

ციფრული უსაფრთხოების მთავარი წესები

გამოიყენე რთული პაროლი

01

შექმენი გრძელი, 8-12 სიმბოლოიანი პაროლი, რთული კომბინაციით

02

ხშირად შეცვალე პაროლი



03

არ გაუზიარო იგი სხვებს

04

გამოიყენე პაროლის შემნახველი აპლიკაციები - *NORTON, NORDPASS, PASTPASS*

გამოიყენე ორფაქტიანი ავთენტიფიკაცია

უცხო პირებს შენს ელფოსტასა და სოციალურ ქსელებში შესვლა გაუჭირდებათ

234588



ანგარიშზე შესასვლელად, უნდა შეიყვანო მობილურზე დამატებითი მოსული კოდი

გამოიყენე მხოლოდ დაცული ვებგვერდები

• მისამართები <https://>-ით უნდა იწყებოდეს

• დააკვირდი ვებგვერდის დასახელებას

არასდროს გადახვიდე უცნობი ან საეჭვო მისამართებიდან მიღებულ წერილებში მითითებულ ბმულზე

არ გახსნა უცნობი მისამართებიდან მიღებულ გზავნილებში მითითებული ფაილები



დაიცავი ანონიმურობა ქსელში

- გამოიყენე „ვირტუალური პირადი ქსელი“ (VPN)
- გამოიყენე TOR BROWSER და დაფარე, რას აკეთებ ინტერნეტში



დამატებითი რჩევები იხილეთ აქ





გამოიყენე უსაფრთხო კომპიუტერი

- ფინანსური ოპერაციები საკუთარი კომპიუტერით განახორციელე
- გახსოვდეს, სამსახურის კომპიუტერი შენი არ არის!



გამოიყენე ლიცენზირებული ოპერაციული სისტემები

ან მათი უფასო ანალოგები!



კომპიუტერს არ შეუერთო ვირუსიანი ინფორმაციის გადამტანები

- გამორთე ავტომატური გადმოწერის ფუნქცია
- ერიდე სხვის მესსინჯინგის ბარათს, CD - ბარათებს, სმარტფონს

საზოგადოებრივი თავშეყრის ადგილებში კომპიუტერი ჩართული არ დატოვო



საზოგადოებრივი Wi-Fi-სთან გამოიყენე „ვირტუალური პირადი ქსელი“ (VPN)

კომპიუტერი უხსო ვირებს არ ატხოვო

ან მხოლოდ სტუმრის ანგარიშიდან დაუშვი შენს კომპიუტერზე



აუცილებლად გამოიყენე ანტივირუსი

- უფასო ღირებულების მქონე მაგალითები AVG ან AVAST
- ასევე, დაბადებული BITDEFENDER

დამატური რჩევები იხილეთ აქ



ინფორმაციის თავისუფლების განვითარების ინსტიტუტი