# ინტერნეტ და მობაილ ბანკის უსაფრთხოება

ინტერნეტ და მობაილ ბანკინგი არის საბანკო სერვისებზე წვდომის უსაფრთხო და მოსახერხებელი საშუალება. მაგრამ ამ სერვისების უსაფრთხო გამოყენებისთვის უნდა ვიაზრებდეთ, რომ კიბერ კრიმინალებმა და თაღლითებმა შესაძლებელია მოიპოვონ წვდომა ჩვენს ანგარიშზე. როგორ წესი ეს ხდება ინტერნეტ და მობაილ ბანკის პაროლების, მომხმარებლის სახელის, პინ კოდების არალეგალურად მოპოვების გზით.

## როგორ გამოვიყენოთ ინტერნეტ ბანკი უსაფრთხოდ

**ჩამონათვალში მოცემულია ძირითადი რჩევები, რომლიც უნდა დავიცვათ**

- არასოდეს გადახვიდეთ ინტერნეტ ბანკის ვებ გვერდზე მეილებში არსებული ბმულებიდან, იმ შემთხვევაშიც კი, თუ მეილი მოსულია ფინკა ბანკის სახელით. ყოველთვის აკრიფეთ ინტერნეტ ბანკის მისამართი თავად უშაულოდ ვებ ბრაუზერში.

- ინტერნეტ ბანკინგის ვერ გვერდის უსაფრთხოება უზრუნველყოფილია კრიპტაციის მექანიზმით. ინტერნეტ ბანკის ვებ გვერდზე შესვლისას უნდა ჩანდეს დაკეტილი ბოქლომის გამოსახულება, რომელზე დაჭერითაც შესაძლებელია გადამოწმდეს ვებ გვერდის სისწორე. გარდა ამისა, ინტერნეტ ბანკის გვერდზე შესვილისას მისამართის დასაწყისში ‘http’ უნდა შეიცვალოს ‘https’-ით

- ყურადღებით მოეკიდეთ ე.წ. pop-up ფანჯრებს, რომელიც შესაძლოა გაჩნდეს ეკრანზე ინტერნეტ ბანკში მუშაობის დროს.

- არასოდეს არ გაუზიაროთ მესამე პირებს კონფიდენციალური ინფორმაცია (მომხმარებლის სახელი, პაროლი) ელექტრონული ფოსტის ან ტელეფონის საშუალებით. გახსოვდეთ, ფინკა ბანკი არასოდეს სთხოვს თავის კლიენტებს ინფორმაციის გაზიარებას ტელეფონის ან მეილის საშუალებით.

- კიბერ თაღლითების მიერ კლიენტების შეცდომაში შეყვანის გამოცდილი მეთოდია ე.წ. „საცდელი ტრანზაქცია“, როდესაც ტელეფონით ან სხვა საშუალებით ბანკის სახელით კლიენტს სთხოვენ „საცდელი ტრანზაქციის“ შესრულებას ინტერნეტ ან მობაილ ბანკის საშუალებით. გახსოვდეთ, ფინკა ბანკი არასოდეს სთხოვს კლიენტებს საცდელი ტრანზაქციების შესრულებას ტელეფონის, მეილის ან სხვა ტიპის შეტყობინების საშუალებით.

- პერიოდულად გადაამოწმეთ თქვენი ანგარიშების ამონაწერები. თუ აღმოაჩინეთ არაავტორიზებული ან საჭვო ოპერაცია, დაუყონებლივ მიმართეთ ფინკა ბანკს.

- სანამ შეასრულებთ ოპერაციას ინტერნეტ ბანკის მეშვეობით, გადაამოწმეთ ოპერაციის თანხის, მიმღების რეკვიზიტების და დანიშნულების სისწორე.

- დააყენეთ და რეგულარულად განაახლეთ ანტივირუსი თქვენს კომპიუტერზე. გამოიყენოთ ბრაუზერის უსაფრთო პარამეტრები. დამატებითი ინფორმაცია შეგიძლია მოიძიოთ შემდეგ ბმულზე https://www.us-cert.gov/publications/securing-your-web-browser#why

- ბანკები იყენებენ განსხვავებულ სისტემებს და მოწყობილობებს იმისათის, რომ დარწმუნდნენ იმ პირის ვალიდურობაში, რომელიც დისტანციურად უკავშირდება ბანკს და ახორციელებს ოპერაციას ინტერნეტ ბანკის ან მობაილ ბანკის საშუალებით. ამ მიზნით ფინკა ბანკი იყენებს ერთჯერად კოდებს, რომელიც ეგზავნება კლიენტს მის მიერ მითითებულ მობილური ტელეფონის ნომერზე.ამ მექანიზმს ეწოდება ორფაქტროიანი აუტენტიფიკაცია. ერთჯერადი სმს კოდი გამოიყენება როგორც უსაფრთიების დამატებითი მექანიზმი ოპერაციის შესრულებისას. არასოდეს გამოიყენოთ სმს კოდი, როემლიც მიიღეთ ნომრიდან, რომელიც არ ეკუთვნის ფინკას ბანკს.

- დარწმუნდით იმაში, რომ ფინკა ბანკში დაფიქსირებულია თქვენი განახლებული და სწორი საკონტაქტო ინფორმაცია, განსაკუთრებით მობილური ტელეფონის ნომერი. სასურველია გამოიყენოთ ტელეფონის ნომერი, რომელიც გაფორმებულია თქვენს სახელზე.

# მობაილ ბანკის უსაფრთხოება

ფინკა ბანკი გაძლევთ საშუალებას განახორციელოთ ოპერაციები სმარტფონის ან სხვა თავსებადი მობილური მოწყობილობის საშაულებით. ამისათვის უნდა ჩამოტვირთოთ და დააყენოთ თქვენს მობილურ მოწყობილობაზე აპლიკაცია (ე.წ. „აპი“). აპი არის პროგრამა, რომელიც სპეციალურად შექმნილია სმარტფონებისთვის და სხვა თავსებადი მობილური მოწყობილობებისთვის. მობაილ ბანკის აპი არის თქვენი ანგარიშის ონლაინ მართვის მოსახერხებელი საშაულება, მაგრამ აპის გამოყენებისას აუცილებლად უნდა მოხდეს უსაფრთხოების წესების დაცვა.

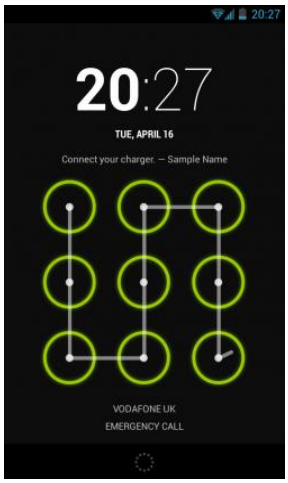
**უსაფრთხოების ძირითადი წესები**

- სასურველია სმარტფონში მხოლოდ ოფიციალური და შემოწმებული აპების დაყენება, რომელიც ხელმისაწვდომია Google Play-ზე (android მოწყობილობებისთვის) და App Store (აიფონებისთვის). უფასო აპები ძალიან მოსახერხებელია, მაგრამ, გახსოვდეთ, რომ არაოფიციალური წყაროებიდან ჩამოტვირთული აპიმ შესაძლოა თქვენი მოწყობილობაში ვირუსი ან „ჯაშუში“ პროგრამა დააყენოს. გახსოვდეთ, რომ android მოხმარებლები, რომელიც იყენებენ ე.წ. .apk ფაილებს არაოფიციალური წყაროებიდან, ისევე როგორც jalebraked iOS-მოწყობილობების მფლობელები არიან მაღალი რისკის ქვეშ, რადგან ე.წ. ჯეილბრეიკინგი ან რუტინგი (rooting) ასუსტებს სმარტფონის სისტემის უსაფრთხოებას.


- გამოიყენეთ მხოლოდ ფინკა ბანკის მიერ შექმნილი ოფიციალრუ აპი. თუ ეჭვი გეპარებათ აპის აუთენტურობაში დაუკავშირდით ქოლ ცენტრს ან მოიძიეთ ინფორამცია ფინკა ბანკის ოფიციალურ ვებ გვერდზე.

- კარგად გადაამოწმეთ თუ რა წვდომას ითხოვს აპი ინსტალაციის დროს. კარგად დაფიქრდით, სანამ მოახდენთ სმარტფონის უსაფრთხოების პარამეტრების გამორთვას.

- ისევე როგორ ყველა სხვა შემთხვევაში, არასოდეს გაუზიაროთ თქვენი მობილური მოწყობილობის უსაფრთხოების აპრამეტრები მესამე პირებს. არ შეინახოთ კონფიდენციალური ინფორმაცია სმარტფონში არსებული „ნოუტებში“. ყოველთვის დაიცავით სმარტფონი კოდის ან ე.წ. პატერნის საშუალებით.





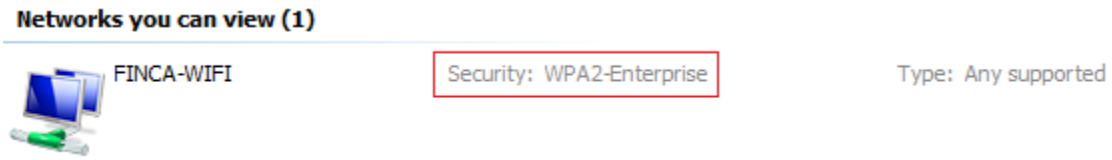
- ისევე როგორც კომპიუტერზე, სმარტფონზე უნდა დაყენდეს და პერიოდულად განახლდეს ანტივირუსი. ანტივირუსის შერჩევისას შეგიძლიათ დაეყრდნოთ მწარმოებლის ცნობადობას და ბრენდს. ამასთან ყოველთვის დააყენეთ სმარტფონის სისტემის განახლებები. გამოიყენეთ მხოლოდ ოფიცლაური წყაროები.
- ყურადღებით მოეკიდეთ ბმულებს, რომელსაც ღებულობთ მოკლე ტექსტური შეტყობინების საშუალებით ან სმარტფონის მეილ კლიენტის საშუალებით. ფინკა ბანკი არასოდეს გამოგიზავნით მოკლე ტექსტურ შეტყობინებას ან ელექტრონულ წერილს, რომელიც ითხოვს კონფიდენცუალრი ინფორმაციის გაზიარებას.

## Wi-Fi წვდომა

განსაკუთრებული სიფრთხილით უნდა მოეკიდოთ Wi-Fi წვდომას. Wi-Fi არის ინტერნეტთან დაკავშირების მოსახერებელი საშუალება, მაგრამ უნდა გახსოვდეთ, რომ Wi-Fi შესაძლოა იყოს საფრთხის შემცველი. დაკავშირება ინტერნეტ ბანკინგთან და მობაილბანკინგთან ე.წ. ღიაWi-Fi სპოთების საშუალებით არ არის რეკომენდირებული.

**გამოუვალი სიტუაციის შემთხვევაში, როდესაც აუცილებელი ხდება ამგვარი ჰოტსპოთის გამოყენება უნდა დაიცვათ შემდეგი წესები**

- **შეეცადეთ გამოიყენოთ შედარებით დაცული Wi-fi ქსელი.** Wi-Fi ქსელების უსაფრთხოების პარამეტრები განსხვავდება. იმ შემთხვევაში არის არჩევანი უნდა დავუკავშირდენ Wi-Fi-ს, რომელიც უზურნველყოფს WPA2 უსაფრთობას, შემდეგ WAP, ხოლო ყველაზე რისკიანია WEP-ით დაცული Wi-Fiკავშირი. უსაფრთოების დონე შეგიძლიათ გადაამოწმოთ დაკავშირების წინ (სურათი). ჰოთსპოტთან დაკავშირების შემდეგ, როგორ წესი ოპერაციული სისტემა ითხოვს უსაფრთოების დონის მინიჭებას, ყიველთვის აირჩიეთ ‘Public Network’ ოფცია - ამ შემთხვევაში აირიდებთ თავიდან თქვენი კომპიუტერის ფაილებზე არასასრუველ წვდომას იმ Wi-Fi-დან, რომელსაც უკავშირდებით.




- **გამოიყენეთ VPN კლიენტი.** იმ შემთხვევაშ,ი თუ რეგულარულად გიწევთ Wi-Fi ქსელის გამოყენება მობაილ ან ინტერნეტ ბანკით სარგებლობისას, რეკომენდირებულია VPN კლიენტის გამოყენება. VPN კლიენტი არის პროგრამა, რომელიც უზრუნველყოფს დაცულს კავშირს თქვენ კომპიუტერს (ან სმარტფონს) და ონლაინ ბანკის სისტემას შორის იმ შემთხვევაშიც კი, როდესაც იყენებთ Wi-Fi-ს. არსებობს VPN კლიენტის როგორც ფასიანი, ისე უფასო ვერსიები, რომელიც ხელმისაწვდომია, როგორც პერსონალუტრი კომპიუტერებისთვის ისე მობილური მოწყობილობებისთვის.