022). *Annual Report 2022*. (გვ 203)
https://agm.db.com/files/documents/2023/Annual-Report-2022.pdf
[37] Deutsche Bank. (2022). *Annual Report 2022*. (გვ 91)
https://agm.db.com/files/documents/2023/Annual-Report-2022.pdf
[38] Global Finance. (2023) *World's Best Digital Banks 2023.*
https://gfmag.com/award/award-winners/worlds-best-digital-banks-2023-round-1/

დასკვნა:

ფინანსური უსაფრთხოების სექტორი მუდმივად ვითარდება, რაც მოითხოვს მკაცრ პრევენციულ ზომებს არაავტორიზებული წვდომის აღკვეთისა და საბანკო ანგარიშების დასაცავად. რამდენადაც კიბერ საფრთხეების ტენდენციურობა დღითიდღე უფრო პოპულარული ხდება ფინანსური ინსტიტუტების პასუხისმგებლობაც იზრდება მომხმარებლების ფინანსური თაღლითისგან დაცვის თვალსაზრისით. ადაპტირებული თავდაცვის მექანიზმების საჭიროება, შესაბამისად, აუცილებლობას წარმოადგენს დღევანდელი ფინანსური სექტორისთვის, რისთვისაც განუწყვეტლად ხდება სტრატეგიებისა და საერთაშორისო პრაქტიკების შემუშავება.

კვლევამ შეისწავლა რთული დინამიკა მარეგულირებელ ჩარჩოებს, კიბერუსაფრთხოების სტრატეგიებსა და ფინანსური ინსტიტუტების მიერ ციფრული ფინანსური სისტემების დასაცავად გაწეულ ძალისხმევას შორის. გლობალური ფინანსური ლანდშაფტის ტრანსფორმაციამ, რომელიც განპირობებულია ტექნოლოგიების უპრეცედენტოდ სწრაფი განვითარებით, გააფართოვა სექტორის თვალსაწიერი და გაზარდა მომხმარებელთა სეგმენტი, თუმცა, ამ დიგიტალიზაციამ ასევე წარმოშვა ახალი, დახვეწილი კიბერ საფრთხეები, რომლებიც მნიშვნელოვან გამოწვევებს უქმნის ფინანსური სისტემებისა და მომხმარებელთა მონაცემების დაცვას.

შესწავლილი მარეგულირებელი ჩარჩოები, როგორც გლობალურ, ისე ეროვნულ დონეზე, ხაზს უსვამს ისეთი ღონისძიებების მნიშვნელობას, როგორიცაა KYC რეგულაციები, AML კანონები, PSD2, GDPR, კიბერუსაფრთხოების საერთაშორისო სტანდარტები და სხვა. ეს სტანდარტები მიზნად ისახავს საბანკო სერვისების მთლიანობის უზრუნველყოფას, ტრანზაქციების უსაფრთხოებას და მომხმარებელთა სენსიტიური ინფორმაციის დაცვას. საერთაშორისო ორგანიზაციები, როგორიცაა Financial Action Task Force (FATF) და ბაზელის საბანკო ზედამხედველობის კომიტეტი გადამწყვეტ როლს ასრულებენ გლობალური ნორმების ჩამოყალიბებაში, რაც ხაზს უსვამს მარეგულირებელი სტანდარტების ჰარმონიზაციის აუცილებლობას.

საქართველოს პროაქტიული რეაგირება მზარდ კიბერ საფრთხეებზე, როგორც ეს საქართველოს ეროვნული ბანკის ინიციატივებიდან ჩანს, გამოკვეთს განვითარებად ქვეყნებში

მორგებული კიბერუსაფრთხოების ზომების საჭიროებას. კიბერუსაფრთხოების ინდექსში კი ქვეყნის აღიარება და რეიტინგი ხაზს უსვამს მისი ძალისხმევის წარმატებას.

წამყვანი გლობალური ბანკების, მათ შორის JPMorgan Chase, HSBC, Royal Bank of Canada, BNP Paribas და Deutsche Bank-ის ყოველწლიური ანგარიშებისა და პრაქტიკის შესწავლა ავლენს მათ კიბერუსაფრთხოების მიდგომებში საერთო მსგავსებებს. შესაბამისად, კვლევის ფარგლებში, იდენტიფიცირებადი ხდება საბანკო სექტორში არსებული სტანდარტიზებული საერთაშორისო პრაქტიკის არსებობა. აღნიშნული ფინანსური ორგანიზაციები მნიშვნელოვან ინვესტიციას ახდენენ ისეთ ტექნოლოგიებში, როგორიცაა მრავალფაქტორიანი ავთენტიფიკაცია, თაღლითობის გამოვლენილი სისტემები, მონაცემთა დაშიფვრის პროგრამები და ხელოვნური ინტელექტისა და მანქანათმცოდნეობის გამოყენება. კიბერუსაფრთხოებისადმი არსებობს ერთობლივი ვალდებულება ფინანსური ინსტიტუტების მხრიდან, რაც ქმნის გლობალურ ტენდენციას, რომლის ფარგლებშიც პრიორიტეტული ხდება მომხმარებლების აქტივების დაცვა არაავტორიზებული წვდომისა და კიბერ საფრთხეებისგან.

მომავალში, ფინანსური ინდუსტრიისთვის აუცილებელია კიბერ რისკებთან სიფხიზლის გამოჩენა და მათთან ადაპტირება, რათა შესაძლებელი გახდეს მოსალოდნელი ზარალის მინიმუმამდე შემცირდება. კვლევის შედეგად გამოტანილი დასკვნა ხაზს უსვამს ინვესტიციების მუდმივ საჭიროებას უსაფრთხოების უახლესი ტექნოლოგიების, თანამშრომლების ტრენინგსა და მომხმარებელთა ინფორმირებულობის პროგრამებში. კვლევის გამოვლენილი ტენდენციები გზას უხსნის მომავალ კვლევებს განვითარებადი კიბერ რისკებისა და კონტროლის აქტივობების შესასწავლად, რაც ხელს უწყობს ფინანსური უსაფრთხოების ზომების უწყვეტ გაძლიერებას.

საბოლოოდ, კვლევა ხელს უწყობს საზოგადოებაში აღქმადობის გაზრდას კიბერუსაფრთხოებისა და მომხმარებელთა მონაცემთა დაცვის, მათი მოპარვის სქემების იდენტიფიცირების მეშვეობით. ასევე იგი თვალსაჩინოს ხდის ურთიერთდამოკიდებულებას მარეგულირებელ ჩარჩოებს, კიბერუსაფრთხოების სტრატეგიებსა და გლობალურ ფინანსურ ინსტიტუტებს შორის.

იქიდან გამომდინარე, რომ ფინანსური ინდუსტრია აგრძელებს განვითარებას, ასევე იხვეწება კიბერკრიმინალების მიერ გამოყენებული მეთოდები საბანკო ანგარიშებზე არაავტორიზებული წვდომის მოსაპოვებლად. რათა მოხდეს ბალანსის შენარჩუნება და რისკების ეფექტურად მართვა კიბერუსაფრთხოებისა და ფინანსური ინსტიტუტების

მედეგობის გასაძლიერებლად, აუცილებელია ბანკებმა განაგრძონ ფულადი სახსრების ინვესტირება უსაფრთხოების უახლეს ტექნოლოგიებში, თანამშრომელთა ტრენინგებსა და საგანმანათლებლო პროცედურებში და აამაღლონ თავიანთი მომხმარებლების ცნობიერება. ქვემოთ მოცემულია კვლევის ფარგლებში იდენტიფიცირებული ტენდენციები და სამომავლო კიბერ რისკების კონტროლის აქტივობები:

- საბანკო სექტორში არსებობს პრაქტიკათა საერთო სტრუქტურა, რომელიც მოითხოვს მსგავს ნაბიჯებს ეროვნულ თუ საერთაშორისო დონეზე.
- ბანკებმა მასიურად უნდა განახორციელონ ინვესტიცია უსაფრთხოების უახლესი ტექნოლოგიებში, როგორიცაა მრავალფაქტორიანი ავთენტიფიკაცია და მონაცემთა დაშიფვრა.
- ბანკებმა უნდა ასწავლონ თავიანთ თანამშრომლებს უახლესი კიბერ საფრთხეების შესახებ და როგორ დაიცვან თავი მათგან.
- ბანკებმა უნდა აამაღლონ თავიანთი მომხმარებლების ინფორმირებულობა არაავტორიზებული წვდომის რისკების შესახებ და როგორ დაიცვან თავიანთი ანგარიშები.
- ამ რეკომენდაციების დაცვით, ბანკებს შეუძლიათ დაეხმარონ ფინანსური უსაფრთხოების განმტკიცებაში და დაიცვან თავიანთი მომხმარებლები არაავტორიზებული წვდომისგან.